



Panduan Pengguna

# AWS Systems Manager Referensi buku runbook otomatisasi



# AWS Systems Manager Referensi buku runbook otomatisasi: Panduan Pengguna

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara para pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan properti dari masing-masing pemilik, yang mungkin berafiliasi, terkait dengan, atau disponsori oleh Amazon, atau tidak.

---

# Table of Contents

Referensi runbook otomatisasi .....	1
Lihat konten runbook .....	3
API Gateway .....	4
AWSConfigRemediation-DeleteAPIGatewayStage .....	4
AWSConfigRemediation-EnableAPIGatewayTracing .....	5
AWSConfigRemediation-UpdateAPIGatewayMethodCaching .....	7
AWS Batch .....	8
AWSSupport-TroubleshootAWSBatchJob .....	9
AWS CloudFormation .....	14
AWS-DeleteCloudFormationStack .....	15
AWS-EnableCloudFormationSNSNotification .....	16
AWS-RunCfnLint .....	18
AWSSupport-TroubleshootCFNCustomResource .....	20
AWS-UpdateCloudFormationStack .....	22
CloudFront .....	23
AWSConfigRemediation-EnableCloudFrontDefaultRootObject .....	23
AWSConfigRemediation-EnableCloudFrontAccessLogs .....	25
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity .....	27
AWSConfigRemediation-EnableCloudFrontOriginFailover .....	28
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS .....	30
CloudTrail .....	32
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail .....	32
AWS-EnableCloudTrail .....	34
AWS-EnableCloudTrailCloudWatchLogs .....	35
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS .....	37
AWS-EnableCloudTrailKmsEncryption .....	38
AWSConfigRemediation-EnableCloudTrailLogFileValidation .....	40
AWS-EnableCloudTrailLogFileValidation .....	41
AWS-QueryCloudTrailLogs .....	42
CloudWatch .....	45
AWS-ConfigureCloudWatchOnEC2Instance .....	45
AWS-EnableCWAlarm .....	46
Amazon DocumentDB .....	49
AWS-EnableDocDbClusterBackupRetentionPeriod .....	49

CodeBuild .....	51
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMCMK .....	52
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject .....	53
AWS CodeDeploy .....	55
AWSSupport-TroubleshootCodeDeploy .....	55
AWS Config .....	57
AWSSupport-SetupConfig .....	57
Amazon Connect .....	60
AWSSupport-AssociatePhoneNumbersToConnectContactFlows .....	60
AWS Directory Service .....	68
AWS-CreateDSManagementInstance .....	68
AWSSupport-TroubleshootADConnectorConnectivity .....	73
AWSSupport-TroubleshootDirectoryTrust .....	77
AWS AppSync .....	80
AWS-EnableAppSyncGraphQLApiLogging .....	80
Amazon Athena .....	83
AWS-EnableAthenaWorkGroupEncryptionAtRest .....	83
DynamoDB .....	85
AWS-ChangeDDBRWCapacityMode .....	86
AWS-CreateDynamoDBBackup .....	88
AWS-DeleteDynamoDbBackup .....	89
AWSConfigRemediation-DeleteDynamoDbTable .....	90
AWS-DeleteDynamoDbTableBackups .....	91
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable .....	93
AWSConfigRemediation-EnablePITRForDynamoDbTable .....	94
AWS-EnableDynamoDbAutoscaling .....	96
AWS-RestoreDynamoDBTable .....	99
Amazon EBS .....	101
AWSSupport-AnalyzeEBSResourceUsage .....	102
AWS-ArchiveEBSSnapshots .....	108
AWS-AttachEBSVolume .....	111
AWSSupport-CalculateEBSPerformanceMetrics .....	112
AWS-CopySnapshot .....	118
AWS-CreateSnapshot .....	119
AWS-DeleteSnapshot .....	120
AWSConfigRemediation-DeleteUnusedEBSVolume .....	121

AWS-DeregisterAMIs .....	123
AWS-DetachEBSVolume .....	124
AWSConfigRemediation-EnableEbsEncryptionByDefault .....	125
AWS-ExtendEbsVolume .....	127
AWSSupport-ModifyEBSSnapshotPermission .....	129
AWSConfigRemediation-ModifyEBSVolumeType .....	131
Amazon EC2 .....	133
AWS-ASGEnterStandby .....	135
AWS-ASGExitStandby .....	136
AWS-CreateImage .....	137
AWS-DeleteImage .....	138
AWS-PatchAsgInstance .....	140
AWS-PatchInstanceWithRollback .....	142
AWS-QuarantineEC2Instance .....	145
AWS-ResizeInstance .....	147
AWS-RestartEC2Instance .....	148
AWS-SetupJupyter .....	149
AWS-StartEC2Instance .....	152
AWS-StopEC2Instance .....	153
AWS-TerminateEC2Instance .....	154
AWS-UpdateLinuxAmi .....	155
AWS-UpdateWindowsAmi .....	157
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck .....	161
AWSConfigRemediation-EnforceEC2InstanceIMDSv2 .....	163
AWSEC2-CloneInstanceAndUpgradeSQLServer .....	164
AWSEC2-CloneInstanceAndUpgradeWindows .....	168
AWSEC2-ConfigureSTIG .....	172
AWSEC2-PatchLoadBalancerInstance .....	199
AWSEC2-SQLServerDBRestore .....	200
AWSSupport-ActivateWindowsWithAmazonLicense .....	206
AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 .....	209
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD .....	213
AWSSupport-CheckXenToNitroMigrationRequirements .....	219
AWSSupport-ConfigureEC2Metadata .....	222
AWSSupport-CopyEC2Instance .....	226
AWSSupport-EnableWindowsEC2SerialConsole .....	231

AWSSupport-ExecuteEC2Rescue .....	240
AWSSupport-ListEC2Resources .....	242
AWSSupport-ManageRDPSettings .....	245
AWSSupport-ManageWindowsService .....	247
AWSSupport-MigrateEC2ClassicToVPC .....	250
AWSSupport-MigrateXenToNitroLinux .....	256
AWSSupport-ResetAccess .....	268
AWSSupport-ResetLinuxUserPassword .....	271
AWSPremiumSupport-ResizeNitroInstance .....	277
AWSSupport-RestoreEC2InstanceFromSnapshot .....	284
AWSSupport-SendLogBundleToS3Bucket .....	289
AWSSupport-StartEC2RescueWorkflow .....	291
AWSPremiumSupport-TroubleshootEC2DiskUsage .....	301
AWSSupport-TroubleshootEC2InstanceConnect .....	306
AWSSupport-TroubleshootRDP .....	312
AWSSupport-TroubleshootSSH .....	318
AWSSupport-TroubleshootSUSERegistration .....	321
AWSSupport-TroubleshootWindowsPerformance .....	323
AWSSupport-TroubleshootWindowsUpdate .....	331
AWSSupport-UpgradeWindowsAWSDrivers .....	338
Amazon ECS .....	342
AWSSupport-CollectECSInstanceLogs .....	342
AWS-InstallAmazonECSAgent .....	345
AWS-ECSRunTask .....	346
AWSSupport-TroubleshootECSContainerInstance .....	350
AWSSupport-TroubleshootECSTaskFailedToStart .....	352
AWS-UpdateAmazonECSAgent .....	356
Amazon EFS .....	358
AWSSupport-CheckAndMountEFS .....	358
Amazon EKS .....	362
AWSSupport-CollectEKSIInstanceLogs .....	362
AWS-CreateEKSClusterWithFargateProfile .....	364
AWS-CreateEKSClusterWithNodegroup .....	368
AWS-DeleteEKSCluster .....	371
AWS-MigrateToNewEKSSelfManagedNodeGroup .....	375
AWSPremiumSupport-TroubleshootEKSCluster .....	381

AWSSupport-TroubleshootEKSSWorkerNode .....	385
AWS-UpdateEKSCluster .....	387
AWS-UpdateEKSMANAGEDNodeGroup .....	388
AWS-UpdateEKSSelfManagedLinuxNodeGroups .....	392
Elastic Beanstalk .....	396
AWSSupport-CollectElasticBeanstalkLogs .....	397
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ..	400
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications .....	401
AWSSupport-TroubleshootElasticBeanstalk .....	403
Penyeimbang Beban Elastis .....	406
AWSConfigRemediation-DropInvalidHeadersForALB .....	406
AWS-EnableCLBAccessLogs .....	408
AWS-EnableCLBConnectionDraining .....	409
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing .....	411
AWSConfigRemediation-EnableELBDeletionProtection .....	413
AWSConfigRemediation-EnableLoggingForALBAndCLB .....	414
AWSSupport-TroubleshootCLBConnectivity .....	415
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing .....	419
AWS-UpdateALB DesyncMitigationMode .....	420
AWS-UpdateCLB DesyncMitigationMode .....	422
Amazon EMR .....	424
AWSSupport-AnalyzeEMRLogs .....	424
OpenSearch Layanan Amazon .....	430
AWSConfigRemediation-DeleteOpenSearchDomain .....	431
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain .....	432
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups .....	433
AWSSupport-TroubleshootOpenSearchRedYellowCluster .....	435
AWSSupport-TroubleshootOpenSearchHighCPU .....	441
EventBridge .....	447
AWS-AddOpsItemDedupStringToEventBridgeRule .....	447
AWS-DisableEventBridgeRule .....	449
GuardDuty .....	450
AWSConfigRemediation-CreateGuardDutyDetector .....	450
IAM .....	452
AWS-AttachIAMToInstance .....	452
AWS-DeleteIAMInlinePolicy .....	454

AWSConfigRemediation-DeleteIAMRole .....	456
AWSConfigRemediation-DeleteIAMUser .....	457
AWSConfigRemediation-DeleteUnusedIAMGroup .....	460
AWSConfigRemediation-DeleteUnusedIAMPolicy .....	461
AWSConfigRemediation-DetachIAMPolicy .....	463
AWSConfigRemediation-EnableAccountAccessAnalyzer .....	464
AWSSupport-GrantPermissionsToIAMUser .....	466
AWSConfigRemediation-RemoveUserPolicies .....	471
AWSConfigRemediation-ReplaceIAMInlinePolicy .....	472
AWSConfigRemediation-RevokeUnusedIAMUserCredentials .....	474
AWSConfigRemediation-SetIAMPASSWORDPolicy .....	476
Amazon Kinesis Data Streams .....	479
AWS-EnableKinesisStreamEncryption .....	479
AWS KMS .....	481
AWSConfigRemediation-CancelKeyDeletion .....	481
AWSConfigRemediation-EnableKeyRotation .....	483
Lambda .....	484
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing .....	484
AWSConfigRemediation-DeleteLambdaFunction .....	486
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK .....	487
AWSConfigRemediation-MoveLambdaToVPC .....	489
AWSSupport-RemediateLambdaS3Event .....	491
AWSSupport-TroubleshootLambdaInternetAccess .....	493
AWSSupport-TroubleshootLambdaS3Event .....	497
Amazon Managed Workflows for Apache Airflow (MWAA) .....	499
AWSSupport-TroubleshootMWAAEnvironmentCreation .....	499
Neptune .....	505
AWS-EnableNeptuneDbAuditLogsToCloudWatch .....	505
AWS-EnableNeptuneDbBackupRetentionPeriod .....	507
AWS-EnableNeptuneClusterDeletionProtection .....	509
Amazon RDS .....	510
AWS-CreateEncryptedRdsSnapshot .....	511
AWS-CreateRdsSnapshot .....	514
AWSConfigRemediation-DeleteRDSCluster .....	515
AWSConfigRemediation-DeleteRDSClusterSnapshot .....	517
AWSConfigRemediation-DeleteRDSInstance .....	518



AWSConfigRemediation-DeleteRDSInstanceSnapshot .....	520
AWSConfigRemediation-DisablePublicAccessToRDSInstance .....	521
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster .....	523
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance .....	525
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance .....	526
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS .....	528
AWSConfigRemediation-EnableMultiAZOnRDSInstance .....	530
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance .....	532
AWSConfigRemediation-EnableRDSClusterDeletionProtection .....	534
AWSConfigRemediation-EnableRDSInstanceBackup .....	535
AWSConfigRemediation-EnableRDSInstanceDeletionProtection .....	537
AWSConfigRemediation-ModifyRDSInstancePortNumber .....	539
AWSSupport-ModifyRDSSnapshotPermission .....	541
AWSPremiumSupport-PostgreSQLWorkloadReview .....	543
AWS-RebootRdsInstance .....	559
AWSSupport-ShareRDSSnapshot .....	560
AWS-StartRdsInstance .....	564
AWS-StartStopAuroraCluster .....	565
AWS-StopRdsInstance .....	567
AWSSupport-TroubleshootConnectivityToRDS .....	568
AWSSupport-TroubleshootRDSIAMAuthentication .....	570
AWSSupport-ValidateRdsNetworkConfiguration .....	578
Amazon Redshift .....	584
AWSConfigRemediation-DeleteRedshiftCluster .....	584
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster .....	586
AWSConfigRemediation-EnableRedshiftClusterAuditLogging .....	587
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot .....	589
AWSConfigRemediation-EnableRedshiftClusterEncryption .....	590
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting .....	592
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster .....	593
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings .....	595
AWSConfigRemediation-ModifyRedshiftClusterNodeType .....	597
Amazon S3 .....	599
AWS-ArchiveS3BucketToIntelligentTiering .....	599
AWS-ConfigureS3BucketLogging .....	602
AWS-ConfigureS3BucketVersioning .....	604

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock .....	605
AWSConfigRemediation-ConfigureS3PublicAccessBlock .....	607
AWS-CreateS3PolicyToExpireMultipartUploads .....	609
AWS-DisableS3BucketPublicReadWrite .....	611
AWS-EnableS3BucketEncryption .....	612
AWS-EnableS3BucketKeys .....	613
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy .....	615
AWSConfigRemediation-RestrictBucketSSLRequestsOnly .....	616
AWSSupport-TroubleshootS3PublicRead .....	618
SageMaker .....	623
AWS-DisableSageMakerNotebookRootAccess .....	624
Secrets Manager .....	626
AWSConfigRemediation-DeleteSecret .....	626
AWSConfigRemediation-RotateSecret .....	628
Security Hub .....	629
AWSConfigRemediation-EnableSecurityHub .....	630
AWS Shield .....	631
AWSPremiumSupport-DDoSResiliencyAssessment .....	631
Amazon SNS .....	640
AWS-EnableSNSTopicDeliveryStatusLogging .....	640
AWSConfigRemediation-EncryptSNSTopic .....	643
AWS-PublishSNSNotification .....	645
Amazon SQS .....	646
AWS-EnableSQSEncryption .....	646
Step Functions .....	648
AWS-EnableStepFunctionsStateMachineLogging .....	648
Systems Manager .....	651
AWS-BulkDeleteAssociation .....	651
AWS-BulkEditOpsItems .....	652
AWS-BulkResolveOpsItems .....	656
AWS-ConfigureMaintenanceWindows .....	658
AWS-CreateManagedLinuxInstance .....	660
AWS-CreateManagedWindowsInstance .....	662
AWSConfigRemediation-EnableCWLoggingForSessionManager .....	665
AWS-ExportOpsDataToS3 .....	666
AWS-ExportPatchReportToS3 .....	668

AWS-SetupInventory .....	670
AWS-SetupManagedInstance .....	674
AWS-SetupManagedRoleOnEC2Instance .....	675
AWSsupport-TroubleshootManagedInstance .....	676
AWSsupport-TroubleshootPatchManagerLinux .....	679
AWSsupport-TroubleshootSessionManager .....	683
Pihak ketiga .....	688
AWS-CreateJiraIssue .....	688
AWS-CreateServiceNowIncident .....	691
AWS-RunPacker .....	693
Amazon VPC .....	695
AWS-CloseSecurityGroup .....	696
AWSsupport-ConfigureDNSQueryLogging .....	697
AWSsupport-ConfigureTrafficMirroring .....	700
AWSsupport-ConnectivityTroubleshooter .....	703
AWSsupport-TroubleshootVPN .....	706
AWSConfigRemediation-DeleteEgressOnlyInternetGateway .....	712
AWSConfigRemediation-DeleteUnusedENI .....	714
AWSConfigRemediation-DeleteUnusedSecurityGroup .....	715
AWSConfigRemediation-DeleteUnusedVPCNetworkACL .....	716
AWSConfigRemediation-DeleteVPCFlowLog .....	718
AWSConfigRemediation-DetachAndDeleteInternetGateway .....	719
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway .....	721
AWS-DisableIncomingSSHOnPort22 .....	723
AWS-DisablePublicAccessForSecurityGroup .....	724
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP .....	726
AWSsupport-EnableVPCFlowLogs .....	727
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch .....	731
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket .....	733
AWS-ReleaseElasticIP .....	735
AWS-RemoveNetworkACLUnrestrictedSSHRDP .....	736
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules .....	737
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules .....	739
AWSsupport-SetupIPMonitoringFromVPC .....	740
AWSsupport-TerminateIPMonitoringFromVPC .....	752
AWS WAF .....	755

---

AWS-AddWAFRegionalRuleToRuleGroup .....	756
AWS-AddWAFRegionalRuleToWebAcl .....	758
AWSConfigRemediation-EnableWAFClassicLogging .....	761
AWSConfigRemediation-EnableWAFClassicRegionalLogging .....	762
AWSConfigRemediation-EnableWAFV2Logging .....	764
Amazon WorkSpaces .....	766
AWS-CreateWorkSpace .....	766
AWSSupport-RecoverWorkSpace .....	769
X-Ray .....	773
AWSConfigRemediation-UpdateXRayKMSKey .....	773
.....	dcclxxvi

# Referensi runbook Otomatisasi Systems Manager

Untuk membantu Anda memulai dengan cepat, AWS Systems Manager sediakan runbook yang telah ditentukan sebelumnya. Runbook ini dikelola oleh Amazon Web Services, AWS Support, dan AWS Config. Referensi buku runbook menjelaskan setiap runbook yang telah ditentukan yang disediakan oleh Systems Manager, AWS Support dan AWS Config

## Important

Jika Anda menjalankan alur kerja otomatisasi yang menjalankan layanan lain dengan menggunakan AWS Identity and Access Management peran layanan (IAM), pastikan bahwa peran layanan harus dikonfigurasi dengan izin untuk menjalankan layanan tersebut. Persyaratan ini berlaku untuk semua AWS Runbook otomatisasi (AWS-\* runbook) seperti `AWS-ConfigureS3BucketLogging`, `AWS-CreateDynamoDBBackup`, dan `AWS-RestartEC2Instance` runbook, untuk beberapa nama. Persyaratan ini juga berlaku untuk setiap runbook Otomasi kustom yang Anda buat yang memanggil AWS layanan lain dengan menggunakan tindakan yang memanggil layanan lain. Misalnya, jika Anda menggunakan `aws:executeAwsApi`, `aws:createStack`, atau `aws:copyImage` tindakan, maka Anda harus mengonfigurasi peran layanan dengan izin untuk memanggil layanan tersebut. Anda dapat mengaktifkan izin ke AWS layanan lain dengan menambahkan kebijakan inline IAM ke peran tersebut. Untuk informasi selengkapnya, lihat [Menambahkan kebijakan sebaris Otomasi untuk memanggil layanan lain AWS](#).

Referensi ini mencakup topik yang menjelaskan setiap runbook Systems Manager yang dimiliki oleh AWS, AWS Support, dan AWS Config. Runbook diatur oleh yang relevan Layanan AWS. Setiap halaman memberikan penjelasan tentang parameter yang diperlukan dan opsional yang dapat Anda tentukan saat menggunakan runbook. Setiap halaman juga mencantumkan langkah-langkah di runbook dan output otomatisasi, jika ada.

Referensi ini tidak menyertakan halaman terpisah untuk runbook yang memerlukan persetujuan seperti `AWS-CreateManagedLinuxInstanceWithApproval` atau `AWS-StopEC2InstanceWithApproval` runbook. Nama runbook apa pun yang menyertakan `WithApproval`, berarti runbook menyertakan tindakan. [aws:approve](#) Tindakan ini menghentikan sementara otomatisasi sampai kepala sekolah yang ditunjuk menyetujui atau menolak tindakan tersebut. Setelah jumlah persetujuan yang diperlukan tercapai, otomatisasi dilanjutkan.

Untuk informasi tentang menjalankan otomatisasi, lihat [Menjalankan otomatisasi sederhana](#). Untuk informasi tentang menjalankan otomatisasi pada beberapa target, lihat [Menjalankan otomatisasi yang menggunakan target dan kontrol kecepatan](#).

## Topik

- [Lihat konten runbook](#)
- [API Gateway](#)
- [AWS Batch](#)
- [AWS CloudFormation](#)
- [CloudFront](#)
- [CloudTrail](#)
- [CloudWatch](#)
- [Amazon DocumentDB](#)
- [CodeBuild](#)
- [AWS CodeDeploy](#)
- [AWS Config](#)
- [Amazon Connect](#)
- [AWS Directory Service](#)
- [AWS AppSync](#)
- [Amazon Athena](#)
- [DynamoDB](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [Amazon ECS](#)
- [Amazon EFS](#)
- [Amazon EKS](#)
- [Elastic Beanstalk](#)
- [Penyeimbang Beban Elastis](#)
- [Amazon EMR](#)
- [OpenSearch Layanan Amazon](#)
- [EventBridge](#)

- [GuardDuty](#)
- [IAM](#)
- [Amazon Kinesis Data Streams](#)
- [AWS KMS](#)
- [Lambda](#)
- [Amazon Managed Workflows for Apache Airflow \(MWAA\)](#)
- [Neptune](#)
- [Amazon RDS](#)
- [Amazon Redshift](#)
- [Amazon S3](#)
- [SageMaker](#)
- [Secrets Manager](#)
- [Security Hub](#)
- [AWS Shield](#)
- [Amazon SNS](#)
- [Amazon SQS](#)
- [Step Functions](#)
- [Systems Manager](#)
- [Pihak ketiga](#)
- [Amazon VPC](#)
- [AWS WAF](#)
- [Amazon WorkSpaces](#)
- [X-Ray](#)

## Lihat konten runbook

Anda dapat melihat konten untuk runbook di konsol Systems Manager.

Untuk melihat konten runbook

1. Buka AWS Systems Manager konsol di <https://console.aws.amazon.com/systems-manager/>.
2. Di panel navigasi, pilih Dokumen.

-atau-

Jika AWS Systems Manager halaman beranda terbuka terlebih dahulu, pilih ikon menu



untuk membuka panel navigasi, lalu pilih Dokumen di panel navigasi.

3. Di bagian Kategori, pilih Dokumen otomatisasi.
4. Pilih runbook, lalu pilih Tampilkan detail.
5. Pilih tab Daftar Isi.

## API Gateway

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon API Gateway. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSConfigRemediation-DeleteAPIGatewayStage](#)
- [AWSConfigRemediation-EnableAPIGatewayTracing](#)
- [AWSConfigRemediation-UpdateAPIGatewayMethodCaching](#)

## AWSConfigRemediation-DeleteAPIGatewayStage

Deskripsi

AWSConfigRemediation-DeleteAPIGatewayStageRunbook menghapus tahap Amazon API Gateway (API Gateway). AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon



## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- StageArn

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari tahap API Gateway yang ingin Anda hapus.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- apigateway:GET
- apigateway:DELETE

## Langkah Dokumen

- aws:executeScript- Menghapus tahap API Gateway ditentukan dalam StageArn parameter.

# **AWSConfigRemediation-EnableAPIGatewayTracing**

## Deskripsi

`AWSConfigRemediation-EnableAPIGatewayTracingRunbook` memungkinkan penelusuran pada tahap Amazon API Gateway (API Gateway). AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- `StageArn`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari tahap API Gateway yang ingin Anda aktifkan penelusuran.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`

- `config:GetResourceConfigHistory`
- `apigateway:GET`
- `apigateway:PATCH`

### Langkah Dokumen

- `aws:executeScript`- Memungkinkan pelacakan pada tahap API Gateway yang ditentukan dalam `StageArn` parameter.

## **AWSConfigRemediation-UpdateAPIGatewayMethodCaching**

### Deskripsi

`AWSConfigRemediation-UpdateAPIGatewayMethodCachingRunbook` memperbarui setelan metode cache untuk sumber daya tahap Amazon API Gateway.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- `CachingAuthorizedMethods`

### Jenis: StringList

Deskripsi: (Diperlukan) Metode yang diizinkan untuk mengaktifkan caching. Daftar harus beberapa kombinasi dari DELETE, GET, HEAD, OPTIONS, PATCH, POST, dan PUT. Caching diaktifkan untuk metode yang dipilih dan dinonaktifkan untuk metode yang tidak dipilih. Caching diaktifkan untuk semua metode jika ANY dipilih dan dinonaktifkan untuk semua metode jika NONE dipilih.

- StageArn

Jenis: String

Deskripsi: (Diperlukan) API Gateway tahap ARN untuk REST API.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- apigateway:PATCH
- apigateway:GET

Langkah Dokumen

- aws:executeScript- Menerima ID sumber daya panggung sebagai input, memperbarui pengaturan metode cache untuk tahap API Gateway menggunakan tindakan UpdateStage API, dan memverifikasi pembaruan.

## AWS Batch

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS Batch Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSSupport-TroubleshootAWSBatchJob](#)

# AWSSupport-TroubleshootAWSBatchJob

## Deskripsi

AWSSupport-TroubleshootAWSBatchJobRunbook membantu Anda memecahkan masalah yang mencegah AWS Batch pekerjaan berkembang dari status ke status. RUNNABLE STARTING

Bagaimana cara kerjanya?

Runbook ini melakukan pemeriksaan berikut:

- Jika lingkungan komputasi dalam DISABLED keadaan INVALID atau.
- Jika Max vCPU parameter lingkungan komputasi cukup besar untuk mengakomodasi volume pekerjaan dalam antrian pekerjaan.
- Jika pekerjaan membutuhkan lebih banyak vCPU atau sumber daya memori daripada yang dapat disediakan oleh tipe instans lingkungan komputasi.
- Jika pekerjaan harus dijalankan pada instance berbasis GPU tetapi lingkungan komputasi tidak dikonfigurasi untuk menggunakan instance berbasis GPU.
- Jika grup Auto Scaling untuk lingkungan komputasi gagal meluncurkan instance.
- [Jika instans yang diluncurkan dapat bergabung dengan cluster Amazon Elastic Container Service \(Amazon ECS\) yang mendasarinya; jika tidak, instans menjalankan runbook -TroubleShootecs.AWSSupport ContainerInstance](#)
- Jika ada masalah izin yang memblokir tindakan tertentu yang diperlukan untuk menjalankan pekerjaan.

### Important

- Runbook ini harus dimulai di AWS Wilayah yang sama dengan pekerjaan Anda yang terjebak dalam RUNNABLE status.
- Runbook ini dapat dimulai untuk AWS Batch lowongan yang dijadwalkan di Amazon ECS, atau instans AWS Fargate Amazon Elastic Compute Cloud (Amazon EC2). Jika otomatisasi dimulai untuk AWS Batch pekerjaan di Amazon Elastic Kubernetes Service (Amazon EKS), inisiasi berhenti.
- Jika instans tersedia untuk menjalankan pekerjaan tetapi gagal mendaftarkan cluster Amazon ECS, runbook ini memulai runbook AWSSupport-TroubleshootECSContainerInstance otomatisasi untuk mencoba menentukan

alasan. Untuk informasi lebih lanjut, rujuk runbook [AWSSupportContainerInstance-Troubleshoots](#).

## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- JobId

Jenis: String

Deskripsi: (Wajib) ID dari AWS Batch Job yang terjebak dalam RUNNABLE status.

Pola yang Diizinkan:  $^[a-f0-9]{8}(-[a-f0-9]{4}){3}-[a-f0-9]{12}(:[0-9]+)?(\#[0-9]+)?\$$

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `autoscaling:DescribeAutoScalingGroups`
- `autoscaling:DescribeScalingActivities`
- `batch:DescribeComputeEnvironments`
- `batch:DescribeJobs`
- `batch:DescribeJobQueues`
- `batch:ListJobs`
- `cloudtrail:LookupEvents`
- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetRequestHistory`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ecs:DescribeClusters`
- `ecs:DescribeContainerInstances`
- `ecs:ListContainerInstances`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListRoles`
- `iam:PassRole`
- `iam:SimulateCustomPolicy`
- `iam:SimulatePrincipalPolicy`

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sts:GetCallerIdentity`

## Instruksi

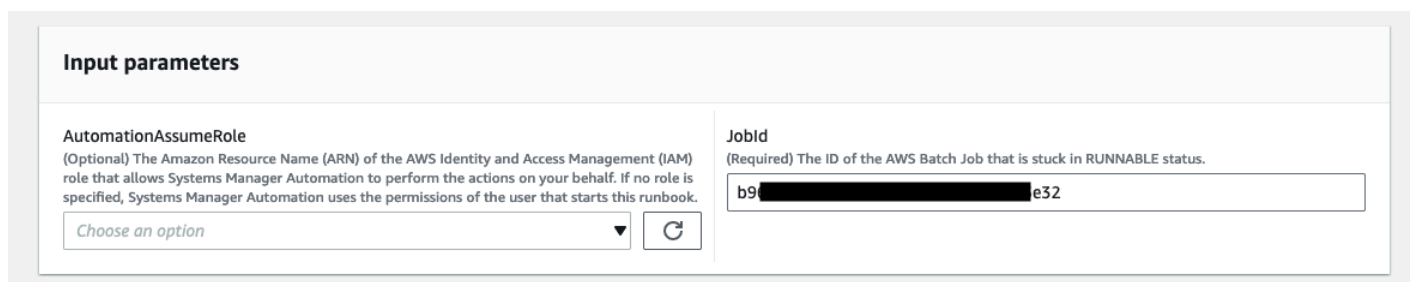
1. Arahkan ke [AWSSupport-TroubleshootAWSBatchJob di Konsol](#). AWS Systems Manager
2. Pilih Jalankan Otomasi
3. Untuk parameter input, masukkan yang berikut ini:

- `AutomationAssumeRole` (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `JobId` (Diperlukan):

ID dari AWS Batch Job yang terjebak dalam `RUNNABLE` status.



**Input parameters**

<b>AutomationAssumeRole</b> (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.	<b>JobId</b> (Required) The ID of the AWS Batch Job that is stuck in <code>RUNNABLE</code> status.
<input type="text" value="Choose an option"/> <input type="button" value="↻"/>	<input type="text" value="b9[REDACTED]e32"/>

4. Pilih Jalankan.
5. Perhatikan bahwa otomatisasi dimulai.
6. Dokumen melakukan langkah-langkah berikut:

- `PreflightPermissionChecks`:

Melakukan pemeriksaan izin IAM preflight terhadap pengguna/peran yang memulai. Jika ada izin yang hilang, langkah ini menyediakan Tindakan API yang hilang di bagian output global.

- `ProceedOnlyIfUserHasPermission`:



Cabang berdasarkan jika Anda memiliki izin untuk semua tindakan yang diperlukan untuk runbook.

- `AWSBatchJobEvaluation`:

Melakukan pemeriksaan terhadap AWS Batch Job yang memverifikasi bahwa itu ada dan berada dalam `RUNNABLE` status.

- `ProceedOnlyIfBatchJobExistsAndIsInRunnableState`:

Cabang berdasarkan apakah pekerjaan itu ada dan dalam `RUNNABLE` status.

- `BatchComputeEnvironmentEvaluation`:

Melakukan pemeriksaan terhadap Lingkungan AWS Batch Komputasi.

- `ProceedOnlyIfComputeEnvironmentChecksAreOK`:

Cabang berdasarkan apakah pemeriksaan lingkungan komputasi berhasil.

- `UnderlyingInfraEvaluation`:

Melakukan pemeriksaan terhadap Grup Auto Scaling atau Permintaan Armada Spot yang mendasarinya.

- `ProceedOnlyIfInstancesNotJoiningEcsKluster`:

Cabang berdasarkan jika ada instance yang tidak bergabung dengan cluster Amazon ECS.

- `EcsAutomationRunner`:

Menjalankan otomatisasi Amazon ECS untuk instans yang tidak bergabung dengan cluster.

- `ExecutionResults`:

Menghasilkan output berdasarkan langkah sebelumnya.

## 7. Setelah selesai, URI untuk file HTML laporan penilaian disediakan:

Tautan Konsol S3 dan URI Amazon S3 untuk Laporan tentang keberhasilan eksekusi runbook

## ▼ Outputs

ExecutionResults.message

```
#####
EXECUTION RESULT SUMMARY
#####
Here is the summary of the execution of this runbook:
```

```

✔ [INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKn0NEEWmt8eY":
❌ [ERROR]: Job "411[REDACTED]606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKn0NEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/updating-compute-environments.html
! [WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKn0NEEWmt8eY".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html
#####
❌ [ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.

#####
RUNBOOK EXECUTION LOGS
#####

+++++
STEP:PreflightPermissionChecks
+++++
✔ [INFO]: The IAM Identity used to execute the runbook has all required permissions, proceeding further for next steps in execution.

+++++
STEP:AWSBatchJobEvaluation
+++++
✔ [INFO]: Job with ID "411[REDACTED]606" exists and is in RUNNABLE status, proceeding further for next steps in execution.

+++++
STEP:BatchComputeEnvironmentEvaluation
+++++

✔ [INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKn0NEEWmt8eY":
❌ [ERROR]: Job "411[REDACTED]606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKn0NEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/updating-compute-environments.html
! [WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKn0NEEWmt8eY".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html
#####
❌ [ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.
```

## Referensi

## Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

## AWS CloudFormation

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS CloudFormation Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWS-DeleteCloudFormationStack](#)
- [AWS-EnableCloudFormationSNSNotification](#)

- [AWS-RunCfnLint](#)
- [AWSSupport-TroubleshootCFNCustomResource](#)
- [AWS-UpdateCloudFormationStack](#)

## AWS-DeleteCloudFormationStack

Deskripsi

Hapus AWS CloudFormation tumpukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- StackNameOrId

Jenis: String

Deskripsi: (Diperlukan) Nama atau ID Unik CloudFormation tumpukan yang akan dihapus

# AWS-EnableCloudFormationSNSNotification

## Deskripsi

AWS-EnableCloudFormationSNSNotificationRunbook mengaktifkan notifikasi Amazon Simple Notification Service (Amazon SNS) untuk tumpukan AWS CloudFormation (AWS CloudFormation) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- StackArn

Jenis: String

Deskripsi: (Diperlukan) ARN atau nama AWS CloudFormation tumpukan yang ingin Anda aktifkan notifikasi Amazon SNS.

- NotificationArn

Jenis: String

Deskripsi: (Wajib) ARN dari topik Amazon SNS yang ingin Anda kaitkan dengan tumpukan. AWS CloudFormation

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm: GetAutomationExecution
- ssm: StartAutomationExecution
- pembentukan awan: DescribeStacks
- pembentukan awan: UpdateStack
- kms:Decrypt
- km: GenerateDataKey
- SNS:Publish
- persegi: GetQueueAttributes

Langkah Dokumen

- CheckCfnSnsLimits (AWS:executeScript) - Memverifikasi jumlah maksimum topik Amazon SNS yang belum dikaitkan dengan tumpukan yang Anda tentukan. AWS CloudFormation
- EnableCfnSnsNotification (aws:executeAwsApi) - Mengaktifkan notifikasi Amazon SNS untuk tumpukan. AWS CloudFormation
- VerificationCfnSnsNotification (AWS: ExecuteScript) - Memverifikasi bahwa notifikasi Amazon SNS telah diaktifkan untuk tumpukan. AWS CloudFormation

Keluaran

CheckCfnSnsLimits. NotificationArnList - Daftar ARN yang menerima notifikasi Amazon SNS untuk AWS CloudFormation tumpukan.

VerificationCfnSnsNotification. VerifySnsTopicsResponse - Respon dari operasi API yang mengonfirmasi notifikasi Amazon SNS telah diaktifkan untuk tumpukan. AWS CloudFormation

# AWS-RunCfnLint

## Deskripsi

Runbook ini menggunakan [AWS CloudFormationLinter](#) (`cfn-python-lint`) untuk memvalidasi template YAKL dan JSON terhadap spesifikasi sumber daya. AWS CloudFormation `AWS-RunCfnLintRunbook` melakukan pemeriksaan tambahan, seperti memastikan bahwa nilai yang valid telah dimasukkan untuk properti sumber daya. Jika validasi tidak berhasil, `RunCfnLintAgainstTemplate` langkah gagal dan output alat linter disediakan dalam pesan kesalahan. Runbook ini menggunakan `cfn-lint v0.24.4`.

## [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `ConfigureRuleFlag`

Jenis: String

Deskripsi: (Opsional) Opsi konfigurasi untuk aturan untuk diteruskan ke `--configure-rule` parameter.

Contoh: E2001:Strict=false, E3012: Strict=false.

- FormatFlag

Jenis: String

Deskripsi: (Opsional) Nilai untuk diteruskan ke `--format` parameter untuk menentukan format keluaran.

Nilai yang valid: Default | quiet | parseable | json

Default: Default

- IgnoreChecksFlag

Jenis: String

Deskripsi: (Opsional) ID aturan untuk diteruskan ke parameter `--ignore-checks`. Aturan-aturan ini tidak diperiksa.

Contoh: E1001, E1003, W7001

- IncludeChecksFlag

Jenis: String

Deskripsi: (Opsional) ID aturan untuk diteruskan ke `--include-checks` parameter. Aturan-aturan ini diperiksa.

Contoh: E1001, E1003, W7001

- InfoFlag

Jenis: String

Deskripsi: (Opsional) Opsi untuk `--info` parameter. Sertakan opsi untuk mengaktifkan informasi logging tambahan tentang pemrosesan template.

Default: salah

- TemplateFileName

Jenis: String

Deskripsi: Nama, atau kunci, file template di bucket S3.

- **Template3 BucketName**

Jenis: String

Deskripsi: Nama bucket S3 yang berisi template packer.

- **RegionsFlag**

Jenis: String

Deskripsi: (Opsional) Nilai untuk diteruskan ke `--regions` parameter for untuk menguji template terhadap yang ditentukanWilayah AWS.

Contoh: us-timur-1, kami-barat-1

### Langkah Dokumen

RunCfnLintAgainstTemplate- Menjalankan `cfn-python-lint` alat terhadap AWS CloudFormation template yang ditentukan.

### Keluaran

RunCfnLintAgainstTemplate.output - Stdout dari alat. `cfn-python-lint`

## **AWSSupport-TroubleshootCFNCustomResource**

### Deskripsi

AWSSupport-TroubleshootCFNCustomResourceRunbook membantu mendiagnosis mengapa AWS CloudFormation tumpukan gagal dalam membuat, memperbarui, atau menghapus sumber daya kustom. Runbook memeriksa token layanan yang digunakan untuk sumber daya kustom dan pesan kesalahan yang dikembalikan. Setelah meninjau detail untuk sumber daya kustom, output runbook memberikan penjelasan tentang perilaku tumpukan dan langkah-langkah pemecahan masalah untuk sumber daya kustom.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik



## Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- StackName

Jenis: String

Deskripsi: (Diperlukan) Nama AWS CloudFormation tumpukan tempat sumber daya kustom gagal.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- cloudformation:ListStackResources
- ec2:DescribeRouteTables
- ec2:DescribeNatGateways
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:DescribeVpcEndpoints
- ec2:DescribeSubnets
- logs:FilterLogEvents

## Langkah Dokumen

- `validateCloudFormationStack`- Memverifikasi bahwa AWS CloudFormation tumpukan ada di sama Akun AWS dan Wilayah AWS.
- `checkCustomResource`- Menganalisis AWS CloudFormation tumpukan, memeriksa sumber daya kustom yang gagal, dan mengeluarkan informasi tentang cara memecahkan masalah sumber daya kustom yang gagal.

## AWS-UpdateCloudFormationStack

### Deskripsi

Perbarui AWS CloudFormation tumpukan dengan menggunakan AWS CloudFormation template yang disimpan dalam bucket Amazon S3.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `LambdaAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) ARN peran yang diasumsikan oleh Lambda

- StackNameOrId

Jenis: String

Deskripsi: (Diperlukan) Nama atau ID Unik AWS CloudFormation tumpukan yang akan diperbarui

- TemplateUrl

Jenis: String

Deskripsi: (Diperlukan) Lokasi bucket S3 yang berisi CloudFormation template yang diperbarui (mis. <https://s3.amazonaws.com/doc-example-bucket/updated.template>)

## CloudFront

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon CloudFront Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSConfigRemediation-EnableCloudFrontDefaultRootObject](#)
- [AWSConfigRemediation-EnableCloudFrontAccessLogs](#)
- [AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity](#)
- [AWSConfigRemediation-EnableCloudFrontOriginFailover](#)
- [AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS](#)

## **AWSConfigRemediation-EnableCloudFrontDefaultRootObject**

Deskripsi

AWSConfigRemediation-EnableCloudFrontDefaultRootObjectRunbook mengonfigurasi objek root default untuk distribusi Amazon CloudFront (CloudFront) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- `CloudFrontDistributionId`

Jenis: String

Deskripsi: (Diperlukan) ID CloudFront distribusi yang ingin Anda konfigurasi objek root default.

- `DefaultRootObject`

Jenis: String

Deskripsi: (Diperlukan) Objek yang CloudFront ingin Anda kembalikan saat permintaan pemirsa menunjuk ke URL root Anda.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`

- `cloudfront:UpdateDistribution`

### Langkah Dokumen

- `aws:executeScript`- Mengkonfigurasi objek root default untuk CloudFront distribusi yang Anda tentukan dalam `CloudFrontDistributionId` parameter.

## **AWSConfigRemediation-EnableCloudFrontAccessLogs**

### Deskripsi

AWSConfigRemediation-EnableCloudFrontAccessLogsRunbook memungkinkan pencatatan akses untuk distribusi Amazon CloudFront (CloudFront) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `BucketName`

Jenis: String

Deskripsi: (Wajib) Nama bucket Amazon Simple Storage Service (Amazon S3) yang ingin Anda simpan log akses. Ember di af-selatan-1, ap-timur-1, eu-selatan-1, dan me-selatan-1 tidak didukung. Wilayah AWS

- CloudFrontId

Jenis: String

Deskripsi: (Wajib) ID CloudFront distribusi yang ingin Anda aktifkan akses masuk.

- IncludeCookies

Jenis: Boolean

Nilai yang valid: benar/salah

Deskripsi: (Wajib) Tetapkan parameter ini ke `true`, jika Anda ingin cookie disertakan dalam log akses.

- Awalan

Jenis: String

Deskripsi: (Opsional) String opsional yang CloudFront ingin Anda awalan ke log akses filenames untuk distribusi Anda, misalnya, `myprefix/`.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistribution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`
- `s3:GetBucketLocation`
- `s3:GetBucketAcl`
- `s3:PutBucketAcl`

**Note**

s3:GetBucketLocationAPI hanya dapat digunakan untuk bucket S3 di akun yang sama. Anda tidak dapat menggunakannya untuk bucket S3 lintas akun.

**Langkah Dokumen**

- `aws:executeScript`- Mengaktifkan akses logging untuk CloudFront distribusi yang Anda tentukan dalam `CloudFrontDistributionId` parameter.

## **AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity**

**Deskripsi**

`AWSConfigRemediation-EnableCloudFrontOriginAccessIdentityRunbook` memungkinkan identitas akses asal untuk distribusi Amazon CloudFront (CloudFront) yang Anda tentukan. Otomatisasi ini menetapkan CloudFront Origin Access Identity yang sama untuk semua Origins of the Amazon Simple Storage Service (Amazon S3) jenis asal tanpa identitas akses asal untuk CloudFront distribusi yang Anda tentukan. Otomatisasi ini tidak memberikan izin baca ke identitas akses asal CloudFront untuk mengakses objek di bucket Amazon S3 Anda. Anda harus memperbarui izin bucket Amazon S3 Anda untuk mengizinkan akses.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- `CloudFrontDistributionId`

Jenis: String

Deskripsi: (Diperlukan) ID CloudFront distribusi yang ingin Anda aktifkan failover asal.

- `OriginAccessIdentityId`

Jenis: String

Deskripsi: (Diperlukan) ID identitas akses CloudFront asal untuk dikaitkan dengan asal.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`

Langkah Dokumen

- `aws:executeScript`- Memungkinkan identitas akses asal untuk CloudFront distribusi yang Anda tentukan dalam `CloudFrontDistributionId` parameter, dan memverifikasi identitas akses asal ditugaskan.

## **AWSConfigRemediation-EnableCloudFrontOriginFailover**

Deskripsi



`AWSConfigRemediation-EnableCloudFrontOriginFailover` Runbook memungkinkan failover asal untuk distribusi Amazon CloudFront (CloudFront) yang Anda tentukan.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- `CloudFrontDistributionId`

Jenis: String

Deskripsi: (Diperlukan) ID CloudFront distribusi yang ingin Anda aktifkan failover asal.

- `OriginGroupId`

Jenis: String

Deskripsi: (Diperlukan) ID grup asal.

- `PrimaryOriginId`

Jenis: String

Deskripsi: (Diperlukan) ID asal utama dalam grup asal.

- `SecondaryOriginId`

Jenis: String

Deskripsi: (Diperlukan) ID asal sekunder dalam kelompok asal.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`

Langkah Dokumen

- `aws:executeScript`- Memungkinkan failover asal untuk CloudFront distribusi yang Anda tentukan dalam `CloudFrontDistributionId` parameter, dan memverifikasi bahwa failover telah diaktifkan.

## **AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS**

Deskripsi

`AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS` runbook memungkinkan kebijakan protokol penampil untuk distribusi Amazon CloudFront (CloudFront) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- `CloudFrontDistributionId`

Jenis: String

Deskripsi: (Diperlukan) ID CloudFront distribusi yang ingin Anda aktifkan pada kebijakan protokol penampil.

- `ViewerProtocolPolicy`

Jenis: String

Nilai yang valid: `https-saja`, `redirect-to-https`

Deskripsi: (Diperlukan) Protokol yang dapat digunakan pemirsa untuk mengakses file di asal.

## Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`
- `cloudfront:GetDistribution`

## Langkah Dokumen

- `aws:executeScript`- Mengaktifkan kebijakan protokol penampil untuk CloudFront distribusi yang Anda tentukan dalam `CloudFrontDistributionId` parameter, dan memverifikasi kebijakan telah ditetapkan.

## CloudTrail

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS CloudTrail Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSConfigRemediation-CreateCloudTrailMultiRegionTrail](#)
- [AWS-EnableCloudTrail](#)
- [AWS-EnableCloudTrailCloudWatchLogs](#)
- [AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS](#)
- [AWS-EnableCloudTrailKmsEncryption](#)
- [AWSConfigRemediation-EnableCloudTrailLogFileValidation](#)
- [AWS-EnableCloudTrailLogFileValidation](#)
- [AWS-QueryCloudTrailLogs](#)

## AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

### Deskripsi

`AWSConfigRemediation-CreateCloudTrailMultiRegionTrail` Buku runbook membuat jejak AWS CloudTrail (CloudTrail) yang mengirimkan file log dari beberapa Wilayah AWS ke bucket Amazon Simple Storage Service (Amazon S3) pilihan Anda.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- BucketName

Jenis: String

Deskripsi: (Diperlukan) Nama bucket Amazon S3 yang ingin Anda unggah log.

- KeyPrefix

Jenis: String

Deskripsi: (Opsional) Awalan kunci Amazon S3 yang muncul setelah nama bucket yang Anda tetapkan untuk pengiriman file log.

- TrailName

Jenis: String

Deskripsi: (Diperlukan) Nama CloudTrail jejak yang akan dibuat.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:CreateTrail`
- `cloudtrail:StartLogging`

- `cloudtrail:GetTrail`
- `s3:PutObject`
- `s3:GetBucketAcl`
- `s3:PutBucketLogging`
- `s3:ListBucket`

### Langkah Dokumen

- `aws:executeAwsApi`- Menerima nama jejak dan nama bucket Amazon S3 sebagai input dan membuat CloudTrail jejak.
- `aws:executeAwsApi`- Memungkinkan pencatatan log pada jejak yang dibuat dan memulai pengiriman log ke bucket Amazon S3 yang Anda tentukan.
- `aws:assertAwsResourceProperty`- Memverifikasi bahwa CloudTrail jejak telah dibuat.

## AWS-EnableCloudTrail

### Deskripsi

Buat AWS CloudTrail jejak dan konfigurasi logging ke bucket S3.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`


Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- S3 BucketName

Jenis: String

Deskripsi: (Diperlukan) Nama bucket S3 yang ditunjuk untuk menerbitkan file log.

 Note

Bucket S3 harus ada dan kebijakan bucket harus memberikan CloudTrail izin untuk menulis ke sana. Untuk informasi, lihat [Kebijakan Bucket Amazon S3 untuk CloudTrail](#).

- TrailName

Jenis: String

Deskripsi: (Diperlukan) Nama jejak baru.

## AWS-EnableCloudTrailCloudWatchLogs

Deskripsi

Runbook ini memperbarui konfigurasi satu atau beberapa AWS CloudTrail jejak untuk mengirim peristiwa ke grup CloudWatch log Amazon Logs.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

## Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `CloudWatchLogsLogGroupArn`

Jenis: String

Deskripsi: (Wajib) ARN dari grup CloudWatch log Log tempat CloudTrail log akan dikirimkan.

- `CloudWatchLogsRoleArn`

Jenis: String

Deskripsi: (Wajib) ARN dari CloudWatch Log Log peran IAM mengasumsikan untuk menulis ke grup log yang ditentukan.

- `TrailNames`

Jenis: StringList

Deskripsi: (Wajib) Daftar nama CloudTrail jalur yang dipisahkan koma yang peristiwanya ingin Anda kirim ke CloudWatch Log.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudtrail:UpdateTrail`
- `iam:PassRole`

### Langkah Dokumen



- `aws:executeScript`- Memperbarui CloudTrail jejak yang ditentukan untuk mengirimkan peristiwa ke grup CloudWatch log Log yang ditentukan.

## AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

### Deskripsi

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMSRunbook mengenkripsi jejak AWS CloudTrail (CloudTrail) menggunakan kunci yang dikelola pelanggan AWS Key Management Service (AWS KMS) yang Anda tentukan. Runbook ini hanya boleh digunakan sebagai dasar untuk memastikan bahwa CloudTrail jejak Anda dienkripsi sesuai dengan praktik terbaik keamanan minimum yang direkomendasikan. Sebaiknya enkripsi beberapa jalur dengan kunci KMS yang berbeda. CloudTrailfile digest tidak dienkripsi. Jika sebelumnya Anda telah menetapkan `EnableLogFileValidation` parameter `true` untuk jejak, lihat bagian “Gunakan enkripsi sisi server dengan kunci AWS KMS terkelola” dari topik [Praktik Terbaik Keamanan CloudTrail Pencegahan](#) di Panduan AWS CloudTrail Pengguna untuk informasi selengkapnya.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux,macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- `KMS KeyId`

Jenis: String

Deskripsi: (Diperlukan) ARN, ID kunci, atau alias kunci kunci kunci yang dikelola pelanggan yang ingin Anda gunakan untuk mengenkripsi jejak yang Anda tentukan dalam parameter.

TrailName

- TrailName

Jenis: String

Deskripsi: (Diperlukan) ARN atau nama jejak yang ingin Anda perbarui untuk dienkripsi.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:GetTrail`
- `cloudtrail:UpdateTrail`

Langkah Dokumen

- `aws:executeAwsApi`- Memungkinkan enkripsi pada jejak yang Anda tentukan dalam `TrailName` parameter.
- `aws:executeAwsApi`- Mengumpulkan ARN untuk kunci yang dikelola pelanggan yang Anda tentukan dalam parameter. `KMSKeyId`
- `aws:assertAwsResourceProperty`- Memverifikasi bahwa enkripsi telah diaktifkan di CloudTrail jalan.

## AWS-EnableCloudTrailKmsEncryption

Deskripsi

Runbook ini memperbarui konfigurasi satu atau beberapa AWS CloudTrail jejak untuk menggunakan enkripsi AWS Key Management Service (AWS KMS).

## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- KMS KeyId

Jenis: String

Deskripsi: (Wajib) ID kunci dari kunci terkelola pelanggan yang ingin Anda gunakan untuk mengenkripsi jejak yang Anda tentukan dalam `TrailName` parameter. Nilai dapat berupa nama alias yang diawali dengan "alias/", ARN yang ditentukan sepenuhnya ke alias, atau ARN yang ditentukan sepenuhnya ke kunci.

- TrailNames

Jenis: StringList

Deskripsi: (Wajib) Daftar jejak yang dipisahkan koma yang ingin Anda perbarui untuk dienkripsi.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudtrail:UpdateTrail`
- `kms:DescribeKey`
- `kms:ListKeys`

### Langkah Dokumen

- `aws:executeScript`- Mengaktifkan AWS KMS enkripsi pada jalur yang Anda tentukan dalam `TrailName` parameter.

## **AWSConfigRemediation-EnableCloudTrailLogFileValidation**

### Deskripsi

AWSConfigRemediation-EnableCloudTrailLogFileValidationRunbook memungkinkan validasi file log untuk jejak Anda AWS CloudTrail.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- **TrailName**

Jenis: String

Deskripsi: (Wajib) Nama atau Nama Sumber Daya Amazon (ARN) dari jejak yang ingin Anda aktifkan validasi log.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:GetTrail`
- `cloudtrail:UpdateTrail`

Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan validasi log untuk AWS CloudTrail jejak yang Anda tentukan dalam `TrailName` parameter.
- `aws:assertAwsResourceProperty`- Memverifikasi validasi log diaktifkan untuk jejak Anda.

## **AWS-EnableCloudTrailLogFileValidation**

Deskripsi

AWS-EnableCloudTrailLogFileValidationRunbook memungkinkan validasi file log untuk AWS CloudTrail jejak yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

## Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `TrailNames`

Jenis: StringList

Deskripsi: (Wajib) Daftar nama CloudTrail jejak yang dipisahkan koma yang ingin Anda aktifkan validasi log.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudtrail:GetTrail`
- `cloudtrail:UpdateTrail`

### Langkah Dokumen

- `aws:executeScript`- Mengaktifkan validasi log untuk AWS CloudTrail jejak yang Anda tentukan dalam parameter. `TrailNames`

## AWS-QueryCloudTrailLogs

### Deskripsi

AWS-QueryCloudTrailLogsBuku runbook membuat tabel Amazon Athena dari bucket Amazon Simple Storage Service (Amazon S3) pilihan Anda yang berisi AWS CloudTrail (CloudTrail) log. Setelah membuat tabel, otomatisasi menjalankan kueri SQL yang Anda tentukan dan kemudian menghapus tabel.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis data

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Kueri

Jenis: String

Deskripsi: (Diperlukan) Kueri SQL yang ingin Anda jalankan.

- SourceBucketPath

Jenis: String

Deskripsi: (Diperlukan) Nama bucket Amazon S3 yang berisi file CloudTrail log yang ingin Anda kueri.

- TableName

Jenis: String

Keterangan: (Opsional) Nama tabel Athena dibuat oleh otomatisasi.

Bawaan: cloudtrail\_logs

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `athena:GetQueryResults`
- `athena:GetQueryExecution`
- `athena:StartQueryExecution`
- `glue:CreateTable`
- `glue>DeleteTable`
- `glue:GetDatabase`
- `glue:GetPartitions`
- `glue:GetTable`
- `s3:AbortMultipartUpload`
- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`

Langkah Dokumen

- `aws:executeAwsApi`- Membuat meja Athena.
- `aws:executeAwsApi`- Menjalankan string kueri yang Anda tentukan dalam Query parameter.
- `aws:executeScript`- Jajak pendapat dan menunggu kueri selesai.



- `aws:executeAwsApi`- Mendapat hasil query.
- `aws:executeAwsApi`- Menghapus tabel yang dibuat oleh otomatisasi.

## CloudWatch

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon CloudWatch. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-ConfigureCloudWatchOnEC2Instance](#)
- [AWS-EnableCWAlarm](#)

## AWS-ConfigureCloudWatchOnEC2Instance

### Deskripsi

Mengaktifkan atau menonaktifkan pemantauan CloudWatch terperinci Amazon pada instans terkelola.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans Amazon EC2 yang ingin Anda aktifkan CloudWatch pemantauan.

- properti

Jenis: String

Deskripsi: (Opsional) Parameter ini tidak didukung. Hal ini tercantum di sini untuk kompatibilitas mundur.

- status

Nilai yang valid: Diaktifkan | Dinonaktifkan

Deskripsi: (Opsional) Menentukan apakah akan mengaktifkan atau menonaktifkan CloudWatch.

Default: Diaktifkan

## Langkah Dokumen

configureCloudWatch- Mengkonfigurasi CloudWatch pada instans Amazon EC2 dengan status yang diberikan.

## Keluaran

Otomatisasi ini tidak memiliki output.

## **AWS-EnableCWAlarm**

### Deskripsi

AWS-EnableCWAlarmRunbook membuat alarm Amazon CloudWatch (CloudWatch) untuk AWS sumber daya di Akun AWS yang belum memilikinya. CloudWatch alarm dibuat untuk AWS sumber daya berikut:

- Instans Amazon Elastic Compute Cloud (Amazon EC2)
- Volume Amazon Elastic Block Store (Amazon EBS)
- Ember Amazon Simple Storage Service (Amazon S3)
- Cluster Amazon Relational Database Service (Amazon RDS)

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ComparisonOperator

Jenis: String

Nilai yang valid: GreaterThanOrEqualToThreshold | GreaterThanThreshold  
GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpper Threshold |  
LessThanLowerThreshold LessThanOrEqualToThreshold LessThanThreshold

Deskripsi: (Wajib) Operasi aritmatika yang digunakan saat membandingkan statistik dan ambang batas yang ditentukan.

- **MetricName**

Jenis: String

Deskripsi: (Wajib) Nama untuk metrik yang terkait dengan alarm.

- **Periode**

Jenis: Integer

Nilai yang valid: 10 | 30 | 60 | Kelipatan 60

Deskripsi: (Wajib) Periode, dalam detik, di mana statistik diterapkan.

- **Sumber DayaEarns**

Jenis: StringList

Deskripsi: (Wajib) Daftar ARN sumber daya yang dipisahkan koma untuk membuat alarm CloudWatch

- **Statistik**

Jenis: String

Nilai yang valid: Rata-rata | Maksimum | Minimum | SampleCount | Jumlah

Deskripsi: (Wajib) Statistik untuk metrik yang terkait dengan alarm.

- **Ambang**

Jenis: Integer

Deskripsi: (Wajib) Nilai untuk dibandingkan dengan statistik yang ditentukan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudwatch:PutMetricAlarm`

## Langkah Dokumen

- `aws:executeScript`- Membuat CloudWatch alarm sesuai dengan nilai yang ditentukan dalam parameter runbook untuk sumber daya yang Anda tentukan dalam `ResourceARNs` parameter.

## Keluaran

`EnableWalarm.FailedResources`: Daftar peta ARN sumber daya yang CloudWatch alarmnya tidak dibuat dan alasan kegagalannya.

`EnableWalarm.SuccessfulResources`: Daftar ARN sumber daya yang CloudWatch alarmnya berhasil dibuat.

# Amazon DocumentDB

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon DocumentDB (dengan kompatibilitas MongoDB). Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWS-EnableDocDbClusterBackupRetentionPeriod](#)

## AWS-EnableDocDbClusterBackupRetentionPeriod

### Deskripsi

`AWS-EnableDocDbClusterBackupRetentionPeriodRunbook` memungkinkan periode retensi cadangan untuk klaster Amazon DocumentDB yang Anda tentukan. Fitur ini menetapkan jumlah hari di mana cadangan otomatis disimpan. Untuk memodifikasi cluster, cluster harus dalam keadaan yang tersedia dengan tipe `mesindocdb`.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

## Platform

Linux, macOS, Windows

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `DB ClusterResourceid`

Jenis: String

Deskripsi: (Diperlukan) ID sumber daya untuk klaster Amazon DocumentDB yang ingin Anda aktifkan periode retensi cadangan.

- `BackupRetentionPeriod`

Jenis: Integer

Deskripsi: (Wajib) Jumlah hari di mana cadangan otomatis dipertahankan. Harus nilai dari 7-35 hari.

- `PreferredBackupWindow`

Jenis: String

Deskripsi: (Opsional) Rentang waktu harian dalam Universal Time Coordinated (UTC) dalam format hh24: mm-hh24: mm, misalnya 07:14-07:44. Nilai harus minimal 30 menit dan tidak dapat bertentangan dengan jendela pemeliharaan yang diinginkan.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `docdb:DescribeDBClusters`
- `docdb:ModifyDBCluster`
- `rds:DescribeDBClusters`

- `rds:ModifyDBCluster`

### Langkah Dokumen

- `GetDocDbClusterIdentifier` (`aws:executeAwsApi`) - Mengembalikan pengidentifikasi kluster Amazon DocumentDB menggunakan ID sumber daya yang disediakan.
- `VerifyDocDbEngine` (`aws:assertAwsResource Properti`) - Memverifikasi jenis mesin Amazon DocumentDB adalah untuk mencegah perubahan yang tidak disengaja pada docdb jenis mesin Amazon RDS lainnya.
- `VerifyDocDbStatus` (`aws:waitAwsResource Properti`) - Memverifikasi status cluster Amazon DocumentDB adalah `available`
- `ModifyDocDbRetentionPeriod` (`aws:executeAwsApi`) - Menyetel periode retensi menggunakan nilai yang disediakan untuk kluster Amazon DocumentDB yang ditentukan.
- `VerifyDocDbBackupsEnabled` (`AWS:executeScript`) - Memverifikasi periode retensi untuk kluster Amazon DocumentDB dan jendela cadangan pilihan, jika ditentukan, berhasil disetel.

### Keluaran

`ModifyDocDbRetentionPeriod`. `ModifyDbClusterResponse` - Respon dari operasi `ModifyDBCluster` API.

`VerifyDocDbBackupsEnabled`. `VerifyDbClusterBackupsEnabledResponse` - Output dari `VerifyDocDbBackupsEnabled` langkah yang mengonfirmasi keberhasilan modifikasi cluster Amazon DocumentDB.

## CodeBuild

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS CodeBuild Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSConfigRemediation-ConfigureCodeBuildProjectWithKMScmk](#)
- [AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject](#)

# AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

## Deskripsi

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMKRunbook mengenkripsi artefak build proyek AWS CodeBuild (CodeBuild) menggunakan kunci terkelola pelanggan AWS Key Management Service (AWS KMS) yang Anda tentukan. AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

## [Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

## Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- KMS KeyId

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari kunci terkelola AWS KMS pelanggan yang ingin Anda gunakan untuk mengenkripsi CodeBuild proyek yang Anda tentukan dalam parameter. ProjectId

- ProjectId



Jenis: String

Deskripsi: (Wajib) ID CodeBuild proyek yang artefak pembuatannya ingin Anda enkripsi.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `codebuild:BatchGetProjects`
- `codebuild:UpdateProject`
- `config:GetResourceConfigHistory`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan nama CodeBuild proyek dari ID proyek.
- `aws:executeAwsApi`- Mengaktifkan enkripsi pada CodeBuild proyek yang Anda tentukan dalam `ProjectId` parameter.
- `aws:assertAwsResourceProperty`- Memverifikasi bahwa enkripsi telah diaktifkan pada CodeBuild proyek.

Keluaran

`UpdateLambdaConfig.UpdateFunctionConfigurationResponse` - Respon dari panggilan `UpdateFunctionConfiguration` API.

## **AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject**

Deskripsi

`AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProjectRunbook` menghapus variabel `AWS_ACCESS_KEY_ID` dan `AWS_SECRET_ACCESS_KEY` lingkungan dari proyek AWS

CodeBuild (CodeBuild) yang Anda tentukan. AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- ResourceId

Jenis: String

Deskripsi: (Diperlukan) ID CodeBuild proyek yang variabel lingkungan kunci aksesnya ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`

- `codebuild:BatchGetProjects`
- `codebuild:UpdateProject`

### Langkah Dokumen

- `aws:executeScript`- Menghapus variabel lingkungan kunci akses untuk CodeBuild proyek yang ditentukan dalam parameter. `ResourceId`

## AWS CodeDeploy

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS CodeDeploy Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSSupport-TroubleshootCodeDeploy](#)

## AWSSupport - TroubleshootCodeDeploy

### Deskripsi

`AWSSupport-TroubleshootCodeDeployRunbook` membantu mendiagnosis mengapa AWS CodeDeploy penerapan gagal pada instans Amazon Elastic Compute Cloud (Amazon EC2). Runbook mengeluarkan langkah-langkah untuk membantu Anda menyelesaikan masalah atau memecahkan masalah lebih lanjut. Praktik terbaik juga CodeDeploy disediakan untuk membantu Anda menghindari masalah serupa di masa depan.

Runbook ini dapat membantu Anda menyelesaikan masalah berikut:

- `CodeDeployAgent` tidak diinstal atau tidak berjalan pada instans Amazon EC2
- Instans Amazon EC2 tidak memiliki profil instans AWS Identity and Access Management (IAM) yang terpasang
- Profil instans IAM yang dilampirkan ke instans Amazon EC2 tidak memiliki izin Amazon Simple Storage Service (Amazon S3) yang diperlukan
- Revisi yang disimpan di Amazon S3 tidak ada, atau bucket Amazon S3 yang digunakan dalam Wilayah AWS yang berbeda dari instans Amazon EC2

- Spesifikasi aplikasi (AppSpec) masalah file
- Kesalahan “File sudah ada di lokasi”
- Kait peristiwa siklus hidup CodeDeploy terkelola yang gagal
- Kait peristiwa siklus hidup terkelola pelanggan yang gagal
- Skala-dalam peristiwa selama penyebaran

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DeploymentId

Jenis: String

Deskripsi: (Diperlukan) ID penyebaran yang gagal.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans Amazon EC2 tempat penyebaran gagal.

## Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `codedeploy:GetDeployment`
- `codedeploy:GetDeploymentTarget`
- `ec2:DescribeInstances`

## Langkah Dokumen

- `aws:executeAwsApi`- Memverifikasi nilai-nilai yang disediakan untuk `DeploymentId` dan `InstanceId` parameter.
- `aws:executeScript`- Mengumpulkan informasi dari instans Amazon EC2 seperti status instans dan detail profil instans IAM.
- `aws:executeScript`- Meninjau penyebaran yang ditentukan, dan mengembalikan analisis mengenai mengapa penyebaran gagal.

## AWS Config

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk. `AWS Config Untuk` informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSSupport-SetupConfig](#)

## AWSSupport-SetupConfig

### Deskripsi

`AWSSupport-SetupConfigRunbook` membuat peran terkait layanan AWS Identity and Access Management (IAM), perekam konfigurasi yang didukung oleh `AWS Config`, dan saluran pengiriman dengan bucket Amazon Simple Storage Service (Amazon S3) yang `AWS Config` mengirimkan snapshot konfigurasi dan file riwayat konfigurasi. Jika Anda menentukan nilai untuk `AggregatorAccountId` dan `AggregatorAccountRegion` parameter, runbook juga membuat

otorisasi untuk agregasi data untuk mengumpulkan data AWS Config konfigurasi dan kepatuhan dari beberapa dan beberapa. Akun AWS Wilayah AWS Untuk mempelajari lebih lanjut tentang menggabungkan data dari beberapa akun dan Wilayah, lihat [Agregasi Data Multi-Wilayah Multi-Akun](#) di Panduan Pengembang. AWS Config

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- AggregatorAccountId

Jenis: String

Deskripsi: (Opsional) ID Akun AWS tempat agregator akan ditambahkan ke data AWS Config konfigurasi dan kepatuhan agregat dari beberapa akun dan. Wilayah AWS Akun ini juga digunakan oleh agregator untuk mengotorisasi akun sumber.

- AggregatorAccountRegion

Jenis: String

Deskripsi: (Opsional) Wilayah tempat agregator akan ditambahkan ke data AWS Config konfigurasi dan kepatuhan gabungan dari beberapa akun dan Wilayah.

- `IncludeGlobalResourcesRegion`

Jenis: String

Default: kami-timur-1

Deskripsi: (Diperlukan) Untuk menghindari perekaman data sumber daya global di setiap Wilayah, tentukan satu Wilayah untuk merekam data sumber daya global.

- `Partition`

Jenis: String

Default: aws

Deskripsi: (Diperlukan) Partisi tempat Anda ingin mengumpulkan data AWS Config konfigurasi dan kepatuhan.

- `S3 BucketName`

Jenis: String

Default: aws-config-delivery-channel

Deskripsi: (Opsional) Nama yang ingin Anda terapkan ke bucket Amazon S3 yang dibuat untuk saluran pengiriman. ID akun ditambahkan ke akhir nama.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:DescribeConfigurationRecorders`
- `config:DescribeDeliveryChannels`
- `config:PutAggregationAuthorization`
- `config:PutConfigurationRecorder`
- `config:PutDeliveryChannel`
- `config:StartConfigurationRecorder`

- `iam:CreateServiceLinkedRole`
- `iam:PassRole`
- `s3:CreateBucket`
- `s3:ListAllMyBuckets`
- `s3:PutBucketPolicy`

## Langkah Dokumen

- `aws:executeScript`- Membuat peran IAM terkait layanan AWS Config jika seseorang belum ada.
- `aws:executeScript`- Membuat perekam konfigurasi jika salah satu belum ada.
- `aws:executeScript`- Membuat bucket Amazon S3 untuk digunakan oleh saluran pengiriman jika tidak ada.
- `aws:executeScript`- Membuat saluran pengiriman menggunakan sumber daya yang dibuat oleh runbook.
- `aws:executeAwsApi`- Mulai perekam konfigurasi.
- `aws:executeScript`- Jika Anda menentukan nilai untuk `AggregatorAccountId` dan `AggregatorAccountRegion` parameter, otorisasi untuk multi-akun dan agregasi data Multi-wilayah dikonfigurasi.

## Amazon Connect

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Connect. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSSupport-AssociatePhoneNumbersToConnectContactFlows](#)

## **AWSSupport-AssociatePhoneNumbersToConnectContactFlows**

### Deskripsi

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows` ini membantu Anda mengaitkan nomor telepon ke alur kontak di instans Amazon Connect Anda. Dengan menyediakan



pemetaan nomor telepon dan alur kontak dalam file input comma-separated values (CSV), runbook mengaitkan sebanyak mungkin nomor telepon ke arus kontak dalam waktu 14,5 menit. Runbook menghasilkan file CSV dari semua nomor telepon dan pasangan aliran kontak yang tidak dapat dikaitkan dalam batas waktu sehingga Anda dapat memasukkannya dalam proses berikutnya.

Bagaimana cara kerjanya?

Runbook `AWSsupport-AssociatePhoneNumbersToConnectContactFlows` membantu Anda mengaitkan nomor telepon ke alur kontak di instans Amazon Connect menggunakan file CSV untuk memetakan data yang disimpan dalam bucket Amazon Simple Storage Service (Amazon S3). File CSV input harus sejajar dengan format berikut, dengan `PhoneNumber` nilai dalam format [E.164](#).

Contoh file CSV masukan

```
PhoneNumber,ContactFlowName
+1800555xxxx,ContactFlowA
+1800555yyyy,ContactFlowB
+1800555zzzz,ContactFlowC
```

Runbook otomatisasi juga membuat file berikut di lokasi tujuan yang ditentukan dalam `DestinationFileBucket` dan `DestinationFilePath`.

- **`automation:EXECUTION_ID/ResourceIdList.csv`**: File sementara yang berisi `PhoneNumberId` dan `ContactFlowId` pasangan yang diperlukan untuk `AssociatePhoneNumberContactFlow` API.
- **`automation:EXECUTION_ID/ErrorResourceList.csv`**: File yang berisi nomor telepon dan pasangan aliran kontak yang tidak dapat diproses karena kesalahan, seperti `ResourceNotFoundException` dalam `formatPhoneNumber,ContactFlowName,ErrorMessage`.
- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`**: File yang berisi nomor telepon dan pasangan alur kontak yang tidak diproses. Runbook mencoba memproses nomor telepon dan arus kontak sebanyak mungkin dalam 14,5 menit (15 menit waktu tunggu AWS Lambda fungsi - 30 detik buffer). Jika ada beberapa nomor telepon/alur kontak yang tidak dapat diproses karena keterbatasan waktu, runbook menyertakannya dalam file CSV untuk digunakan sebagai input untuk eksekusi runbook berikutnya.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

```
{
  "Statement": [
    {
      "Action": [
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectAttributes",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": [
        "arn:aws:s3:::YOUR-BUCKET/*",
        "arn:aws:s3:::YOUR-BUCKET"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation>DeleteStack",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam:GetRole",
        "iam:PutRolePolicy",
```

```

        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:TagResource",
        "connect:AssociatePhoneNumberContactFlow",
        "logs:CreateLogGroup",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "logs>DeleteLogGroup",
        "s3:GetAccountPublicAccessBlock"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "connect:DescribeInstance",
        "connect:ListPhoneNumbers",
        "connect:ListContactFlows",
        "ds:DescribeDirectories"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Condition": {
        "StringLikeIfExists": {
            "iam:PassedToService": [
                "ssm.amazonaws.com",
                "lambda.amazonaws.com"
            ]
        }
    },
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - Associate Phone Numbers To Connect Contact Flows Systems Manager](#) di bawah Dokumen.

2. Pilih Jalankan otomatisasi.

3. Untuk parameter input, masukkan yang berikut ini:

- AutomationAssumeRole (Opsional)

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ConnectInstanceId (Diperlukan)

ID instans Amazon Connect Anda.

- SourceFileBucket (Diperlukan)

Bucket Amazon S3 yang menyimpan file CSV yang berisi nomor telepon dan pasangan alur kontak.

- SourceFilePath (Diperlukan)

Kunci objek Amazon S3 dari file CSV yang berisi nomor telepon dan pasangan aliran kontak. Misalnya, `path/to/input.csv`.

- DestinationFileBucket (Diperlukan)

Bucket Amazon S3 di mana otomatisasi akan menempatkan file perantara dan laporan hasil.

- DestinationFilePath (Opsional)

Jalur objek Amazon S3 DestinationFileBucket di mana file perantara dan laporan hasil harus disimpan. Misalnya, jika Anda menentukan `path/to/files/`, file disimpan di bawah `s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`.

- S3 BucketOwnerAccount (Opsional)

Nomor AWS Akun yang memiliki bucket Amazon S3 tempat Anda ingin mengunggah Log Aliran Kontak. Jika Anda tidak menentukan parameter ini, runbook menggunakan ID AWS akun pengguna atau peran di mana Otomasi berjalan.

- S3 BucketOwnerRoleArn (Opsional)

ARN peran IAM dengan izin untuk mendapatkan bucket Amazon S3 dan pengaturan pemblokiran akun akses publik, konfigurasi enkripsi bucket, ACL bucket, status kebijakan bucket, dan mengunggah objek ke bucket. Jika parameter ini tidak ditentukan, runbook menggunakan `AutomationAssumeRole` (jika ditentukan) atau pengguna yang memulai runbook ini (jika tidak `AutomationAssumeRole` ditentukan). Silakan lihat bagian izin yang diperlukan di deskripsi buku runbook.

**Input parameters**

<p><b>AutomationAssumeRole</b> <small>(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</small></p> <p>test-role <input type="text"/></p> <p><b>SourceFileBucket</b> <small>(Required) The Amazon S3 bucket name that stores the CSV file which contains the pairs of phone numbers and Contact Flows.</small></p> <p><input type="text"/></p> <p><b>DestinationFileBucket</b> <small>(Required) The Amazon S3 bucket that the automation will copy the file to be processed, the report, and any non-processed phone number and Contact Flow pair.</small></p> <p><input type="text"/></p> <p><b>S3BucketOwnerAccount</b> <small>(Optional) The AWS Account Number that owns the Amazon S3 bucket where you want to upload the Contact Flow Log. If you do not specify this parameter, the runbooks uses the AWS account ID of the user or role in which the Automation runs.</small></p> <p><input type="text"/></p>	<p><b>ConnectInstanceid</b> <small>(Required) The ID of your Amazon Connect instance.</small></p> <p>01234567-89ab-cdef-0123-456789abcdef <input type="text"/></p> <p><b>SourceFilePath</b> <small>(Required) The Amazon S3 object key of the CSV file that contains the pairs of phone numbers and Contact Flows. Example: 'path/to/input.csv'.</small></p> <p><input type="text"/></p> <p><b>DestinationFilePath</b> <small>(Optional) The Amazon S3 object path in 'DestinationFileBucket' to copy the file to be processed, the report, and any non-processed phone number and Contact Flow pair. For example, if you specify 'path/to/files/', the files will be stored under 's3://-DestinationFileBucket-/path/to/files/&lt;automation:EXECUTION_ID&gt;'.</small></p> <p><input type="text"/></p> <p><b>S3BucketOwnerRoleArn</b> <small>(Optional) The ARN of the IAM role with permissions to get the Amazon S3 bucket and account block public access settings, bucket encryption configuration, the bucket ACLs, the bucket policy status, and upload objects to the bucket. If this parameter is not specified, the runbook uses the 'AutomationAssumeRole' (if specified) or user that starts this runbook (if 'AutomationAssumeRole' is not specified). Please see the required permissions section in the runbook description.</small></p> <p><input type="text"/></p>
--	--

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- CheckConnectInstanceExistence

Memeriksa apakah instans Amazon Connect yang disediakan `ConnectInstanceId` ada.

- Ceks3 BucketPublicStatus

Memeriksa apakah bucket Amazon S3 ditentukan dalam `SourceFileBucket` dan `DestinationFileBucket` mengizinkan izin akses baca atau tulis anonim atau publik.

- CheckSourceFileExistenceAndSize

Memeriksa apakah file CSV sumber yang ditentukan dalam `SourceFilePath` ada dan jika ukuran file melebihi batas 25 MiB.

- GenerateResourceIdMap

Mengunduh file CSV sumber yang ditentukan dalam `SourceFilePath` dan mengidentifikasi `PhoneNumberId` dan `ContactFlowId` untuk setiap sumber daya. Setelah selesai, ia mengunggah file CSV yang berisi `PhoneNumber`, `PhoneNumberIdContactFlowName`, dan `ContactFlowId` ke bucket Amazon S3 tujuan yang ditentukan. `DestinationFileBucket` Jika `PhoneNumberId` tidak dapat diidentifikasi untuk nomor tertentu, yang diajukan akan kosong di file CSV.

- **AssociatePhoneNumbersToContactFlows**

Membuat AWS Lambda fungsi di akun Anda menggunakan AWS CloudFormation tumpukan. AWS Lambda Fungsi ini mengaitkan setiap nomor ke alur kontak yang tercantum dalam file CSV sumber yang ditentukan dalam `SourceFileBucket` dan `SourceFilePath` dan AWS CloudFormation tumpukan memanggil fungsi. AWS Lambda Fungsi memetakan nomor telepon sebanyak mungkin untuk menghubungi arus sebelum waktu habis (15 menit). Daftar nomor telepon dan alur kontak yang tidak dapat diproses karena kesalahan diunggah. `[automation:EXECUTION_ID]/ErrorResourceList.csv` Yang tidak dapat diproses karena kelebihan jumlah maksimum nomor telepon yang dapat diproses dalam satu eksekusi diunggah. `[automation:EXECUTION_ID]/NonProcessedResourceList.csv` Jika langkah ini gagal, lanjutkan ke `DescribeCloudFormationErrorFromStackEvents` langkah untuk menunjukkan mengapa gagal dari peristiwa AWS CloudFormation tumpukan.

- **WaitForPhoneNumberContactFlowAssociationCompletion**

Menunggu hingga AWS Lambda fungsi yang memetakan nomor telepon ke alur kontak dibuat dan AWS CloudFormation tumpukan menyelesaikan pemanggilannya.

- **GenerateReport**

Menghasilkan laporan yang berisi jumlah nomor telepon yang dipetakan ke arus kontak, yang tidak dapat diproses karena kesalahan, dan yang tidak dapat diproses karena kelebihan jumlah maksimum nomor telepon yang dapat diproses dalam eksekusi tunggal. Laporan ini juga menunjukkan lokasi (URI Amazon S3 dan URL konsol Amazon S3) `[automation:EXECUTION_ID]/ErrorResourceList.csv` untuk `[automation:EXECUTION_ID]/NonProcessedResourceList.csv` atau, jika berlaku.

- **DeleteCloudFormationStack**

Menghapus AWS CloudFormation tumpukan, termasuk fungsi Lambda untuk pemetaan.

- **DescribeCloudFormationErrorFromStackEvent**

Menjelaskan kesalahan dari AWS CloudFormation tumpukan `AssociatePhoneNumbersToContactFlows` langkah.

7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci:

- `GenerateReport.OutputPayload`

Output nomor telepon dan asosiasi aliran kontak. Laporan ini berisi informasi berikut:

- Jumlah pasangan nomor telepon dan alur kontak yang tercantum dalam file CSV masukan
- Jumlah nomor telepon yang terkait dengan alur kontak sebagaimana ditentukan dalam file CSV input
- Jumlah nomor telepon yang tidak dapat dikaitkan dengan arus kontak karena kesalahan
- Jumlah nomor telepon yang tidak terkait dengan arus kontak karena keterbatasan waktu
- Lokasi (Amazon S3 URI dan URL konsol Amazon S3) dari file CSV yang berisi nomor telepon dan pasangan alur kontak yang tidak dapat dikaitkan karena kesalahan
- Lokasi (URI Amazon S3 dan URL Konsol Amazon S3) dari file CSV yang berisi nomor telepon dan pasangan alur kontak yang tidak terkait karena keterbatasan waktu
- `DescribeCloudFormationErrorFromStackEvents.Acara`

Output yang menunjukkan peristiwa AWS CloudFormation tumpukan jika `AssociatePhoneNumbersToContactFlows` langkah gagal.

Output eksekusi dengan sejumlah kecil nomor telepon dan arus kontak

```

▼ Outputs
DescribeCloudFormationErrorFromStackEvents.Events
No output available yet because the step is not successfully executed
GenerateReport.OutputPayload
{"Payload": "
-----
Amazon Connect Phone Number Mapping Result
-----
* Phone number and Contact Flow pairs listed in the provided input: 7
* Phone numbers associated with Contact Flow processed: 7
* Phone numbers that could not be associated with Contact Flow due to an error: 0
* Phone numbers that weren't associated with Contact Flow due to the time constraint: 0
"}

```

Output eksekusi dengan sejumlah besar nomor telepon dan alur kontak dan nomor telepon yang tidak terkait karena kesalahan atau kendala waktu

```

▼ Outputs

DescribeCloudFormationErrorFromStackEvents.Events
No output available yet because the step is not successfully executed

GenerateReport.OutputPayload
{"Payload": "
=====
Amazon Connect Phone Number Mapping Result
=====
* Phone number and Contact Flow pairs listed in the provided input: 1634
* Phone numbers associated with Contact Flow processed: 1153
* Phone numbers that could not be associated with Contact Flow due to an error: 8
* Phone numbers that weren't associated with Contact Flow due to the time constraint: 473

=====
Error list file location
=====
* S3 URI: s3://[REDACTED]/ErrorResourceList.csv
* S3 Console URL: https://s3.console.aws.amazon.com/s3/object/[REDACTED]/ErrorResourceList.csv
INFO: The above file contains the list of phone numbers and Contact Flows that could not be associated due to an error.You can look into the error detail in order to address the issue.

=====
Unprocessed list file location
=====
* S3 URI: s3://[REDACTED]/NonProcessedResourceList.csv
* S3 Console URL: https://s3.console.aws.amazon.com/s3/object/[REDACTED]/NonProcessedResourceList.csv
INFO: The above file contains the list of phone numbers and Contact Flows that weren't associated due to the time constraint (15 minutes).You can execute this runbook again by specifying the file as an input \"SourceFileLocation\" so that you can process them.

"}

```

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

## AWS Directory Service

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS Directory Service Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-CreateDSManagementInstance](#)
- [AWSSupport-TroubleshootADConnectorConnectivity](#)
- [AWSSupport-TroubleshootDirectoryTrust](#)

## AWS-CreateDSManagementInstance

### Deskripsi

AWS-CreateDSManagementInstanceRunbook membuat instans Windows Amazon Elastic Compute Cloud (Amazon EC2) yang dapat Anda gunakan untuk mengelola direktori Anda. AWS



Directory Service Instance manajemen tidak dapat digunakan untuk mengelola direktori AD Connector.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- AMIID

Jenis: String

Default: `{{ ssm:/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-Base }}`

Deskripsi: (Diperlukan) ID dari Amazon Machine Image (AMI) yang ingin Anda gunakan untuk meluncurkan instance manajemen.

- DirectoryId

Jenis: String

Deskripsi: (Diperlukan) ID AWS Directory Service direktori yang ingin Anda kelola. Instance bergabung ke direktori yang Anda tentukan.

- **iamInstanceProfileName**

Jenis: String

Deskripsi: (Diperlukan) Nama yang Anda tentukan diterapkan ke profil instans IAM yang dibuat oleh otomatisasi dan dilampirkan ke instance manajemen.

- **InstanceType**

Jenis: String

Bawaan: t3.medium

Nilai yang diizinkan:

- t2.nano
- t2.mikro
- t2.small
- t2.medium
- t2.besar
- t2.xbesar
- t2.2xbesar
- t3.nano
- t3.mikro
- t3.kecil
- t3.sedang
- t3.large
- t3.xbesar
- t3.2xbesar

Deskripsi: (Diperlukan) Jenis instans yang ingin Anda luncurkan.

- **KeyPairName**

Jenis: String

Deskripsi: (Opsional) Pasangan kunci yang akan digunakan saat membuat instance. Jika Anda tidak menentukan nilai, tidak ada pasangan kunci yang terkait dengan instance.

- **RemoteAccessCidr**

Jenis: String

Deskripsi: (Diperlukan) Blok CIDR yang ingin Anda izinkan lalu lintas RDP (port 3389). Blok CIDR yang Anda tentukan diterapkan ke aturan masuk yang ditambahkan ke grup keamanan yang dibuat oleh otomatisasi.

- SecurityGroupName

Jenis: String

Deskripsi: (Diperlukan) Nama yang Anda tentukan diterapkan ke grup keamanan yang dibuat oleh otomatisasi dan terkait dengan instance manajemen.

- Tanda

Jenis: MapList

Deskripsi: (Opsional) Pasangan kunci-nilai yang ingin Anda terapkan ke sumber daya yang dibuat oleh otomatisasi.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- ds:DescribeDirectories
- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateSecurityGroup
- ec2:CreateTags
- ec2>DeleteSecurityGroup
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeKeyPairs
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:RunInstances
- ec2:TerminateInstances

- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam>DeleteInstanceProfile
- iam>DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam>ListAttachedRolePolicies
- iam>ListInstanceProfiles
- iam>ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm>DeleteDocument
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetParameters
- ssm>ListCommandInvocations
- ssm>ListCommands
- ssm>ListDocuments
- ssm:SendCommand
- ssm:StartAutomationExecution

## Langkah Dokumen

- aws:executeAwsApi- Mengumpulkan rincian tentang direktori yang Anda tentukan dalam DirectoryId parameter.

- `aws:executeAwsApi`- Mendapat blok CIDR dari cloud pribadi virtual (VPC) tempat direktori diluncurkan.
- `aws:executeAwsApi`- Membuat grup keamanan menggunakan nilai yang Anda tentukan dalam `SecurityGroupName` parameter.
- `aws:executeAwsApi`- Membuat aturan masuk untuk grup keamanan yang baru dibuat yang memungkinkan lalu lintas RDP dari CIDR yang Anda tentukan dalam parameter `RemoteAccessCidr`.
- `aws:executeAwsApi`- Membuat peran IAM dan profil contoh menggunakan nilai yang Anda tentukan dalam `IamInstanceProfileName` parameter.
- `aws:executeAwsApi`- Meluncurkan instans Amazon EC2 berdasarkan nilai yang Anda tentukan dalam parameter runbook.
- `aws:executeAwsApi`- Membuat AWS Systems Manager dokumen untuk bergabung dengan instance yang baru diluncurkan ke direktori Anda.
- `aws:runCommand`- Bergabung dengan contoh baru ke direktori Anda.
- `aws:runCommand`- Menginstal alat administrasi server jarak jauh pada contoh baru.

## **AWSsupport-TroubleshootADConnectorConnectivity**

### Deskripsi

`AWSsupport-TroubleshootADConnectorConnectivityRunbook` memverifikasi prasyarat berikut untuk Konektor AD:

- Memeriksa apakah lalu lintas yang diperlukan diizinkan oleh grup keamanan dan aturan daftar kontrol akses jaringan (ACL) yang terkait dengan Konektor AD Anda.
- Memeriksa apakah AWS Systems Manager, AWS Security Token Service, dan titik akhir VPC CloudWatch antarmuka Amazon ada di cloud pribadi virtual (VPC) yang sama dengan Konektor AD.

Ketika pemeriksaan prasyarat berhasil diselesaikan, runbook meluncurkan dua instans t2.micro Linux Amazon Elastic Compute Cloud (Amazon EC2) dalam subnet yang sama dengan Konektor AD Anda. Tes konektivitas jaringan kemudian dilakukan dengan menggunakan `netcat` dan `nslookup` utilitas.

[Jalankan Otomasi ini \(konsol\)](#)

**⚠ Important**

Menggunakan runbook ini mungkin dikenakan biaya tambahan untuk instans Amazon EC2, volume Amazon Elastic Block Store, dan Amazon Machine Image (AMI) yang dibuat Akun AWS selama otomatisasi. Untuk informasi selengkapnya, lihat Harga [Amazon Elastic Compute Cloud](#) dan Harga [Amazon Elastic Block Store](#).

Jika `aws:deletestack` langkah gagal, buka AWS CloudFormation konsol untuk menghapus tumpukan secara manual. Nama tumpukan yang dibuat oleh runbook ini dimulai dengan `AWSsupport-TroubleshootADConnectorConnectivity`. Untuk informasi tentang menghapus AWS CloudFormation tumpukan, lihat [Menghapus tumpukan di Panduan Pengguna](#). AWS CloudFormation

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `DirectoryId`

Jenis: String

Deskripsi: (Diperlukan) ID direktori Konektor AD yang ingin Anda pecahkan masalah konektivitas.

- `Ec2 InstanceProfile`

Jenis: String

Karakter maksimum: 128

Deskripsi: (Diperlukan) Nama profil instans yang ingin Anda tetapkan ke instans yang diluncurkan untuk melakukan pengujian konektivitas. Profil instans yang Anda tentukan harus memiliki AmazonSSMManagedInstanceCore kebijakan atau izin yang setara.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- ec2:DescribeInstances
- ec2:DescribeImages
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls
- ec2:DescribeVpcEndpoints
- ec2:CreateTags
- ec2:RunInstances
- ec2:StopInstances
- ec2:TerminateInstances
- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation:ListStackResources
- cloudformation>DeleteStack
- ds:DescribeDirectories
- ssm:SendCommand
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:GetParameters
- ssm:DescribeInstanceInformation

- `iam:PassRole`

## Langkah Dokumen

- `aws:assertAwsResourceProperty`- Mengkonfirmasi direktori yang ditentukan dalam `DirectoryId` parameter adalah Konektor AD.
- `aws:executeAwsApi`- Mengumpulkan informasi tentang Konektor AD.
- `aws:executeAwsApi`- Mengumpulkan informasi tentang grup keamanan yang terkait dengan Konektor AD.
- `aws:executeAwsApi`- Mengumpulkan informasi tentang aturan ACL jaringan yang terkait dengan subnet untuk Konektor AD.
- `aws:executeScript`- Mengevaluasi aturan grup keamanan Konektor AD untuk memverifikasi bahwa lalu lintas keluar yang diperlukan diperbolehkan.
- `aws:executeScript`- Mengevaluasi aturan ACL jaringan AD Connector untuk memverifikasi bahwa lalu lintas jaringan keluar dan masuk yang diperlukan diperbolehkan.
- `aws:executeScript`- Memeriksa apakah AWS Systems Manager, AWS Security Token Service dan titik akhir CloudWatch antarmuka Amazon ada di VPC yang sama dengan Konektor AD.
- `aws:executeScript`- Mengkompilasi output dari pemeriksaan yang dilakukan pada langkah sebelumnya.
- `aws:branch`- Cabang otomatisasi tergantung pada output dari langkah-langkah sebelumnya. Otomatisasi berhenti di sini jika aturan keluar dan masuk yang diperlukan hilang untuk grup keamanan dan ACL jaringan.
- `aws:createStack`- Membuat AWS CloudFormation tumpukan untuk meluncurkan instans Amazon EC2 untuk melakukan pengujian konektivitas.
- `aws:executeAwsApi`- Mengumpulkan ID instans Amazon EC2 yang baru diluncurkan.
- `aws:waitForAwsResourceProperty`- Menunggu instans Amazon EC2 pertama yang baru diluncurkan untuk dilaporkan sebagaimana dikelola oleh AWS Systems Manager
- `aws:waitForAwsResourceProperty`- Menunggu instans Amazon EC2 kedua yang baru diluncurkan untuk dilaporkan sebagaimana dikelola oleh AWS Systems Manager
- `aws:runCommand`- Melakukan pengujian konektivitas jaringan ke alamat IP server DNS lokal dari instans Amazon EC2 pertama.
- `aws:runCommand`- Melakukan pengujian konektivitas jaringan ke alamat IP server DNS lokal dari instans Amazon EC2 kedua.



- `aws:changeInstanceState`- Menghentikan instans Amazon EC2 yang digunakan untuk pengujian konektivitas.
- `aws:deleteStack`- Menghapus AWS CloudFormation tumpukan.
- `aws:executeScript`- Mengeluarkan instruksi tentang cara menghapus AWS CloudFormation tumpukan secara manual jika otomatisasi gagal menghapus tumpukan.

## **AWSsupport-TroubleshootDirectoryTrust**

### Deskripsi

AWSsupport-TroubleshootDirectoryTrustRunbook mendiagnosis masalah pembuatan kepercayaan antara AWS Managed Microsoft AD dan Microsoft Active Directory. Otomatisasi memastikan jenis direktori mendukung kepercayaan, dan kemudian memeriksa aturan grup keamanan terkait, daftar kontrol akses jaringan (ACL jaringan), dan tabel rute untuk potensi masalah konektivitas.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DirectoryId

Jenis: String

Pola yang diizinkan: `^d-[a-z0-9]{10}$`

Deskripsi: (Diperlukan) ID AWS Managed Microsoft AD untuk memecahkan masalah.

- RemoteDomainCidrs

Jenis: StringList

Pola yang diizinkan: `^((([0-9] | [1-9] [0-9] | 1 [0-9] {2} | 2 [0-4] [0-9] | 25 [0-5])\.) {3} ([0-9] | [1-9] [0-9] | 1 [0-9] {2} | 2 [0-4] [0-9] | 25 [0-5]) (v(3 [0-2] | [1-2] [0-9] | [1-9])) $`

Deskripsi: (Diperlukan) CIDR dari domain jarak jauh yang Anda coba buat hubungan kepercayaan. Anda dapat menambahkan beberapa CIDR menggunakan nilai yang dipisahkan koma. Misalnya, 172.31.48.0/20, 192.168.1.10/32.

- RemoteDomainName

Jenis: String

Deskripsi: (Diperlukan) Nama domain yang memenuhi syarat sepenuhnya dari domain jarak jauh tempat Anda menjalin hubungan kepercayaan.

- RequiredTrafficACL

Jenis: String

Deskripsi: (Diperlukan) Persyaratan port default untuk AWS Managed Microsoft AD. Dalam kebanyakan kasus, Anda tidak boleh mengubah nilai default.

Default: `{"masuk": {"tcp": [[53,53], [88,88], [135,135], [389,389], [445,445], [464,464], [636,636], [1024,65535]], "udp": [[53,53], [88,88], [123,123], [138,138], [389,389], [445,445], [464,464]], "icmp": [[-1, -1]]}, "outbound": {"-1": [[0,65535]]}}`

- RequiredTrafficSG

Jenis: String

Deskripsi: (Diperlukan) Persyaratan port default untuk AWS Managed Microsoft AD. Dalam kebanyakan kasus, Anda tidak boleh mengubah nilai default.

```
Default: {"masuk": {"tcp": [[53,53], [88,88], [135,135], [389,389], [445,445], [464,464], [636,636], [1024,65535]], "udp": [[53,53], [88,88], [123,123], [138,138], [389,389], [445,445], [464,464]], "icmp": [[-1, -1]]}, "outbound": {" -1": [[0,65535]]}}
```

- TrustId

Jenis: String

Deskripsi: (Opsional) ID hubungan kepercayaan untuk memecahkan masalah.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- ds:DescribeConditionalForwarders
- ds:DescribeDirectories
- ds:DescribeTrusts
- ds:ListIpRoutes
- ec2:DescribeNetworkAcls
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets

### Langkah Dokumen

- aws:assertAwsResourceProperty- Mengkonfirmasi jenis direktori adalahAWS Managed Microsoft AD.
- aws:executeAwsApi- Mendapat informasi tentangAWS Managed Microsoft AD.
- aws:branch- Otomatisasi cabang jika nilai disediakan untuk parameter TrustId input.
- aws:executeAwsApi- Mendapat informasi tentang hubungan kepercayaan.
- aws:executeAwsApi- Mendapat forwarder bersyarat alamat DNS IP untuk. RemoteDomainName
- aws:executeAwsApi- Mendapat informasi tentang rute IP yang telah ditambahkan keAWS Managed Microsoft AD.
- aws:executeAwsApi- Mendapat CIDR dari subnet. AWS Managed Microsoft AD

- `aws:executeAwsApi`- Mendapat informasi tentang kelompok keamanan yang terkait dengan AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Mendapat informasi tentang ACL jaringan yang terkait dengan AWS Managed Microsoft AD
- `aws:executeScript`- Mengkonfirmasi `RemoteDomainCidrs` adalah nilai yang valid. Menegaskan bahwa AWS Managed Microsoft AD memiliki forwarder bersyarat untuk `RemoteDomainCidrs`, dan bahwa rute IP yang diperlukan telah ditambahkan ke AWS Managed Microsoft AD jika `RemoteDomainCidrs` adalah non-RFC 1918 alamat IP.
- `aws:executeScript`- Mengevaluasi aturan kelompok keamanan.
- `aws:executeScript`- Mengevaluasi ACL jaringan.

## Keluaran

`evalDirectorySecurityGroup.output` - Hasil dari mengevaluasi apakah aturan kelompok keamanan yang terkait dengan AWS Managed Microsoft AD memungkinkan lalu lintas yang diperlukan untuk penciptaan kepercayaan.

`evalAclEntries.output` - Hasil dari mengevaluasi apakah ACL jaringan terkait dengan AWS Managed Microsoft AD memungkinkan lalu lintas yang diperlukan untuk penciptaan kepercayaan.

`evaluateRemoteDomainCIDR.output` - Hasil dari mengevaluasi apakah adalah nilai yang valid. `RemoteDomainCidrs` Menegaskan bahwa AWS Managed Microsoft AD memiliki forwarder bersyarat untuk `RemoteDomainCidrs`, dan bahwa rute IP yang diperlukan telah ditambahkan ke AWS Managed Microsoft AD jika `RemoteDomainCidrs` adalah non-RFC 1918 alamat IP.

## AWS AppSync

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS AppSync Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-EnableAppSyncGraphQLApiLogging](#)

## AWS-EnableAppSyncGraphQLApiLogging

### Deskripsi

AWS-EnableAppSyncGraphQLApiLoggingRunbook memungkinkan pencatatan tingkat bidang dan pencatatan tingkat permintaan untuk GraphQL API yang Anda tentukan. AWS AppSync Runbook akan menerapkan perubahan pada GraphQL API yang ditentukan meskipun logging telah diaktifkan.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Apild

Jenis: String

Deskripsi: (Wajib) ID API yang ingin Anda aktifkan untuk logging.

- FieldLogLevel

Jenis: String

Nilai Valid: ERROR | SEMUA

Deskripsi: (Wajib) Tingkat logging bidang.

- CloudWatchLogsRoleArn

Jenis: String

Deskripsi: (Wajib) ARN dari peran layanan yang AWS AppSync diasumsikan untuk dipublikasikan ke Amazon Logs. CloudWatch

- ExcludeVerboseContent

Jenis: Boolean

Default: Salah

Deskripsi: (Opsional) Setel `True` untuk mengecualikan informasi seperti header, konteks, dan templat pemetaan yang dievaluasi, terlepas dari tingkat pencatatan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `appsync:GetGraphQLApi`
- `appsync:UpdateGraphQLApi`
- `iam:PassRole`

Langkah Dokumen

- `aws:executeAwsApi` - Mengumpulkan jenis otentikasi dan informasi konfigurasi yang relevan untuk jenis otentikasi utama.
- `aws:branch` - Cabang berdasarkan jenis otentikasi.
- `aws:executeAwsApi` - Memperbarui konfigurasi logging untuk AWS AppSync GraphQL API berdasarkan nilai yang ditentukan untuk parameter input runbook.

Keluaran

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Tanggapan dari `UpdateGraphQLApi` panggilan.

- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Tanggapan dari `UpdateGraphQLApi` panggilan.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Tanggapan dari `UpdateGraphQLApi` panggilan.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Tanggapan dari `UpdateGraphQLApi` panggilan.

## Amazon Athena

AWS Systems Manager Otomasi menyediakan runbook standar untuk Amazon Athena. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWS-EnableAthenaWorkGroupEncryptionAtRest](#)

## AWS-EnableAthenaWorkGroupEncryptionAtRest

Deskripsi

`AWS-EnableAthenaWorkGroupEncryptionAtRestRunbook` memungkinkan enkripsi saat istirahat untuk workgroup Amazon Athena yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- WorkGroup

Jenis: String

Deskripsi: (Wajib) Kelompok kerja yang ingin Anda aktifkan enkripsi saat istirahat.

- EncryptionOption

Jenis: String

Nilai Valid: SSE\_S3 | SSE\_KMS | CSE\_KMS

Deskripsi: (Wajib) Menentukan pilihan enkripsi yang digunakan. Anda dapat memilih enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE\_S3), enkripsi sisi server dengan kunci terkelola (SSE\_KMS), atau enkripsi sisi klien dengan kunci AWS KMS terkelola (CSE\_KMS). AWS KMS

- KmsKeyId

Jenis: String

Deskripsi: (Opsional) Jika Anda menggunakan opsi AWS KMS enkripsi, tentukan kunci ARN, ID kunci, atau alias kunci kunci yang ingin Anda gunakan.

- EnableMinimumEncryptionConfiguration

Jenis: Boolean

Bawaan: BETUL

Deskripsi: (Opsional) Menerapkan tingkat enkripsi minimal untuk workgroup untuk hasil kueri dan perhitungan yang ditulis ke Amazon S3. Saat diaktifkan, pengguna workgroup hanya dapat menyetel enkripsi ke tingkat minimum yang ditetapkan oleh administrator atau yang lebih tinggi saat mereka mengirimkan kueri. Pengaturan ini tidak berlaku untuk grup kerja berkemampuan SPARK.

- EnforceWorkGroupConfiguration



Jenis: Boolean

Bawaan: BETUL

Deskripsi: (Opsional) Jika disetel ke `True`, pengaturan untuk grup kerja akan menimpa setelan sisi klien. Jika disetel ke `False`, pengaturan sisi klien digunakan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `athena:GetWorkGroup`
- `athena:UpdateWorkGroup`

Langkah Dokumen

- `aws:branch` - Cabang berdasarkan opsi enkripsi yang ditentukan dalam parameter. `EncryptionOption`
- `aws:executeAwsApi` - Langkah ini memperbarui Grup Kerja Athena dengan pengaturan enkripsi yang ditentukan.
- `aws:executeAwsApi` - Memperbarui Grup Kerja Athena dengan pengaturan enkripsi yang ditentukan.
- `aws:assertAwsResourceProperty` - Memverifikasi bahwa enkripsi untuk workgroup telah diaktifkan.

## DynamoDB

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon DynamoDB. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWS-ChangeDDBRWCapacityMode](#)

- [AWS-CreateDynamoDBBackup](#)
- [AWS-DeleteDynamoDbBackup](#)
- [AWSConfigRemediation-DeleteDynamoDbTable](#)
- [AWS-DeleteDynamoDbTableBackups](#)
- [AWSConfigRemediation-EnableEncryptionOnDynamoDbTable](#)
- [AWSConfigRemediation-EnablePITRForDynamoDbTable](#)
- [AWS-EnableDynamoDbAutoscaling](#)
- [AWS-RestoreDynamoDBTable](#)

## AWS - ChangeDDBRWCapacityMode

### Deskripsi

AWS - ChangeDDBRWCapacityModeRunbook mengubah mode kapasitas baca/tulis untuk satu atau beberapa tabel Amazon DynamoDB (DynamoDB) ke mode sesuai permintaan, atau mode yang disediakan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis data

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan

tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- CapacityMode

Jenis: String

Nilai yang valid: DISEDIAKAN | PAY\_PER\_REQUEST

Deskripsi: (Diperlukan) Mode kapasitas baca/tulis yang diinginkan. Saat beralih dari on-demand (pay-per-request) ke kapasitas yang disediakan, nilai kapasitas awal yang disediakan harus ditetapkan. Nilai kapasitas awal yang disediakan diperkirakan berdasarkan kapasitas baca dan tulis yang dikonsumsi dari tabel Anda dan indeks sekunder global selama 30 menit terakhir.

- ReadCapacityUnits

Jenis: Integer

Default: 0

Deskripsi: (Opsional) Jumlah maksimum pembacaan yang sangat konsisten yang dikonsumsi per detik sebelum DynamoDB mengembalikan pengecualian pelambatan.

- TableNames

Jenis: String

Deskripsi: (Wajib) Daftar nama tabel DynamoDB yang dipisahkan koma untuk mengubah mode kapasitas baca/tulis untuk..

- WriteCapacityUnits

Jenis: Integer

Default: 0

Deskripsi: (Opsional) Jumlah maksimum penulisan yang dikonsumsi per detik sebelum DynamoDB mengembalikan pengecualian pelambatan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `dynamodb:DescribeTable`
- `dynamodb:UpdateTable`

### Langkah Dokumen

- `aws:executeScript`- Mengubah mode kapasitas baca/tulis untuk tabel DynamoDB yang ditentukan dalam parameter. `TableNames`

### Keluaran

`DiubahDBRWCapacityMode.SuccessesTables` - Daftar nama tabel DynamoDB di mana mode kapasitas berhasil diubah

`DiubahDBRWCapacityMode.FailedTables` - Maplist nama tabel DynamoDB di mana mengubah mode kapasitas gagal dan alasan kegagalan.

## AWS-CreateDynamoDBBackup

### Deskripsi

Buat cadangan tabel Amazon DynamoDB.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Basis data

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- BackupName

Jenis: String

Deskripsi: (Diperlukan) Nama cadangan untuk membuat.

- LambdaAssumeRole

Jenis: String

Deskripsi: (Opsional) ARN peran yang memungkinkan Lambda dibuat oleh Automation untuk melakukan tindakan atas nama Anda. Jika tidak ditentukan peran sementara akan dibuat untuk menjalankan fungsi Lambda.

- TableName

Jenis: String

Deskripsi: (Diperlukan) Nama tabel DynamoDB.

## AWS-DeleteDynamoDbBackup

Deskripsi

Hapus cadangan tabel Amazon DynamoDB.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis data

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- BackupArn

Jenis: String

Deskripsi: (Diperlukan) ARN cadangan tabel DynamoDB untuk dihapus.

## **AWSConfigRemediation-DeleteDynamoDbTable**

### Deskripsi

AWSConfigRemediation-DeleteDynamoDbTableRunbook menghapus tabel Amazon DynamoDB (DynamoDB) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis data

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- TableName

Jenis: String

Deskripsi: (Diperlukan) Nama tabel DynamoDB yang ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- dynamodb>DeleteTable
- dynamodb:DescribeTable

Langkah Dokumen

- aws:executeScript- Menghapus tabel DynamoDB yang ditentukan dalam parameter. TableName
- aws:executeScript- Memverifikasi tabel DynamoDB telah dihapus.

## AWS-DeleteDynamoDbTableBackups

Deskripsi

Hapus cadangan tabel DynamoDB berdasarkan hari retensi atau hitungan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

## Amazon

### Platform

### Basis data

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LambdaAssumeRole

Jenis: String

Deskripsi: (Opsional) ARN peran yang memungkinkan Lambda dibuat oleh Automation untuk melakukan tindakan atas nama Anda. Jika tidak ditentukan peran sementara akan dibuat untuk menjalankan fungsi Lambda.

- RetentionCount

Jenis: String

Default: 10

Deskripsi: (Opsional) Jumlah backup untuk mempertahankan untuk tabel. Jika ada lebih dari jumlah cadangan yang ditentukan, cadangan tertua di luar nomor itu akan dihapus. Entah RetentionCount atau RetentionDays bisa digunakan, bukan keduanya.

- RetentionDays

Jenis: String

Deskripsi: (Opsional) Jumlah hari untuk menyimpan cadangan untuk tabel. Backup yang lebih lama dari jumlah hari yang ditentukan akan dihapus. Entah RetentionCount atau RetentionDays bisa digunakan, bukan keduanya.

- TableName



Jenis: String

Deskripsi: (Diperlukan) Nama tabel DynamoDB.

## **AWSConfigRemediation-EnableEncryptionOnDynamoDbTable**

Deskripsi

AWSConfigRemediation-EnableEncryptionOnDynamoDbTableRunbook mengenkripsi tabel Amazon DynamoDB (DynamoDB) menggunakan () kunci terkelola pelanggan yang Anda tentukan untuk AWS Key Management Service parameter.AWS KMSKMSKeyId

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- KMS KeyId

Jenis: String

Deskripsi: (Wajib) ARN dari kunci terkelola pelanggan yang ingin Anda gunakan untuk mengenkripsi tabel DynamoDB yang Anda tentukan dalam parameter. TableName

- **TableName**

Jenis: String

Deskripsi: (Wajib) Nama tabel DynamoDB yang ingin Anda enkripsi.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `dynamodb:DescribeTable`
- `dynamodb:UpdateTable`

Langkah Dokumen

- `aws:executeAwsApi`- Mengenkripsi tabel DynamoDB yang Anda tentukan dalam parameter. `TableName`
- `aws:waitForAwsResourceProperty`- Memverifikasi `Enabled` properti untuk tabel `SSESpecification` DynamoDB diatur ke `true`
- `aws:assertAwsResourceProperty`- Memverifikasi tabel DynamoDB dienkripsi dengan kunci dikelola pelanggan yang ditentukan dalam parameter. `KMSKeyId`

## **AWSConfigRemediation-EnablePITRForDynamoDbTable**

Deskripsi

`AWSConfigRemediation-EnablePITRForDynamoDbTableRunbook` memungkinkan point-in-time pemulihan (PITR) pada tabel Amazon DynamoDB yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

## Pemilik

Amazon

Platform

Basis data

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- `TableName`

Jenis: String

Deskripsi: (Diperlukan) Nama tabel DynamoDB untuk mengaktifkan point-in-time pemulihan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `dynamodb:DescribeContinuousBackups`
- `dynamodb:UpdateContinuousBackups`

Langkah Dokumen

- `aws:executeAwsApi`- Memungkinkan point-in-time pemulihan pada tabel DynamoDB yang Anda tentukan dalam parameter. `TableName`
- `aws:assertAwsResourceProperty`- Mengkonfirmasi point-in-time pemulihan diaktifkan pada tabel DynamoDB.

# AWS-EnableDynamoDbAutoscaling

## Deskripsi

AWS-EnableDynamoDbAutoscalingRunbook mengaktifkan Application Auto Scaling untuk tabel Amazon DynamoDB kapasitas yang disediakan yang Anda tentukan. Application Auto Scaling secara dinamis menyesuaikan kapasitas throughput yang disediakan sebagai respons terhadap pola lalu lintas. Untuk informasi selengkapnya, lihat [Mengelola kapasitas throughput secara otomatis dengan penskalaan otomatis DynamoDB di Panduan Pengembang Amazon DynamoDB](#).

## Jenis dokumen

## Otomatisasi

## Pemilik

## Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- TableName

Jenis: String

Deskripsi: (Wajib) Nama tabel DynamoDB yang ingin Anda aktifkan Application Auto Scaling.

- MinReadCapacity

Jenis: Integer

Deskripsi: (Wajib) Jumlah minimum unit kapasitas baca throughput yang disediakan untuk tabel DynamoDB.

- MaxReadCapacity

Jenis: Integer

Deskripsi: (Wajib) Jumlah maksimum unit kapasitas baca throughput yang disediakan untuk tabel DynamoDB.

- TargetReadCapacityUtilization

Jenis: Integer

Deskripsi: (Wajib) Pemanfaatan kapasitas baca target yang diinginkan. Pemanfaatan target adalah persentase throughput yang disediakan yang dikonsumsi pada suatu titik waktu. Anda dapat mengatur nilai pemanfaatan target penskalaan otomatis antara 20 dan 90 persen.

- ReadScaleOutCooldown

Jenis: Integer

Deskripsi: (Wajib) Jumlah waktu dalam hitungan detik untuk menunggu aktivitas penskalaan kapasitas baca sebelumnya diterapkan.

- ReadScaleInCooldown

Jenis: Integer

Deskripsi: (Wajib) Jumlah waktu dalam detik setelah aktivitas penskalaan kapasitas baca selesai sebelum aktivitas penskalaan lainnya dapat dimulai.

- MinWriteCapacity

Jenis: Integer

Deskripsi: (Wajib) Jumlah minimum unit penulisan throughput yang disediakan untuk tabel DynamoDB.

- MaxWriteCapacity

Jenis: Integer

Deskripsi: (Wajib) Jumlah maksimum unit penulisan throughput yang disediakan untuk tabel DynamoDB.

- `TargetWriteCapacityUtilization`

Jenis: Integer

Deskripsi: (Wajib) Pemanfaatan kapasitas tulis target yang diinginkan. Pemanfaatan target adalah persentase throughput yang disediakan yang dikonsumsi pada suatu titik waktu. Anda dapat mengatur nilai pemanfaatan target penskalaan otomatis antara 20 dan 90 persen.

- `WriteScaleOutCooldown`

Jenis: Integer

Deskripsi: (Wajib) Jumlah waktu dalam hitungan detik untuk menunggu aktivitas penskalaan kapasitas tulis sebelumnya diterapkan.

- `WriteScaleInCooldown`

Jenis: Integer

Deskripsi: (Wajib) Jumlah waktu dalam detik setelah aktivitas penskalaan kapasitas tulis selesai sebelum aktivitas penskalaan lainnya dapat dimulai.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `application-autoscaling:DescribeScalableTargets`
- `application-autoscaling:DescribeScalingPolicies`
- `application-autoscaling:PutScalingPolicy`
- `application-autoscaling:RegisterScalableTarget`
- `RegisterAppAutoscalingTargetWrite` (`aws:executeAwsApi`) - Mengonfigurasi Application Auto Scaling pada tabel DynamoDB yang Anda tentukan.
- `RegisterAppAutoscalingTargetWriteDelay` (`aws:sleep`) - Tidur untuk menghindari pelambatan API.
- `PutScalingPolicyWrite` (`aws:executeAwsApi`) - Mengkonfigurasi pemanfaatan kapasitas tulis target untuk tabel DynamoDB.

- `PutScalingPolicyWriteDelay` (`aws:sleep`) - Tidur untuk menghindari pelambatan API.
- `RegisterAppAutoscalingTargetRead` (`aws:executeAwsApi`) - Mengkonfigurasi unit kapasitas baca minimum dan maksimum untuk tabel DynamoDB.
- `RegisterAppAutoscalingTargetReadDelay` (`aws:sleep`) - Tidur untuk menghindari pelambatan API.
- `PutScalingPolicyRead` (`aws:executeAwsApi`) - Mengkonfigurasi pemanfaatan kapasitas baca target untuk tabel DynamoDB.
- `VerifyDynamoDbAutoscalingEnabled` (`AWS:ExecuteScript`) - Verifies Application Auto Scaling diaktifkan untuk tabel DynamoDB sesuai dengan nilai yang Anda tentukan.

## Keluaran

- `RegisterAppAutoscalingTargetWrite.Respon`
- `PutScalingPolicyWrite.Respon`
- `RegisterAppAutoscalingTargetRead.Respon`
- `PutScalingPolicyRead.Respon`
- `VerifyDynamoDbAutoscalingEnabled.DynamoDbAutoscalingEnabledResponse`

## AWS-RestoreDynamoDBTable

### Deskripsi

`AWS-RestoreDynamoDBTableRunbook` mengembalikan tabel Amazon DynamoDB yang Anda tentukan menggunakan point-in-time recovery (PITR).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis data

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- EnablePointInTimeRecoverAsNeeded

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Menentukan apakah otomatisasi mengaktifkan point-in-time pemulihan sesuai kebutuhan untuk memulihkan tabel.

- GlobalSecondaryIndexOverride

Jenis: String

Deskripsi: (Opsional) Indeks sekunder global baru untuk menggantikan indeks sekunder yang ada untuk tabel baru.

- LocalSecondaryIndexOverride

Jenis: String

Deskripsi: (Opsional) Indeks sekunder lokal baru untuk menggantikan indeks sekunder yang ada untuk tabel baru.

- RestoreDateTime

Jenis: String

Deskripsi: (Diperlukan) point-in-time Pemulihan yang ingin Anda pulihkan meja Anda selama 35 hari terakhir. Tentukan tanggal dan waktu menggunakan format berikut: DD/MM/YYYY HH:MM:SS

- SourceTableArn

Jenis: String

Deskripsi: (Diperlukan) ARN tabel yang ingin Anda pulihkan.

- SseSpecificationOverride



Jenis: String

Deskripsi: (Opsional) Pengaturan enkripsi sisi server yang digunakan untuk tabel baru.

- TargetTableName

Jenis: String

Keterangan: (Diperlukan) Nama tabel untuk mengembalikan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- dynamodb:BatchWriteItem
- dynamodb>DeleteItem
- dynamodb:DescribeTable
- dynamodb:GetItem
- dynamodb:PutItem
- dynamodb:Query
- dynamodb:RestoreTableToPointInTime
- dynamodb:Scan
- dynamodb:UpdateItem

Langkah Dokumen

- `aws:executeScript`- Mengembalikan tabel DynamoDB yang Anda tentukan dalam TargetTableName parameter menggunakan pemulihan. point-in-time

## Amazon EBS

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Elastic Block Store. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWSSupport-AnalyzeEBSResourceUsage](#)
- [AWS-ArchiveEBSSnapshots](#)
- [AWS-AttachEBSVolume](#)
- [AWSSupport-CalculateEBSPerformanceMetrics](#)
- [AWS-CopySnapshot](#)
- [AWS-CreateSnapshot](#)
- [AWS-DeleteSnapshot](#)
- [AWSConfigRemediation-DeleteUnusedEBSVolume](#)
- [AWS-DeregisterAMIs](#)
- [AWS-DetachEBSVolume](#)
- [AWSConfigRemediation-EnableEbsEncryptionByDefault](#)
- [AWS-ExtendEbsVolume](#)
- [AWSSupport-ModifyEBSSnapshotPermission](#)
- [AWSConfigRemediation-ModifyEBSVolumeType](#)

## AWSSupport - AnalyzeEBSResourceUsage

### Deskripsi

Runbook `AWSSupport-AnalyzeEBSResourceUsage` otomatisasi digunakan untuk menganalisis penggunaan sumber daya di Amazon Elastic Block Store (Amazon EBS). Ini menganalisis penggunaan volume dan mengidentifikasi volume, gambar, dan snapshot yang ditinggalkan di Wilayah tertentu. AWS

### Bagaimana cara kerjanya?

Runbook melakukan empat tugas berikut:

1. Memverifikasi bahwa bucket Amazon Simple Storage Service (Amazon S3) ada, atau membuat bucket Amazon S3 baru.
2. Mengumpulkan semua volume Amazon EBS dalam keadaan tersedia.
3. Mengumpulkan semua snapshot Amazon EBS yang volume sumbernya telah dihapus.
4. Mengumpulkan semua Amazon Machine Images (AMI) yang tidak digunakan oleh instans Amazon Elastic Compute Cloud (Amazon EC2) yang tidak dihentikan.

Runbook menghasilkan laporan CSV dan menyimpannya di bucket Amazon S3 yang disediakan pengguna. Bucket yang disediakan harus diamankan mengikuti praktik terbaik AWS keamanan seperti yang diuraikan pada akhirnya. Jika bucket Amazon S3 yang disediakan pengguna tidak ada di akun, runbook akan membuat bucket Amazon S3 baru dengan format nama, dienkripsi dengan kunci kustom AWS Key Management Service (AWS KMS) <User-provided-name>-awssupport-YYYY-MM-DD, dengan versi objek diaktifkan, akses publik yang diblokir, dan memerlukan permintaan untuk menggunakan SSL/TLS.

Jika Anda ingin menentukan bucket Amazon S3 Anda sendiri, pastikan bucket tersebut dikonfigurasi mengikuti praktik terbaik berikut:

- Blokir akses publik ke bucket (atur `IsPublic` ke `False`).
- Aktifkan pencatatan akses Amazon S3.
- [Izinkan hanya permintaan SSL ke bucket Anda](#).
- Nyalakan versi objek.
- Gunakan kunci AWS Key Management Service (AWS KMS) untuk mengenkripsi bucket Anda.

#### Important

Menggunakan runbook ini mungkin dikenakan biaya tambahan terhadap akun Anda untuk pembuatan bucket dan objek Amazon S3. Lihat [Harga Amazon S3](#) untuk detail selengkapnya tentang biaya yang mungkin dikenakan.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- S3 BucketName

Tipe: `AWS::S3::Bucket::Name`

Deskripsi: (Wajib) Bucket Amazon S3 di akun Anda untuk mengunggah laporan. Pastikan kebijakan bucket tidak memberikan izin baca/tulis yang tidak perlu kepada pihak yang tidak memerlukan akses ke log yang dikumpulkan. Jika bucket yang ditentukan tidak ada di akun, maka otomatisasi akan membuat bucket baru di Wilayah tempat otomatisasi dimulai dengan format nama `<User-provided-name>-awssupport-YYYY-MM-DD`, dienkripsi dengan kunci khusus. AWS KMS

Pola yang Diizinkan: `$|^((?!^((([0-9]{1,3}[.])?){3}[0-9]{1,3}$)))(?!xn-)(?!.*-s3alias))[a-z0-9][-.a-z0-9]{1,61}[a-z0-9]$`

- CustomerManagedKmsKeyArn

Jenis: String

Deskripsi: (Opsional) AWS KMS Kunci kustom Nama Sumber Daya Amazon (ARN) untuk mengenkripsi bucket Amazon S3 baru yang akan dibuat jika bucket yang ditentukan tidak ada di akun. Otomatisasi gagal jika pembuatan bucket dicoba tanpa menentukan AWS KMS ARN kunci khusus.

Pola yang Diizinkan: `(^$|^arn:aws:kms:[-a-z0-9]:[0-9]:key/[-a-z0-9]*$)`

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeSnapshots`

- `ec2:DescribeVolumes`
- `kms:Decrypt`
- `kms:GenerateDataKey`
- `s3:CreateBucket`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:ListBucket`
- `s3:ListAllMyBuckets`
- `s3:PutObject`
- `s3:PutBucketLogging`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutBucketTagging`
- `s3:PutBucketVersioning`
- `s3:PutEncryptionConfiguration`
- `ssm:DescribeAutomationExecutions`

Contoh kebijakan dengan Izin IAM minimum yang diperlukan untuk menjalankan runbook ini:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "Read_Only_Permissions",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeSnapshots",
      "ec2:DescribeVolumes",
      "ssm:DescribeAutomationExecutions"
    ],
    "Resource": ""
  }]
```

```

    }, {
      "Sid": "KMS_Generate_Permissions",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }, {
      "Sid": "S3_Read_Only_Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketAcl",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::awsexamplebucket1",
        "arn:aws:s3:::awsexamplebucket1/"
      ]
    }, {
      "Sid": "S3_Create_Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketLogging",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "*"
    }
  ]
}

```

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-AnalyzeEBS ResourceUsage](#) di konsol. AWS Systems Manager
2. Untuk parameter input masukkan yang berikut:

- AutomationAssumeRole (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- S3 BucketName (Diperlukan):

Bucket Amazon S3 di akun Anda untuk mengunggah laporan.

- CustomerManagedKmsKeyArn (Opsional):

AWS KMSKunci khusus Nama Sumber Daya Amazon (ARN) untuk mengenkripsi bucket Amazon S3 baru yang akan dibuat jika bucket yang ditentukan tidak ada di akun.

**Input parameters**

**S3BucketName**  
(Optional) The Amazon Simple Storage Service (S3) bucket in your account to upload the report to. Please make sure the bucket policy does not grant unnecessary read/write permissions to parties that do not need access to the collected logs. If the bucket specified does not exist in the account, then automation will create a new bucket in region where automation is executed with name format \*\*<User-provided-name>-awssupport-YYYY-MM-DD\*\*, encrypted with custom Key Management Service (KMS) key

Enter the name of an existing S3 Bucket

**S3 Bucket**  
  
Example: s3-bucket-name

**AutomationAssumeRole**  
(Optional) The ARN of the role that allows Automation to perform the actions on your behalf. If role is not specified, Systems Manager Automation uses the permission of the user that runs this document.

Select an existing IAM Role

arn:aws:iam::[redacted]:role/[redacted]

**CustomerManagedKmsKeyArn**  
(Optional) The custom KMS key ARN for encrypting the new Amazon Simple Storage Service (S3) bucket that will be created in case the bucket specified does not exist in the account. Automation will fail if bucket creation is attempted without specifying custom KMS key ARN

3. Pilih Jalankan.

4. Otomatisasi dimulai.

5. Runbook otomatisasi melakukan langkah-langkah berikut:

- CheckConcurrency:

Memastikan hanya ada satu inisiasi runbook ini di Wilayah. Jika runbook menemukan eksekusi lain yang sedang berlangsung, ia mengembalikan kesalahan dan berakhir.

- verifyOrCreateS3bucket:

Memverifikasi apakah bucket Amazon S3 ada. Jika tidak, itu membuat bucket Amazon S3 baru di Wilayah di mana otomatisasi dimulai dengan format nama<User-provided-name>-awssupport-YYYY-MM-DD, dienkripsi dengan kunci khusus. AWS KMS

- gatherAmiDetails:

Pencarian untuk AMI, yang tidak digunakan oleh instans Amazon EC2, menghasilkan laporan dengan `<region>-images.csv` format nama, dan mengunggahnya ke bucket Amazon S3.

- `gatherVolumeDetails`:

Memverifikasi volume Amazon EBS dalam status yang tersedia, membuat laporan dengan format nama `<region>-volume.csv`, dan mengunggahnya dalam bucket Amazon S3.

- `gatherSnapshotDetails`:

Mencari snapshot Amazon EBS dari volume Amazon EBS yang sudah dihapus, menghasilkan laporan dengan format nama `<region>-snapshot.csv`, dan mengunggahnya ke bucket Amazon S3.

6. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci.

▼ Outputs	
<code>gatherVolumeDetails.gatherVolumeDetailsOutput</code> No volume found in available state in region eu-central-1	<code>verifyOrCreateS3bucket.createdNewBucket</code> true
<code>gatherAmiDetails.gatherAmiDetailsOutput</code> File eu-central-1-image.csv have been uploaded to bucket aws-support-ssm-██████████1-awssupport-2023-11-27. Please review the file carefully and verify if you need to keep those AMI.	
<code>gatherSnapshotDetails.gatherSnapshotDetailsOutput</code> File eu-central-1-snapshot.csv have been uploaded to bucket aws-support-ssm-██████████1-awssupport-2023-11-27. Please review the file carefully and verify if you need to keep those snapshots.	

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

## AWS-ArchiveEBSSnapshots

### Deskripsi

AWS-ArchiveEBSSnapshotsRunbook membantu Anda mengarsipkan snapshot untuk volume Amazon Elastic Block Store (Amazon EBS) dengan menentukan tag yang telah Anda terapkan ke snapshot Anda. Atau, Anda dapat memberikan ID volume jika snapshot Anda tidak ditandai.

[Jalankan Otomasi ini \(konsol\)](#)



## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Deskripsi

Jenis: String

Deskripsi: (Opsional) Deskripsi untuk snapshot Amazon EBS.

- DryRun

Jenis: String

Nilai yang valid: Ya | Tidak

Deskripsi: (Wajib) Memeriksa apakah Anda memiliki izin yang diperlukan untuk tindakan tersebut, tanpa benar-benar membuat permintaan, dan memberikan respons kesalahan.

- RetentionCount

Jenis: String

Deskripsi: (Opsional) Jumlah snapshot yang ingin Anda arsipkan. Jangan tentukan nilai untuk parameter ini jika Anda menentukan nilai untuk `RetentionDays`.

- **RetentionDays**

Jenis: String

Deskripsi: (Opsional) Jumlah snapshot hari sebelumnya yang ingin Anda arsipkan. Jangan tentukan nilai untuk parameter ini jika Anda menentukan nilai untuk `RetentionCount`.

- **SnapshotWithTag**

Jenis: String

Nilai yang valid: Ya | Tidak

Deskripsi: (Wajib) Menentukan apakah snapshot yang ingin Anda arsipkan ditandai.

- **TagKey**

Jenis: String

Deskripsi: (Opsional) Kunci tag yang ditetapkan ke snapshot yang ingin Anda arsipkan.

- **TagValue**

Jenis: String

Deskripsi: (Opsional) Nilai tag yang ditetapkan ke snapshot yang ingin Anda arsipkan.

- **Volumeld**

Jenis: String

Deskripsi: (Opsional) ID volume yang snapshotnya ingin Anda arsipkan. Gunakan parameter ini jika snapshot Anda tidak ditandai.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:ArchiveSnapshots`
- `ec2:DescribeSnapshots`

## Langkah Dokumen

`aws:executeScript`- Arsip snapshot menggunakan tag yang Anda tentukan menggunakan `TagKey` dan `TagValue` parameter, atau `VolumeId` parameter.

## AWS-AttachEBSVolume

### Deskripsi

Lampirkan volume Amazon Elastic Block Store (Amazon EBS) ke instans Amazon Elastic Compute Cloud (Amazon EC2).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `Perangkat`

Jenis: String

Deskripsi: (Wajib) Nama perangkat (misalnya, `/dev/sdh` atau `xvdh`).

- `InstancedId`

Jenis: String

Deskripsi: (Wajib) ID dari instance tempat Anda ingin melampirkan volume.

- Volumeld

Jenis: String

Deskripsi: (Wajib) ID volume Amazon EBS. Volume dan instans harus berada dalam Zona Ketersediaan yang sama.

## AWSSupport-CalculateEBSPerformanceMetrics

### Deskripsi

AWSSupport-CalculateEBSPerformanceMetricsRunbook membantu mendiagnosis masalah kinerja Amazon EBS dengan menghitung dan menerbitkan metrik kinerja ke dasbor. CloudWatch Dasbor menampilkan perkiraan rata-rata IOPS dan throughput untuk target volume Amazon EBS atau semua volume yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) target. Untuk instans Amazon EC2, ini juga menunjukkan IOPS dan throughput rata-rata instans. Runbook menampilkan tautan ke CloudWatch dasbor yang baru dibuat yang menampilkan metrik terhitung CloudWatch yang relevan. CloudWatch Dasbor dibuat di akun Anda dengan nama:AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION\_ID>.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Memastikan bahwa stempel waktu yang ditentukan valid.
- Memvalidasi jika ID Sumber Daya (Volume Amazon EBS atau Instans Amazon EC2) valid.
- Saat Anda menyediakan Amazon EC2 sebagai ResourceID, Amazon EC2 akan membuat CloudWatch dasbor dengan Total IOP/Throughput Aktual untuk instans Amazon EC2 dan grafik Estimasi Rata-rata IOPS/throughput untuk semua volume Amazon EBS yang dilampirkan ke instans Amazon EC2.
- Saat Anda memberikan Volume Amazon EBS sebagai ResourceID, Volume EBS Amazon akan membuat dasbor dengan grafik Estimasi Rata-Rata CloudWatch IOPS/throughput untuk volume tersebut.
- Setelah CloudWatch dasbor dibuat, jika Estimasi Rata-rata IOPS atau Estimasi Rata-rata Throughput masing-masing lebih dari IOPS Maksimum atau Throughput Maksimum, maka microbursting dimungkinkan untuk volume atau volume yang dilampirkan ke instans Amazon EC2.

**Note**

Untuk volume burstable (gp2, sc2, dan st1), IOP/throughput maksimum harus dipertimbangkan, sampai Anda memiliki keseimbangan burst. Setelah keseimbangan burst sepenuhnya digunakan yaitu menjadi nol, pertimbangkan metrik IOP/throughput dasar.

**⚠ Important**

Membuat CloudWatch dasbor dapat mengakibatkan biaya tambahan ke akun Anda. Untuk informasi lebih lanjut, lihat [panduan CloudWatch Harga Amazon](#).

### Jalankan Otomasi ini (konsol)

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ec2:DescribeVolumes
- ec2:DescribeInstances
- ec2:DescribeInstanceTypes
- cloudwatch:PutDashboard

Kebijakan Sampel

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "cloudwatch:PutDashboard",
      "Resource": "arn:aws:cloudwatch::Account-id:dashboard/*-EBS-
Performance-*"
    }
  ],
}
```

```
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceTypes"
      ],
      "Resource": "*"
    }
  ]
}
```

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - Calculate EBS Performance Metrics](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
  - AutomationAssumeRole (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ResourceId (Diperlukan):

ID instans Amazon EC2 atau volume Amazon EBS.

- Waktu mulai (Diperlukan):

Waktu mulai untuk melihat data di CloudWatch. Waktu harus dalam format yyyy-mm-ddThh:mm:ss dan dalam UTC.

- Waktu akhir (Diperlukan):

Waktu akhir untuk melihat data di CloudWatch. Waktu harus dalam format yyyy-mm-ddThh:mm:ss dan dalam UTC.

Input parameters	
<b>AutomationAssumeRole</b> <small>(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</small> <input type="text" value="Choose an option"/>	<b>ResourceId</b> <small>(Required) The ID of the EC2 Instance or EBS Volume.</small> <input type="text" value="String"/>
<b>StartTime</b> <small>(Required) The start time to view the data in CloudWatch. The time must be in the format 'yyyy-mm-ddTHH:mm:ss' and in UTC.</small> <input type="text" value="String"/>	<b>EndTime</b> <small>(Required) The end time to view the data in CloudWatch. The time must be in the format 'yyyy-mm-ddTHH:mm:ss' and in UTC.</small> <input type="text" value="String"/>

#### 4. Pilih Jalankan.

#### 5. Otomatisasi dimulai.

#### 6. Dokumen melakukan langkah-langkah berikut:

- **CheckResourceIdAndTimeStamps:**

Memeriksa apakah waktu akhir lebih besar dari waktu mulai setidaknya satu menit dan jika sumber daya yang disediakan ada.

- **CreateCloudWatchDashboard:**

Menghitung kinerja Amazon EBS dan menampilkan grafik berdasarkan ID Sumber Daya Anda. Jika Anda memberikan ID Volume Amazon EBS untuk parameter Resource ID, runbook ini akan membuat dasbor dengan perkiraan IOPS rata-rata dan estimasi throughput rata-rata untuk volume Amazon EBS. Jika Anda memberikan ID Instans Amazon EC2 untuk parameter ID Sumber Daya, runbook ini akan membuat CloudWatch dasbor dengan IOPS Total Rata-rata dan Total Throughput Rata-rata untuk instans Amazon EC2 dan dengan Estimasi rata-rata IOPS dan estimasi throughput rata-rata untuk semua volume Amazon EBS yang dilampirkan ke instans Amazon EC2.

#### 7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci:

▼ Outputs
<b>CreateCloudWatchDashboard.CloudWatchDashboardLink</b> https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#dashboards:name=AWSsupport-1-██████████-EBS-Performance-443096c1-df23-44ba-96dd-2d005b5ae971
<b>CreateCloudWatchDashboard.CloudWatchDashboardMessage</b> Open the CloudWatch Dashboard URL in your browser to see the performance metrics for the target resource '1-██████████'. You can delete the CloudWatch Dashboard from the CloudWatch console.

#### Contoh CloudWatch Dasbor Untuk ID Sumber Daya sebagai instans Amazon EC2

### Aggregated Metrics for EC2 Instance i-[redacted]

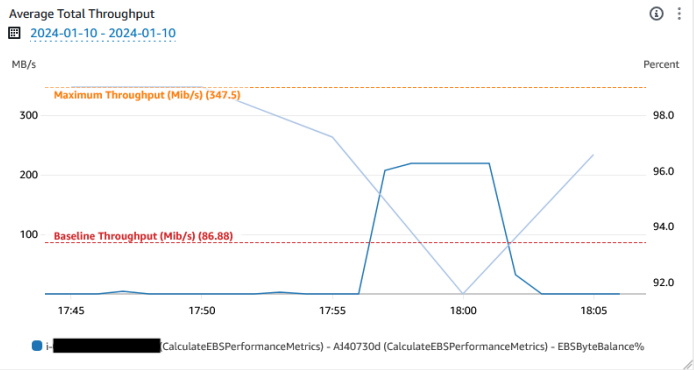
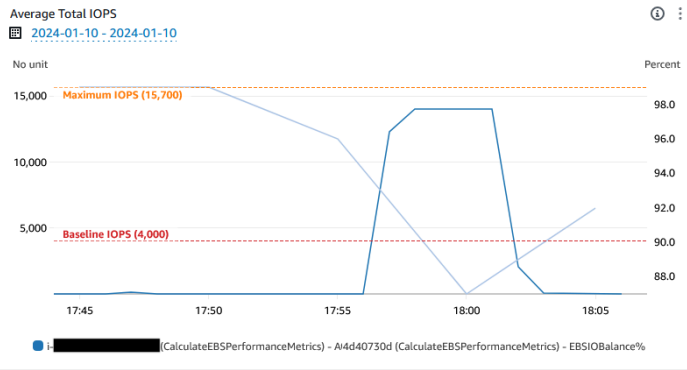
- Instance Type: t3.large
- EBS Optimized: True

[More details on EBS Optimized instances](#) [More details on EBS Volume Types](#)

How do I use CloudWatch to view the aggregate Amazon EBS performance metrics for an EC2 instance?

Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	$SUM(\text{For All Volumes}[(SUM(\text{VolumeReadOps}) + SUM(\text{VolumeWriteOps}))]) / \text{Period}$	IOPS
Average Total Throughput	$SUM(\text{For All Volumes}[(SUM(\text{VolumeReadBytes}) + SUM(\text{VolumeWriteBytes}))]) / \text{Period} / 1024 / 1024$	MiB/s

Note: The maximum performance can only be achieved if `BurstBalance%` for EBS volume or `EBSIOBalance%`, `EBSByteBalance%` for instance is greater than zero.



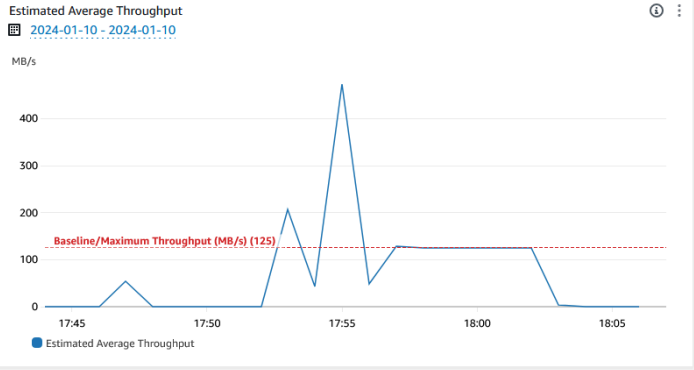
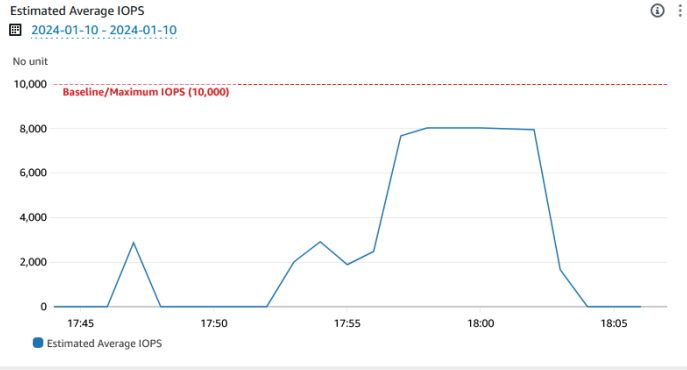
### EBS Volume(s) Metrics

Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	$(SUM(\text{VolumeReadOps}) + SUM(\text{VolumeWriteOps})) / (\text{Period} - SUM(\text{VolumeIdleTime}))$	IOPS
Estimated Average Throughput	$(SUM(\text{VolumeReadBytes}) + SUM(\text{VolumeWriteBytes})) / (\text{Period} - SUM(\text{VolumeIdleTime})) / 1024 / 1024$	MiB/s

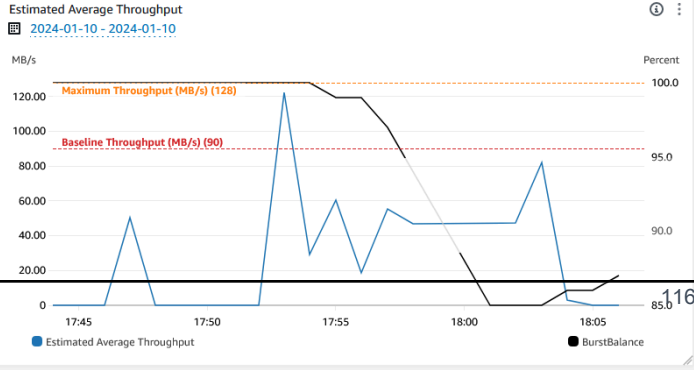
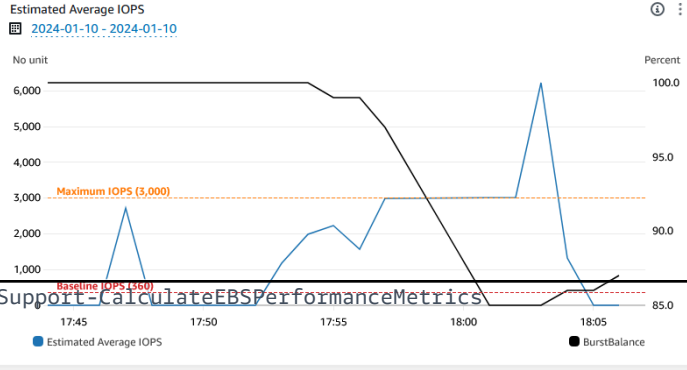
Note: If Estimated Average IOPS / Estimated Average Throughput is more than Maximum IOPS / Maximum Throughput, then microbursting is happening for that particular volume. Realtime analysis for Microbursting may vary, to confirm further you can use OS-level tool that has a finer granularity than CloudWatch. Also, the maximum performance for certain volume types can only be achieved if `BurstBalance%` is greater than zero.

For more information, please review - [How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?](#)

Volume: vol-[redacted] Type: gp3



Volume: vol-[redacted] Type: gp2

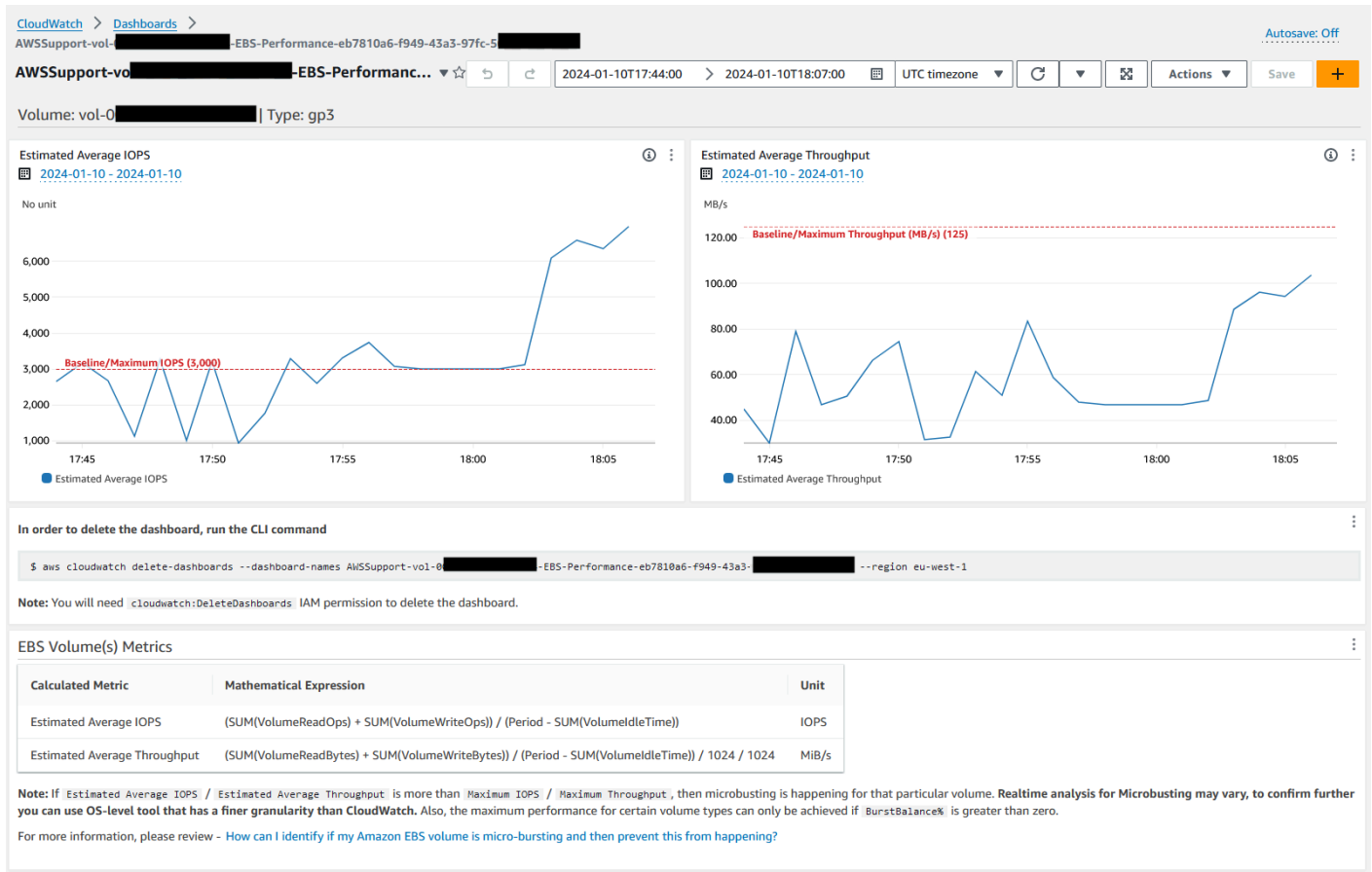


Volume: vol-[redacted] Type: gp3





## Contoh CloudWatch Dasbor Untuk ID Sumber Daya sebagai id volume Amazon EBS



## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

### AWSdokumentasi layanan

- [Bagaimana saya bisa mengidentifikasi apakah volume Amazon EBS saya meledak mikro dan kemudian mencegah hal ini terjadi?](#)
- [Bagaimana cara saya menggunakan CloudWatch metrik kinerja Amazon EBS agregat untuk instans EC2?](#)

# AWS - CopySnapshot

## Deskripsi

Menyalin point-in-time snapshot volume Amazon Elastic Block Store (Amazon EBS). Anda dapat menyalin snapshot dalam yang sama Wilayah AWS atau dari satu Wilayah ke Wilayah lainnya. Salinan snapshot Amazon EBS terenkripsi tetap dienkripsi. Salinan snapshot yang tidak terenkripsi tetap tidak terenkripsi. Untuk menyalin snapshot terenkripsi yang dibagikan dari akun lain, Anda harus memiliki izin untuk kunci KMS yang digunakan untuk mengenkripsi snapshot. Snapshot yang dibuat dengan menyalin snapshot lain memiliki ID volume arbitrer yang tidak boleh digunakan untuk tujuan apa pun.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

## Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Deskripsi

Jenis: String

Deskripsi: (Opsional) Deskripsi untuk snapshot Amazon EBS.

- SnapshotId

Jenis: String

Deskripsi: (Wajib) ID snapshot Amazon EBS untuk disalin.

- SourceRegion

Jenis: String

Deskripsi: (Wajib) Wilayah tempat snapshot sumber saat ini ada.

Langkah Dokumen

CopySnapshot - Menyalin snapshot dari volume Amazon EBS.

Keluaran

CopySnapshot. SnapshotId - ID snapshot baru.

## **AWS-CreateSnapshot**

Deskripsi

Buat snapshot volume Amazon EBS.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Deskripsi

Jenis: String

Deskripsi: (Opsional) Deskripsi untuk snapshot

- Volumeld

Jenis: String

Deskripsi: (Wajib) ID volume.

## AWS-DeleteSnapshot

Deskripsi

Hapus snapshot volume Amazon EBS.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- SnapshotId

Jenis: String

Deskripsi: (Wajib) ID snapshot EBS.

## **AWSConfigRemediation-DeleteUnusedEBSVolume**

Deskripsi

AWSConfigRemediation-DeleteUnusedEBSVolumeRunbook menghapus volume Amazon Elastic Block Store (Amazon EBS) yang tidak terpakai.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `CreateSnapshot`

Jenis: Boolean

Deskripsi: (Opsional) Jika disetel ke `true`, otomatisasi akan membuat snapshot volume Amazon EBS sebelum dihapus.

- `VolumeId`

Jenis: String

Deskripsi: (Wajib) ID volume Amazon EBS yang ingin Anda hapus.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateSnapshot`
- `ec2>DeleteVolume`
- `ec2:DescribeSnapshots`
- `ec2:DescribeVolumes`

Langkah Dokumen

- `aws:executeScript`- Memverifikasi volume Amazon EBS yang Anda tentukan dalam `VolumeId` parameter tidak digunakan, dan membuat snapshot tergantung pada nilai yang Anda pilih untuk parameter. `CreateSnapshot`
- `aws:branch`- Cabang berdasarkan nilai yang Anda pilih untuk `CreateSnapshot` parameter.
- `aws:waitForAwsResourceProperty`- Menunggu snapshot selesai.
- `aws:executeAwsApi`- Menghapus snapshot jika pembuatan snapshot gagal.
- `aws:executeAwsApi`- Menghapus volume Amazon EBS yang Anda tentukan dalam parameter. `VolumeId`
- `aws:executeScript`- Memverifikasi volume Amazon EBS telah dihapus.

# AWS-DeregisterAMIs

## Deskripsi

AWS-DeregisterAMIsRunbook membantu Anda deregister Amazon Machine Images (AMIs) dengan menentukan tag yang telah Anda terapkan ke tag Anda. AMIs

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DryRun

Jenis: String

Nilai yang valid: Ya | Tidak

Deskripsi: (Wajib) Memeriksa apakah Anda memiliki izin yang diperlukan untuk tindakan tersebut, tanpa benar-benar membuat permintaan, dan memberikan respons kesalahan.

- RetainNumber

Jenis: String

Deskripsi: (Opsional) Jumlah AMIs yang ingin Anda pertahankan. Jangan tentukan nilai untuk parameter ini jika Anda menentukan nilai untuk `Age`.

- `Umur`

Jenis: String

Deskripsi: (Opsional) Jumlah hari sebelumnya AMIs yang ingin Anda pertahankan. Jangan tentukan nilai untuk parameter ini jika Anda menentukan nilai untuk `RetainNumber`.

- `TagKey`

Jenis: String

Deskripsi: (Wajib) Kunci tag yang ditetapkan untuk AMIs yang ingin Anda deregister.

- `TagValue`

Jenis: String

Deskripsi: (Wajib) Nilai tag yang ditetapkan untuk AMIs yang ingin Anda deregister.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DeregisterImage`
- `ec2:DescribeImages`

Langkah Dokumen

- `aws:executeAwsApi`- Memvalidasi nilai yang Anda tentukan untuk parameter input runbook.
- `aws:executeAwsApi`- Deregisters AMIs menggunakan tag yang Anda tentukan menggunakan dan parameter. `TagKey` `TagValue`

## AWS-DetachEBSVolume

Deskripsi



Lepaskan volume Amazon EBS dari instans Amazon Elastic Compute Cloud (Amazon EC2).

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LambdaAssumeRole

Jenis: String

Deskripsi: (Opsional) ARN dari peran yang diambil oleh Lambda

- Volumeld

Jenis: String

Deskripsi: (Wajib) ID volume EBS. Volume dan instance harus berada dalam Availability Zone yang sama

## **AWSConfigRemediation-EnableEbsEncryptionByDefault**

Deskripsi

`AWSConfigRemediation-EnableEbsEncryptionByDefaultRunbook` memungkinkan enkripsi pada semua volume Amazon Elastic Block Store (Amazon EBS) baru di Akun AWS dan di Wilayah AWS mana Anda menjalankan otomatisasi. Volume yang dibuat sebelum Anda menjalankan otomatisasi tidak dienkripsi.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:EnableEbsEncryptionByDefault`
- `ec2:GetEbsEncryptionByDefault`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan pengaturan enkripsi Amazon EBS default di akun saat ini dan Wilayah.
- `aws:assertAwsResourceProperty`- Memverifikasi bahwa pengaturan enkripsi Amazon EBS default telah diaktifkan.

## AWS - ExtendEbsVolume

### Deskripsi

AWS-ExtendEbsVolumeRunbook meningkatkan ukuran volume Amazon EBS dan memperluas sistem file. Otomatisasi ini mendukung xfs dan sistem ext4 file.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `DriveLetter`

Jenis: String

Deskripsi: (Opsional) Huruf drive yang sistem filenya ingin Anda perpanjang. Parameter ini diperlukan untuk Windows instance.

- InstanceId

Jenis: String

Deskripsi: (Opsional) ID instans Amazon EC2 yang dilampirkan dengan volume Amazon EBS yang ingin Anda perpanjang.

- KeepSnapshot

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Menentukan apakah akan menyimpan snapshot yang dibuat sebelum meningkatkan ukuran volume Amazon EBS Anda.

- MountPoint

Jenis: String

Deskripsi: (Opsional) Titik pemasangan drive yang sistem filenya ingin Anda perpanjang. Parameter ini diperlukan untuk instance Linux.

- SizeGib

Jenis: String

Deskripsi: (Wajib) Ukuran dalam GiB yang ingin Anda ubah volume Amazon EBS Anda.

- VolumeId

Jenis: String

Deskripsi: (Wajib) ID volume EBS yang ingin Anda perpanjang.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ec2:CreateSnapshot
- ec2:CreateTags
- ec2:DeleteSnapshot

- `ec2:DescribeVolumes`
- `ec2:ModifyVolume`
- `ssm:DescribeInstanceInformation`
- `ssm:GetCommandInvocation`
- `ssm:SendCommand`

### Langkah Dokumen

- `aws:executeScript`- Meningkatkan ukuran volume ke nilai yang Anda tentukan dalam `VolumeId` parameter dan memperluas sistem file.

## **AWSsupport-ModifyEBSSnapshotPermission**

### Deskripsi

AWSsupport-ModifyEBSSnapshotPermissionRunbook membantu Anda mengubah izin untuk beberapa snapshot Amazon Elastic Block Store (Amazon EBS). Menggunakan runbook ini, Anda dapat membuat snapshot `Public` atau `Private` dan membagikannya dengan yang lain. Akun AWS Snapshot yang dienkripsi dengan kunci KMS default tidak dapat dibagikan dengan akun lain menggunakan runbook ini.

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Linux,macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- AccountIds

Jenis: StringList

Default: tidak ada

Deskripsi: (Opsional) ID akun yang ingin Anda bagikan snapshot. Parameter ini diperlukan jika Anda memasukkan No nilai Private parameter.

- AccountPermissionOperation

Jenis: String

Nilai yang valid: tambahkan | hapus

Default: tidak ada

Deskripsi: (Opsional) Jenis operasi yang harus dilakukan.

- Privat

Jenis: String

Nilai yang valid: Ya | Tidak

Deskripsi: (Wajib) Masukkan No nilai jika Anda ingin berbagi snapshot dengan akun tertentu.

- SnapshotIds

Jenis: StringList

Deskripsi: (Wajib) ID snapshot Amazon EBS yang izinnnya ingin Anda ubah.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSnapshots`
- `ec2:ModifySnapshotAttribute`

## Langkah Dokumen

1. `aws:executeScript`- Memverifikasi ID snapshot yang disediakan dalam parameter. `SnapshotIds` Setelah memverifikasi ID, skrip memeriksa snapshot terenkripsi dan mengeluarkan daftar jika ada yang ditemukan.
2. `aws:branch`- Cabang otomatisasi berdasarkan nilai yang Anda masukkan untuk `Private` parameter.
3. `aws:executeScript`- Memodifikasi izin snapshot yang ditentukan untuk membagikannya dengan akun yang ditentukan.
4. `aws:executeScript`- Memodifikasi izin snapshot untuk mengubahnya dari ke. `Public` `Private`

## Keluaran

`ValidateSnapshots.EncryptedSnapshots`

`SharewithOtherAccounts.Hasil`

`MakePrivate.Hasil`

`MakePrivate.Commands`

## **AWSConfigRemediation-ModifyEBSVolumeType**

### Deskripsi

`AWSConfigRemediation-ModifyEBSVolumeTypeRunbook` memodifikasi jenis volume volume volume Amazon Elastic Block Store (Amazon EBS) volume. Setelah jenis volume dimodifikasi, volume memasuki `optimizing` keadaan. Untuk informasi tentang memantau kemajuan modifikasi volume, lihat [Memantau kemajuan modifikasi volume](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- EbsVolumeld

Jenis: String

Deskripsi: (Wajib) ID volume Amazon EBS yang ingin Anda ubah.

- EbsVolumeType

Jenis: String

Nilai yang valid: standar | io1 | io2 | gp2 | gp3 | sc1 | st1

Deskripsi: Jenis volume yang ingin Anda ubah menjadi volume Amazon EBS. Untuk informasi tentang jenis volume Amazon EBS, lihat [Jenis volume Amazon EBS](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution



- `ssm:GetAutomationExecution`
- `ec2:DescribeVolumes`
- `ec2:ModifyVolume`

### Langkah Dokumen

- `aws:waitForAwsResourceProperty`- Memverifikasi status volume adalah `available` atau `in-use`.
- `aws:executeAwsApi`- Memodifikasi volume Amazon EBS yang Anda tentukan dalam parameter `EbsVolumeId`
- `aws:waitForAwsResourceProperty`- Memverifikasi jenis volume telah diubah ke nilai yang Anda tentukan dalam `EbsVolumeType` parameter.

## Amazon EC2

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Elastic Compute Cloud. Runbook untuk Amazon Elastic Block Store terletak di [Amazon EBS](#) bagian referensi runbook. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-ASGEnterStandby](#)
- [AWS-ASGExitStandby](#)
- [AWS-CreatelImage](#)
- [AWS-DeletelImage](#)
- [AWS-PatchAsgInstance](#)
- [AWS-PatchInstanceWithRollback](#)
- [AWS-QuarantineEC2Instance](#)
- [AWS-ResizeInstance](#)
- [AWS-RestartEC2Instance](#)
- [AWS-SetupJupyter](#)
- [AWS-StartEC2Instance](#)
- [AWS-StopEC2Instance](#)

- [AWS-TerminateEC2Instance](#)
- [AWS-UpdateLinuxAmi](#)
- [AWS-UpdateWindowsAmi](#)
- [AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck](#)
- [AWSConfigRemediation-EnforceEC2InstanceIMDSv2](#)
- [AWSEC2-CloneInstanceAndUpgradeSQLServer](#)
- [AWSEC2-CloneInstanceAndUpgradeWindows](#)
- [AWSEC2-ConfigureSTIG](#)
- [AWSEC2-PatchLoadBalancerInstance](#)
- [AWSEC2-SQLServerDBRestore](#)
- [AWSsupport-ActivateWindowsWithAmazonLicense](#)
- [AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2](#)
- [AWSPremiumSupport-ChangeInstanceTypeIntelToAMD](#)
- [AWSsupport-CheckXenToNitroMigrationRequirements](#)
- [AWSsupport-ConfigureEC2Metadata](#)
- [AWSsupport-CopyEC2Instance](#)
- [AWSsupport-EnableWindowsEC2SerialConsole](#)
- [AWSsupport-ExecuteEC2Rescue](#)
- [AWSsupport-ListEC2Resources](#)
- [AWSsupport-ManageRDPSettings](#)
- [AWSsupport-ManageWindowsService](#)
- [AWSsupport-MigrateEC2ClassicToVPC](#)
- [AWSsupport-MigrateXenToNitroLinux](#)
- [AWSsupport-ResetAccess](#)
- [AWSsupport-ResetLinuxUserPassword](#)
- [AWSPremiumSupport-ResizeNitroInstance](#)
- [AWSsupport-RestoreEC2InstanceFromSnapshot](#)
- [AWSsupport-SendLogBundleToS3Bucket](#)
- [AWSsupport-StartEC2RescueWorkflow](#)
- [AWSPremiumSupport-TroubleshootEC2DiskUsage](#)

- [AWSSupport-TroubleshootEC2InstanceConnect](#)
- [AWSSupport-TroubleshootRDP](#)
- [AWSSupport-TroubleshootSSH](#)
- [AWSSupport-TroubleshootSUSERegistration](#)
- [AWSSupport-TroubleshootWindowsPerformance](#)
- [AWSSupport-TroubleshootWindowsUpdate](#)
- [AWSSupport-UpgradeWindowsAWSDrivers](#)

## AWS-ASGEnterStandby

### Deskripsi

Ubah status siaga instans Amazon Elastic Compute Cloud (Amazon EC2) dalam grup Penskalaan Otomatis.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: ID (Diperlukan) instans Amazon EC2 yang ingin Anda ubah status siaga dalam grup Penskalaan Otomatis.

- LambdaRoleArn

Jenis: String

Deskripsi: (Opsional) ARN peran yang memungkinkan Lambda dibuat oleh Automation untuk melakukan tindakan atas nama Anda. Jika tidak ditentukan peran sementara akan dibuat untuk menjalankan fungsi Lambda.

## AWS-ASGExitStandby

Deskripsi

Ubah status siaga instans Amazon Elastic Compute Cloud (Amazon EC2) dalam grup Penskalaan Otomatis.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan

tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: ID (Diperlukan) instans EC2 yang ingin Anda ubah status siaga dalam grup Penskalaan Otomatis.

- LambdaRoleArn

Jenis: String

Deskripsi: (Opsional) ARN peran yang memungkinkan Lambda dibuat oleh Automation untuk melakukan tindakan atas nama Anda. Jika tidak ditentukan peran sementara akan dibuat untuk menjalankan fungsi Lambda.

## AWS-CreateImage

Deskripsi

Buat Amazon Machine Image (AMI) baru dari instans Amazon Elastic Compute Cloud (Amazon EC2).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans EC2.

- NoReboot

Jenis: Boolean

Deskripsi: (Opsional) Jangan reboot instance sebelum membuat gambar.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateImage",
        "ec2:DescribeImages"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

## AWS-DeleteImage

Deskripsi

Hapus Amazon Machine Image (AMI) dan semua snapshot terkait.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ImageId

Jenis: String

Deskripsi: (Diperlukan) ID AMI.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

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

```
    "Action": "ec2:DeleteSnapshot",
    "Resource": "arn:aws:ec2:{region}::snapshot/*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:DescribeImages",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:DeregisterImage",
    "Resource": "*"
  }
]
```

## AWS-PatchAsgInstance

### Deskripsi

Menambal instans Amazon Elastic Compute Cloud (Amazon EC2) dalam grup Penskalaan Otomatis.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan



tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instance untuk ditambal. Jangan tentukan ID instance yang dikonfigurasi untuk dijalankan selama jendela pemeliharaan.

- LambdaRoleArn

Jenis: String

Deskripsi: (Opsional) ARN peran yang memungkinkan Lambda yang dibuat oleh Automation untuk melakukan tindakan atas nama Anda. Jika tidak ditentukan, peran sementara akan dibuat untuk menjalankan fungsi Lambda.

- WaitForInstance

Jenis: String

Bawaan: PT2M

Deskripsi: (Opsional) Durasi bahwa Otomasi harus tidur untuk memungkinkan instans kembali ke layanan.

- WaitForReboot

Jenis: String

Default: PT5M

Deskripsi: (Opsional) Durasi bahwa Otomasi harus tidur untuk memungkinkan instance yang ditambal di-boot ulang.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

- `ssm:GetCommandInvocation`
- `ssm:GetParameter`
- `ssm:SendCommand`
- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStacks`
- `ec2:CreateTags`
- `ec2:DescribeInstances`
- `ec2:RunInstances`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:GetFunction`
- `lambda:InvokeFunction`

## **AWS-PatchInstanceWithRollback**

### Deskripsi

Membawa instans EC2 sesuai dengan dasar patch yang berlaku. Rolls kembali volume root pada kegagalan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

## Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) EC2 InstanceId yang kami terapkan patch-baseline.

- LambdaAssumeRole

Jenis: String

Deskripsi: (Opsional) ARN peran yang memungkinkan Lambda dibuat oleh Automation untuk melakukan tindakan atas nama Anda. Jika tidak ditentukan peran sementara akan dibuat untuk menjalankan fungsi Lambda.

- Laporan3bucket

Jenis: String

Deskripsi: (Opsional) Tujuan Amazon S3 Bucket untuk Laporan Kepatuhan yang dihasilkan selama proses.

## Langkah Dokumen

Nomor langkah	Nama langkah	Tindakan otomatisasi
1	createDocumentStack	aws:createStack
2	IdentifyRootVolume	aws:invokeLambdaFunction
3	PrePatchSnapshot	aws:executeAutomation
4	installMissingUpdates	aws:runCommand
5	SleepThruInstallation	aws:invokeLambdaFunction
6	CheckCompliance	aws:invokeLambdaFunction
7	SaveComplianceReportToS3	aws:invokeLambdaFunction
8	ReportSuccessOrFailure	aws:invokeLambdaFunction
9	RestoreFromSnapshot	aws:invokeLambdaFunction
10	DeleteSnapshot	aws:invokeLambdaFunction
11	deleteCloudFormationTemplate	aws:deleteStack

Keluaran

IdentifyRootVolume.Muatan

PrePatchSnapshot.Keluaran

SaveComplianceReportToS3.muatan

RestoreFromSnapshot.Muatan

CheckCompliance.Muatan

## AWS-QuarantineEC2Instance

Deskripsi

Dengan AWS-QuarantineEC2Instance runbook, Anda dapat menetapkan grup keamanan ke instans Amazon Elastic Compute Cloud (Amazon EC2) yang tidak mengizinkan lalu lintas masuk atau keluar.

### Important

Perubahan pada pengaturan RDP harus ditinjau dengan cermat sebelum menjalankan runbook ini.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans terkelola untuk mengelola pengaturan RDP dari.

- IsolationSecurityGroup

Jenis: String

Deskripsi: (Diperlukan) Nama grup keamanan yang ingin Anda tetapkan ke instans untuk mencegah lalu lintas masuk atau keluar.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `autoscaling:DescribeAutoScalingInstances`
- `autoscaling:DetachInstances`
- `ec2:CreateSecurityGroup`
- `ec2:CreateSnapshot`
- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSnapshots`
- `ec2:ModifyInstanceAttribute`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan rincian tentang contoh.
- `aws:executeScript`- Memverifikasi instance bukan bagian dari grup Auto Scaling.
- `aws:executeAwsApi`- Membuat snapshot dari volume root yang melekat pada instance.
- `aws:waitForAwsResourceProperty`- Menunggu keadaan snapshot menjadi `completed`
- `aws:executeAwsApi`- Menetapkan grup keamanan yang ditentukan dalam `IsolationSecurityGroup` parameter ke instance Anda.

## Keluaran

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

## AWS-ResizeInstance

### Deskripsi

Ubah jenis instans instans Amazon Elastic Compute Cloud (Amazon EC2).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `InstanceId`

Jenis: String

Deskripsi: (Diperlukan) ID instance.

- InstanceType

Jenis: String

Deskripsi: (Diperlukan) Jenis instans.

- LambdaAssumeRole

Jenis: String

Deskripsi: (Opsional) ARN peran yang diasumsikan oleh Lambda.

## AWS-RestartEC2Instance

### Deskripsi

Mulai ulang satu atau beberapa instans Amazon Elastic Compute Cloud (Amazon EC2).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId



Jenis: StringList

Deskripsi: (Diperlukan) ID instans Amazon EC2 untuk memulai ulang.

## AWS-SetupJupyter

Deskripsi

AWS-SetupJupyterRunbook membantu Anda menyiapkan Notebook Jupyter pada instans Amazon Elastic Compute Cloud (Amazon EC2). Anda dapat menentukan instance yang ada, atau memberikan ID Amazon Machine Image (AMI) untuk otomatisasi untuk meluncurkan dan menyiapkan instance baru. Sebelum memulai, Anda harus membuat SecureString parameter di Parameter Store untuk digunakan sebagai kata sandi untuk Notebook Jupyter. penyimpanan Parameter adalah sebuah kemampuan AWS Systems Manager. Untuk informasi tentang membuat parameter, lihat [Membuat parameter](#) di Panduan AWS Systems Manager Pengguna.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Amild

Jenis: String

Deskripsi: (Opsional) ID AMI yang ingin Anda gunakan untuk meluncurkan instance baru dan menyiapkan Notebook Jupyter.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans yang ingin Anda atur Jupyter Notebook.

- InstanceType

Jenis: String

Bawaan: t3.medium

Deskripsi: (Opsional) Jika Anda meluncurkan instance baru untuk menyiapkan Notebook Jupyter, tentukan jenis instans yang ingin Anda gunakan.

- JupyterPasswordSSMKey

Jenis: String

Deskripsi: (Diperlukan) Nama SecureString parameter di Parameter Store yang ingin Anda gunakan sebagai kata sandi untuk Notebook Jupyter.

- KeyPairName

Jenis: String

Deskripsi: (Opsional) Pasangan kunci yang ingin Anda kaitkan dengan instans yang baru diluncurkan.

- RemoteAccessCidr

Jenis: String

Default 0.0.0.0/0

Deskripsi: (Opsional) Rentang CIDR yang Anda inginkan untuk mengizinkan lalu lintas SSH.

- RoleName

Jenis: String

Default: `SSM ManagedInstanceProfileRole`

Deskripsi: (Opsional) Nama profil instans untuk instans yang baru diluncurkan.

- `StackName`

Jenis: String

Default: `CreateManagedInstanceStack {{Automation: execution_ID}}`

Deskripsi: (Opsional) Nama AWS CloudFormation tumpukan yang Anda inginkan untuk digunakan otomatisasi.

- `SubnetId`

Jenis: String

Default: Default

Deskripsi: (Opsional) Subnet yang ingin Anda luncurkan instance baru untuk digunakan.

- `VpcId`

Jenis: String

Default: Default

Deskripsi: (Opsional) ID cloud pribadi virtual (VPC) yang ingin Anda luncurkan instance baru.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ssm:GetParameter`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`
- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`

- `cloudformation:DescribeStacks`
- `ec2:DescribeInstances`
- `ec2:DescribeKeyPairs`
- `ec2:RunInstances`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:GetFunction`
- `lambda:InvokeFunction`

### Langkah Dokumen

- `aws:executeScript`- Mengatur Notebook Jupyter pada instance yang Anda tentukan, atau pada instance yang baru diluncurkan, menggunakan nilai yang Anda tentukan untuk parameter input runbook.

## AWS-StartEC2Instance

### Deskripsi

Mulai satu atau beberapa instans Amazon Elastic Compute Cloud (Amazon EC2).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: StringList

Deskripsi: (Diperlukan) instans EC2 untuk memulai.

## AWS-StopEC2Instance

### Deskripsi

Menghentikan satu atau beberapa instans Amazon Elastic Compute Cloud (Amazon EC2).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: StringList

Deskripsi: (Diperlukan) instans EC2 untuk berhenti.

## AWS-TerminateEC2Instance

### Deskripsi

Hentikan satu atau beberapa instans Amazon Elastic Compute Cloud (Amazon EC2).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: StringList

Deskripsi: ID (Diperlukan) dari satu atau beberapa instans EC2 untuk diakhiri.

## AWS-UpdateLinuxAmi

Deskripsi

Perbarui Amazon Machine Image (AMI) dengan paket distribusi Linux dan perangkat lunak Amazon.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ExcludePackages

Jenis: String

Default: tidak ada

Deskripsi: (Opsional) Nama paket untuk menahan pembaruan, dalam semua kondisi. Secara default (“tidak ada”), tidak ada paket yang dikecualikan.

- `iamInstanceProfileName`

Jenis: String

Default: `ManagedInstanceProfile`

Deskripsi: (Wajib) Profil instans yang memungkinkan Systems Manager mengelola instance.

- `IncludePackages`

Jenis: String

Default: semua

Deskripsi: (Opsional) Hanya perbarui paket bernama ini. Secara default (“semua”), semua pembaruan yang tersedia diterapkan.

- `InstanceType`

Jenis: String

Default: `t2.micro`

Deskripsi: (Opsional) Jenis instance yang akan diluncurkan sebagai host ruang kerja. Jenis instans bervariasi menurut Wilayah.

- `MetadataOptions`

Jenis: `StringMap`

Default: `{"HttpEndpoint": "enabled", "HttpTokens": "optional"}`

Deskripsi: (Opsional) Opsi metadata untuk instance. Untuk informasi lebih lanjut, lihat [InstanceMetadataOptionsRequest](#).

- `PostUpdateScript`

Jenis: String



Default: tidak ada

Deskripsi: (Opsional) URL skrip untuk dijalankan setelah pembaruan paket diterapkan. Default (“none”) adalah tidak menjalankan skrip.

- PreUpdateScript

Jenis: String

Default: tidak ada

Deskripsi: (Opsional) URL skrip untuk dijalankan sebelum pembaruan diterapkan. Default (“none”) adalah tidak menjalankan skrip.

- SourceAmild

Jenis: String

Deskripsi: (Wajib) Sumber Amazon Machine Image ID.

- SubnetId

Jenis: String

Deskripsi: (Opsional) ID subnet yang ingin Anda luncurkan instance. Jika Anda telah menghapus VPC default Anda, parameter ini diperlukan.

- TargetAmiName

Jenis: String

Default: UpdateLinuxAmi \_dari\_ {{SourceAmild}} \_pada\_ {{global:date\_time}}

Deskripsi: (Opsional) Nama AMI baru yang akan dibuat. Default adalah string yang dihasilkan sistem termasuk id AMI sumber, dan waktu dan tanggal pembuatan.

## AWS-UpdateWindowsAmi

Deskripsi

Perbarui Microsoft Windows Amazon Machine Image (AMI). Secara default, runbook ini menginstal semua pembaruan Windows, perangkat lunak Amazon, dan driver Amazon. Kemudian menjalankan Sysprep untuk membuat AMI baru. Mendukung Windows Server 2008 R2 atau yang lebih baru.

**⚠ Important**

Jika instans Anda terhubung AWS Systems Manager menggunakan titik akhir VPC, runbook ini akan gagal kecuali digunakan di Wilayah us-east-1. Instans harus mengaktifkan TLS 1.2 untuk menggunakan runbook ini.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Kategori

Jenis: String

Deskripsi: (Opsional) Tentukan satu atau beberapa kategori pembaruan. Anda dapat memfilter kategori menggunakan nilai yang dipisahkan koma. Opsi: Aplikasi, Konektor, CriticalUpdates, DefinitionUpdates, DeveloperKits, DriverFeaturePacks,, Panduan, Microsoft SecurityUpdates,, ServicePacks, Alat,UpdateRollups, Pembaruan. Format yang valid mencakup satu entri, misalnya:CriticalUpdates. Atau Anda dapat menentukan daftar dipisahkan koma:CriticalUpdates,SecurityUpdates. CATATAN: Tidak ada spasi di sekitar koma.

- ExcludeKbs

Jenis: String

Deskripsi: (Opsional) Tentukan satu atau beberapa ID artikel Microsoft Knowledge Base (KB) yang akan dikecualikan. Anda dapat mengecualikan beberapa ID menggunakan nilai yang dipisahkan koma. Format yang valid: KB9876543 atau 9876543.

- IamInstanceProfileName

Jenis: String

Default: ManagedInstanceProfile

Deskripsi: (Wajib) Nama peran yang memungkinkan Systems Manager mengelola instance.

- IncludeKbs

Jenis: String

Deskripsi: (Opsional) Tentukan satu atau beberapa ID artikel Microsoft Knowledge Base (KB) yang akan disertakan. Anda dapat menginstal beberapa ID menggunakan nilai dipisahkan koma. Format yang valid: KB9876543 atau 9876543.

- InstanceType

Jenis: String

Default: t2.medium

Deskripsi: (Opsional) Jenis instance yang akan diluncurkan sebagai host ruang kerja. Jenis instans bervariasi menurut wilayah. Defaultnya adalah t2.medium.

- MetadataOptions

Jenis: StringMap

Default: {"HttpEndpoint": "enabled", "HttpTokens": "optional"}

Deskripsi: (Opsional) Opsi metadata untuk instance. Untuk informasi lebih lanjut, lihat [InstanceMetadataOptionsRequest](#).

- PostUpdateScript

Jenis: String

Deskripsi: (Opsional) Skrip yang disediakan sebagai string. Ini akan berjalan setelah menginstal pembaruan OS.

- PreUpdateScript

Jenis: String

Deskripsi: (Opsional) Skrip yang disediakan sebagai string. Ini akan berjalan sebelum menginstal pembaruan OS.

- PublishedDateAfter

Jenis: String

Deskripsi: (Opsional) Tentukan tanggal pembaruan harus dipublikasikan setelahnya. Misalnya, jika 01/01/2017 ditentukan, pembaruan apa pun yang ditemukan selama pencarian Pembaruan Windows yang telah dipublikasikan pada atau setelah 01/01/2017 akan dikembalikan.

- PublishedDateBefore

Jenis: String

Deskripsi: (Opsional) Tentukan tanggal pembaruan harus dipublikasikan sebelumnya. Misalnya, jika 01/01/2017 ditentukan, pembaruan apa pun yang ditemukan selama pencarian Pembaruan Windows yang telah dipublikasikan pada atau sebelum 01/01/2017 akan dikembalikan.

- PublishedDaysOld

Jenis: String

Deskripsi: (Opsional) Tentukan jumlah hari pembaruan harus dari tanggal yang dipublikasikan. Misalnya, jika 10 ditentukan, pembaruan apa pun yang ditemukan selama pencarian Pembaruan Windows yang telah diterbitkan 10 hari atau lebih yang lalu akan dikembalikan.

- SeverityLevels

Jenis: String

Deskripsi: (Opsional) Tentukan satu atau beberapa tingkat keparahan MSRC yang terkait dengan pembaruan. Anda dapat memfilter tingkat keparahan menggunakan nilai yang dipisahkan koma. Secara default patch untuk semua tingkat keamanan dipilih. Jika nilai diberikan, daftar pembaruan disaring oleh nilai-nilai tersebut. Pilihan: Kritis, Penting, Rendah, Sedang atau Tidak Ditentukan.

Format yang valid mencakup satu entri, misalnya: Kritis. Atau, Anda dapat menentukan daftar yang dipisahkan koma: Kritis,Penting,Rendah.

- SourceAmild

Jenis: String

Deskripsi: (Wajib) Sumber Amazon Machine Image ID.

- SubnetId

Jenis: String

Deskripsi: (Opsional) ID subnet yang ingin Anda luncurkan instance. Jika Anda telah menghapus VPC default Anda, parameter ini diperlukan.

- TargetAmiName

Jenis: String

Default: UpdateWindowsAmi \_dari\_ {{SourceAmild}} \_pada\_ {{global:date\_time}}

Deskripsi: (Opsional) Nama AMI baru yang akan dibuat. Default adalah string yang dihasilkan sistem termasuk id AMI sumber, dan waktu dan tanggal pembuatan.

## **AWSConfigRemediation- EnableAutoScalingGroupELBHealthCheck**

Deskripsi

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheckRunbook memungkinkan pemeriksaan kesehatan untuk grup Amazon EC2 Auto Scaling (Auto Scaling) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- `AutoScalingGroupARN`

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) grup penskalaan otomatis yang ingin Anda aktifkan pemeriksaan kesehatan.

- `HealthCheckGracePeriod`

Tipe: Bilangan Bulat

Default: 300

Deskripsi: (Opsional) Jumlah waktu, dalam hitungan detik, Penskalaan Otomatis menunggu sebelum memeriksa status kesehatan instans Amazon Elastic Compute Cloud (Amazon EC2) yang telah tersedia.

## Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeAutoScalingGroups`
- `ec2:UpdateAutoScalingGroup`

## Langkah Dokumen

- `aws:executeScript`- Memungkinkan pemeriksaan kesehatan pada grup Auto Scaling yang Anda tentukan dalam `AutoScalingGroupARN` parameter.

## **AWSConfigRemediation-EnforceEC2InstanceIMDSv2**

### Deskripsi

AWSConfigRemediation-EnforceEC2InstanceIMDSv2Runbook memerlukan instans Amazon Elastic Compute Cloud (Amazon EC2) yang Anda tentukan untuk menggunakan Instans Metadata Service Version 2 (IMDSv2).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `InstanceID`

Jenis: String

Deskripsi: (Wajib) ID instans Amazon EC2 yang ingin Anda perlukan untuk menggunakan IMDSv2.

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `HttpPutResponseHopLimit`

Jenis: Integer

Deskripsi: (Opsional) Batas respons Hop dari layanan IMDS kembali ke pemohon. Setel ke 2 atau lebih untuk wadah hosting instans EC2. Setel ke 0 agar tidak berubah (Default).

Pola yang diizinkan: `^[1-5]?\d|6[0-4]$`

Default: 0

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeInstances`
- `ec2:ModifyInstanceMetadataOptions`

Langkah Dokumen

- `aws:executeScript`- Menetapkan `HttpTokens` opsi ke `required` instans Amazon EC2 yang Anda tentukan dalam parameter. `InstanceId`
- `aws:assertAwsResourceProperty`- Memverifikasi `IMDSv2` diperlukan pada instans Amazon EC2.

## AWSEC2-CloneInstanceAndUpgradeSQLServer

Deskripsi

Buat AMI dari contoh EC2 untuk Windows Server menjalankan SQL Server 2008 atau yang lebih baru, dan kemudian upgrade AMI ke versi SQL Server yang lebih baru.

Jalur pemutakhiran berikut didukung:

- SQL Server 2008 untuk SQL Server 2017, 2016, atau 2014
- SQL Server 2008 R2 ke SQL Server 2017, 2016, atau 2014



- SQL Server 2012 untuk SQL Server 2019, 2017, 2016, atau 2014
- SQL Server 2014 untuk SQL Server 2019, 2017, atau 2016
- SQL Server 2016 ke SQL Server 2019 atau 2017
- SQL Server 2017 ke SQL Server 2019

Jika Anda menggunakan versi Windows Server yang lebih lama yang tidak kompatibel dengan SQL Server 2019, dokumen otomatisasi harus meningkatkan versi Windows Server Anda ke 2016.

Upgrade adalah proses multi-langkah yang dapat memakan waktu 2 jam untuk menyelesaikannya. Otomatisasi membuat AMI dari instance, dan kemudian meluncurkan instance sementara dari yang baru AMI dalam yang ditentukan SubnetID. Grup keamanan yang terkait dengan instans asli Anda diterapkan ke instans sementara. Otomatisasi kemudian melakukan upgrade TargetSQLVersion di tempat ke instans sementara. Setelah upgrade, otomatisasi membuat baru AMI dari instance sementara dan kemudian mengakhiri instance sementara.

Anda dapat menguji fungsionalitas aplikasi dengan meluncurkan yang baru AMI di VPC Anda. Setelah Anda menyelesaikan pengujian, dan sebelum Anda melakukan peningkatan lain, jadwalkan waktu henti aplikasi sebelum sepenuhnya beralih ke instans yang ditingkatkan.

#### Note

Jika Anda ingin memodifikasi nama komputer dari instans EC2 yang diluncurkan dari yang baru AMI, lihat [Mengubah nama komputer yang Host Instans Stand-Alone SQL Server](#).

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter

## Prasyarat

- TLS versi 1.2.
- Instans EC2 harus menggunakan versi yang Windows Server 2008 R2 (atau Windows Server yang lebih baru) dan SQL Server 2008 (atau yang lebih baru).
- Verifikasi bahwa Agen SSM diinstal pada instans Anda. Untuk informasi selengkapnya, lihat [Menginstal dan mengonfigurasi Agen SSM pada instans EC2](#) untuk Windows Server.
- Konfigurasi instance untuk menggunakan peran profil instance AWS Identity and Access Management (IAM). Untuk informasi selengkapnya, lihat [Buat profil instans IAM untuk Systems Manager](#).
- Verifikasi bahwa instance memiliki 20 GB ruang disk kosong di disk boot instance.
- Untuk instance yang menggunakan versi SQL Server Bring Your Own License (BYOL), prasyarat tambahan berikut berlaku:
  - Berikan ID snapshot EBS yang menyertakan media instalasi SQL Server target. Untuk melakukannya:
    1. Verifikasi bahwa instans EC2 menjalankan Windows Server 2008 R2 atau yang lebih baru.
    2. Buat volume EBS 6 GB di Availability Zone yang sama dengan tempat instans berjalan. Pasang volume ke instans. Pasang, misalnya, sebagai drive D.
    3. Klik kanan ISO dan mount ke instance sebagai, misalnya, drive E.
    4. Salin isi ISO dari drive E:\ ke drive D:\
    5. Buat snapshot EBS dari volume 6 GB yang dibuat pada langkah 2.

## Keterbatasan

- Upgrade dapat dilakukan hanya pada SQL Server menggunakan otentikasi Windows.
- Verifikasi bahwa tidak ada pembaruan patch keamanan yang tertunda pada instans. Buka Control Panel, lalu pilih Periksa pembaruan.
- Penyebaran SQL Server dalam mode HA dan mirroring tidak didukung.

## Parameter

- `IamInstanceProfile`

Jenis: String

Deskripsi: (Diperlukan) Profil instans IAM.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) Instance yang menjalankan Windows Server 2008 R2 (atau yang lebih baru) dan SQL Server 2008 (atau yang lebih baru).

- KeepPreUpgradeImageBackUp

Jenis: String

Deskripsi: (Opsional) Jika disetel ke `true`, otomatisasi tidak menghapus AMI yang dibuat dari instans sebelum upgrade. Jika diatur ke `true`, maka Anda harus menghapus AMI. Secara default, AMI dihapus.

- SubnetId

Jenis: String

Deskripsi: (Diperlukan) Menyediakan subnet untuk proses upgrade. Pastikan subnet memiliki konektivitas keluar ke AWS layanan, Amazon S3, dan Microsoft (untuk mengunduh tambalan).

- SQLServerSnapshotId

Jenis: String

Deskripsi: ID Snapshot (Bersyarat) untuk media instalasi SQL Server target. Parameter ini diperlukan untuk instance yang menggunakan versi BYOL SQL Server. Parameter ini opsional untuk instans yang disertakan lisensi SQL Server (instans diluncurkan menggunakan Amazon Machine Image untuk Windows Server yang AWS disediakan dengan Microsoft SQL Server).

- RebootInstanceBeforeTakingImage

Jenis: String

Deskripsi: (Opsional) Jika diatur ke `true`, otomatisasi me-reboot instans sebelum membuat AMI pra-upgrade. Secara default, otomatisasi tidak reboot sebelum upgrade.

- TargetSqlVersion

Jenis: String

Deskripsi: (Opsional) Pilih versi SQL Server target.

Target yang mungkin:

- SQL Server 2019
- SQL Server 2017
- SQL Server 2016
- SQL Server 2014

Target default: SQL Server 2016

Keluaran

AMIID: ID AMI yang dibuat dari instance yang ditingkatkan ke versi SQL Server yang lebih baru.

## **AWSEC2-CloneInstanceAndUpgradeWindows**

Deskripsi

Buat Amazon Machine Image (AMI) dari instance Windows Server 2008 R2, 2012 R2, 2016, atau 2019, lalu tingkatkan AMI ke Windows Server 2016, 2019, atau 2022. Jalur pemutakhiran yang didukung adalah sebagai berikut.

- Windows Server2008 R2 hingga Windows Server 2016.
- Windows Server2012 R2 hingga Windows Server 2016.
- Windows Server2012 R2 hingga Windows Server 2019.
- Windows Server2012 R2 hingga Windows Server 2022.
- Windows Server2016 hingga Windows Server 2019.
- Windows Server2016 hingga Windows Server 2022.
- Windows Server2019 hingga Windows Server 2022.

Operasi upgrade adalah proses multi-langkah yang dapat memakan waktu 2 jam untuk menyelesaikannya. Kami merekomendasikan untuk melakukan pemutakhiran sistem operasi pada instans dengan setidaknya 2 vCPU dan RAM 4 GB. Otomatisasi membuat AMI dari instance dan kemudian meluncurkan instance sementara dari AMI yang baru dibuat di SubnetId yang Anda tentukan. Grup keamanan yang terkait dengan instans asli Anda diterapkan ke instans sementara. Otomatisasi kemudian melakukan peningkatan di tempat ke TargetWindowsVersion pada instance sementara. Untuk memutakhirkan instans R2 Windows Server 2008 Anda ke Windows

Server 2016, 2019, atau 2022, peningkatan di tempat dilakukan dua kali karena secara langsung memutakhirkan Windows Server 2008 R2 ke Windows Server 2016, 2019, atau 2022 tidak didukung. Otomatisasi juga memperbarui atau menginstal AWS driver yang diperlukan oleh instance sementara. Setelah pemutakhiran, otomatisasi membuat AMI baru dari instance sementara dan kemudian menghentikan instance sementara.

Anda dapat menguji fungsionalitas aplikasi dengan meluncurkan instance pengujian dari AMI yang ditingkatkan di Amazon Virtual Private Cloud (Amazon VPC). Setelah Anda menyelesaikan pengujian, dan sebelum Anda melakukan peningkatan lain, jadwalkan waktu henti aplikasi sebelum sepenuhnya beralih ke AMI yang ditingkatkan.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis Dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows Server 2008 R2, 2012 R2, 2016, atau 2019 edisi Standard dan Datacenter

Prasyarat

- TLS versi 1.2.
- Pastikan bahwa SSM Agent diinstal pada instans Anda. Untuk informasi selengkapnya, lihat [Menginstal dan mengonfigurasi Agen SSM pada instans EC2](#) untuk Windows Server.
- Windows PowerShell 3.0 atau yang lebih baru harus diinstal pada instans Anda.
- Untuk instans yang bergabung dengan domain Microsoft Active Directory, sebaiknya tentukan SubnetId yang tidak memiliki konektivitas ke kontroler domain Anda untuk membantu menghindari konflik nama host.
- Subnet instance harus memiliki konektivitas keluar ke internet, yang menyediakan akses ke Layanan AWS seperti Amazon S3 dan akses untuk mengunduh tambalan dari Microsoft. Persyaratan ini terpenuhi jika subnet adalah subnet publik dan instans memiliki alamat IP publik, atau jika subnet adalah subnet pribadi dengan rute yang mengirimkan lalu lintas internet ke perangkat NAT publik.

- Otomasi ini hanya berfungsi dengan Windows Server instans 2008 R2, 2012 R2, 2016, dan 2019.
- Konfigurasi Windows Server instance dengan profil instans AWS Identity and Access Management (IAM) yang menyediakan izin yang diperlukan untuk Systems Manager. Untuk informasi selengkapnya, lihat [Buat profil instans IAM untuk Systems Manager](#).
- Verifikasi bahwa instans memiliki 20 GB ruang disk kosong di disk boot.
- Jika instance tidak menggunakan lisensi Windows AWS yang disediakan, tentukan ID snapshot Amazon EBS yang menyertakan media penginstalan Windows Server 2012 R2. Untuk melakukannya:
  - Verifikasi bahwa instans EC2 menjalankan Windows Server 2012 atau yang lebih baru.
  - Buat volume EBS 6 GB di Availability Zone yang sama di mana instans berjalan. Lampirkan volume ke instans. Pasang, misalnya, sebagai drive D.
  - Klik kanan ISO dan pasang ke instans sebagai, misalnya, drive E.
  - Salin konten ISO dari drive E:\ ke drive D:\
  - Buat snapshot EBS dari volume 6 GB yang dibuat pada langkah 2 di atas.

## Batasan

Otomatisasi ini tidak mendukung peningkatan pengontrol domain Windows, cluster, atau sistem operasi desktop Windows. Otomatisasi ini juga tidak mendukung instans EC2 Windows Server dengan peran berikut diinstal.

- Host Sesi Desktop Jarak Jauh (RDSH)
- Broker Koneksi Desktop Jarak Jauh (RDCB)
- Host Virtualisasi Desktop Jarak Jauh (RDVH)
- Akses Web Desktop Jarak Jauh (RDWA)

## Parameter

- `AlternativeKeyPairName`

Jenis: String

Deskripsi: (Opsional) Nama key pair alternatif untuk digunakan selama proses upgrade. Ini berguna dalam situasi di mana key pair yang ditetapkan ke instance asli tidak tersedia. Jika instance asli tidak diberi key pair, Anda harus menentukan nilai untuk parameter ini.

- `BYOL WindowsMediaSnapshotId`

Jenis: String

Deskripsi: (Opsional) ID snapshot Amazon EBS untuk disalin yang menyertakan media instalasi Windows Server 2012R2. Diperlukan hanya jika Anda memutakhirkan instance BYOL.

- `IamInstanceProfile`

Jenis: String

Deskripsi: (Wajib) Nama profil instans IAM yang memungkinkan Systems Manager mengelola instans.

- `InstanceId`

Jenis: String

Deskripsi: (Diperlukan) Instans EC2 yang menjalankan Windows Server 2008 R2, 2012 R2, 2016, atau 2019.

- `KeepPreUpgradeImageBackUp`

Jenis: String

Deskripsi: (Opsional) Jika disetel Benar, Otomasi tidak akan menghapus AMI yang dibuat dari instans EC2 sebelum upgrade. Jika disetel ke True, maka Anda harus menghapus AMI. Secara default, AMI dihapus.

- `SubnetId`

Jenis: String

Deskripsi: (Wajib) Ini adalah subnet untuk proses pemutakhiran dan tempat instans EC2 sumber Anda berada. Verifikasi bahwa subnet memiliki konektivitas keluar ke AWS layanan, Amazon S3, dan Microsoft (untuk mengunduh tambalan).

- `TargetWindowsVersion`

Jenis: String

Deskripsi: (Diperlukan) Pilih versi Windows target.

Bawaan: 2022

- `RebootInstanceBeforeTakingImage`

Jenis: String

Deskripsi: (Opsional) Jika disetel True, Automation akan me-reboot instance sebelum membuat AMI pra-upgrade. Secara default, Automation tidak reboot sebelum upgrade.

## AWSEC2-ConfigureSTIG

Security Technical Implementation Guides (STIGs) adalah standar pengerasan konfigurasi yang dibuat oleh Badan Sistem Informasi Pertahanan (DISA) untuk mengamankan sistem informasi dan perangkat lunak. Untuk membuat sistem Anda sesuai dengan standar STIG, Anda harus menginstal, mengonfigurasi, dan menguji berbagai pengaturan keamanan.

Amazon EC2 menyediakan runbook Systems ManagerAWSEC2-ConfigureSTIG, yang dapat Anda gunakan untuk menerapkan pengaturan STIG ke instans. Dokumen ini membantu Anda membuat gambar yang sesuai dengan standar STIG dengan cepat. Dokumen STIG Systems Manager memindai kesalahan konfigurasi dan menjalankan skrip remediasi. Ini juga menginstal InstallRoot dari Departemen Pertahanan (DoD) pada AMI Windows untuk menginstal dan memperbarui sertifikat DoD dan untuk menghapus sertifikat yang tidak perlu untuk mempertahankan kepatuhan STIG. Tidak ada biaya tambahan untuk menggunakan dokumen STIG Systems Manager.

### Important

Dengan beberapa pengecualian, komponen pengerasan STIG yang diunduh dokumen Systems Manager tidak menginstal paket pihak ketiga. Jika paket pihak ketiga sudah diinstal pada instance, dan jika ada STIG terkait yang didukung Amazon EC2 untuk paket itu, STIG tersebut diterapkan.

Halaman ini mencantumkan semua STIG yang didukung Amazon EC2 yang diterapkan komponen pengerasan STIG pada instans EC2 Anda.

Anda dapat memilih kategori kepatuhan STIG mana yang akan diterapkan.

Tingkat kepatuhan

- Tinggi (Kategori I)

Risiko paling parah. Termasuk kerentanan apa pun yang dapat mengakibatkan hilangnya kerahasiaan, ketersediaan, atau integritas.



- Sedang (Kategori II)

Termasuk kerentanan apa pun yang dapat mengakibatkan hilangnya kerahasiaan, ketersediaan, atau integritas tetapi risikonya dapat dikurangi.

- Rendah (Kategori III)

Termasuk kerentanan apa pun yang menurunkan tindakan untuk melindungi terhadap hilangnya kerahasiaan, ketersediaan, atau integritas.

## Topik

- [Unduhan komponen pengerasan STIG](#)
- [Pengaturan STIG Windows](#)
- [Riwayat versi Windows STIG](#)
- [Pengaturan STIG Linux](#)
- [Riwayat versi Linux STIG](#)

## Unduhan komponen pengerasan STIG

Amazon mengelompokkan komponen pengerasan STIG bersama-sama ke dalam bundel terkait sistem operasi untuk setiap rilis. Bundel adalah file arsip yang sesuai untuk sistem operasi target tempat mereka mengunduh dan menjalankannya. Bundel komponen Linux disimpan sebagai file TAR (ekstensi file.tgz). Bundel komponen Windows disimpan sebagai file ZIP (ekstensi file.zip).

Amazon menyimpan bundel komponen di STIG bucket Image Builder S3 di masing-masing Wilayah AWS. Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.

Pola dan contoh untuk jalur penyimpanan komponen dan nama file bundel adalah sebagai berikut:

Jalur penyimpanan komponen

```
s3://aws-windows-downloads-<region>/STIG/<bundle file name>
```

Variabel jalur komponen

region

Wilayah AWS (Setiap Wilayah memiliki ember komponennya sendiri.)

## bundle file name

Formatnya adalah <os bundle name>\_ <YYYY>\_Q <quarter>[\_<release>]. <file extension>. Perhatikan bahwa nama memiliki garis bawah antara node, bukan periode.

### os bundle name

Awalan nama standar untuk bundel sistem operasi adalah salah satu LinuxAWSConfigureSTIG atauAWSConfigureSTIG. Untuk mempertahankan kompatibilitas mundur, unduhan untuk Windows tidak menyertakan awalan platform.

### YYYY

Empat digit tahun rilis.

### quarter

Mengidentifikasi kuartal tahun: 1, 2, 3, atau 4.

### release

Jumlah tambahan yang dimulai dari satu, dan bertambah satu untuk setiap rilis baru. Rilis ini tidak termasuk untuk rilis pertama dalam seperempat dan hanya ditambahkan untuk rilis berikutnya.

### file extension

Format file terkompresi tgz (Linux) atau zip (Windows).

### Contoh nama file bundel

- LinuxAWSConfigureSTIG\_2023\_Q1\_2.tgz
- AWSConfigureSTIG\_2022\_Q4.zip

## Pengaturan STIG Windows

Amazon EC2 Windows STIG AMI dan komponen pengerasan dirancang untuk server mandiri dan menerapkan Kebijakan Grup Lokal. Komponen yang sesuai dengan STIG diinstal InstallRoot dari Departemen Pertahanan (DoD) pada AMI Windows untuk mengunduh, menginstal, dan memperbarui sertifikat DoD. Mereka juga menghapus sertifikat yang tidak perlu untuk mempertahankan kepatuhan STIG. Saat ini, Amazon EC2 mendukung baseline STIG untuk versi Windows Server berikut: 2012 R2, 2016, 2019, dan 2022.

Bagian ini mencantumkan pengaturan STIG saat ini yang didukung Amazon EC2 untuk infrastruktur Windows Anda, diikuti oleh log riwayat versi.

Anda dapat menerapkan pengaturan STIG rendah, sedang, atau tinggi.

### Windows STIG Rendah (Kategori III)

Daftar berikut berisi pengaturan STIG yang didukung Amazon EC2 ke infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewati setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkap STIG Windows, lihat [Perpustakaan Dokumen STIG](#). Untuk informasi tentang cara melihat daftar lengkap, lihat [Alat Melihat STIG](#).

- Windows Server 2022 STIG Versi 1 Rilis 1

V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363, dan V-254481

- Windows Server 2019 STIG Versi 2 Rilis 5

V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871, dan V-205923

- Windows Server 2016 STIG Versi 2 Rilis 5

V-224916, V-224917, V-224918, V-224919, V-224931, V-224942, dan V-225060

- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5

V-225537, V-225536, V-225526, V-225525, V-225514, V-225511, V-225490, V-225489, V-225488, V-225487, V-225485, V-225483, V-225482, V-225481, V-225425V-225479, V-225476, V-225473, V-225468, V-225462, V-225460, V-225459, V-225412, V-225394, V-225392, V-225376, V-225363, V-225362, V-225360, V-225359, V-225359 358, V-225357, V-225355, V-225343, V-225342, V-225336, V-225335, V-225334, V-225333, V-225332, V-225331, V-225330, V-225328, V-225327, V-225324, V-225319, V-225319, V-225319, 225318, dan V-225250

- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2

Tidak ada pengaturan STIG yang berlaku untuk kerentanan Microsoft .NET Framework untuk Kategori III.

- Windows Firewall STIG Versi 2 Rilis 1

V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007, dan V-242008

- Internet Explorer 11 STIG Versi 2 Rilis 3

V-46477, V-46629, dan V-97527

- Microsoft Edge STIG Versi 1 Rilis 6 (hanya Windows Server 2022)

V-235727, V-235731, V-235751, V-235752, dan V-235765

## Windows STIG Medium (Kategori II)

Daftar berikut berisi pengaturan STIG yang didukung Amazon EC2 ke infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewati setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkap STIG Windows, lihat [Perpustakaan Dokumen STIG](#). Untuk informasi tentang cara melihat daftar lengkap, lihat [Alat Melihat STIG](#).

### Note

Kategori Windows STIG Medium mencakup semua pengaturan pengerasan STIG terdaftar yang berlaku untuk Windows STIG rendah (Kategori III), selain pengaturan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II.

- Windows Server 2022 STIG Versi 1 Rilis 1

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori III (Rendah), ditambah:

V-254247, V-254265, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254288, V-254288 V-254290, V-254291, V-254292, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V-254310, V-254311, V-254312, V-254312, V-254312, V-254313, V-254314, V-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254330, V-254331, V-254332, V-254333, V-254334, V-254339, V-254341, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254358, V-254359, V-254360, V-254361, V-254362, V-254364, V-254365, V-254366, V-254366 367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380,

V-254382, V-254383, V-254431, V-254432, V-254433, V-254433, V-254433, V-254434, V-254435, V-254436, V-254438, V-254439, V-254442, V-254443, V-254444, V-254445, V-254449, V-254450, V-254451, V-254452, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254476, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254484, V-254486, V-254487, V-254488, V-254488, V-254488 4489, V-254490, V-254493, V-254494, V-254495, V-254497, V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254507, V-254508, V-254509, V-254510, V-254511, dan V-254512

- Windows Server 2019 STIG Versi 2 Rilis 5

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori III (Rendah), ditambah:

V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205643, V-205648, V-205649, V-205650, V-205651, V-205651, V-205652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205679, V-205680, V-205681, V-205683, V-205684, V-205685, V-205685, V-205685 V-205687, V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205720, V-205722, V-205729, V-205730, V-205733, V-205747, V-205751, V-205752, V-205754, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205764, V-205766, V-205767, V-205768, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205781, V-205782, V-205783, V-205795, V-205796, V-205797, V-205797, V-205797, V-205797, V-205797, V-205797, V-205797 98, V-205801, V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205827, V-205828, V-205830, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838, V-205839, V-205840, V-205841, V-205861, V-205863, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205924, V-205925, dan V-236001

- Windows Server 2016 STIG Versi 2 Rilis 5

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori III (Rendah), ditambah:

V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224870, V-224871, V-224871, V-224871, V-224871, V-224871

V-224872, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224894, V-224894, V-224894, V-224894 24895, V-224896, V-224897, V-224898, V-224899, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224910, V-224910, V-224910 224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224946, V-224946, V-224946, V-224946 47, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040, V-225041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225061, V-225062, V-225062, V-225063, V-225064, V-225066, V-225067, V-225068, V-225069, V-225072, V-225072, V-225072 25073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093 dan V-236000

- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori III (Rendah), ditambah:

V-225574, V-225573, V-225572, V-225571, V-225570, V-225569, V-225568, V-225567, V-225566, V-225565, V-225564, V-225563, V-225562, V-225561, V-225560, V-2552560 9, V-225558, V-225557, V-225555, V-225554, V-225553, V-225551, V-225550, V-225549, V-225548, V-225546, V-225545, V-225544, V-225543, V-225542, V-225541, V-225541, V-225541, V-225541, V-225541, V-225541 540, V-225539, V-225538, V-225535, V-225534, V-225533, V-225532, V-225531, V-225530, V-225529, V-225528, V-225527, V-225524, V-225523, V-225522, V-225521, V-225521, V-225521, V-225520, V-225519, V-225518, V-225517, V-225516, V-225515, V-225513, V-225510, V-225509, V-225508, V-225506, V-225504, V-225503, V-225502, V-225501, V-225500, V-225494, V-225486, V-225478, V-225477, V-225475, V-225474, V-225472, V-225471, V-225470, V-225469, V-225464, V-225463, V-225461, V-225458, V-225457, V-225456, V-225455, V-225454, V-225453, V-225452, V-225448, V-225443, V-225442, V-225441, V-225415, V-225415, V-225415, V-225415 414, V-225413, V-225411, V-225410, V-225409, V-225408, V-225407, V-225406, V-225405, V-225404, V-225402, V-225401, V-225398, V-225397, V-225395, V-225395, V-225395, V-225395, V-225395 25393, V-225391, V-225389, V-225386, V-225385, V-225384, V-225383, V-225382, V-225381, V-225380, V-225379, V-225378, V-225377, V-225375, V-225374, V-225373, V-225372, V-225371, V-225370, V-225369, V-225368, V-225367, V-225356, V-225353,

V-225352, V-235252, V-23525252, V-23525252 1, V-225350, V-225349, V-225348, V-225347, V-225346, V-225345, V-225344, V-225341, V-225340, V-225339, V-225338, V-225337, V-225329, V-225326, V-225325, V-225325, V-225325, V-225325, V-225325 317, V-225316, V-225315, V-225314, V-225305, V-225304, V-225303, V-225302, V-225301, V-225300, V-225299, V-225298, V-225297, V-225296, V-225295, V-225294, V-225294, V-225294, V-225294, V-225294 293, V-225292, V-225291, V-225290, V-225289, V-225288, V-225287, V-225286, V-225285, V-225284, V-225283, V-225282, V-225281, V-225280, V-225279, V-225278, V-225277, V-225276, V-225275, V-225273, V-225272, V-225271, V-225270, V-225269, V-225268, V-225267, V-225266, V-225265, V-225264, V-225263, V-225261, V-225260, V-225259, dan V-225239

- Microsoft .NET Framework STIG 4.0 Versi 2 Rilis 2

Termasuk semua setelan penguatan STIG yang didukung Amazon EC2 untuk kerentanan Kategori III (Rendah), ditambah:

V-225238

- Windows Firewall STIG Versi 2 Rilis 1

Termasuk semua setelan penguatan STIG yang didukung Amazon EC2 untuk kerentanan Kategori III (Rendah), ditambah:

V-241989, V-241990, V-241991, V-241993, V-241998, dan V-242003

- Internet Explorer 11 STIG Versi 2 Rilis 3

Termasuk semua setelan penguatan STIG yang didukung Amazon EC2 untuk kerentanan Kategori III (Rendah), ditambah:

V-46473, V-46475, V-46481, V-46483, V-46501, V-46507, V-46509, V-46511, V-46513, V-46515, V-46517, V-46521, V-46523, V-46525, V-46543, V-46545, V-46547, V-46549, V-46553, V-46555, V-46573, V-46575, V-46577, V-46579, V-46581, V-46583, V-46587, V-46589, V-46591, V-46593, V-46597, V-46599, V-46601, V-46603, V-46605, V-46607, V-46609, V-46660 V-46617, V-46619, V-46621, V-46625, V-46633, V-46635, V-46637, V-46639, V-46641, V-46643, V-46645, V-46647, V-46649, V-46653, V-46663, V-46665, V-46669, V-46681, V-46681, V-46681, V-46681, V-46681 685, V-46689, V-46691, V-46693, V-46695, V-46701, V-46705, V- 46709, V-46711, V-46713, V-46715, V-46717, V-46719, V-46721, V-46723, V-46725, V-46727, V-46729, V-46731, V-46733, V-46779, V-46787, V-46789, V-46791, V-46797, V-46799, V-46801, V-46807, V-46811, V-46815, V-46819, V-46829, V-46841, V-46847, V-46849, V-46853, V-46857, V-46859, V-46861, V-46865, V-46879, V-46883, V-46885, V-46889, V-46893, V-46895, V-46897, V-46903, V-46907, V-46921, V-46927, V-46939, V-46975, V-46981, V-46987, V-46995, V-46997, V-46999, V-47003, V-47005,

V-47009, V-647009 11, V-64713, V-64715, V-64717, V-64719, V-64721, V-64723, V-64725, V-64729, V-72757, V-72759, V-72761, V-72763, V-75169, dan V-75171

- Microsoft Edge STIG Versi 1 Rilis 6 (hanya Windows Server 2022)

V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235768, V-235768, V-235768 69, V-235770, V-235771, V-235772, V-235773, V-235774, dan V-246736

- Defender STIG Versi 2 Rilis 4 (hanya Windows Server 2022)

V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213439, V-213440, V-213441, V-213442, V-213442, V-213442 43, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465, dan V-213466

## Windows STIG Tinggi (Kategori I)

Daftar berikut berisi pengaturan STIG yang didukung Amazon EC2 ke infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewati setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkap STIG Windows, lihat [Perpustakaan Dokumen STIG](#). Untuk informasi tentang cara melihat daftar lengkap, lihat [Alat Melihat STIG](#).

### Note

Kategori Windows STIG High mencakup semua pengaturan pengerasan STIG terdaftar yang berlaku untuk kategori Windows STIG Medium dan Low, selain pengaturan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori I.

- Windows Server 2022 STIG Versi 1 Rilis 1

V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475, dan V-254500



- Windows Server 2019 STIG Versi 2 Rilis 5

Termasuk semua setelan penguatan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914, dan V-205919

- Windows Server 2016 STIG Versi 2 Rilis 5

Termasuk semua setelan penguatan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054, dan V-225079

- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5

Termasuk semua setelan penguatan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-225556, V-225552, V-225547, V-225507, V-225505, V-225498, V-225497, V-225496, V-225493, V-225492, V-225491, V-225449, V-225399, V-225396, V-2253256, V-23256 90, V-225366, V-225365, V-225364, V-225354, dan V-225274

- Microsoft .NET Framework STIG 4.0 Versi 2 Rilis 2

Termasuk semua pengaturan penguatan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah) untuk Microsoft .NET Framework. Tidak ada pengaturan STIG tambahan yang berlaku untuk kerentanan Kategori I.

- Windows Firewall STIG Versi 2 Rilis 1

Termasuk semua setelan penguatan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-241992, V-241997, dan V-242002

- Internet Explorer 11 STIG Versi 2 Rilis 3

Termasuk semua pengaturan penguatan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah) untuk Internet Explorer 11. Tidak ada pengaturan STIG tambahan yang berlaku untuk kerentanan Kategori I.

- Microsoft Edge STIG Versi 1 Rilis 6 (hanya Windows Server 2022)

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-235758 dan V-235759

- Defender STIG Versi 2 Rilis 4 (hanya Windows Server 2022)

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

V-213426, V-213452, dan V-213453

## Riwayat versi Windows STIG

Bagian ini mencatat riwayat versi komponen Windows untuk pembaruan STIG triwulanan. Untuk melihat perubahan dan versi yang diterbitkan selama seperempat, pilih judul untuk memperluas informasi.

Perubahan Q1 2024 - 23/02/2024 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal pertama 2024.

Perubahan Q4 2023 - 12/07/2023 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal keempat 2023.

Perubahan Q3 2023 - 10/04/2023 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal ketiga 2023.

Perubahan Q2 2023 - 05/03/2023 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal kedua 2023.

Perubahan Q1 2023 - 27/03/2023 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal pertama 2023.

2022 Perubahan Q4 - 02/01/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis Q4 2022 sebagai berikut:

## STIG-Build-Windows-versi rendah 2022.4.0

- Windows Server 2022 STIG Versi 1 Rilis 1
- Windows Server 2019 STIG Versi 2 Rilis 5
- Windows Server 2016 STIG Versi 2 Rilis 5
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 2 Rilis 3
- Microsoft Edge STIG Versi 1 Rilis 6 (hanya Windows Server 2022)

## STIG-Build-Windows-versi menengah 2022.4.0

- Windows Server 2022 STIG Versi 1 Rilis 1
- Windows Server 2019 STIG Versi 2 Rilis 5
- Windows Server 2016 STIG Versi 2 Rilis 5
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 2 Rilis 3
- Microsoft Edge STIG Versi 1 Rilis 6 (hanya Windows Server 2022)
- Defender STIG Versi 2 Rilis 4 (hanya Windows Server 2022)

## STIG-Build-Windows-versi tinggi 2022.4.0

- Windows Server 2022 STIG Versi 1 Rilis 1
- Windows Server 2019 STIG Versi 2 Rilis 5
- Windows Server 2016 STIG Versi 2 Rilis 5
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 5
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 2
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 2 Rilis 3

- Microsoft Edge STIG Versi 1 Rilis 6 (hanya Windows Server 2022)
- Defender STIG Versi 2 Rilis 4 (hanya Windows Server 2022)

2022 Perubahan Q3 - 30/09/2022 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal ketiga 2022.

2022 Perubahan Q2 - 08/02/2022:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis Q2 2022.

STIG-Build-Windows-Low versi 1.5.0

- Windows Server 2019 STIG Versi 2 Rilis 4
- Windows Server 2016 STIG Versi 2 Rilis 4
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

STIG-Build-Windows-Medium versi 1.5.0

- Windows Server 2019 STIG Versi 2 Rilis 4
- Windows Server 2016 STIG Versi 2 Rilis 4
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

STIG-Build-Windows-High versi 1.5.0

- Windows Server 2019 STIG Versi 2 Rilis 4
- Windows Server 2016 STIG Versi 2 Rilis 4
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3

- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

2022 Perubahan Q1 - 08/02/2022 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Windows STIGS untuk rilis kuartal pertama 2022.

2021 Perubahan Q4 - 12/20/2021:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal keempat 2021.

STIG-Build-Windows-Low versi 1.5.0

- Windows Server 2019 STIG Versi 2 Rilis 3
- Windows Server 2016 STIG Versi 2 Rilis 3
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

STIG-Build-Windows-Medium versi 1.5.0

- Windows Server 2019 STIG Versi 2 Rilis 3
- Windows Server 2016 STIG Versi 2 Rilis 3
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

STIG-Build-Windows-High versi 1.5.0

- Windows Server 2019 STIG Versi 2 Rilis 3
- Windows Server 2016 STIG Versi 2 Rilis 3
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 3

- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 2 Rilis 1
- Internet Explorer 11 STIG Versi 1 Rilis 19

2021 Perubahan Q3 - 09/30/2021:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal ketiga 2021.

STIG-Build-Windows-Low versi 1.4.0

- Windows Server 2019 STIG Versi 2 Rilis 2
- Windows Server 2016 STIG Versi 2 Rilis 2
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 2
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 1 Rilis 7
- Internet Explorer 11 STIG Versi 1 Rilis 19

STIG-Build-Windows-Medium versi 1.4.0

- Windows Server 2019 STIG Versi 2 Rilis 2
- Windows Server 2016 STIG Versi 2 Rilis 2
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 2
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 1 Rilis 7
- Internet Explorer 11 STIG Versi 1 Rilis 19

STIG-Build-Windows-High versi 1.4.0

- Windows Server 2019 STIG Versi 2 Rilis 2
- Windows Server 2016 STIG Versi 2 Rilis 2
- Windows Server 2012 R2 MS STIG Versi 3 Rilis 2
- Microsoft .NET Framework 4.0 STIG Versi 2 Rilis 1
- Windows Firewall STIG Versi 1 Rilis 7

- Internet Explorer 11 STIG Versi 1 Rilis 19

## Pengaturan STIG Linux

Bagian ini berisi informasi tentang pengaturan penerapan STIG Linux yang didukung Amazon EC2, diikuti oleh log riwayat versi. Jika distribusi Linux tidak memiliki pengaturan penerapan STIG sendiri, Amazon EC2 menggunakan pengaturan RHEL. Pengaturan penerapan STIG yang didukung berlaku untuk AMI Amazon EC2 Linux dan komponen berdasarkan distribusi Linux, sebagai berikut:

- Red Hat Enterprise Linux (RHEL) 7 pengaturan STIG
  - RHEL 7
  - CentOS 7
  - Amazon Linux 2 (AL2)
- Pengaturan RHEL 8 STIG
  - RHEL 8
  - CentOS 8
  - Amazon Linux 2023 (AL 2023)

### Linux STIG Rendah (Kategori III)

Daftar berikut berisi pengaturan STIG yang didukung Amazon EC2 ke infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewati setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan penerapan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkapnya, lihat [Pustaka Dokumen STIGs](#). Untuk informasi tentang cara melihat daftar lengkap, lihat [Alat Melihat STIG](#).

### RHEL 7 STIG Versi 3 Rilis 14

- RHEL 7/CentOS 7  
  
V-204452, V-204576, dan V-204605
- AL2  
  
V-204452, V-204576, dan V-204605

## RHEL 8 STIG Versi 1 Rilis 13

- RHEL 8/CentOS 8/AL 2023

V-230241, V-244527, V-230269, V-230270, V-230285, V-230253, V-230346, V-230381, V-230395, V-230468, V-230469, V-230491, V-230485, V-230486, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499, dan V-230281

## Ubuntu 18.04 STIG Versi 2 Rilis 13

V-219172, V-219173, V-219174, V-219175, V-219210, V-219164, V-219165, V-219178, V-219180, V-219301, V-219163, V-219332, V-219327, dan V-219333

## Ubuntu 20.04 STIG Versi 1 Rilis 11

V-238202, V-238234, V-238235, V-238237, V-238323, V-238373, V-238221, V-238222, V-238223, V-238223, V-238224, V-238226, V-238362, V-238357, dan V-238308

## Linux STIG Medium (Kategori II)

Daftar berikut berisi pengaturan STIG yang didukung Amazon EC2 ke infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewati setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkapnya, lihat [Pustaka Dokumen STIGs](#). Untuk informasi tentang cara melihat daftar lengkap, lihat [Alat Melihat STIG](#).

### Note

Kategori Linux STIG Medium mencakup semua pengaturan pengerasan STIG terdaftar yang berlaku untuk Linux STIG Low (Kategori III), selain pengaturan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II.

## RHEL 7 STIG Versi 3 Rilis 14

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori III (Rendah), ditambah:



- RHEL 7/CentOS 7

V-204585, V-204490, V-204491, V-255928, V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204415, V-204422, V-204423, V-204423, V-204423, V-204423, V-204423 27, V-204416, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204587, V-204588, V-204589, V-204591, V-204592, V-204593, V-204596, V-204596, V-204597, V-204597, V-204597, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204568, V-204572, V-204584, V-20448 609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204450, V-204451, V-204619, V-204619, V-204579, V-204631, V-204633, dan V-256970

- AL2:

V-204585, V-204490, V-204491, V-255928, V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204415, V-204422, V-204423, V-204423, V-204423, V-204423, V-204423 27, V-204416, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204587, V-204588, V-204589, V-204591, V-204592, V-204593, V-204596, V-204596, V-204597, V-204597, V-204597, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204568, V-204572, V-204584, V-20448 609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204450, V-204451, V-204619, V-204619, V-204579, V-204631, V-204633, dan V-256970

## RHEL 8 STIG Versi 1 Rilis 13

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori III (Rendah), ditambah:

- RHEL 8/CentOS 8/AL 2023

V-230257, V-230258, V-230259, V-230550, V-230248, V-230249, V-230250, V-230245, V-230246, V-230247, V-230397, V-230399, V-230400, V-230401, V-230228, V-230298, V-230298, V-230298, V-230298, V-230387, V-230231, V-230233, V-230324, V-230365, V-230370, V-230378, V-230383, V-230236, V-230314, V-230315, V-244523, V-230266, V-230267, V-230268, V-230280, V-230280, V-230280 30310, V-230311, V-230312, V-230502, V-230532, V-230535, V-230536, V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230549, V-244550, V-244551, V-244552, V-244553, V-244554, V-250317, V-251718, V-230237, V-230313, V-230356, V-230357, V-230358, V-230359, V-230360, V-230361, V-230362, V-230363, V-230368, V-230369, V-230375, V-230376, V-230376, V-230377, V-244524, V-244533, V-251713, V-251717, V-251714, V-251715, V-251716, V-230332, V-230334, V-230336, V-230338, V-230340, V-230342, V-230344, V-230333, V-230335, V-230335, V-230337, V-230339, V-230341, V-230343, V-230345, V-230240, V-230282, V-250315, V-250316, V-230255, V-230277, V-230278, V-230348, V-230353, V-230386, V-230390, V-230390, V-230392, V-230394, V-230396, V-230393, V-230398, V-230402, V-230403, V-230404, V-230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, V-230418, V-230419, V-230421, V-230422, V-230423, V-230424, V-230424, V-230424, V-230424, V-230424, V-230424 25, V-230426, V-230427, V-230428, V-230429, V-230430, V-230431, V-230432, V-230433, V-230434, V-230435, V-230436, V-230437, V-230438, V-230439, V-230444, V-230444, V-230444, V-230444, V-230444 30446, V-230447, V-230448, V-230449, V-230455, V-230456, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V-230471, V-230472, V-230473, V-230474, V-230480, V-230483, V-244542, V-230503, V-230244, V-230286, V-230287, V-230288, V-230290, V-230291, V-230296, V-230330, V-230382, V-230526, V-230527, V-230555, V-230556, V-244526, V-244528, V-237642, V-237643, V-251711, V-230238, V-230239, V-230273, V-230275, V-230275, V-230275 478, V-230488, V-230489, V-230559, V-230560, V-230561, V-237640, dan V-256974

## Ubuntu 18.04 STIG Versi 2 Rilis 13

V-219188, V-219190, V-219191, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219303, V-219326, V-219328, V-219330, V-219342, V-219189, V-219192, V-219193, V-219194, V-219315, V-219195, V-219196, V-219197, V-219213, V-219214, V-219215, V-219215, V-219215, V-219215, V-219215, V-219215 16, V-219217, V-219218, V-219219, V-219220, V-219221, V-219222, V-219223, V-219224, V-219227, V-219228, V-219229, V-219231, V-219232, V-219233, V-219223, V-219233, V-219229 34, V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243, V-219244, V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267,

V-219268, V-219269, V-219270, V-219271, V-219272, V-219273, V-219274, V-219275, V-219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219297, V-219298, V-219299, V-219300, V-219309, V-219310, V-219311, V-219312, V-233779, V-233780, V-255906, V-219336, V-219338, V-219344, V-219181, V-219184, V-219186, V-219155, V-219156, V-219160, V-219306, V-219166, V-219176, V-219339, V-219331, V-219337, dan V-219335

### Ubuntu 20.04 STIG Versi 1 Rilis 11

V-238205, V-238207, V-238329, V-238337, V-238339, V-238340, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238351, V-238352, V-238376, V-238377, V-238378, V-238209, V-238325, V-238330, V-238333, V-238369, V-238338, V-238341, V-238342, V-238343, V-238324, V-238353, V-238228, V-238225, V-238227, V-238299, V-238238, V-238239, V-238240, V-238241, V-238242, V-238244, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238253, V-238253, V-238253, V-238253, V-238253 8254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238300, V-238301, V-238302, V-238304, V-238309, V-238310, V-238315, V-238316, V-238318, V-238319, V-238320, V-251505, V-23805, V-231505, V-23832 8360, V-238211, V-238212, V-238213, V-238216, V-238220, V-255912, V-238355, V-238236, V-238303, V-238358, V-238356, V-238359, V-238370, dan V-238334

### Linux STIG Tinggi (Kategori I)

Daftar berikut berisi pengaturan STIG yang didukung Amazon EC2 ke infrastruktur Anda. Jika setelan yang didukung tidak berlaku untuk infrastruktur Anda, Amazon EC2 melewati setelan itu, dan melanjutkan. Misalnya, beberapa pengaturan pengerasan STIG mungkin tidak berlaku untuk server mandiri. Kebijakan khusus organisasi juga dapat memengaruhi pengaturan mana yang berlaku, seperti persyaratan bagi administrator untuk meninjau setelan dokumen.

Untuk daftar lengkapnya, lihat [Pustaka Dokumen STIGs](#). Untuk informasi tentang cara melihat daftar lengkap, lihat [Alat Melihat STIG](#).

#### Note

Kategori Linux STIG High mencakup semua pengaturan pengerasan STIG terdaftar yang berlaku untuk kategori Linux STIG Medium dan Low, selain pengaturan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori I.

## RHEL 7 STIG Versi 3 Rilis 14

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

- RHEL 7/CentOS 7

V-204425, V-204594, V-204455, V-204424, V-204442, V-204443, V-204447, V-204448, V-204502, V-204620, dan V-204621

- AL2:

V-204425, V-204594, V-204455, V-204424, V-204442, V-204443, V-204447, V-204448, V-204502, V-204620, dan V-204621

## RHEL 8 STIG Versi 1 Rilis 13

Termasuk semua setelan pengerasan STIG yang didukung Amazon EC2 untuk kerentanan Kategori II dan III (Sedang dan Rendah), ditambah:

- RHEL 8/CentOS 8/AL 2023

V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533, dan V-230558

## Ubuntu 18.04 STIG Versi 2 Rilis 13

V-219157, V-219158, V-219177, V-219212 V-219308, V-219314, V-219316, dan V-251507

## Ubuntu 20.04 STIG Versi 1 Rilis 11

V-238218, V-238219, V-238201, V-238326, V-238327, V-238380 dan V-251504

## Riwayat versi Linux STIG

Bagian ini mencatat riwayat versi komponen Linux untuk pembaruan STIG triwulanan. Untuk melihat perubahan dan versi yang diterbitkan selama seperempat, pilih judul untuk memperluas informasi.

Perubahan Q1 2024 - 02/06/2024:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal pertama 2024 sebagai berikut:

## STIG-Build-Linux-versi rendah 2024.1.x

- RHEL 7 STIG Versi 3 Rilis 14
- RHEL 8 STIG Versi 1 Rilis 13
- Ubuntu 18.04 STIG Versi 2 Rilis 13
- Ubuntu 20.04 STIG Versi 1 Rilis 11

## STIG-build-linux-versi menengah 2024.1.x

- RHEL 7 STIG Versi 3 Rilis 14
- RHEL 8 STIG Versi 1 Rilis 13
- Ubuntu 18.04 STIG Versi 2 Rilis 13
- Ubuntu 20.04 STIG Versi 1 Rilis 11

## STIG-Build-Linux-versi tinggi 2024.1.x

- RHEL 7 STIG Versi 3 Rilis 14
- RHEL 8 STIG Versi 1 Rilis 13
- Ubuntu 18.04 STIG Versi 2 Rilis 13
- Ubuntu 20.04 STIG Versi 1 Rilis 11

Perubahan Q4 2023 - 12/07/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal keempat 2023 sebagai berikut:

## STIG-Build-Linux-versi rendah 2023.4.x

- RHEL 7 STIG Versi 3 Rilis 13
- RHEL 8 STIG Versi 1 Rilis 12
- Ubuntu 18.04 STIG Versi 2 Rilis 12
- Ubuntu 20.04 STIG Versi 1 Rilis 10

## STIG-build-linux-versi menengah 2023.4.x

- RHEL 7 STIG Versi 3 Rilis 13

- RHEL 8 STIG Versi 1 Rilis 12
- Ubuntu 18.04 STIG Versi 2 Rilis 12
- Ubuntu 20.04 STIG Versi 1 Rilis 10

#### STIG-Build-Linux-versi tinggi 2023.4.x

- RHEL 7 STIG Versi 3 Rilis 13
- RHEL 8 STIG Versi 1 Rilis 12
- Ubuntu 18.04 STIG Versi 2 Rilis 12
- Ubuntu 20.04 STIG Versi 1 Rilis 10

Perubahan Q3 2023 - 10/04/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal ketiga 2023 sebagai berikut:

#### Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 12
- RHEL 8 STIG Versi 1 Rilis 11
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 9

#### Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 12
- RHEL 8 STIG Versi 1 Rilis 11
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 9

#### Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 12
- RHEL 8 STIG Versi 1 Rilis 11
- Ubuntu 18.04 STIG Versi 2 Rilis 11

- Ubuntu 20.04 STIG Versi 1 Rilis 9

Perubahan Q2 2023 - 05/03/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal kedua 2023 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 11
- RHEL 8 STIG Versi 1 Rilis 10
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 8

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 11
- RHEL 8 STIG Versi 1 Rilis 10
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 8

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 11
- RHEL 8 STIG Versi 1 Rilis 10
- Ubuntu 18.04 STIG Versi 2 Rilis 11
- Ubuntu 20.04 STIG Versi 1 Rilis 8

Perubahan Q1 2023 - 27/03/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal pertama 2023 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 10
- RHEL 8 STIG Versi 1 Rilis 9

- Ubuntu 18.04 STIG Versi 2 Rilis 10
- Ubuntu 20.04 STIG Versi 1 Rilis 7

#### Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 10
- RHEL 8 STIG Versi 1 Rilis 9
- Ubuntu 18.04 STIG Versi 2 Rilis 10
- Ubuntu 20.04 STIG Versi 1 Rilis 7

#### Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 10
- RHEL 8 STIG Versi 1 Rilis 9
- Ubuntu 18.04 STIG Versi 2 Rilis 10
- Ubuntu 20.04 STIG Versi 1 Rilis 7

2022 Perubahan Q4 - 02/01/2023:

Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal keempat 2022 sebagai berikut:

#### Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 9
- RHEL 8 STIG Versi 1 Rilis 8
- Ubuntu 18.04 STIG Versi 2 Rilis 9
- Ubuntu 20.04 STIG Versi 1 Rilis 6

#### Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 9
- RHEL 8 STIG Versi 1 Rilis 8
- Ubuntu 18.04 STIG Versi 2 Rilis 9
- Ubuntu 20.04 STIG Versi 1 Rilis 6



## Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 9
- RHEL 8 STIG Versi 1 Rilis 8
- Ubuntu 18.04 STIG Versi 2 Rilis 9
- Ubuntu 20.04 STIG Versi 1 Rilis 6

2022 Perubahan Q3 - 30/09/2022 (tidak ada perubahan):

Tidak ada perubahan untuk komponen Linux STIGS untuk rilis kuartal ketiga 2022.

2022 Perubahan Q2 - 08/02/2022:

Memperkenalkan dukungan Ubuntu, versi STIG yang diperbarui, dan menerapkan STIGS untuk rilis kuartal kedua 2022 sebagai berikut:

## Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 7
- RHEL 8 STIG Versi 1 Rilis 6
- Ubuntu 18.04 STIG Versi 2 Rilis 6 (baru)
- Ubuntu 20.04 STIG Versi 1 Rilis 4 (baru)

## Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 7
- RHEL 8 STIG Versi 1 Rilis 6
- Ubuntu 18.04 STIG Versi 2 Rilis 6 (baru)
- Ubuntu 20.04 STIG Versi 1 Rilis 4 (baru)

## Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 7
- RHEL 8 STIG Versi 1 Rilis 6
- Ubuntu 18.04 STIG Versi 2 Rilis 6 (baru)

- Ubuntu 20.04 STIG Versi 1 Rilis 4 (baru)

2022 Perubahan Q1 - 26/04/2022:

Difaktorkan ulang untuk menyertakan dukungan yang lebih baik untuk wadah. Menggabungkan skrip AL2 sebelumnya dengan RHEL 7. Versi STIG yang diperbarui dan menerapkan STIGS untuk rilis kuartal pertama 2022 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 6
- RHEL 8 STIG Versi 1 Rilis 5

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 6
- RHEL 8 STIG Versi 1 Rilis 5

Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 6
- RHEL 8 STIG Versi 1 Rilis 5

2021 Perubahan Q4 - 12/20/2021:

Versi STIG yang diperbarui, dan menerapkan STIGS untuk rilis kuartal keempat 2021 sebagai berikut:

Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 5
- RHEL 8 STIG Versi 1 Rilis 4

Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 5
- RHEL 8 STIG Versi 1 Rilis 4

## Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 5
- RHEL 8 STIG Versi 1 Rilis 4

2021 Perubahan Q3 - 09/30/2021:

Versi STIG yang diperbarui, dan menerapkan STIGS untuk rilis kuartal ketiga 2021 sebagai berikut:

## Linux STIG Rendah (Kategori III)

- RHEL 7 STIG Versi 3 Rilis 4
- RHEL 8 STIG Versi 1 Rilis 3

## Linux STIG Medium (Kategori II)

- RHEL 7 STIG Versi 3 Rilis 4
- RHEL 8 STIG Versi 1 Rilis 3

## Linux STIG Tinggi (Kategori I)

- RHEL 7 STIG Versi 3 Rilis 4
- RHEL 8 STIG Versi 1 Rilis 3

# AWSEC2-PatchLoadBalancerInstance

## Deskripsi

Upgrade dan patch versi minor instans Amazon EC2 (Windows atau Linux) yang dilampirkan ke penyeimbang muatan (klasik, ALB, atau NLB). Waktu pengeringan koneksi default diterapkan sebelum instance ditambah. Anda dapat mengganti waktu tunggu dengan memasukkan waktu pengeringan khusus Anda dalam hitungan menit (1-59) untuk parameter. ConnectionDrainTime

Alur kerja otomatisasi adalah sebagai berikut:

1. Penyeimbang beban atau grup target tempat instance dilampirkan ditentukan, dan instance diverifikasi sebagai sehat.

2. Instance dihapus dari load balancer atau grup target.
3. Otomatisasi menunggu periode waktu yang ditentukan untuk waktu pengeringan koneksi.
4. [AWS- RunPatchBaseline](#) otomatisasi dipanggil untuk menambal instans.
5. Instance ini dipasang kembali ke load balancer atau grup target.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis Dokumen

Otomatisasi

Pemilik

Amazon

Prasyarat

- Verifikasi bahwa Agen SSM diinstal pada instans Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan Agen SSM pada instans EC2 untuk Windows Server](#).

Parameter

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans untuk ditambal yang dikaitkan dengan penyeimbang muatan (klasik, ALB, atau NLB).

- ConnectionDrainTime

Jenis: String

Keterangan: (Opsional) Waktu pengeringan koneksi penyeimbang beban, dalam hitungan menit (1-59).

## **AWSEC2-SQLServerDBRestore**

Deskripsi

AWSEC2-SQLServerDBRestoreRunbook mengembalikan cadangan database Microsoft SQL Server yang disimpan di Amazon S3 ke SQL Server 2017 yang berjalan pada instans Linux Amazon Elastic Compute Cloud (EC2). Anda dapat memberikan contoh EC2 Anda sendiri yang menjalankan SQL Server 2017 Linux. Jika instans EC2 tidak disediakan, otomatisasi meluncurkan dan mengkonfigurasi instans Ubuntu 16.04 EC2 baru dengan SQL Server 2017. Otomatisasi mendukung pemulihan penuh, diferensial, dan cadangan log transaksional. Otomatisasi ini menerima beberapa file backup database dan secara otomatis mengembalikan cadangan valid terbaru dari setiap database dalam file yang disediakan.

Untuk mengotomatiskan pencadangan dan pemulihan database SQL Server lokal ke instans EC2 yang menjalankan SQL Server 2017 Linux, Anda dapat menggunakan skrip -signed. AWS PowerShell [MigrateSQLServerToEC2Linux](#)

#### Important

Runbook ini mengatur ulang kata sandi pengguna administrator server SQL Server (SA) setiap kali otomatisasi berjalan. Setelah otomatisasi selesai, Anda harus mengatur sandi pengguna SA Anda sendiri lagi sebelum Anda menyambung ke contoh SQL Server.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis Dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Prasyarat

Untuk menjalankan otomatisasi ini, Anda harus memenuhi prasyarat berikut:

- Pengguna IAM atau peran yang menjalankan otomatisasi ini harus memiliki kebijakan sebaris yang dilampirkan dengan izin yang diuraikan. [Izin IAM yang diperlukan](#)
- Jika Anda memberikan instans EC2 Anda sendiri:

- Instans EC2 yang Anda berikan harus berupa instance Linux yang menjalankan Microsoft SQL Server 2017.
- Instans EC2 yang Anda berikan harus dikonfigurasi dengan profil instans AWS Identity and Access Management (IAM) yang memiliki kebijakan AmazonSSMManagedInstanceCore terkelola terlampir. Untuk informasi selengkapnya, lihat [Buat profil instans IAM untuk Systems Manager](#).
- Agen SSM harus diinstal pada instans EC2 Anda. Untuk informasi selengkapnya, lihat [Menginstal dan mengonfigurasi Agen SSM pada instans EC2](#) untuk Linux.
- Instans EC2 harus memiliki ruang disk kosong yang cukup untuk mengunduh dan memulihkan cadangan SQL Server.

## Keterbatasan:

Otomatisasi ini tidak mendukung pemulihan ke SQL Server yang berjalan pada contoh EC2 untuk Windows Server. Otomatisasi ini hanya mengembalikan backup database yang kompatibel dengan SQL Server Linux 2017. Untuk informasi selengkapnya, lihat [Edisi dan Fitur yang Didukung SQL Server 2017 di Linux](#).

## Parameter

Otomatisasi ini memiliki parameter berikut:

- DatabaseNames

Jenis: String

Deskripsi: (Opsional) Daftar nama database yang dipisahkan koma untuk dipulihkan.

- DataDirectorySize

Jenis: String

Deskripsi: (Opsional) Ukuran volume yang diinginkan (GiB) dari direktori Data SQL Server untuk instans EC2 baru.

Nilai default: 100

- KeyPair

Jenis: String

Deskripsi: (Opsional) Pasangan kunci yang akan digunakan saat membuat instans EC2 baru.

- `IamInstanceProfileName`

Jenis: String

Deskripsi: (Opsional) Profil instans IAM untuk dilampirkan ke instans EC2 baru. Profil instans IAM harus memiliki kebijakan `AmazonSSMManagedInstanceCore` terkelola yang dilampirkan.

- `InstanceId`

Jenis: String

Deskripsi: (Opsional) Instance yang menjalankan SQL Server 2017 di Linux. Jika tidak `InstanceId` ada yang disediakan, otomatisasi meluncurkan instans EC2 baru menggunakan `InstanceType` dan `SQL ServerEdition` yang disediakan.

- `InstanceType`

Jenis: String

Deskripsi: (Opsional) Jenis instans EC2 yang akan diluncurkan.

- `ISS3 PresignedUrl`

Jenis: String

Deskripsi: (Opsional) Jika `S3Input` adalah URL S3 yang telah ditandatangani sebelumnya, tunjukkan. `yes`

Nilai default: tidak

Nilai yang valid: `ya` | `tidak`

- `LogDirectorySize`

Jenis: String

Deskripsi: (Opsional) Ukuran volume yang diinginkan (GiB) dari direktori SQL Server Log untuk instans EC2 baru.

Nilai default: 100

- `S3Masukan`

Jenis: String

Deskripsi: Nama bucket S3 (Diperlukan), daftar kunci objek S3 yang dipisahkan koma, atau daftar URL S3 yang telah ditandatangani sebelumnya yang dipisahkan koma yang berisi file cadangan SQL yang akan dipulihkan.

- SQL ServerEdition

Jenis: String

Deskripsi: (Opsional) Edisi SQL Server 2017 yang akan diinstal pada instans EC2 yang baru dibuat.

Nilai yang valid: Standar | Perusahaan | Web | Express

- SubnetId

Jenis: String

Deskripsi: (Opsional) Subnet untuk meluncurkan instans EC2 baru. Subnet harus memiliki konektivitas keluar ke AWS layanan. Jika nilai untuk tidak SubnetId disediakan, otomatisasi menggunakan subnet default.

- TempDbDirectorySize

Jenis: String

Deskripsi: (Opsional) Ukuran volume yang diinginkan (GiB) dari direktori SQL Server TempDB untuk instans EC2 baru.

Nilai default: 100

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk berhasil menggunakan runbook.

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



```

    "Action": [
      "ec2:CreateTags",
      "ec2:DescribeImages",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeInstances",
      "ec2:RebootInstances",
      "ec2:RunInstances",
      "ssm:DescribeInstanceInformation",
      "ssm:GetAutomationExecution",
      "ssm:ListCommandInvocations",
      "ssm:ListCommands",
      "ssm:SendCommand",
      "ssm:StartAutomationExecution"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::ACCOUNTID:role/ROLENAME"
  }
]
}

```

## Langkah Dokumen

Untuk menggunakan otomatisasi ini, ikuti langkah-langkah yang berlaku untuk jenis instans Anda:

Untuk instans EC2 baru:

1. `aws:executeAwsApi`- Ambil ID AMI untuk SQL Server 2017 di Ubuntu 16.04.
2. `aws:runInstances`- Luncurkan contoh EC2 baru untuk Linux.
3. `aws:waitForAwsResourceProperty`- Tunggu instans EC2 yang baru dibuat siap.
4. `aws:executeAwsApi`- Reboot instance jika instance belum siap.
5. `aws:assertAwsResourceProperty`- Verifikasi bahwa SSM Agen diinstal.
6. `aws:runCommand`- Jalankan skrip pemulihan SQL Server diPowerShell.

Untuk instans EC2 yang ada:

1. `aws:waitForAwsResourceProperty`- Verifikasi bahwa instans EC2 sudah siap.

2. `aws:executeAwsApi`- Reboot instance jika instance belum siap.
3. `aws:assertAwsResourceProperty`- Verifikasi bahwa SSM Agen diinstal.
4. `aws:runCommand`- Jalankan skrip pemulihan SQL Server diPowerShell.

Keluaran

`GetInstance`. `InstanceId`

`restoreToNewInstance`. Output

`restoreToExistingInstance`. Output

## **AWSSupport-ActivateWindowsWithAmazonLicense**

Deskripsi

`AWSSupport-ActivateWindowsWithAmazonLicenseRunbook` mengaktifkan instans Amazon Elastic Compute Cloud (Amazon EC2) Windows Server dengan lisensi yang disediakan oleh Amazon. Otomatisasi memverifikasi dan mengkonfigurasi pengaturan sistem operasi layanan manajemen kunci yang diperlukan dan upaya aktivasi. Ini termasuk rute sistem operasi ke server manajemen kunci Amazon dan pengaturan sistem operasi layanan manajemen kunci. Mengatur `AllowOffline` parameter untuk `true` memungkinkan otomatisasi berhasil menargetkan instance yang tidak dikelola oleh AWS Systems Manager, tetapi memerlukan stop dan start instance.

### Note

Runbook ini tidak dapat digunakan pada contoh model Windows Server Bring Your Own License (BYOL). Untuk informasi tentang menggunakan lisensi Anda sendiri, lihat [Lisensi Microsoft](#) aktif. AWS

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

## Platform

## Windows

### Parameter

- AllowOffline

Jenis: String

Nilai yang valid: benar/salah

Default: salah

Deskripsi: (Opsional) Setel ke `true` jika Anda mengizinkan remediasi aktivasi Windows offline jika pemecahan masalah online gagal, atau jika instans yang disediakan bukan instans terkelola.

#### Important

Metode offline mengharuskan instans EC2 yang disediakan dihentikan dan kemudian dimulai. Data yang disimpan dalam volume toko instance akan hilang. Alamat IP publik akan berubah jika Anda tidak menggunakan Elastic IP.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ForceActivation

Jenis: String

Nilai yang valid: benar/salah

Default: salah

Deskripsi: (Opsional) Setel ke `true` jika Anda ingin melanjutkan bahkan jika Windows sudah diaktifkan.

- **InstanceId**

Jenis: String

Deskripsi: (Wajib) ID instans EC2 terkelola Anda untuk Windows Server.

- **SubnetId**

Jenis: String

Bawaan: CreateNew VPC

Deskripsi: (Opsional) Hanya offline - ID subnet untuk instans EC2 Rescue yang digunakan untuk melakukan pemecahan masalah offline. Gunakan `SelectedInstanceSubnet` untuk menggunakan subnet yang sama dengan instans Anda, atau gunakan `CreateNewVPC` untuk membuat VPC baru. PENTING: Subnet harus berada di Availability Zone yang sama dengan `InstanceId`, dan harus mengizinkan akses ke endpoint SSM.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

Kami menyarankan agar instans EC2 yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon `AmazonSSMManagedInstanceCore` yang terpasang. Anda harus memiliki setidaknya `ssm:StartAutomationExecution` dan `ssm:SendCommand` untuk menjalankan otomatisasi dan mengirim perintah ke instance, ditambah `ssm:GetAutomationExecution` untuk dapat membaca output otomatisasi. Untuk remediasi offline, lihat izin yang dibutuhkan oleh `AWSSupport-StartEC2RescueWorkflow`

### Langkah Dokumen

1. `aws:assertAwsResourceProperty`- Periksa platform instance yang disediakan adalah Windows.
2. `aws:assertAwsResourceProperty`- Konfirmasikan instance yang disediakan adalah instance yang dikelola:
  - a. (Perbaikan aktivasi online) Jika instance input adalah instance terkelola, maka jalankan `aws:runCommand` untuk menjalankan PowerShell skrip untuk mencoba memperbaiki aktivasi Windows.
  - b. (Perbaikan aktivasi offline) Jika instance input bukan instance terkelola:

- i. `aws:assertAwsResourceProperty`- Memverifikasi `AllowOffline` bendera diatur ke `true`. Jika demikian, perbaikan offline dimulai; jika tidak otomatisasi berakhir.
- ii. `aws:executeAutomation`- Memanggil `AWSSupport-StartEC2RescueWorkflow` dengan skrip perbaikan offline aktivasi Windows. Script menggunakan `EC2config` atau `EC2Launch`, tergantung pada versi OS.
- iii. `aws:executeAwsApi`- Baca hasilnya dari `AWSSupport-StartEC2RescueWorkflow`.

Keluaran

AktifkanWindows.output

`getActivateWindowsOfflineResult`.Keluaran

## AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Deskripsi

`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook menganalisis konektivitas dari instans Amazon Elastic Compute Cloud (Amazon EC2) atau antarmuka elastic network ke titik akhir. Layanan AWS IPv6 tidak didukung. Runbook menggunakan nilai yang Anda tentukan untuk `ServiceEndpoint` parameter untuk menganalisis konektivitas ke titik akhir. Jika AWS PrivateLink titik akhir tidak dapat ditemukan di VPC Anda, runbook menggunakan alamat IP publik untuk layanan saat ini. Wilayah AWS Otomatisasi ini menggunakan Reachability Analyzer dari Amazon Virtual Private Cloud. Untuk informasi selengkapnya, lihat [Apa itu Reachability Analyzer?](#), di Reachability Analyzer.

Otomatisasi ini memeriksa hal-hal berikut:

- Memeriksa apakah virtual private cloud (VPC) Anda dikonfigurasi untuk menggunakan server DNS yang disediakan Amazon.
- Memeriksa apakah AWS PrivateLink titik akhir ada di VPC untuk yang Anda Layanan AWS tentukan. Jika titik akhir ditemukan, otomatisasi memverifikasi bahwa `privateDns` atribut diaktifkan.
- Memeriksa apakah AWS PrivateLink titik akhir menggunakan kebijakan titik akhir default.

Pertimbangan-pertimbangan

- Anda dikenakan biaya per analisis yang dijalankan antara sumber dan tujuan. Untuk informasi lebih lanjut, lihat [Harga Amazon VPC](#).
- Selama otomatisasi, jalur wawasan jaringan dan analisis wawasan jaringan dibuat. Jika otomatisasi berhasil diselesaikan, runbook menghapus sumber daya ini. Jika langkah pembersihan gagal, jalur wawasan jaringan tidak dihapus oleh runbook dan Anda harus menghapusnya secara manual. Jika Anda tidak menghapus jalur wawasan jaringan secara manual, jalur tersebut terus dihitung terhadap kuota untuk Anda. Untuk informasi selengkapnya tentang kuota untuk Reachability Analyzer, lihat Kuota untuk Reachability Analyzer di [Reachability Analyzer](#).
- Konfigurasi tingkat sistem operasi seperti penggunaan proxy, resolver DNS lokal, atau file host dapat memengaruhi konektivitas bahkan jika Reachability Analyzer kembali. PASS
- Tinjau evaluasi semua pemeriksaan yang dilakukan oleh Reachability Analyzer. Jika salah satu cek kembali dengan status FAIL, itu mungkin memengaruhi konektivitas bahkan jika pemeriksaan jangkauan keseluruhan mengembalikan status. PASS

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Sumber

Jenis: String

Deskripsi: (Wajib) ID instans Amazon EC2 atau antarmuka jaringan tempat Anda ingin menganalisis keterjangkauan.

- ServiceEndpoint

Jenis: String

Deskripsi: (Wajib) Nama host dari titik akhir layanan yang ingin Anda analisis jangkauan.

- RetainVpcReachabilityAnalysis

Jenis: String

Bawaan: salah

Deskripsi: (Opsional) Menentukan apakah jalur wawasan jaringan dan analisis terkait yang dibuat dipertahankan. Secara default, sumber daya yang digunakan untuk menganalisis jangkauan dihapus setelah analisis berhasil. Jika Anda memilih untuk mempertahankan analisis, runbook tidak menghapus analisis dan Anda dapat memvisualisasikannya di konsol VPC Amazon. Tautan konsol tersedia di output otomatisasi.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ec2:CreateNetworkInsightsPath
- ec2>DeleteNetworkInsightsAnalysis
- ec2>DeleteNetworkInsightsPath
- ec2:DescribeAvailabilityZones
- ec2:DescribeCustomerGateways
- ec2:DescribeDhcpOptions
- 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:DescribeTransitGatewayPeeringAttachments`
- `ec2:DescribeTransitGatewayConnects`
- `ec2:DescribeTransitGatewayRouteTables`
- `ec2:DescribeTransitGateways`
- `ec2:DescribeTransitGatewayVpcAttachments`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcEndpointServiceConfigurations`
- `ec2:DescribeVpcPeeringConnections`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpnConnections`
- `ec2:DescribeVpnGateways`
- `ec2:GetManagedPrefixListEntries`
- `ec2:GetTransitGatewayRouteTablePropagations`
- `ec2:SearchTransitGatewayRoutes`
- `ec2:StartNetworkInsightsAnalysis`
- `elasticloadbalancing:DescribeListeners`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeRules`



- `elasticloadbalancing:DescribeTags`
- `elasticloadbalancing:DescribeTargetGroups`
- `elasticloadbalancing:DescribeTargetHealth`
- `tiros>CreateQuery`
- `tiros:GetQueryAnswer`
- `tiros:GetQueryExplanation`

## Langkah Dokumen

1. `aws:executeScript`: Memvalidasi titik akhir layanan dengan mencoba menyelesaikan nama host.
2. `aws:executeScript`: Mengumpulkan detail tentang VPC dan subnet.
3. `aws:executeScript`: Mengevaluasi konfigurasi DNS VPC.
4. `aws:executeScript`: Mengevaluasi pemeriksaan titik akhir VPC.
5. `aws:executeScript`: Menemukan gateway internet untuk terhubung ke titik akhir layanan publik.
6. `aws:executeScript`: Menentukan tujuan yang akan digunakan untuk analisis jangkauan.
7. `aws:executeScript`: Menganalisis jangkauan dari sumber ke titik akhir menggunakan Reachability Analyzer dan membersihkan sumber daya jika analisis berhasil.
8. `aws:executeScript`: Menghasilkan laporan evaluasi jangkauan.
9. `aws:executeScript`: Menghasilkan output di JSON.

## Keluaran

- `generateReport.EvalReport`- Hasil pemeriksaan yang dilakukan oleh otomatisasi dalam format teks.
- `generateJsonOutput.Output`- Versi minimal hasil dalam format JSON.

## **AWSPremiumSupport-ChangeInstanceTypeIntelToAMD**

### Deskripsi

`AWSPremiumSupport-ChangeInstanceTypeIntelToAMDRunbook` mengotomatiskan migrasi dari instans Amazon Elastic Compute Cloud (Amazon EC2) yang didukung Intel ke jenis instans

bertenaga AMD yang setara. Runbook ini mendukung instance tujuan umum (M), tujuan umum burstable (T), komputasi yang dioptimalkan (C), dan memori yang dioptimalkan (R) yang dibangun di atas sistem Nitro. Runbook ini dapat digunakan pada instance yang tidak dikelola oleh Systems Manager.

Untuk mengurangi potensi risiko kehilangan dan waktu henti data, runbook memeriksa perilaku stop instans, apakah instans berada dalam grup Amazon EC2 Auto Scaling, kesehatan instans, dan bahwa jenis instans bertenaga AMD yang setara tersedia di Availability Zone yang sama. Secara default, runbook ini tidak akan mengubah jenis instance jika volume penyimpanan instance terpasang, atau jika instance adalah bagian dari AWS CloudFormation tumpukan. Jika Anda ingin mengubah perilaku ini, tentukan `yes` untuk salah satu `AllowCloudFormationInstances` parameter `AllowInstanceStoreInstances` dan.

#### Important

Akses ke `AWSPremiumSupport` - \* runbook memerlukan Langganan Dukungan Perusahaan atau Bisnis. Untuk informasi selengkapnya, lihat [Bandingkan AWS Support Paket](#).

## Pertimbangan

- Sebaiknya buat cadangan instans Anda sebelum menggunakan runbook ini.
- Mengubah jenis instans memerlukan runbook untuk menghentikan instance Anda. Ketika instans dihentikan, data apa pun yang disimpan dalam RAM atau volume penyimpanan instans hilang, dan alamat IPv4 publik otomatis dirilis. Untuk informasi selengkapnya, lihat [Berhenti dan mulai instans Anda](#).
- Jika Anda tidak menentukan nilai untuk `TargetInstanceType` parameter, runbook mencoba mengidentifikasi instans AMD yang setara dalam hal CPU virtual dan memori dalam keluarga instans yang sama. Runbook berakhir jika tidak dapat mengidentifikasi jenis instans AMD yang setara.
- Dengan menggunakan `DryRun` opsi ini, Anda dapat menangkap jenis instans AMD yang setara, dan memvalidasi persyaratan tanpa benar-benar mengubah jenis instance.

## [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Mengakui

Jenis: String

Deskripsi: (Diperlukan) Enter yes untuk mengakui bahwa instance target Anda akan dihentikan jika sedang berjalan.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans Amazon EC2 yang jenisnya ingin Anda ubah.

- TargetInstanceType

Jenis: String

Default: otomatis

Deskripsi: (Opsional) Jenis instans AMD yang ingin Anda ubah instans. automaticNilai default menggunakan jenis instance yang setara dalam hal CPU virtual dan memori. Misalnya, m5.large akan diubah menjadi m5a.large.

- AllowInstanceStoreInstances

Jenis: String

Nilai yang valid: tidak | ya

Default: tidak

Deskripsi: (Opsional) Jika Anda menentukanyes, runbook berjalan pada instance yang memiliki volume penyimpanan instans yang terpasang.

- AllowCloudFormationInstances

Jenis: String

Nilai yang valid: tidak | ya

Default: tidak

Deskripsi: (Opsional) Jika diatur keyes, runbook berjalan pada instance yang merupakan bagian dari tumpukan. AWS CloudFormation

- AllowCrossGeneration

Jenis: String

Nilai yang valid: tidak | ya

Default: tidak

Deskripsi: (Opsional) Jika diatur keyes, runbook mencoba menemukan jenis instans AMD setara terbaru dalam keluarga instans yang sama.

- DryRun

Jenis: String

Nilai yang valid: tidak | ya

Default: tidak

Deskripsi: (Opsional) Jika diatur keyes, runbook mengembalikan jenis instans AMD yang setara dan memvalidasi persyaratan migrasi tanpa membuat perubahan pada jenis instans.

- SleepWait

Jenis: String

## Bawaan: PT3S

Deskripsi: (Opsional) Waktu runbook harus menunggu sebelum memulai otomatisasi baru. Nilai yang Anda berikan untuk parameter ini harus sesuai dengan standar ISO 8601. Untuk informasi selengkapnya tentang membuat string ISO 8601, lihat [Memformat string tanggal dan waktu untuk Manajer Sistem](#).

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ec2:GetInstanceTypesFromInstanceRequirements`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeTags`
- `ec2:ModifyInstanceAttribute`
- `ec2:StartInstances`
- `ec2:StopInstances`

### Langkah Dokumen

1. `aws:assertAwsResourceProperty`: Mengonfirmasi status instans Amazon EC2 target adalah `running`, `pendingstopped`, atau `stopping` Jika tidak, otomatisasi berakhir.
2. `aws:executeAwsApi`: Mengumpulkan properti dari instans Amazon EC2 target.
3. `aws:branch`: Cabang otomatisasi berdasarkan status instans Amazon EC2.

- a. Jika `stopped` atau `stopping`, otomatisasi berjalan `aws:waitForAwsResourceProperty` hingga instans Amazon EC2 dihentikan sepenuhnya.
- b. Jika `running` atau `pending`, otomatisasi berjalan `aws:waitForAwsResourceProperty` hingga instans Amazon EC2 melewati pemeriksaan status.
4. `aws:assertAwsResourceProperty`: Mengonfirmasi bahwa instans Amazon EC2 bukan bagian dari grup Penskalaan Otomatis dengan memeriksa apakah `aws:autoscaling:groupName` tag diterapkan.
5. `aws:executeAwsApi`: Mengumpulkan properti jenis instance saat ini untuk menemukan jenis instans AMD yang setara.
6. `aws:assertAwsResourceProperty`: Mengonfirmasi bahwa kode AWS Marketplace produk tidak terkait dengan instans Amazon EC2. Beberapa produk tidak tersedia di semua jenis instans.
7. `aws:branch`: Cabang otomatisasi tergantung pada apakah Anda ingin otomatisasi memeriksa apakah instans Amazon EC2 adalah bagian dari tumpukan AWS CloudFormation
  - a. Jika `aws:cloudformation:stack-name` tag diterapkan ke instance, otomatisasi berjalan `aws:assertAwsResourceProperty` untuk mengonfirmasi instance bukan bagian dari AWS CloudFormation tumpukan.
8. `aws:branch`: Cabang otomatisasi berdasarkan apakah jenis volume root instans adalah Amazon Elastic Block Store (Amazon EBS).
9. `aws:assertAwsResourceProperty`: Mengonfirmasi perilaku shutdown instance stop dan tidak `terminate`.
10. `aws:executeScript`: Mengonfirmasi hanya ada satu otomatisasi runbook ini yang menargetkan instance saat ini. Jika otomatisasi lain sudah berlangsung menargetkan instance yang sama, ia mengembalikan kesalahan dan berakhir.
11. `aws:executeAwsApi`: Mengembalikan daftar jenis instance AMD dengan jumlah memori dan vCPU yang sama.
12. `aws:executeScript`: Memeriksa apakah jenis instance saat ini didukung dan mengembalikan jenis instans AMD yang setara. Jika tidak ada yang setara, otomatisasi berakhir.
13. `aws:executeScript`: Mengonfirmasi jenis instans AMD tersedia di Availability Zone yang sama, dan memverifikasi izin IAM yang disediakan.
14. `aws:branch`: Cabang otomatisasi berdasarkan apakah nilai `DryRun` parameter `yes`.
15. `aws:branch`: Memeriksa apakah jenis instance asli dan target sama. Jika mereka sama, otomatisasi berakhir.
16. `aws:executeAwsApi`: Mendapat keadaan contoh saat ini.

17.aws:changeInstanceState: Menghentikan instans Amazon EC2.

18.aws:changeInstanceState: Memaksa instance untuk berhenti jika terjebak dalam keadaan berhenti.

19.aws:executeAwsApi: Mengubah jenis instance ke tipe instans AMD target.

20.aws:sleep: Menunggu 3 detik setelah mengubah jenis instans untuk konsistensi akhirnya.

21.aws:branch: Cabang otomatisasi berdasarkan status instans sebelumnya. Jika ya`running`, instance dimulai.

- a. aws:changeInstanceState: Memulai instans Amazon EC2 jika sedang berjalan sebelum mengubah jenis instans.
- b. aws:waitForAwsResourceProperty: Menunggu instans Amazon EC2 untuk lulus pemeriksaan status. Jika instance tidak lulus pemeriksaan status, instance diubah kembali ke jenis instance aslinya.
  - i. aws:changeInstanceState: Menghentikan instans Amazon EC2 sebelum mengubahnya ke jenis instans aslinya.
  - ii. aws:changeInstanceState: Memaksa instans Amazon EC2 untuk berhenti sebelum mengubahnya ke jenis instans aslinya jika terjebak dalam keadaan berhenti.
  - iii. aws:executeAwsApi: Mengubah instans Amazon EC2 ke jenis aslinya.
  - iv. aws:sleep: Menunggu 3 detik setelah mengubah jenis instans untuk konsistensi akhirnya.
  - v. aws:changeInstanceState: Memulai instans Amazon EC2 jika sedang berjalan sebelum mengubah jenis instans.
  - vi. aws:waitForAwsResourceProperty: Menunggu instans Amazon EC2 untuk lulus pemeriksaan status.

22.aws:sleep: Menunggu sebelum mengakhiri runbook.

## **AWSsupport-CheckXenToNitroMigrationRequirements**

### Deskripsi

AWSsupport-CheckXenToNitroMigrationRequirementsRunbook memverifikasi bahwa instans Amazon Elastic Compute Cloud (Amazon EC2) memenuhi prasyarat untuk berhasil mengubah jenis instans dari instans tipe Xen ke jenis instans berbasis Nitro. Otomatisasi ini memeriksa hal berikut:

- Perangkat root adalah volume Amazon Elastic Block Store (Amazon EBS).

- `enaSupportAtribut` diaktifkan.
- Modul ENA diinstal pada instance.
- Modul NVMe diinstal pada instance. Jika ya, modul diinstal dan skrip memverifikasi bahwa modul dimuat dalam `initramfs` gambar.
- Menganalisis `/etc/fstab` dan mencari perangkat blok yang dipasang menggunakan nama perangkat.
- Menentukan apakah sistem operasi (OS) menggunakan nama antarmuka jaringan yang dapat diprediksi secara default.

Runbook ini mendukung sistem operasi berikut:

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Debian Server
- Ubuntu Server
- SUSE Linux Enterprise Server15 SP2
- SUSE Linux Enterprise Server12 SP5

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- `AutomationAssumeRole`



Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Default: salah

Deskripsi: (Diperlukan) ID instans Amazon EC2 yang ingin Anda periksa prasyarat sebelum bermigrasi ke jenis instans berbasis Nitro.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:DescribeInstanceInformation
- ssm:DescribeInstanceProperties
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:ListDocuments
- ssm:StartAutomationExecution
- ssm:SendCommand
- iam:ListRoles

- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypes`

### Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan rincian tentang contoh.
- `aws:executeAwsApi`- Mengumpulkan informasi tentang hypervisor untuk instance.
- `aws:branch`- Cabang berdasarkan apakah instance target sudah menjalankan tipe instans berbasis Nitro.
- `aws:branch`- Memeriksa apakah OS instance didukung oleh instance berbasis Nitro.
- `aws:assertAwsResourceProperty`- Memverifikasi instance yang Anda tentukan dikelola oleh Systems Manager, dan statusnya adalah `Online`.
- `aws:branch`- Cabang berdasarkan apakah perangkat root instans adalah volume Amazon EBS.
- `aws:branch`- Cabang berdasarkan apakah atribut ENA diaktifkan untuk contoh.
- `aws:runCommand`- Memeriksa driver ENA pada instance.
- `aws:runCommand`- Memeriksa driver NVMe pada instance.
- `aws:runCommand`- Memeriksa `fstab` file untuk format yang tidak dikenal.
- `aws:runCommand`- Memeriksa konfigurasi nama antarmuka yang dapat diprediksi pada instance.
- `aws:executeScript`- Menghasilkan output berdasarkan langkah-langkah sebelumnya.

### Keluaran

`FinalOutput.output` - Hasil pemeriksaan yang dilakukan oleh otomatisasi.

## **AWSsupport-ConfigureEC2Metadata**

### Deskripsi

Runbook ini membantu Anda mengonfigurasi opsi layanan metadata instans (IMDS) untuk instans Amazon Elastic Compute Cloud (Amazon EC2). Dengan menggunakan runbook ini, Anda dapat mengonfigurasi yang berikut:

- Menegakkan penggunaan IMDSv2 misalnya metadata.
- Konfigurasi `HttpPutResponseHopLimit` nilainya.
- Izinkan atau tolak akses metadata instance.

Untuk informasi selengkapnya tentang metadata instans, lihat [Mengonfigurasi Layanan Metadata Instans](#) dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- PenegakanIMDSv2

Jenis: String

Nilai yang valid: diperlukan | opsional

Default: opsional

Deskripsi: (Opsional) Menegakkan IMDSv2. Jika Anda memilih `required`, instans Amazon EC2 hanya akan menggunakan IMDSv2. Jika Anda memilih `optional`, Anda dapat memilih antara IMDSv1 dan IMDSv2 untuk akses metadata.

#### Important

Jika Anda menerapkan IMDSv2, aplikasi yang menggunakan IMDSv1 mungkin tidak berfungsi dengan benar. Sebelum menegakkan IMDSv2, pastikan aplikasi Anda yang

menggunakan IMDS ditingkatkan ke versi yang mendukung IMDSv2. Untuk informasi tentang Layanan Metadata Instans Versi 2 (IMDSv2), lihat [Mengonfigurasi Layanan Metadata Instans](#) dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.

- `HttpPutResponseHopLimit`

Tipe: Bilangan Bulat

Nilai yang valid: 0-64

Default: 0

Deskripsi: (Opsional) Nilai batas hop respons HTTP PUT yang diinginkan (1-64) untuk permintaan metadata misalnya. Nilai ini mengontrol jumlah hop yang dapat dilalui oleh respons PUT. Untuk mencegah respons berjalan di luar instance, tentukan 1 nilai parameter.

- `InstanceID`

Jenis: String

Deskripsi: (Diperlukan) ID instans Amazon EC2 yang pengaturan metadatanya ingin Anda konfigurasi.

- `MetadataAccess`

Jenis: String

Nilai yang valid: diaktifkan | dinonaktifkan

Default: diaktifkan

Deskripsi: (Opsional) Mengizinkan atau menolak akses metadata instans di instans Amazon EC2. Jika Anda menentukandisabled, semua parameter lain akan diabaikan dan akses metadata akan ditolak untuk instance.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeInstances`
- `ec2:ModifyInstanceMetadataOptions`

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`

## Langkah Dokumen

1. `branchOnMetadataAccess` - Cabang otomatisasi berdasarkan nilai `MetadataAccess` parameter.
2. `disableMetadataAccess`- Memanggil tindakan `ModifyInstanceMetadataOptions` API untuk menonaktifkan akses endpoint metadata.
3. `branchOnHttpPutResponseHopLimit`- Otomatisasi cabang berdasarkan nilai `HttpPutResponseHopLimit` parameter.
4. `maintainHopLimitAndConfigureImdsVersion`- Jika `HttpPutResponseHopLimit` 0, mempertahankan batas hop saat ini dan perubahan pilihan metadata lainnya.
5. `waitBeforeAssertingIMDSv2State` - Menunggu 30 detik sebelum menegaskan status IMDSv2.
6. `setHopLimitAndConfigureImdsVersion`- Jika `HttpPutResponseHopLimit` lebih besar dari 0, mengkonfigurasi opsi metadata menggunakan parameter masukan yang diberikan.
7. `waitBeforeAssertingHopLimit`- Menunggu 30 detik sebelum menegaskan opsi metadata.
8. `assertHopLimit`- Menegaskan `HttpPutResponseHopLimit` properti diatur ke nilai yang Anda tentukan.
9. `branchVerificationOnIMDSV2Option` - Verifikasi cabang berdasarkan nilai parameter. `EnforceIMDSv2`
10. `AssertImdsv2IsOptional` - `HttpTokens` Menegaskan nilai diatur ke. `optional`
11. `AssertImdsv2IsEnforced` - `HttpTokens` Menegaskan nilai diatur ke. `required`
12. `waitBeforeAssertingMetadataState`- Menunggu 30 detik sebelum menyatakan status metadata dinonaktifkan.
13. `assertMetadataIsDinonaktifkan` - Menegaskan metadata adalah. `disabled`
14. `describeMetadataOptions`- Mendapat opsi metadata setelah perubahan yang Anda tentukan telah diterapkan.

## Keluaran

`describeMetadataOptions.Negara`

`describeMetadataOptions.MetadataAccess`

`describeMetadataOptions.IMDSv2`

`describeMetadataOptions.HttpPutResponseHopLimit`

## **AWSsupport-CopyEC2Instance**

### Deskripsi

AWSsupport-CopyEC2InstanceRunbook menyediakan solusi otomatis untuk prosedur yang diuraikan dalam artikel Pusat Pengetahuan [Bagaimana cara memindahkan instans EC2 saya ke subnet lain, Availability Zone](#), atau VPC? Cabang otomatisasi tergantung pada nilai yang Anda tentukan untuk Region dan SubnetId parameter.

Jika Anda menentukan nilai untuk SubnetId parameter tetapi bukan nilai untuk Region parameter, otomatisasi membuat Amazon Machine Image (AMI) dari instance target dan meluncurkan instance baru dari subnet AMI dalam yang Anda tentukan.

Jika Anda menentukan nilai untuk SubnetId parameter dan Region parameter, otomatisasi menciptakan contoh AMI target, menyalin AMI ke yang Wilayah AWS Anda tentukan, dan meluncurkan contoh baru dari AMI dalam subnet yang Anda tentukan.

Jika Anda menentukan nilai untuk Region parameter tetapi bukan nilai untuk SubnetId parameter, otomatisasi membuat instance AMI target, menyalin AMI ke Wilayah yang Anda tentukan, dan meluncurkan instance baru dari subnet default cloud pribadi virtual Anda (VPC) di Wilayah tujuan.

### AMI

Jika tidak ada nilai yang ditentukan untuk SubnetId parameter Region atau, otomatisasi membuat instance AMI target, dan meluncurkan instance baru dari subnet default VPC Anda. AMI

Untuk menyalin AMI ke Wilayah yang berbeda, Anda harus memberikan nilai untuk AutomationAssumeRole parameter. Jika waktu otomatisasi keluar selama waitForAvailableDestinationAmi langkah, AMI mungkin masih menyalin. Jika ini masalahnya, Anda dapat menunggu salinan selesai dan meluncurkan instance secara manual.

Sebelum menjalankan otomatisasi ini, perhatikan hal berikut:

- AMIS didasarkan pada snapshot Amazon Elastic Block Store (Amazon EBS). Untuk sistem file besar tanpa snapshot sebelumnya, AMI pembuatan dapat memakan waktu beberapa jam. Untuk mengurangi waktu AMI pembuatan, buat snapshot Amazon EBS sebelum Anda membuatnya. AMI

- Membuat AMI tidak membuat snapshot misalnya menyimpan volume pada instance. Untuk informasi tentang mencadangkan volume penyimpanan instans ke Amazon EBS, lihat [Bagaimana cara mencadangkan volume penyimpanan instans pada instans Amazon EC2 saya ke Amazon EBS?](#)
- Instans Amazon EC2 baru memiliki IPv4 pribadi atau alamat IP IPv6 publik yang berbeda. Anda harus memperbarui semua referensi ke alamat IP lama (misalnya, dalam entri DNS) dengan alamat IP baru yang ditugaskan ke instance baru. Jika Anda menggunakan alamat IP Elastic pada instance sumber Anda, pastikan untuk melampirkannya ke instance baru.
- Domain keamanan identifier (SID) masalah konflik dapat terjadi ketika salinan meluncurkan dan mencoba untuk menghubungi domain. Sebelum Anda menangkap AMI, gunakan Sysprep atau hapus instance yang bergabung dengan domain dari domain untuk mencegah masalah konflik. Untuk informasi selengkapnya, lihat [Bagaimana saya bisa menggunakan Sysprep untuk membuat dan menginstal AMI Windows yang dapat digunakan kembali?](#)

### [Jalankan Otomasi ini \(konsol\)](#)

#### Important

Kami tidak menyarankan menggunakan runbook ini untuk menyalin contoh Microsoft Active Directory Domain Controller.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instance yang ingin Anda salin.

- KeyPair

Jenis: String

Deskripsi: (Opsional) Pasangan kunci yang ingin Anda kaitkan dengan instance baru yang disalin. Jika Anda menyalin instance ke Wilayah yang berbeda, pastikan pasangan kunci ada di Wilayah yang ditentukan.

- Wilayah

Jenis: String

Deskripsi: (Opsional) Wilayah yang ingin Anda salin instans. Jika Anda menentukan nilai untuk parameter ini, tetapi tidak menentukan nilai untuk SubnetId dan SecurityGroupIds parameter, otomatisasi mencoba untuk meluncurkan instance di VPC default dengan grup keamanan default. Jika EC2-Classic diaktifkan di Wilayah tujuan, peluncuran akan gagal.

- SubnetId

Jenis: String

Deskripsi: (Opsional) ID subnet yang ingin Anda salin instans. Jika EC2-Classic diaktifkan di Wilayah tujuan, Anda harus memberikan nilai untuk parameter ini.

- InstanceType

Jenis: String

Deskripsi: (Opsional) Jenis instans yang disalin harus diluncurkan sebagai. Jika Anda tidak menentukan nilai untuk parameter ini, jenis instance sumber digunakan. Jika jenis instance sumber tidak didukung di Wilayah tempat instance disalin, otomatisasi akan gagal.

- SecurityGroupIds



Jenis: String

Deskripsi: (Opsional) Daftar ID grup keamanan yang dipisahkan koma yang ingin Anda kaitkan dengan instance yang disalin. Jika Anda tidak menentukan nilai untuk parameter ini, dan instance tidak disalin ke Wilayah yang berbeda, grup keamanan yang terkait dengan instance sumber akan digunakan. Jika Anda menyalin instance ke Wilayah yang berbeda, grup keamanan default untuk VPC default di Wilayah tujuan akan digunakan.

- `KeepImageSourceRegion`

Jenis: Boolean

Nilai yang valid: benar/salah

Default: betul

Deskripsi: (Opsional) Jika Anda menentukan `true` parameter ini, otomatisasi tidak menghapus instance sumber. AMI Jika Anda menentukan `false` parameter ini, otomatisasi membatalkan pendaftaran AMI dan menghapus snapshot terkait.

- `KeepImageDestinationRegion`

Jenis: Boolean

Nilai yang valid: benar/salah

Default: betul

Deskripsi: (Opsional) Jika Anda menentukan `true` parameter ini, otomatisasi tidak menghapus AMI yang disalin ke Wilayah yang Anda tentukan. Jika Anda menentukan `false` parameter ini, otomatisasi membatalkan pendaftaran AMI dan menghapus snapshot terkait.

- `NoRebootInstanceBeforeTakingImage`

Jenis: Boolean

Nilai yang valid: benar/salah

Default: salah

Deskripsi: (Opsional) Jika Anda menentukan `true` parameter ini, instance sumber tidak akan dimulai ulang sebelum membuat parameter. AMI Bila opsi ini digunakan, integritas sistem file pada gambar yang dibuat tidak dapat dijamin.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

Jika Anda menyalin instance ke Wilayah yang berbeda, Anda juga memerlukan izin berikut.

- `ec2:CopyImage`

### Langkah Dokumen

- `describeOriginalInstanceDetail` - Mengumpulkan detail dari instance yang akan disalin.
- `assertRootVolumeIsEbs`- Memeriksa apakah jenis perangkat volume root ebs, dan jika tidak, mengakhiri otomatisasi.
- `evalInputParameters`- Mengevaluasi nilai yang disediakan untuk parameter input.
- `createLocalAmi`- Menciptakan AMI contoh sumber.
- `tagLocalAmi`- Tag yang AMI dibuat pada langkah sebelumnya.
- `branchAssertRegionIsSame`- Cabang berdasarkan apakah instance sedang disalin dalam Wilayah yang sama atau ke Wilayah yang berbeda.
- `branchAssertSameRegionWithKeyPair`- Cabang berdasarkan apakah nilai diberikan untuk `KeyPair` parameter untuk instance yang sedang disalin dalam Wilayah yang sama.

- `sameRegionLaunchInstanceWithKeyPair`- Meluncurkan instans Amazon EC2 dari instans sumber di subnet yang sama atau subnet yang Anda tentukan menggunakan pasangan kunci yang Anda tentukan. AMI
- `sameRegionLaunchInstanceWithoutKeyPair`- Meluncurkan instans Amazon EC2 dari instans sumber di subnet yang sama atau subnet yang Anda tentukan tanpa pasangan kunci. AMI
- `copyAmiToWilayah` - Salinan AMI ke Wilayah tujuan.
- `waitForAvailableDestinationAmi`- Menunggu AMI negara yang disalin menjadi. `available`
- `destinationRegionLaunchInstance` - Meluncurkan Instans Amazon EC2 menggunakan salinan. AMI
- `branchAssertDestinationAmiToDelete`- Cabang berdasarkan nilai yang Anda berikan untuk `KeepImageDestinationRegion` parameter.
- `deregisterDestinationAmiAndDeleteSnapshots`- Deregisters disalin AMI dan menghapus snapshot terkait.
- `branchAssertSourceAmiToDelete`- Cabang berdasarkan nilai yang Anda berikan untuk `KeepImageSourceRegion` parameter.
- `deregisterSourceAmiAndDeleteSnapshots`- Deregisters AMI dibuat dari contoh sumber dan menghapus snapshot terkait.
- `tidur` - Tidur otomatisasi selama 2 detik. Ini adalah langkah terminal.

## Keluaran

```
sameRegionLaunchInstanceWithKeyPair.InstanceIds
```

```
sameRegionLaunchInstanceWithoutKeyPair.InstanceIds
```

```
destinationRegionLaunchContoh. DestinationInstanceId
```

## **AWSSupport - EnableWindowsEC2SerialConsole**

### Deskripsi

Runbook `AWSSupport - EnableWindowsEC2SerialConsole` membantu Anda mengaktifkan Konsol Serial Amazon EC2, Konsol Admin Khusus (SAC), dan menu boot di instans Amazon EC2 Windows Anda. Dengan fitur Konsol Serial Amazon Elastic Compute Cloud (Amazon EC2), Anda memiliki akses ke port serial instans Amazon EC2 untuk memecahkan masalah boot, konfigurasi jaringan, dan masalah lainnya. Runbook mengotomatiskan langkah-langkah yang diperlukan untuk mengaktifkan fitur pada instance dalam status berjalan dan dikelola oleh AWS Systems Manager, serta yang dalam status berhenti atau tidak dikelola oleh. AWS Systems Manager

## Bagaimana cara kerjanya?

Runbook `AWSSupport-EnableWindowsEC2SerialConsole` otomatisasi membantu mengaktifkan SAC dan menu boot di instans Amazon EC2 yang menjalankan Microsoft Windows Server. Untuk instance dalam status berjalan dan dikelola oleh AWS Systems Manager, runbook menjalankan PowerShell skrip AWS Systems Manager Run Command untuk mengaktifkan SAC dan menu boot. Untuk instance dalam status berhenti atau tidak dikelola oleh AWS Systems Manager, runbook menggunakan [AWSSupport-StarTec2 RescueWorkflow untuk membuat instans Amazon EC2 sementara](#) untuk melakukan perubahan yang diperlukan secara offline.

Untuk informasi selengkapnya, lihat [Konsol Serial Amazon EC2 untuk instans Windows](#).

### Important

- Jika Anda mengaktifkan SAC pada instans, layanan Amazon EC2 yang mengandalkan pengambilan kata sandi tidak akan berfungsi dari konsol Amazon EC2. Untuk informasi selengkapnya, lihat [Gunakan SAC untuk memecahkan masalah instans Windows Anda](#).
- Untuk mengonfigurasi akses ke konsol serial, Anda harus memberikan akses konsol serial di tingkat akun dan kemudian mengonfigurasi kebijakan AWS Identity and Access Management (IAM) untuk memberikan akses ke pengguna Anda. Anda juga harus mengonfigurasi pengguna berbasis kata sandi pada setiap instans sehingga pengguna dapat menggunakan konsol serial untuk pemecahan masalah. Untuk informasi selengkapnya, lihat [Mengonfigurasi akses ke Konsol Serial Amazon EC2](#).
- Untuk melihat apakah konsol serial diaktifkan di akun Anda, lihat [Lihat status akses akun ke konsol serial](#).
- Akses konsol serial hanya didukung pada instance virtual yang dibangun di Sistem [Nitro](#).

[Untuk informasi selengkapnya, lihat Prasyarat Konsol Serial Amazon EC2.](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

## Windows

### Parameter

#### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingInstances",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:Describe*",
        "ec2:createTags",
        "ec2:createImage",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "iam:GetInstanceProfile",
        "ssm:GetParameters",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource": [
```

```

        "arn:${Partition}:ec2:${Region}:${AccountId}:instance/
${InstanceId}",
        "arn:${Partition}:ec2:${Region}:${AccountId}:volume/
${VolumeId}",
        "arn:${Partition}:iam::${AccountId}:instance-profile/
${InstanceProfileName}",
        "arn:${Partition}:ssm:${Region}::parameter/aws/service/*",
        "arn:${Partition}:ssm:${Region}::automation-definition/
AWSSupport-StartEC2RescueWorkflow:*",
        "arn:${Partition}:ssm:${Region}::document/AWS-
ConfigureAWSPackage",
        "arn:${Partition}:ssm:${Region}::document/AWS-
RunPowerShellScript"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "cloudformation:CreateStack"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "aws:RequestTag/Name": "AWSSupport-EC2Rescue: *"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "AWSSupport-EC2Rescue-AutomationExecution",
          "Name"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "cloudformation:DeleteStack",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStackResource",
      "cloudformation:DescribeStacks",
      "ec2:AttachVolume",
      "ec2:DetachVolume",
      "ec2:RebootInstances",
      "ec2:StopInstances",

```

```
        "ec2:TerminateInstances",
        "ssm:SendCommand"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/Name": "AWSSupport-EC2Rescue: *"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateLaunchTemplate",
        "ec2>DeleteLaunchTemplate",
        "ec2:RunInstances"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": [
                "cloudformation.amazonaws.com"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "*",
    "Condition": {
        "StringLikeIfExists": {
            "iam:PassedToService": [
                "ssm.amazonaws.com",
                "ec2.amazonaws.com"
            ]
        }
    }
}
]
```

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke `AWSSupport-EnableWindowsEC2SerialConsole` dalam AWS Systems Manager konsol.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:

- `InstanceId`: (Diperlukan)

ID instans Amazon EC2 yang ingin Anda aktifkan konsol serial Amazon EC2, (SAC), dan menu boot.

- `AutomationAssumeRole`: (Opsional)

Nama Sumber Daya Amazon (ARN) dari peran IAM yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `HelperInstanceType`: (Bersyarat)

Jenis instans Amazon EC2 yang disediakan runbook untuk mengonfigurasi konsol serial Amazon EC2 untuk instans offline.

- `HelperInstanceProfileName`: (Bersyarat)

Nama profil instans IAM yang ada untuk instance helper. Jika Anda mengaktifkan SAC dan menu boot pada instance yang dalam status berhenti atau tidak dikelola oleh AWS Systems Manager, ini diperlukan. Jika profil instans IAM tidak ditentukan, otomatisasi membuatnya atas nama Anda.

- `SubnetId`: (Bersyarat)

ID subnet untuk instance helper. Secara default, ia menggunakan subnet yang sama di mana instance yang disediakan berada.

### Important

Jika Anda menyediakan subnet kustom, subnet harus berada di Availability Zone yang sama `InstanceId`, dan harus mengizinkan akses ke endpoint Systems Manager. Ini



hanya diperlukan jika instance target dalam status berhenti atau tidak dikelola oleh AWS Systems Manager.

- `CreateInstanceBackupBeforeScriptExecution`: (Opsional)

Tentukan Benar untuk membuat cadangan Amazon Machine Images (AMI) dari instans Amazon EC2 sebelum mengaktifkan SAC dan menu boot. AMI akan bertahan setelah otomatisasi selesai. Anda bertanggung jawab untuk mengamankan akses ke AMI atau menghapusnya.

- `BackupAmazonMachineImagePrefix`: (Bersyarat)

Awalan untuk Amazon Machine Image (AMI) yang dibuat jika `CreateInstanceBackupBeforeScriptExecution` parameter disetel ke `True`.

**Input parameters**

**InstanceId**  
(Required) The ID of Amazon EC2 instance that you want to enable EC2 serial console, Special Admin Console (SAC), and boot menu.  
🔗 [show interactive instance picker](#)

`i-01234567890abcdef0`

**AutomationAssumeRole**  
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.  
EC2SerialConsole-MinimumRole-AutomationAssumeRole-7inoDR7gFLIT

**SubnetId**  
(Conditional) The subnet ID for a helper instance. By default, the same subnet where the provided instance resides is used. Important: If you provide a custom subnet, it must be in the same Availability Zone as InstanceId, and it must allow access to the Systems Manager endpoints. This is only required if the target instance is in 'stopped' state or is not managed by AWS Systems Manager.  
SelectInstanceSubnet

**CreateInstanceBackupBeforeScriptExecution**  
(Optional) Specify 'True' to create an Amazon Machine Images (AMI) backup of the EC2 instance before enabling SAC and boot menu. The AMI will persist after the automation completes. It is your responsibility to secure access to the AMI, or to delete it.  
True

**HelperInstanceType**  
(Conditional) The type of Amazon EC2 instance that the runbook provisions to configure EC2 serial console for an offline instance.  
t3.medium

**HelperInstanceProfileName**  
(Conditional) The name of an existing IAM instance profile for the helper instance. If you are enabling SAC and boot menu on an instance that is in 'stopped' state or not managed by AWS Systems Manager, this is required. If an IAM instance profile is not specified, the automation creates one on your behalf.  
String

**BackupAmazonMachineImagePrefix**  
(Conditional) A prefix for the Amazon Machine Image (AMI) that is created if the 'CreateInstanceBackupBeforeScriptExecution' parameter is set to 'True'.  
AWSsupport

#### 4. Pilih Jalankan.

#### 5. Otomatisasi dimulai.

#### 6. Dokumen melakukan langkah-langkah berikut:

- `CheckIfEc2SerialConsoleAccessEnabled`:

Memeriksa apakah akses Konsol Serial Amazon EC2 diaktifkan di tingkat akun. Catatan: Akses ke konsol serial tidak tersedia secara default. Untuk informasi selengkapnya, lihat [Mengonfigurasi akses ke Konsol Serial Amazon EC2](#).

- `CheckIfEc2InstanceIsWindows`:

Menegaskan jika platform instance target adalah Windows.

- `GetInstanceType`:

Mengambil jenis instance dari instance target.

- `CheckIfInstanceTypeIsNitro`:

Memeriksa apakah hypervisor tipe instance berbasis Nitro. Akses Konsol Serial hanya didukung pada instans virtual yang dibangun di Sistem Nitro.

- `CheckIfInstancesInAutoScalingKelompok`:

Memeriksa apakah instans Amazon EC2 merupakan bagian dari grup Auto Scaling Amazon EC2 dengan memanggil API `DescribeAutoScalingInstances`. Jika instans merupakan bagian dari grup Auto Scaling Amazon EC2, instans ini memastikan bahwa Asisten Porting untuk instans `.NET` dalam status siklus hidup Siaga.

- `WaitForEc2InstanceStateStablized`:

Menunggu instance dalam keadaan berjalan atau berhenti.

- `GetEc2InstanceState`:

Mendapat status saat ini dari instance.

- `BranchOnEc2InstanceState`:

Cabang berdasarkan status instance yang diambil pada langkah sebelumnya. Jika keadaan instance itu berjalan, ia pergi ke `CheckIfEc2InstanceIsManagedBySSM` langkah dan jika tidak, ia pergi ke `CheckIfHelperInstanceProfileIsProvided` langkah.

- `CheckIfEc2 InstancesManagedBy SSM`:

Memeriksa apakah instance dikelola oleh AWS Systems Manager. Jika dikelola, runbook mengaktifkan SAC dan menu boot menggunakan PowerShell Run Command.

- `BranchOnPreEC2: RescueBackup`

Cabang berdasarkan parameter `CreateInstanceBackupBeforeScriptExecution` input.

- `CreateAmazonMachineImageBackup`:

Membuat cadangan AMI dari instance.

- `EnableSacAndBootMenu`:

Mengaktifkan SAC dan menu boot dengan menjalankan skrip PowerShell Run Command.

- `RebootInstance`:

Mem-boot ulang instans Amazon EC2 untuk menerapkan konfigurasi. Ini adalah langkah terakhir jika instance online dan dikelola oleh AWS Systems Manager.

- `CheckIfHelperInstanceProfileIsProvided`:

Memeriksa apakah `HelperInstanceProfileName` yang ditentukan ada sebelum

- `RunAutomationToInjectOfflineScriptForMengaktifkanSacAndBootMenu`:

Menjalankan menu `AWSsupport-StartEC2RescueWorkflow` to enable SAC dan boot saat instance dalam status berhenti atau tidak dikelola oleh AWS Systems Manager.

- `GetExecutionDetails`:

Mengambil ID Gambar dari cadangan dan output skrip offline.

## 7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci:

- `AktifkanSAC.OutputAndBootMenu`:

Output dari eksekusi perintah di `EnableSACAndBootMenu` langkah.

- `GetExecutionDetails.OfflineScriptOutput`:

Output dari skrip offline dieksekusi di

`RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` langkah.

- `GetExecutionDetails.BackupBeforeScriptExecution`:

ID gambar cadangan AMI diambil jika parameter

`CreateInstanceBackupBeforeScriptExecution` input `True`.

## Output eksekusi pada instance yang berjalan dan dikelola oleh AWS Systems Manager

* Outputs	
<pre>GetExecutionDetails.BackupBeforeScriptExecution No output available yet because the step is not successfully executed  EnableSACAndBootMenu.Output The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully.</pre>	<pre>GetExecutionDetails.OfflineScriptOutput No output available yet because the step is not successfully executed</pre>

## Output eksekusi pada instance yang dihentikan atau tidak dikelola oleh AWS Systems Manager

* Outputs	
<pre>EnableSACAndBootMenu.Output No output available yet because the step is not successfully executed  GetExecutionDetails.OfflineScriptOutput Device xvdf mapped to D Offline Windows installation found in directory D:\Windows Windows Server 2016 Datacenter (18.0.14393.6522) BCD Store found in directory D:\Boot\BCD Detecting installed drivers EC2Rescue environment variables set EC2Rescue script variables set The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully. Volume successfully set offline</pre>	<pre>GetExecutionDetails.BackupBeforeScriptExecution ami-09c33701932955dde</pre>

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)

- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

## AWSSupport - ExecuteEC2Rescue

### Deskripsi

Runbook ini menggunakan EC2Rescue alat untuk memecahkan masalah dan, jika memungkinkan, memperbaiki masalah konektivitas umum dengan instans Amazon Elastic Compute Cloud (Amazon EC2) yang ditentukan untuk Linux atau. Windows Server Instans dengan volume root terenkripsi tidak didukung.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- EC2 RescueInstanceType

Jenis: String

Nilai yang valid: `t2.small` | `t2.medium` | `t2.large`

Default: `t2.small`

Deskripsi: (Diperlukan) Jenis instans EC2 untuk EC2Rescue instans. Ukuran yang disarankan: `t2.small`

- `LogDestination`

Jenis: String


Deskripsi: (Opsional) nama bucket Amazon S3 di akun tempat Anda ingin mengupload log pemecahan masalah. Pastikan kebijakan bucket tidak memberikan izin baca/tulis yang tidak perlu kepada pihak yang tidak memerlukan akses ke log yang dikumpulkan.

- `SubnetId`

Jenis: String

Bawaan: `CreateNew VPC`

Deskripsi: (Opsional) ID subnet untuk EC2Rescue instance. Secara default, AWS Systems Manager Automation membuat VPC baru. Atau, gunakan `SelectedInstanceSubnet` untuk menggunakan subnet yang sama dengan instans Anda, atau tentukan ID subnet kustom.

 Important

Subnet harus berada di Availability Zone yang sama dengan `UnreachableInstanceId`, dan harus mengizinkan akses ke endpoint SSM.

- `UnreachableInstancelId`

Jenis: String

Deskripsi: (Diperlukan) ID instans EC2 Anda yang tidak terjangkau.

 Important

Otomatisasi Manajer Sistem menghentikan instans ini, dan membuat AMI sebelum mencoba operasi apa pun. Data yang disimpan dalam volume toko instance akan hilang. Alamat IP publik akan berubah jika Anda tidak menggunakan alamat IP elastis.

## Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

Anda harus memiliki setidaknya `ssm:StartAutomationExecution` dan `ssm:GetAutomationExecution` untuk dapat membaca output otomatisasi. Untuk informasi lebih lanjut tentang izin yang diperlukan, lihat [AWSSupport-StartEC2RescueWorkflow](#).

## Langkah Dokumen

1. `aws:assertAwsResourceProperty`- Menegaskan jika contoh yang disediakan adalah Windows Server
  - a. (`EC2RescueuntukWindows Server`) Jika instance yang disediakan adalah sebuah Windows Server instance:
    - i. `aws:executeAutomation`- Memanggil `AWSSupport-StartEC2RescueWorkflow` dengan `EC2Rescue` untuk Windows Server skrip offline.
    - ii. `aws:executeAwsApi`- Mengambil ID AMI cadangan dari otomatisasi bersarang.
    - iii. `aws:executeAwsApi`- Mengambil ringkasan `EC2Rescue` dari otomatisasi bersarang.
  - b. (`EC2Rescueuntuk Linux`) Jika instance yang disediakan adalah instance Linux:
    - i. `aws:executeAutomation`- Memanggil `AWSSupport-StartEC2RescueWorkflow` dengan `EC2Rescue` untuk skrip offline Linux
    - ii. `aws:executeAwsApi`- Mengambil ID AMI cadangan dari otomatisasi bersarang.
    - iii. `aws:executeAwsApi`- Mengambil ringkasan `EC2Rescue` dari otomatisasi bersarang.

## Keluaran

```
getEC2RescueForWindowsResult.Output
```

```
getWindowsBackupAmi.ImageId
```

```
getEC2RescueForLinuxResult.Output
```

```
getLinuxBackupAmi.ImageId
```

## **AWSSupport-ListEC2Resources**

### Deskripsi

`AWSsupport-ListEC2ResourcesRunbook` mengembalikan informasi tentang instans Amazon EC2 dan sumber daya terkait seperti volume Amazon Elastic Block Store (Amazon EBS), alamat IP Elastic, dan grup Amazon EC2 Auto Scaling dari yang Anda tentukan. Wilayah AWS Secara default, informasi dikumpulkan dari semua Wilayah dan ditampilkan dalam output otomatisasi. Secara opsional, Anda dapat menentukan bucket Amazon Simple Storage Service (Amazon S3) untuk informasi yang akan diunggah sebagai file nilai yang dipisahkan koma (.csv).

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `Bucket`

Jenis: String

Deskripsi: (Opsional) Nama bucket S3 tempat informasi dikumpulkan diunggah.

- `DisplayResourceDeletionDocumentation`

Jenis: String

Default: `betul`

Deskripsi: (Opsional) Jika diatur `true`, otomatisasi membuat tautan dalam output ke dokumentasi yang terkait dengan penghapusan sumber daya Anda.

- `RegionsToQuery`

Jenis: String

Default: Semua

Deskripsi: (Opsional) Wilayah tempat Anda ingin mengumpulkan informasi terkait Amazon EC2.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRegions`
- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

Selain itu, agar berhasil mengunggah informasi yang dikumpulkan ke bucket S3 yang Anda tentukan, tindakan berikut ini `AutomationAssumeRole` memerlukan tindakan berikut:

- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:PutObject`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan Wilayah yang diaktifkan untuk akun.



- `aws:executeScript`- Konfirmasi Daerah diaktifkan untuk akun mendukung Daerah ditentukan dalam `RegionsToQuery` parameter.
- `aws:branch`- Jika tidak ada Wilayah yang diaktifkan untuk akun, otomatisasi akan berakhir.
- `aws:executeScript`- Daftar semua instans EC2 untuk akun dan Wilayah yang Anda tentukan.
- `aws:executeScript`- Daftar semua Amazon Machine Images (AMI) untuk akun dan Wilayah yang Anda tentukan.
- `aws:executeScript`- Daftar semua volume EBS untuk akun dan Wilayah yang Anda tentukan.
- `aws:executeScript`- Daftar semua alamat IP elastis untuk akun dan Wilayah yang Anda tentukan.
- `aws:executeScript`- Daftar semua antarmuka jaringan elastis untuk akun dan Wilayah yang Anda tentukan.
- `aws:executeScript`- Daftar semua grup Auto Scaling untuk akun dan Wilayah yang Anda tentukan.
- `aws:executeScript`- Daftar semua load balancer untuk akun dan Wilayah yang Anda tentukan.
- `aws:executeScript`- Mengunggah informasi yang dikumpulkan ke bucket S3 yang ditentukan jika Anda memberikan nilai untuk `Bucket` parameter.

## AWSSupport-ManageRDPSettings

### Deskripsi

AWSSupport-ManageRDPSettingsRunbook memungkinkan pengguna untuk mengelola pengaturan Remote Desktop Protocol (RDP) umum, seperti port RDP dan Network Layer Authentication (NLA). Secara default, runbook membaca dan mengeluarkan nilai pengaturan.

#### Important

Perubahan pada pengaturan RDP harus ditinjau dengan cermat sebelum menjalankan runbook ini.

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

## Pemilik

Amazon

Platform

Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans terkelola untuk mengelola pengaturan RDP.

- NLA SettingAction

Jenis: String

Nilai yang valid: Periksa | Aktifkan | Nonaktifkan

Default: Periksa

Deskripsi: (Diperlukan) Tindakan yang harus dilakukan pada pengaturan NLA: Periksa, Aktifkan, Nonaktifkan.

- RDPport

Jenis: String

Default: 3389

Deskripsi: (Opsional) Tentukan port RDP baru. Digunakan hanya ketika tindakan diatur ke Memodifikasi. Nomor port harus antara 1025-65535. Catatan: Setelah port diubah, layanan RDP dimulai ulang.

- RDP PortAction

Jenis: String

Nilai yang valid: Periksa | Modifikasi

Default: Periksa

Deskripsi: (Diperlukan) Tindakan untuk diterapkan ke port RDP.

- RemoteConnections

Jenis: String

Nilai yang valid: Periksa | Aktifkan | Nonaktifkan

Default: Periksa

Deskripsi: (Diperlukan) Tindakan yang harus dilakukan pada pengaturan FdenytsConnections.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

Instans EC2 yang menerima perintah harus memiliki peran IAM dengan kebijakan terkelola Amazon AmazonSSM ManagedInstanceCore yang terpasang. Pengguna harus memiliki setidaknya ssm: SendCommand untuk mengirim perintah ke instance, ditambah ssm: GetCommandInvocation untuk dapat membaca output perintah.

Langkah Dokumen

`aws : runCommand-` Jalankan PowerShell script untuk mengubah atau memeriksa pengaturan RDP pada contoh target.

Keluaran

ManajerDPSettings.output

## **AWSsupport-ManageWindowsService**

Deskripsi

AWSSupport-ManageWindowsServiceRunbook memungkinkan Anda untuk menghentikan, memulai, memulai ulang, menjeda, atau menonaktifkan layanan Windows apa pun pada instance target.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans terkelola untuk mengelola layanan.

- ServiceAction

Jenis: String

Nilai yang valid: Periksa | Mulai Ulang | Paksa Mulai Ulang | Mulai | Berhenti | Paksa Berhenti | Jeda

Default: Periksa

Deskripsi: (Diperlukan) Tindakan untuk diterapkan ke layanan Windows. Perhatikan bahwa Force-Restart dan Force-Stop dapat digunakan untuk me-restart dan menghentikan layanan yang memiliki layanan tergantung.

- StartupType

Jenis: String

Nilai yang valid: Periksa | Otomatis | Permintaan | Dinonaktifkan | DelayedAutoStart

Default: Periksa

Deskripsi: (Diperlukan) Jenis startup untuk diterapkan ke layanan Windows.

- WindowsServiceName

Jenis: String

Deskripsi: (Diperlukan) Nama layanan Windows yang valid.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan agar instans EC2 yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon AmazonSSM ManagedInstanceCore yang terpasang. Pengguna harus memiliki setidaknya ssm: StartAutomationExecution dan ssm: SendCommand untuk menjalankan otomatisasi dan mengirim perintah ke instance, ditambah ssm: GetAutomationExecution untuk dapat membaca output otomatisasi.

Langkah Dokumen

aws : runCommand- Jalankan PowerShell skrip untuk menerapkan konfigurasi yang diinginkan ke layanan Windows pada instance target.

Keluaran

manageWindowsService.Keluaran

# AWSsupport-MigrateEC2ClassicToVPC

## Deskripsi

AWSsupport-MigrateEC2ClassicToVPCRunbook memigrasikan instans Amazon Elastic Compute Cloud (Amazon EC2) dari EC2-Classic ke cloud pribadi virtual (VPC). Runbook ini mendukung migrasi instans Amazon EC2 dari jenis virtualisasi mesin virtual perangkat keras (HVM) dengan volume root Amazon Elastic Block Store (Amazon EBS).

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda.

- Persetujuan

Jenis: StringList

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) pengguna IAM yang dapat menyetujui atau menolak tindakan tersebut. Parameter ini hanya berlaku jika Anda menentukan CutOver nilai untuk MigrationType parameter.

- DestinationSecurityGroupId

Jenis: `StringList`

Deskripsi: (Opsional) ID grup keamanan yang ingin Anda kaitkan dengan instans Amazon EC2 yang diluncurkan di VPC Anda. Jika Anda tidak menentukan nilai untuk parameter ini, otomatisasi akan membuat grup keamanan di VPC Anda dan menyalin aturan dari grup keamanan di EC2-Classic. Jika aturan gagal disalin ke grup keamanan baru, grup keamanan default VPC Anda dikaitkan dengan instans Amazon EC2.

- `DestinationSubnetId`

Jenis: `String`

Deskripsi: (Opsional) ID subnet tempat Anda ingin memigrasikan instans Amazon EC2 Anda. Jika Anda tidak menentukan nilai untuk parameter ini, otomatisasi secara acak memilih subnet dari VPC Anda.

- `InstanceId`

Jenis: `String`

Deskripsi: (Diperlukan) ID instans Amazon EC2 yang ingin Anda migrasi.

- `MigrationType`

Jenis: `String`

Nilai yang valid: `CutOver` | `Uji`

Deskripsi: (Diperlukan) Jenis migrasi yang ingin Anda lakukan.

`CutOver` Opsi ini memerlukan persetujuan untuk menghentikan instans Amazon EC2 Anda yang berjalan di EC2-Classic. Setelah tindakan ini disetujui, instans Amazon EC2 dihentikan dan otomatisasi membuat Amazon Machine Image (AMI). Ketika AMI statusnya `available`, instans Amazon EC2 baru diluncurkan dari ini AMI di yang `DestinationSubnetId` Anda tentukan di VPC Anda. Jika instans Amazon EC2 Anda yang berjalan di EC2-Classic memiliki alamat IP Elastic yang terpasang, instans akan dipindahkan ke instans Amazon EC2 yang baru dibuat di VPC Anda. Jika instans Amazon EC2 yang diluncurkan di VPC Anda gagal dibuat karena alasan apa pun, instans akan dihentikan dan persetujuan diminta untuk memulai instans Amazon EC2 Anda di EC2-Classic.

`Test` Opsi ini membuat AMI instans Amazon EC2 Anda yang berjalan di EC2-Classic tanpa me-reboot. Karena instans Amazon EC2 tidak di-reboot, kami tidak dapat menjamin integritas

sistem file dari gambar yang dibuat. Ketika AMI statusnya `available`, instans Amazon EC2 baru diluncurkan dari ini AMI dalam `DestinationSubnetId` yang Anda tentukan di VPC Anda. Jika instans Amazon EC2 yang berjalan di EC2-Classic memiliki alamat IP Elastic yang terpasang, otomatisasi akan memverifikasi bahwa yang `DestinationSubnetId` Anda tentukan bersifat publik. Jika instans Amazon EC2 yang diluncurkan di VPC Anda gagal dibuat karena alasan apa pun, instans akan dihentikan dan otomatisasi berakhir.

- `SNSNotificationARNforApproval`

Jenis: String

Deskripsi: (Opsional) Topik ARN Layanan Pemberitahuan Sederhana Amazon (Amazon SNS) yang ingin Anda kirimkan permintaan persetujuan. Parameter ini hanya berlaku jika Anda menentukan `CutOver` nilai untuk `MigrationType` parameter.

- `TargetInstanceType`

Jenis: String

Default: `t2.2xlarge`

Deskripsi: (Opsional) Jenis instans Amazon EC2 yang ingin Anda luncurkan di VPC Anda. Hanya jenis instans berbasis Xen, seperti T2, M4, atau C4, yang didukung.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetDocument`
- `ssm:ListDocumentVersions`
- `ssm:ListDocuments`
- `ssm:StartAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:ListSubscriptions`
- `sns:ListTopics`
- `sns:Publish`
- `ec2:AssociateAddress`



- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateImage`
- `ec2:CreateSecurityGroup`
- `ec2>DeleteSecurityGroup`
- `ec2:MoveAddressToVpc`
- `ec2:RunInstances`
- `ec2:StopInstances`
- `ec2:CreateTags`
- `ec2:DescribeAddresses`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroupReferences`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeTags`
- `ec2:DescribeVpcs`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeImages`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan detail tentang instans Amazon EC2 yang Anda tentukan dalam parameter. `InstanceId`
- `aws:assertAwsResourceProperty`- Mengonfirmasi jenis instance yang Anda tentukan dalam `TargetInstanceType` parameter berbasis Xen.
- `aws:assertAwsResourceProperty`- Mengonfirmasi instans Amazon EC2 yang Anda tentukan dalam `InstanceId` parameter adalah jenis virtualisasi HVM.
- `aws:assertAwsResourceProperty`- Mengonfirmasi instans Amazon EC2 yang Anda tentukan dalam `InstanceId` parameter memiliki volume root Amazon EBS.

- `aws:executeScript`- Membuat grup keamanan sesuai kebutuhan tergantung pada nilai yang Anda tentukan untuk `DestinationSecurityGroupId` parameter.
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan dalam `DestinationSubnetId` parameter.
- `aws:executeAwsApi`- Mengidentifikasi VPC default di Wilayah AWS tempat Anda menjalankan otomatisasi ini.
- `aws:executeAwsApi`- Secara acak memilih ID subnet yang terletak di VPC default.
- `aws:createImage`- Membuat AMI instans Amazon EC2 tanpa me-reboot.
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan untuk `MigrationType` parameter.
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan untuk `DestinationSubnetId` parameter.
- `aws:runInstances`- Meluncurkan instans baru dari yang AMI dibuat tanpa me-reboot instans Amazon EC2 di EC2-Classic.
- `aws:changeInstanceState`- Mengakhiri instans Amazon EC2 yang baru diluncurkan jika langkah sebelumnya gagal karena alasan apa pun.
- `aws:runInstances`- Meluncurkan instans baru dari yang AMI dibuat tanpa me-reboot instans Amazon EC2 di EC2-Classic dalam jika disediakan. `DestinationSubnetId`
- `aws:changeInstanceState`- Mengakhiri instans Amazon EC2 yang baru diluncurkan jika langkah sebelumnya gagal karena alasan apa pun.
- `aws:assertAwsResourceProperty`- Mengonfirmasi perilaku berhenti untuk instans Amazon EC2 yang berjalan di EC2-Classic.
- `aws:approve`- Menunggu persetujuan untuk menghentikan instans Amazon EC2.
- `aws:changeInstanceState`- Menghentikan instans Amazon EC2 yang berjalan di EC2-Classic.
- `aws:changeInstanceState`- Paksa menghentikan instans Amazon EC2 berjalan di EC2-Classic jika diperlukan.
- `aws:createImage`- Membuat AMI instans Amazon EC2 setelah dihentikan.
- `aws:branch`- Cabang berdasarkan nilai yang ditentukan untuk `DestinationSubnetId` parameter.
- `aws:runInstances`- Meluncurkan instans baru dari pembuatan instans Amazon EC2 yang dihentikan di EC2-Classic. AMI
- `aws:approve`- Menunggu persetujuan untuk menghentikan instans yang baru diluncurkan dan memulai instans Amazon EC2 di EC2-Classic jika langkah sebelumnya gagal karena alasan apa pun.

- `aws:changeInstanceState`- Mengakhiri instans Amazon EC2 yang baru diluncurkan.
- `aws:runInstances`- Meluncurkan instans baru dari pembuatan instans Amazon EC2 yang dihentikan di EC2-Classic dari parameter. `AMI DestinationSubnetId`
- `aws:approve`- Menunggu persetujuan untuk menghentikan instans yang baru diluncurkan dan memulai instans Amazon EC2 di EC2-Classic jika langkah sebelumnya gagal karena alasan apa pun.
- `aws:changeInstanceState`- Mengakhiri instans Amazon EC2 yang baru diluncurkan.
- `aws:changeInstanceState`- Memulai instans Amazon EC2 yang dihentikan di EC2-Classic.
- `aws:branch`- Cabang berdasarkan apakah instans Amazon EC2 memiliki alamat IP publik.
- `aws:executeAwsApi`- Memverifikasi apakah alamat IP publik adalah alamat IP elastis.
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan dalam `MigrationType` parameter.
- `aws:executeAwsApi`- Memindahkan alamat IP elastis ke VPC Anda.
- `aws:executeAwsApi`- Mengumpulkan ID alokasi alamat IP Elastic yang dipindahkan ke VPC Anda.
- `aws:branch`- Cabang berdasarkan subnet instans Amazon EC2 yang berjalan di VPC Anda diluncurkan.
- `aws:executeAwsApi`- Melampirkan alamat IP Elastic ke instance yang baru diluncurkan di VPC Anda.
- `aws:executeScript`- Mengonfirmasi subnet instans Amazon EC2 yang baru diluncurkan yang berjalan di VPC Anda bersifat publik.

## Keluaran

`getInstanceProperties.virtualizationType` - Jenis virtualisasi instans Amazon EC2 yang berjalan di EC2-Classic.

`getInstanceProperties.rootDeviceType`- Jenis perangkat root instans Amazon EC2 yang berjalan di EC2-Classic.

`createAMIWithoutReboot.ImageId`- ID yang AMI dibuat tanpa me-reboot instans Amazon EC2 yang berjalan di EC2-Classic.

`getDefaultVPC.VpcId`- ID VPC default tempat instans Amazon EC2 baru diluncurkan jika nilai untuk `DestinationSubnetId` parameter tidak disediakan.

`getSubnetIdInDefaultVPC.subnetIdFromDefaultVpc`- ID subnet di VPC default tempat instans Amazon EC2 baru diluncurkan jika nilai untuk `DestinationSubnetId` parameter tidak disediakan.

`launchTestInstanceDefaultVPC.InstanceIds`- ID instans Amazon EC2 yang baru diluncurkan di VPC default Anda selama jenis `Test` migrasi.

`launchTestInstanceProvidedSubnet.InstanceIds`- ID instans Amazon EC2 yang baru diluncurkan dalam `DestinationSubnetId` yang Anda tentukan selama jenis `Test` migrasi.

`createAMIAfterStoppingInstance.ImageId`- ID yang AMI dibuat setelah menghentikan instans Amazon EC2 berjalan di `EC2-Classical`.

`launchCutOverInstanceProvidedSubnet.InstanceIds`- ID instans Amazon EC2 yang baru diluncurkan dalam `DestinationSubnetId` yang Anda tentukan selama jenis `CutOver` migrasi.

`launchCutOverInstanceDefaultVPC.InstanceIds`- ID instans Amazon EC2 yang baru diluncurkan di VPC default Anda selama jenis `CutOver` migrasi.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`- Apakah subnet yang dipilih oleh otomatisasi di VPC default Anda bersifat publik.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`- Apakah subnet yang Anda tentukan di `DestinationSubnetId` publik.

## **AWS Support - Migrate Xen To Nitro Linux**

### Deskripsi

[AWS Support - Migrate Xen To Nitro Linux Runbook mengkloning, menyiapkan, dan memigrasikan instans Linux Xen Amazon Elastic Compute Cloud \(Amazon EC2\) ke jenis instans Nitro](#) Runbook ini menyediakan dua opsi untuk jenis operasi:

- `Clone&Migrate`- Alur kerja opsi ini terdiri dari Pemeriksaan Pendahuluan, Pengujian, dan `Clone&Migrate` fase. Alur kerja dijalankan menggunakan `AWS Support - CloneXenEC2InstanceAndMigrateToNitro` runbook.
- `FullMigration`- Opsi ini menjalankan `Clone&Migrate` alur kerja dan kemudian melakukan langkah tambahan Ganti volume Amazon EBS root.

**⚠ Important**

Menggunakan runbook ini menimbulkan biaya ke akun Anda untuk waktu berjalan instans Amazon EC2, pembuatan volume Amazon Elastic Block Store (Amazon EBS), dan AMIs. Untuk detail selengkapnya, lihat Harga [Amazon EC2](#) dan Harga [Amazon EBS](#).

## Pemeriksaan awal

Otomatisasi melakukan pemeriksaan awal berikut sebelum melanjutkan migrasi. Jika salah satu pemeriksaan gagal, otomatisasi berakhir. Fase ini hanya bagian dari Clone&Migrate alur kerja.

- Memeriksa apakah instance target sudah merupakan tipe Nitro instance.
- Memeriksa apakah opsi pembelian Instans Spot digunakan untuk instance target.
- Memeriksa apakah volume penyimpanan instance dilampirkan ke instance target.
- Memverifikasi target misalnya sistem operasi (OS) adalah Linux.
- Memeriksa apakah instans target adalah bagian dari grup Penskalaan Otomatis Amazon EC2. Jika itu adalah bagian dari grup Auto Scaling, otomatisasi memverifikasi bahwa instance berada dalam keadaan standby.
- Memverifikasi bahwa instance dikelola oleh AWS Systems Manager.

## Pengujian

Otomatisasi membuat Amazon Machine Image (AMI) dari instance target dan meluncurkan instance pengujian dari yang baru dibuat AMI. Fase ini adalah bagian dari hanya Clone&Migrate alur kerja.

Jika instans pengujian melewati semua pemeriksaan status, otomatisasi akan dijeda dan persetujuan dari prinsipal yang ditunjuk diminta melalui pemberitahuan Amazon Simple Notification Service (Amazon SNS). Jika persetujuan diberikan, otomatisasi mengakhiri instance pengujian, menghentikan instance target, dan melanjutkan migrasi, sementara yang baru AMI dibuat dibatalkan pendaftaran di akhir alur kerja. Clone&Migrate

**ℹ Note**

Sebelum memberikan persetujuan, sebaiknya verifikasi bahwa semua aplikasi yang berjalan pada instance target telah ditutup dengan anggun.

## Kloning dan Migrasi

Otomatisasi membuat yang lain AMI dari instance target, dan meluncurkan instance baru untuk diubah ke jenis Nitro instance. Otomatisasi melengkapi prasyarat berikut sebelum melanjutkan migrasi. Jika salah satu pemeriksaan gagal, otomatisasi berakhir. Fase ini juga hanya bagian dari `Clone&Migrate` alur kerja.

- Menghidupkan atribut jaringan yang disempurnakan (ENA).
- Menginstal driver ENA versi terbaru jika belum diinstal, atau memperbarui versi driver ENA ke versi terbaru. Untuk memastikan kinerja jaringan maksimum, memperbarui ke versi driver ENA terbaru diperlukan jika jenis Nitro instans adalah generasi ke-6.
- Memverifikasi bahwa modul NVMe diinstal. Jika modul diinstal, otomatisasi memverifikasi bahwa modul dimuat. `initramfs`
- Menganalisis `/etc/fstab` dan mengganti entri dengan nama perangkat blok (`/dev/sd*` atau `/dev/xvd*`) dengan UUID masing-masing. Sebelum memodifikasi konfigurasi, otomatisasi membuat cadangan file di jalur `/etc/fstab*`.
- Mematikan penamaan antarmuka yang dapat diprediksi dengan menambahkan `net.ifnames=0` opsi ke `GRUB_CMDLINE_LINUX` baris dalam `/etc/default/grub` file jika ada, atau ke kernel di `boot/grub/menu.lst`.
- Menghapus `/etc/udev/rules.d/70-persistent-net.rules` file jika ada. Sebelum menghapus file, otomatisasi membuat cadangan file di jalur `/etc/udev/rules.d/`.

Setelah memverifikasi semua persyaratan, jenis instans diubah ke jenis Nitro instans yang Anda tentukan. Otomatisasi menunggu instance yang baru dibuat untuk meneruskan semua pemeriksaan status setelah memulai sebagai jenis Nitro instans. Otomatisasi kemudian menunggu persetujuan dari prinsipal yang ditunjuk untuk membuat instance yang berhasil AMI diluncurkan. Nitro Jika persetujuan ditolak, otomatisasi berakhir, membiarkan instance yang baru dibuat berjalan, dan instance target tetap dihentikan.

### Ganti Volume Amazon EBS root

Jika Anda memilih `FullMigration` sebagai `OperationType`, otomatisasi akan memigrasikan instans Amazon EC2 target ke jenis Nitro instans yang Anda tentukan. Otomatisasi meminta persetujuan dari prinsipal yang ditunjuk untuk mengganti volume akar Amazon EBS dari instans Amazon EC2 target dengan volume akar instans Amazon EC2 yang dikloning. Setelah migrasi berhasil, instans Amazon EC2 yang dikloning dihentikan. Jika otomatisasi gagal, volume root Amazon EBS asli dilampirkan ke instans Amazon EC2 target. Jika volume Amazon EBS root yang dilampirkan

ke instans Amazon EC2 target memiliki tag dengan aws : awalan yang diterapkan, FullMigration operasi tidak didukung.

Sebelum Anda mulai

Instance target harus memiliki akses internet outbound. Ini untuk mengakses repositori untuk driver dan dependensi seperti kernel-devel,,,gcc,patch,, rpm-build wget dracut, make dan. linux-headers unzip Manajer paket digunakan jika diperlukan.

Topik Amazon SNS diperlukan untuk mengirim pemberitahuan untuk persetujuan dan pembaruan. Untuk informasi selengkapnya tentang membuat topik Amazon SNS, lihat [Membuat topik Amazon SNS di Panduan](#) Pengembang Layanan Pemberitahuan Sederhana Amazon.

Runbook ini mendukung sistem operasi berikut:

- RHEL7.x - 8.5
- Amazon Linux (2018.03), Amazon Linux 2
- Debian Server
- Ubuntu Server 18.04 LTS, 20.04 LTS, dan 20.10 STR
- SUSE Linux Enterprise Server(SUSE12SP5, SUSE15SP2)

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Pengakuan

Jenis: String

Deskripsi: (Diperlukan) Baca rincian lengkap dari tindakan yang dilakukan oleh runbook otomatisasi ini, dan masukkan **Yes, I understand and acknowledge** untuk melanjutkan dengan menggunakan runbook.

- Persetujuan

Jenis: String

Deskripsi: (Diperlukan) ARN peran IAM, pengguna, atau nama pengguna yang dapat memberikan persetujuan untuk otomatisasi. Anda dapat menentukan maksimal 10 pemberi persetujuan.

- DeleteResourcesOnFailure

Jenis: Boolean

Deskripsi: (Opsional) Menentukan apakah instans yang baru AMI dibuat dan migrasi akan dihapus jika otomatisasi gagal.

Nilai yang valid: Benar | Salah

Default: BETUL

- MinimumRequiredApprovals

Jenis: String

Deskripsi: (Opsional) Jumlah minimum persetujuan yang diperlukan untuk terus menjalankan otomatisasi saat persetujuan diminta.

Nilai yang valid: 1-10

Default: 1

- NitroInstanceType



Jenis: String

Deskripsi: (Diperlukan) Jenis Nitro instans yang ingin Anda ubah instans. Jenis instans yang didukung termasuk M5, M6, C5, C6, R5, R6, dan T3.

Default: m5.xlarge

- OperationType

Jenis: String

Deskripsi: (Diperlukan) Operasi yang ingin Anda lakukan. FullMigrationOps melakukan tugas yang sama dengan Clone&Migrate dan juga menggantikan volume root instance target Anda. Volume root dari instance target diganti dengan volume root dari instance yang baru dibuat setelah proses migrasi. FullMigrationOperasi tidak mendukung volume root yang ditentukan oleh Logical Volume Manager (LVM).

Nilai yang valid: Clone&Migrate | FullMigration

- SNS TopicArn

Jenis: String

Deskripsi: (Diperlukan) ARN topik Amazon SNS untuk pemberitahuan persetujuan. Topik Amazon SNS digunakan untuk mengirim pemberitahuan persetujuan yang diperlukan selama otomatisasi.

- TargetInstanceid

Jenis: String

Deskripsi: (Diperlukan) ID instans Amazon EC2 untuk bermigrasi.

Clone&Migratealur kerja

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:DescribeAutomationExecutions
- ssm:StartAutomationExecution
- ssm:DescribeInstanceInformation

- `ssm:DescribeAutomationStepExecutions`
- `ssm:SendCommand`
- `ssm:GetAutomationExecution`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeImages`
- `ec2:CreateImage`
- `ec2:RunInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DeregisterImage`
- `ec2>DeleteSnapshot`
- `ec2:TerminateInstances`
- `ec2:StartInstances`
- `ec2:DescribeKeyPairs`
- `ec2:StopInstances`
- `kms:CreateGrant*`
- `kms:ReEncrypt`
- `ec2:ModifyInstanceAttribute`
- `autoscaling:DescribeAutoScalingInstances`
- `iam:passRole`
- `iam:ListRoles`

### Langkah Dokumen

- `startOfPreliminaryChecksBranch`- Cabang ke alur kerja pemeriksaan awal.
- `getTargetInstanceProperties`- Mengumpulkan rincian dari contoh target.

- `checkIfNitroInstanceTypeIsSupportedInAZ`- Menentukan apakah jenis instans Amazon EC2 target didukung di Availability Zone yang sama dengan instans target.
- `getXenInstanceTypeInfo`- Mengumpulkan rincian tentang jenis contoh sumber.
- `checkIfInstanceHypervisorIsNitroAlready`- Memeriksa apakah instance target sudah berjalan sebagai tipe Nitro instance.
- `checkIfTargetInstanceLifecycleIsSpot`- Memeriksa apakah opsi pembelian dari instance target adalah Spot.
- `checkIfOperatingSystemIsLinux`- Memeriksa apakah target contoh OS adalah Linux.
- `verifySSMConnectivityForTargetInstance`- Memverifikasi bahwa contoh target dikelola oleh Systems Manager.
- `checkIfEphemeralVolumeAreSupported`- Memeriksa apakah jenis instance saat ini dari contoh target mendukung volume toko contoh.
- `verifyIfTargetInstanceHasEphemeralVolumesAttached`- Memeriksa apakah instance target memiliki volume penyimpanan instance yang terpasang.
- `checkIfRootVolumeIsEBS`- Memeriksa apakah jenis volume root instance target adalah EBS.
- `checkIfTargetInstanceIsInASG`- Memeriksa apakah instance target adalah bagian dari grup Auto Scaling.
- `endOfPreliminaryChecksBranch`- Akhir dari cabang pemeriksaan awal.
- `startOfTestBranch`- Cabang ke alur kerja Pengujian.
- `createTestImage`- Membuat tes AMI dari contoh target.
- `launchTestInstanceInSameSubnet`- Meluncurkan instance pengujian dari pengujian AMI menggunakan konfigurasi yang sama dengan instance target.
- `cleanupTestInstance`- Mengakhiri contoh uji.
- `endOfTestBranch`- Akhir cabang Pengujian.
- `checkIfTestingBranchSucceeded`- Memeriksa status cabang Pengujian.
- `approvalToStopTargetInstance`- Menunggu persetujuan dari kepala sekolah yang ditunjuk untuk menghentikan contoh target.
- `stopTargetEC2Instance`- Menghentikan contoh target.
- `forceStopTargetEC2Instance`- Force menghentikan instance target hanya jika langkah sebelumnya gagal menghentikan instance.
- `startOfCloneAndMigrateBranch`- Cabang ke Clone&Migrate alur kerja.

- `createBackupImage`- Menciptakan AMI contoh target untuk berfungsi sebagai cadangan.
- `launchInstanceInSameSubnet`- Meluncurkan instance baru dari cadangan AMI menggunakan konfigurasi yang sama dengan instance sumber.
- `waitForClonedInstanceToPassStatusChecks`- Menunggu instance yang baru dibuat untuk lulus semua pemeriksaan status.
- `verifySSMConnectivityForClonedInstance`- Memverifikasi bahwa instance yang baru dibuat dikelola oleh Systems Manager.
- `checkAndInstallENADrivers`- Memeriksa apakah driver ENA diinstal pada instance yang baru dibuat, dan menginstal driver jika diperlukan.
- `checkAndAddNVMeDrivers`- Memeriksa apakah driver NVMe diinstal pada instance yang baru dibuat, dan menginstal driver jika diperlukan.
- `checkAndModifyFSTABEntries`- Memeriksa apakah nama perangkat digunakan `/etc/fstab` dan menggantinya dengan UUID jika diperlukan.
- `stopClonedInstance`- Menghentikan instance yang baru dibuat.
- `forceStopClonedInstance`- Force menghentikan instance yang baru dibuat hanya jika langkah sebelumnya gagal menghentikan instance.
- `checkENAAttributeForClonedInstance`- Memeriksa apakah atribut jaringan yang disempurnakan diaktifkan untuk instance yang baru dibuat.
- `setNitroInstanceTypeForClonedInstance`- Mengubah jenis instance untuk instance yang baru dibuat ke jenis Nitro instance yang Anda tentukan.
- `startClonedInstance`- Memulai instance yang baru dibuat yang tipe instansinya Anda ubah.
- `approvalForCreatingImageAfterDriversInstallation`- Jika instans berhasil dimulai sebagai jenis Nitro instans, otomatisasi menunggu persetujuan dari prinsipal yang diperlukan. Jika persetujuan diberikan, AMI dibuat untuk digunakan sebagai EmasAMI.
- `createImageAfterDriversInstallation`- Menciptakan AMI untuk digunakan sebagai EmasAMI.
- `endOfCloneAndMigrateBranch`- Akhir Clone&Migrate cabang.
- `cleanupTestImage`- Deregisters yang AMI dibuat untuk pengujian.
- `failureHandling`- Memeriksa apakah Anda memilih untuk menghentikan sumber daya pada kegagalan.
- `onFailureTerminateClonedInstance`- Mengakhiri instance yang baru dibuat jika otomatisasi gagal.

- `onFailurecleanupTestImage`- Deregisters yang AMI dibuat untuk pengujian.
- `onFailureApprovalToStartTargetInstance`- Jika otomatisasi gagal, tunggu persetujuan dari prinsipal yang ditunjuk untuk memulai instance target.
- `onFailureStartTargetInstance`- Jika otomatisasi gagal, mulai contoh target.

FullMigrationalur kerja

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:SendCommand`
- `ssm:GetAutomationExecution`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeImages`
- `ec2:CreateImage`
- `ec2:RunInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DeregisterImage`
- `ec2>DeleteSnapshot`
- `ec2:TerminateInstances`
- `ec2:StartInstances`
- `ec2:DescribeKeyPairs`
- `ec2:StopInstances`

- `kms:CreateGrant*`
- `kms:ReEncrypt`
- `ec2:ModifyInstanceAttribute`
- `ec2:DetachVolume`
- `ec2:AttachVolume`
- `ec2:DescribeVolumes`
- `autoscaling:DescribeAutoScalingInstances`
- `iam:PassRole`
- `ec2:CreateTags`
- `cloudformation:DescribeStackResources`

## Langkah Dokumen

`FullMigration` Alur kerja menjalankan langkah yang sama dengan `Clone&Migrate` alur kerja dan juga melakukan langkah-langkah berikut:

- `checkConcurrency`- Memverifikasi bahwa hanya ada satu otomatisasi runbook ini yang menargetkan instans Amazon EC2 yang Anda tentukan. Jika runbook menemukan otomatisasi lain yang sedang berlangsung menargetkan instance yang sama, otomatisasi akan berakhir.
- `getTargetInstanceProperties`- Mengumpulkan rincian dari contoh target.
- `checkRootVolumeTags`- Menentukan apakah volume root instans Amazon EC2 target berisi tag yang AWS dicadangkan.
- `cloneTargetInstanceAndMigrateToNitro`- Memulai otomatisasi anak menggunakan `AWS-CloneXenInstanceToNitro` runbook.
- `branchOnTheOperationType`- Cabang pada nilai yang Anda tentukan untuk `OperationType` parameter.
- `getClonedInstanceId`- Mengambil ID dari instance yang baru diluncurkan dari otomatisasi anak.
- `checkIfRootVolumeIsBasedOnLVM`- Menentukan apakah partisi root dikelola oleh LVM.
- `branchOnTheRootVolumeLVMStatus`- Jika persetujuan minimum yang diperlukan diterima dari prinsipal, otomatisasi berlanjut dengan penggantian volume root.
- `manualInstructionsInCaseOfLVM`- Jika volume root dikelola oleh LVM, otomatisasi mengirimkan output yang berisi instruksi untuk cara mengganti volume root secara manual.

- `startOfReplaceRootEBSVolumeBranch`- Mulai alur kerja cabang Ganti Root EBS Volume.
- `checkIfTargetInstanceIsManagedByCFN`- Menentukan apakah contoh target dikelola oleh AWS CloudFormation tumpukan.
- `branchOnCFNStackStatus`- Cabang berdasarkan status CloudFormation tumpukan.
- `approvalForRootVolumesReplacement(WithCFN)`- Jika instance target diluncurkan oleh CloudFormation, otomatisasi menunggu persetujuan setelah instans yang baru diluncurkan berhasil dimulai sebagai jenis Nitro instans. Ketika persetujuan diberikan, volume Amazon EBS dari instans target diganti dengan volume root dari instans yang baru diluncurkan.
- `approvalForRootVolumesReplacement`- Menunggu persetujuan setelah instance yang baru diluncurkan berhasil dimulai sebagai jenis Nitro instance. Ketika persetujuan diberikan, volume Amazon EBS dari instans target diganti dengan volume root dari instans yang baru diluncurkan.
- `assertIfTargetEC2InstanceIsStillStopped`- Memverifikasi bahwa instance target dalam stopped keadaan sebelum mengganti volume root.
- `stopTargetInstanceForRootVolumeReplacement`- Jika instance target berjalan, otomatisasi menghentikan instance sebelum mengganti volume root.
- `forceStopTargetInstanceForRootVolumeReplacement`- Angkatan menghentikan contoh target jika langkah sebelumnya gagal.
- `stopClonedInstanceForRootVolumeReplacement`- Menghentikan instans yang baru dibuat sebelum mengganti volume Amazon EBS.
- `forceStopClonedInstanceForRootVolumeReplacement`- Force menghentikan instance yang baru dibuat jika langkah sebelumnya gagal.
- `getBlockDeviceMappings`- Mengambil pemetaan perangkat blok untuk target dan instance yang baru dibuat.
- `replaceRootEbsVolumes`- Menggantikan volume root dari instance target dengan volume root dari instance yang baru dibuat.
- `EndOfReplaceRootEBSVolumeBranch`- Akhir Ganti Akar EBS Volume alur kerja cabang.
- `checkENAAttributeForTargetInstance`- Memeriksa apakah atribut jaringan yang disempurnakan (ENA) diaktifkan untuk instans Amazon EC2 target.
- `enableENAAttributeForTargetInstance`- Mengaktifkan atribut ENA untuk instans Amazon EC2 target jika diperlukan.
- `setNitroInstanceTypeForTargetInstance`- Mengubah instance target ke jenis Nitro instance yang Anda tentukan.

- `replicateRootVolumeTags`- Mereplikasi tag pada volume Amazon EBS root dari instans Amazon EC2 target.
- `startTargetInstance`- Memulai instans Amazon EC2 target setelah mengubah jenis instans.
- `onFailureStopTargetEC2Instance`- Menghentikan instans Amazon EC2 target jika gagal memulai sebagai jenis Nitro instans.
- `onFailureForceStopTargetEC2Instance`- Paksa menghentikan instans Amazon EC2 target jika langkah sebelumnya gagal.
- `OnFailureRevertOriginalInstanceType`- Mengembalikan instans Amazon EC2 target ke jenis instans asli jika instans target gagal dimulai sebagai Nitro jenis instans.
- `onFailureRollbackRootVolumeReplacement`- Mengembalikan semua perubahan yang dilakukan oleh `replaceRootEbsVolumes` langkah jika diperlukan.
- `onFailureApprovalToStartTargetInstance`- Menunggu persetujuan pokok yang ditunjuk untuk memulai instans Amazon EC2 target setelah mengembalikan perubahan sebelumnya.
- `onFailureStartTargetInstance`- Memulai instans Amazon EC2 target.
- `terminateClonedEC2Instance`- Mengakhiri instans Amazon EC2 yang dikloning setelah mengganti volume Amazon EBS root.

## AWSsupport - ResetAccess

### Deskripsi

Runbook ini akan menggunakan alat `EC2Rescue` pada instans EC2 yang ditentukan untuk mengaktifkan kembali dekripsi kata sandi menggunakan Konsol EC2 (Windows) atau untuk menghasilkan dan menambahkan pasangan kunci SSH baru (Linux). Jika Anda kehilangan pasangan kunci, otomatisasi ini akan membuat AMI yang diaktifkan kata sandi yang dapat Anda gunakan untuk meluncurkan instans EC2 baru dengan pasangan kunci yang Anda miliki (Windows).

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon



## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- EC2 RescueInstanceType

Jenis: String

Nilai yang valid: t2.small | t2.medium | t2.large

Default: t2.small

Deskripsi: (Diperlukan) Jenis instans EC2 untuk instans EC2Rescue. Ukuran yang disarankan: t2.small.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans EC2 yang ingin Anda setel ulang aksesnya.

### Important

Otomatisasi Manajer Sistem menghentikan instans ini, dan membuat AMI sebelum mencoba operasi apa pun. Data yang disimpan dalam volume toko instance akan hilang. Alamat IP publik akan berubah jika Anda tidak menggunakan Elastic IP.

- SubnetId

Jenis: String

Bawaan: CreateNew VPC

Deskripsi: (Opsional) ID subnet untuk instans EC2Rescue. Secara default, Systems Manager Automation membuat VPC baru. Atau, Gunakan SelectedInstanceSubnet untuk menggunakan subnet yang sama dengan instans Anda, atau tentukan ID subnet kustom.

 Important

Subnet harus berada di Availability Zone yang sama dengan InstanceId, dan harus mengizinkan akses ke endpoint SSM.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

Anda harus memiliki setidaknya ssm: StartAutomationExecution, ssm: GetParameter (untuk mengambil nama parameter kunci SSH) dan ssm: GetAutomationExecution untuk dapat membaca output otomatisasi. Untuk informasi lebih lanjut tentang izin yang diperlukan, lihat [AWSSupport-StartEC2RescueWorkflow](#).

## Langkah Dokumen

1. `aws:assertAwsResourceProperty`- Menegaskan apakah contoh yang disediakan adalah Windows.
  - a. (EC2Rescue untuk Windows) Jika instance yang disediakan adalah Windows:
    - i. `aws:executeAutomation`- Memanggil `AWSSupport-StartEC2RescueWorkflow` dengan EC2Rescue untuk Windows secara offline password reset script
    - ii. `aws:executeAwsApi`- Ambil ID AMI cadangan dari otomatisasi bersarang
    - iii. `aws:executeAwsApi`- Ambil ID AMI yang diaktifkan kata sandi dari otomatisasi bersarang
    - iv. `aws:executeAwsApi`- Ambil ringkasan EC2Rescue dari otomatisasi bersarang
  - b. (EC2Rescue untuk Linux) Jika instance yang disediakan adalah Linux:
    - i. `aws:executeAutomation`- Memanggil `AWSSupport-StartEC2RescueWorkflow` dengan EC2Rescue untuk Linux offline SSH skrip injeksi kunci
    - ii. `aws:executeAwsApi`- Ambil ID AMI cadangan dari otomatisasi bersarang
    - iii. `aws:executeAwsApi`- Ambil nama parameter SSM untuk kunci SSH yang disuntikkan
    - iv. `aws:executeAwsApi`- Ambil ringkasan EC2Rescue dari otomatisasi bersarang

## Keluaran

getEc2. Keluaran RescueForWindowsResult

getWindowsBackupAmi. ImageId

getWindowsPasswordEnabledAmi.ImageId

getEc2. Keluaran RescueForLinuxResult

getLinuxBackupAmi. ImageId

KeyParameterGetLinuxSSH .Nama

## **AWSSupport-ResetLinuxUserPassword**

### Deskripsi

`AWSSupport-ResetLinuxUserPasswordRunbook` membantu Anda mengatur ulang kata sandi pengguna sistem operasi lokal (OS). Runbook ini sangat membantu bagi pengguna yang perlu mengakses instans Amazon Elastic Compute Cloud (Amazon EC2) mereka menggunakan konsol serial. Runbook membuat instans Amazon EC2 sementara dalam peran Anda Akun AWS dan AWS Identity and Access Management (IAM) dengan izin untuk mengambil nilai AWS Secrets Manager rahasia yang berisi kata sandi.

Runbook menghentikan instans Amazon EC2 target Anda, melepaskan volume akar Amazon Elastic Block Store (Amazon EBS), dan menempelkannya ke instans Amazon EC2 sementara. Menggunakan Run Command, skrip berjalan pada instance sementara untuk mengatur kata sandi pengguna OS yang Anda tentukan. Kemudian, volume Amazon EBS root dipasang kembali ke instans target Anda. Runbook juga menyediakan opsi untuk membuat snapshot volume root di awal otomatisasi.

Sebelum Anda mulai

Buat rahasia Manajer Rahasia dengan nilai kata sandi yang ingin Anda tetapkan ke pengguna OS Anda. Nilai harus dalam teks biasa. Untuk informasi selengkapnya, lihat [Membuat AWS Secrets Manager rahasia](#) di Panduan AWS Secrets Manager Pengguna.

### Pertimbangan

- Sebaiknya buat cadangan instans Anda sebelum menggunakan runbook ini. Pertimbangkan untuk mengatur nilai `CreateSnapshot` parameter sebagai **Yes**.

- Mengubah kata sandi pengguna lokal memerlukan runbook untuk menghentikan instance Anda. Ketika sebuah instance dihentikan, data apa pun yang disimpan dalam memori atau pada volume penyimpanan instans akan hilang. Juga, setiap alamat IPv4 publik yang ditugaskan secara otomatis dirilis. Untuk informasi selengkapnya tentang apa yang terjadi saat Anda menghentikan instans, lihat [Menghentikan dan memulai instans Anda](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.
- Jika volume Amazon EBS yang dilampirkan ke instans Amazon EC2 target Anda dienkripsi dengan kunci yang dikelola AWS Key Management Service (AWS KMS) pelanggan, pastikan AWS KMS kunci tidak `deleted` `disabled` atau instans Anda akan gagal dimulai.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `InstanceId`

Jenis: String

Deskripsi: (Diperlukan) ID instans Linux Amazon EC2 yang berisi kata sandi pengguna OS yang ingin Anda atur ulang.

- LinuxUserName

Jenis: String

Default: ec2-pengguna

Deskripsi: (Opsional) Akun pengguna OS yang kata sandinya ingin Anda atur ulang.

- SecretArn

Jenis: String

Deskripsi: (Diperlukan) ARN rahasia Manajer Rahasia Anda yang berisi kata sandi baru.

- SecurityGroupId

Jenis: String

Deskripsi: (Opsional) ID grup keamanan yang akan dilampirkan ke instans Amazon EC2 sementara. Jika Anda tidak memberikan nilai untuk parameter ini, grup keamanan Amazon Virtual Private Cloud (Amazon VPC) default digunakan.

- SubnetId

Jenis: String

Deskripsi: (Opsional) ID subnet yang ingin Anda luncurkan instans sementara Amazon EC2. Secara default, otomatisasi memilih subnet yang sama dengan instance target Anda. Jika Anda memilih untuk menyediakan subnet yang berbeda, subnet harus berada di Availability Zone yang sama dengan instans target dan memiliki akses ke titik akhir Systems Manager.

- CreateSnapshot

Jenis: String

Nilai yang valid: Ya | Tidak

Default: Ya

Deskripsi: (Opsional) Menentukan apakah snapshot volume root instans Amazon EC2 target Anda dibuat sebelum otomatisasi berjalan.

- StopConsent

Jenis: String

Nilai yang valid: Ya | Tidak

Default: tidak

Deskripsi: Masukkan **Yes** untuk mengetahui bahwa instans Amazon EC2 target Anda akan dihentikan selama otomatisasi ini. Ketika instans Amazon EC2 dihentikan, data apa pun yang disimpan dalam memori atau volume penyimpanan instans akan hilang, dan alamat IPv4 publik otomatis dirilis. Untuk informasi selengkapnya, lihat [Menghentikan dan memulai instans Anda](#) di Panduan Pengguna Amazon EC2 untuk Instans Linux.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:DescribeInstanceInformation`
- `ssm:ListTagsForResource`
- `ssm:SendCommand`
- `ec2:AttachVolume`
- `ec2:CreateSnapshot`
- `ec2:CreateSnapshots`
- `ec2:CreateVolume`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeSnapshotAttribute`
- `ec2:DescribeSnapshots`
- `ec2:DescribeSnapshotTierStatus`
- `ec2:DescribeVolumes`
- `ec2:DescribeVolumeStatus`
- `ec2:DetachVolume`
- `ec2:RunInstances`
- `ec2:StartInstances`

- `ec2:StopInstances`
- `ec2:TerminateInstances`
- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation>ListStacks`
- `logs:CreateLogDelivery`
- `logs:CreateLogGroup`
- `logs>DeleteLogDelivery`
- `logs>DeleteLogGroup`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:PutLogEvents`

## Langkah Dokumen

1. `aws:branch`— Cabang berdasarkan apakah Anda telah memberikan persetujuan untuk menghentikan instans Amazon EC2 target.
2. `aws:assertAwsResourceProperty`Memastikan status instans Amazon EC2 dalam stopped keadaan running atau. Jika tidak, otomatisasi berakhir.
3. `aws:executeAwsApi`Mendapatkan properti instans Amazon EC2.
4. `aws:executeAwsApi`Mendapat properti volume akar.
5. `aws:branch`Cabang otomatisasi tergantung pada apakah ID subnet untuk instans Amazon EC2 sementara disediakan.
6. `aws:assertAwsResourceProperty`Memastikan subnet yang Anda tentukan dalam `SubnetId` parameter berada di Availability Zone yang sama dengan instans Amazon EC2 target.
7. `aws:assertAwsResourceProperty`Memastikan volume root instans Amazon EC2 target adalah volume Amazon EBS.
8. `aws:assertAwsResourceProperty`Memastikan arsitektur instans Amazon EC2 adalah `arm64` atau `x86_64`.

9. `aws:assertAwsResourceProperty` Memastikan perilaku shutdown instans Amazon EC2 adalah stop dan tidak terminate.
10. `aws:branch` Memastikan instans Amazon EC2 bukan Instans Spot. Jika tidak, otomatisasi berakhir.
11. `aws:executeScript` Memastikan instans Amazon EC2 bukan bagian dari grup penskalaan otomatis. Jika instans merupakan bagian dari grup penskalaan otomatis, otomatisasi mengonfirmasi instans Amazon EC2 dalam keadaan siklus hidup. Standby
12. `aws:createStack` Membuat instans Amazon EC2 sementara yang digunakan untuk mengatur ulang kata sandi untuk pengguna OS yang Anda tentukan.
13. `aws:waitForAwsResourceProperty` Menunggu hingga instans Amazon EC2 sementara yang baru diluncurkan berjalan.
14. `aws:executeAwsApi` Mendapatkan ID instans Amazon EC2 sementara.
15. `aws:waitForAwsResourceProperty` Menunggu instans Amazon EC2 sementara untuk dilaporkan sebagai dikelola oleh Manajer Sistem.
16. `aws:changeInstanceState` Menghentikan instans Amazon EC2 target.
17. `aws:changeInstanceState` Memaksa instans Amazon EC2 target untuk berhenti jika terjebak dalam keadaan berhenti.
18. `aws:branch` Cabang otomatisasi tergantung pada apakah snapshot volume akar instans Amazon EC2 target diminta.
19. `aws:executeAwsApi` Membuat snapshot target volume Amazon EC2 root instans Amazon EBS.
20. `aws:waitForAwsResourceProperty` Menunggu snapshot berada dalam keadaan. `completed`
21. `aws:executeAwsApi` Melepaskan volume root Amazon EBS dari instans Amazon EC2 target.
22. `aws:waitForAwsResourceProperty` Menunggu volume root Amazon EBS terlepas dari instans Amazon EC2 target.
23. `aws:executeAwsApi` Melampirkan volume Amazon EBS root ke instans Amazon EC2 sementara.
24. `aws:waitForAwsResourceProperty` Menunggu volume root Amazon EBS dilampirkan ke instans Amazon EC2 sementara.
25. `aws:runCommand` Menyetel ulang kata sandi pengguna target dengan menjalankan skrip shell menggunakan Run Command pada instans Amazon EC2 sementara.
26. `aws:executeAwsApi` Melepaskan volume root Amazon EBS dari instans Amazon EC2 sementara.



- 27 `aws:waitForAwsResourceProperty` Menunggu volume root Amazon EBS terlepas dari instans Amazon EC2 sementara.
- 28 `aws:executeAwsApi` Melepaskan volume root Amazon EBS dari instans Amazon EC2 sementara setelah kesalahan.
- 29 `aws:waitForAwsResourceProperty` Menunggu volume root Amazon EBS terlepas dari instans Amazon EC2 sementara setelah kesalahan.
- 30 `aws:branchCabang` otomatisasi tergantung pada apakah snapshot dari volume root diminta untuk menentukan jalur pemulihan jika terjadi kesalahan.
- 31 `aws:executeAwsApi` Menempelkan kembali volume Amazon EBS root ke instans Amazon EC2 target.
- 32 `aws:waitForAwsResourceProperty` Menunggu volume root Amazon EBS dilampirkan ke instans Amazon EC2.
- 33 `aws:executeAwsApi` Membuat volume Amazon EBS baru dari snapshot volume root instans Amazon EC2 target.
- 34 `aws:waitForAwsResourceProperty` Menunggu hingga volume Amazon EBS baru dalam keadaan tertentu. `available`
- 35 `aws:executeAwsApi` Melampirkan volume Amazon EBS baru ke instans target sebagai volume root.
- 36 `aws:waitForAwsResourceProperty` Menunggu volume Amazon EBS berada dalam keadaan tertentu. `attached`
- 37 `aws:executeAwsApi` Menjelaskan kejadian AWS CloudFormation tumpukan jika runbook gagal membuat atau memperbarui tumpukan. AWS CloudFormation
- 38 `aws:branchCabang` otomatisasi tergantung pada status instans Amazon EC2 sebelumnya. Jika negara itu `running`, contoh dimulai. Jika dalam `stopped` keadaan, otomatisasi berlanjut.
- 39 `aws:changeInstanceState` Memulai instans Amazon EC2 jika diperlukan.
- 40 `aws:waitForAwsResourceProperty` Menunggu sampai AWS CloudFormation stack dalam status terminal sebelum dihapus.
- 41 `aws:executeAwsApi` Menghapus AWS CloudFormation tumpukan termasuk instans Amazon EC2 sementara.

## **AWS Premium Support - Resize Nitro Instance**

### Deskripsi

`AWSPremiumSupport-ResizeNitroInstanceRunbook` menyediakan solusi otomatis untuk mengubah ukuran instans Amazon Elastic Compute Cloud (Amazon EC2) yang dibangun di atas Sistem Nitro.

Untuk mengurangi potensi risiko kehilangan data dan downtime, runbook memverifikasi hal berikut:

- Perilaku berhenti misalnya.
- Jika instans merupakan bagian dari grup Penskalaan Otomatis Amazon EC2, dan dalam standby mode.
- negara contoh dan sewa.
- Jenis instans yang ingin Anda ubah untuk mendukung jumlah antarmuka jaringan yang saat ini dilampirkan ke instans Anda.
- Arsitektur prosesor dan jenis virtualisasi untuk jenis instance saat ini dan target adalah sama.
- Jika contoh berjalan, bahwa itu melewati semua pemeriksaan status.
- Jenis instans yang ingin Anda ubah tersedia di Availability Zone yang sama.

Jika Amazon EC2 tidak lulus pemeriksaan status setelah mengubah jenis instans, runbook secara otomatis akan kembali ke jenis instans sebelumnya.

Secara default, runbook ini tidak akan mengubah jenis instance jika sedang berjalan dan volume penyimpanan instance terpasang. Runbook juga tidak akan mengubah jenis instance jika instance adalah bagian dari AWS CloudFormation tumpukan. Jika Anda ingin mengubah salah satu dari perilaku ini, tentukan `yes` untuk `AllowInstanceStoreInstances` dan `AllowCloudFormationInstances` parameter.

Runbook menyediakan dua cara berbeda untuk menentukan jenis instance yang ingin Anda ubah:

- Untuk otomatisasi sederhana yang menargetkan satu instance, tentukan jenis instans yang ingin Anda ubah menggunakan parameter. `TargetInstanceTypeFromParameter`
- Untuk menjalankan otomatisasi pada skala untuk mengubah jenis instans dari beberapa instance, tentukan jenis instance menggunakan parameter. `TargetInstanceTypeFromTagValue` Untuk informasi tentang menjalankan otomatisasi pada skala besar, lihat [Menjalankan otomatisasi pada skala besar](#).

Jika Anda tidak menentukan nilai untuk salah satu parameter, otomatisasi gagal.

**⚠ Important**

Akses ke `AWSPremiumSupport` - \* runbook memerlukan Langganan Dukungan Perusahaan atau Bisnis. Untuk informasi selengkapnya, lihat [Bandingkan AWS Support Paket](#).

**Pertimbangan**

- Sebaiknya buat cadangan instans Anda sebelum menggunakan runbook ini.
- Untuk informasi tentang kompatibilitas untuk mengubah jenis instans, lihat [Kompatibilitas untuk mengubah jenis instans](#).
- Jika otomatisasi gagal dan kembali ke jenis instans asli, lihat [Memecahkan masalah mengubah jenis instans](#).
- Mengubah jenis instans memerlukan runbook untuk menghentikan instance Anda. Ketika sebuah instance dihentikan, data apa pun yang disimpan dalam memori atau pada volume penyimpanan instans akan hilang. Juga, setiap alamat IPv4 publik yang ditugaskan secara otomatis dirilis. Untuk informasi selengkapnya tentang apa yang terjadi saat Anda menghentikan instans, lihat [Berhenti dan mulai instans Anda](#).
- Dengan menggunakan `SkipInstancesWithTagKey` parameter, Anda dapat melewati instans yang memiliki kunci tag Amazon EC2 tertentu yang diterapkan.

**[Jalankan Otomasi ini \(konsol\)](#)**

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, jendela

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Mengakui

Jenis: String

Deskripsi: (Diperlukan) Enter **yes** untuk mengakui bahwa instans Anda akan dihentikan jika saat ini sedang berjalan.

- AllowInstanceStoreInstances

Jenis: String

Nilai yang valid: tidak | ya

Default: tidak

Deskripsi: (Opsional) Jika Anda menentukanyes, Anda mengizinkan runbook berjalan pada instance yang memiliki volume penyimpanan instans yang terpasang.

- AllowCloudFormationInstances

Jenis: String

Nilai yang valid: tidak | ya

Default: tidak

Deskripsi: (Opsional) Jika Anda menentukanyes, runbook berjalan pada instance yang merupakan bagian dari tumpukan. AWS CloudFormation

- DryRun

Jenis: String

Nilai yang valid: tidak | ya

Default: tidak

Deskripsi: (Opsional) Jika Anda menentukanyes, runbook memvalidasi persyaratan pengubahan ukuran tanpa membuat perubahan pada jenis instance.

- `InstanceId`

Jenis: String

Deskripsi: (Diperlukan) ID instans Amazon EC2 yang jenisnya ingin Anda ubah.

- `SkipInstancesWithTagKey`

Jenis: String

Deskripsi: (Opsional) Otomatisasi melewati instance target jika kunci tag yang Anda tentukan diterapkan ke instans.

- `SleepTime`

Jenis: String

Default: 3

Deskripsi: (Opsional) Jumlah detik runbook ini harus tidur setelah selesai.

- `TagInstance`

Jenis: String

Deskripsi: (Opsional) Tag instance dengan kunci dan nilai pilihan Anda menggunakan format berikut: *Key=ChangingType*, Value=True. Opsi ini memungkinkan Anda untuk melacak instance yang telah ditargetkan oleh runbook ini. Kunci dan nilai tag peka huruf besar dan kecil.

- `TargetInstanceTypeFromParameter`

Jenis: String

Deskripsi: (Opsional) Jenis instans yang ingin Anda ubah instans. Biarkan parameter ini kosong jika Anda ingin menggunakan nilai kunci tag yang disediakan dalam `TargetInstanceTypeFromTagValue` parameter.

- `TargetInstanceTypeFromTagValue`

Jenis: String

Deskripsi: (Opsional) Kunci tag yang diterapkan ke instance target Anda yang nilainya berisi jenis instans yang ingin Anda ubah. Jika Anda menentukan nilai untuk `TargetInstanceTypeFromParameter` parameter, itu akan mengganti nilai apa pun yang Anda tentukan untuk parameter ini.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `autoscaling:DescribeAutoScalingInstances`
- `cloudformation:DescribeStackResources`
- `ssm:GetAutomationExecution`
- `ssm:DescribeAutomationExecutions`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DescribeTags`
- `ec2:ModifyInstanceAttribute`
- `ec2:StartInstances`
- `ec2:StopInstances`

## Langkah Dokumen

1. `aws:assertAwsResourceProperty`: Memastikan instans Amazon EC2 tidak ditandai dengan kunci tag sumber daya yang ditentukan dalam `SkipInstancesWithTagKey` parameter. Jika kunci tag ditemukan diterapkan ke instance, langkah gagal dan otomatisasi berakhir.
2. `aws:assertAwsResourceProperty`: Mengonfirmasi status instans Amazon EC2 target adalah `running`, `pendingstopped`, atau `stopping` Jika tidak, otomatisasi berakhir.
3. `aws:executeAwsApi`: Mengumpulkan properti dari instans Amazon EC2.
4. `aws:executeAwsApi`: Mengumpulkan detail tentang jenis instans Amazon EC2 saat ini.
5. `aws:branch`: Memeriksa apakah jenis instance saat ini dan jenis instance yang ditentukan dalam `TargetInstanceTypeFromParameter` parameter adalah sama. Jika ya, otomatisasi berakhir.
6. `aws:assertAwsResourceProperty`: Memastikan instance berjalan pada Sistem Nitro.
7. `aws:branch`: Memastikan jenis volume root instans Amazon EC2 adalah volume Amazon Elastic Block Store (Amazon EBS).

8. `aws:assertAwsResourceProperty`: Mengonfirmasi perilaku shutdown instance adalah stop dan tidak terminate.
9. `aws:branch`: Memastikan instans Amazon EC2 bukan instans Spot.
10. `aws:branch`: Memastikan penyewaan instans Amazon EC2 adalah default dan bukan host khusus, atau instans khusus.
11. `aws:executeScript`: Mengonfirmasi hanya ada satu otomatisasi runbook ini yang menargetkan ID instance saat ini. Jika otomatisasi lain sudah berlangsung menargetkan instance yang sama, otomatisasi mengembalikan kesalahan dan berakhir.
12. `aws:branch`: Cabang otomatisasi berdasarkan status instans Amazon EC2.
  - a. Jika `stopped` atau `stopping`, otomatisasi berjalan `aws:waitForAwsResourceProperty` hingga instans Amazon EC2 dihentikan sepenuhnya.
  - b. Jika `running` atau `pending`, otomatisasi berjalan `aws:waitForAwsResourceProperty` hingga instans Amazon EC2 melewati pemeriksaan status.
13. `aws:assertAwsResourceProperty`: Mengonfirmasi bahwa instans Amazon EC2 bukan bagian dari grup Penskalaan Otomatis dengan memanggil operasi API `DescribeAutoScalingInstances` Jika instans merupakan bagian dari grup Penskalaan Otomatis, pastikan instans Amazon EC2 dalam standby mode.
14. `aws:branch`: Cabang otomatisasi tergantung pada apakah Anda ingin otomatisasi memeriksa apakah instans Amazon EC2 adalah bagian dari AWS CloudFormation tumpukan:
  - a. `aws:executeScript` Memastikan instans Amazon EC2 bukan bagian dari AWS CloudFormation tumpukan dengan memanggil operasi `DescribeStackResources` API.
15. `aws:executeAwsApi`: Mengembalikan daftar jenis instance dengan jenis arsitektur prosesor yang sama, jenis virtualisasi, dan yang mendukung jumlah antarmuka jaringan yang saat ini melekat pada contoh target.
16. `aws:executeAwsApi`: Mendapat nilai jenis contoh target dari kunci tag yang ditentukan dalam `TargetInstanceTypeFromTagValue` parameter.
17. `aws:executeScript`: Mengonfirmasi bahwa jenis instance saat ini dan target kompatibel. Memastikan bahwa jenis instance target tersedia di subnet yang sama. Memverifikasi kepala sekolah yang memulai runbook memiliki izin untuk mengubah jenis instance, dan menghentikan dan memulai instance jika sedang berjalan.
18. `aws:branch`: Cabang otomatisasi berdasarkan apakah nilai `DryRun` parameter diatur `keyes`. Jika `keyes`, otomatisasi berakhir.

19. `aws:branch`: Memeriksa apakah jenis instance asli dan target sama. Jika mereka sama, otomatisasi berakhir.
20. `aws:executeAwsApi`: Mendapat keadaan contoh saat ini.
21. `aws:changeInstanceState`: Menghentikan instans Amazon EC2.
22. `aws:changeInstanceState`: Memaksa instance untuk berhenti jika terjebak di `stopping` negara bagian.
23. `aws:executeAwsApi`: Mengubah jenis instance ke tipe instance target.
24. `aws:sleep`: Menunggu 3 detik setelah mengubah jenis instans untuk konsistensi akhirnya.
25. `aws:branch`: Cabang otomatisasi berdasarkan status instans sebelumnya. Jika `yarunning`, instance dimulai.
- `aws:changeInstanceState`: Memulai instans Amazon EC2 jika sedang berjalan sebelum mengubah jenis instans.
  - `aws:waitForAwsResourceProperty`: Menunggu instans Amazon EC2 untuk lulus pemeriksaan status. Jika instance tidak lulus pemeriksaan status, instance diubah kembali ke jenis instance aslinya.
    - `aws:changeInstanceState`: Menghentikan instans Amazon EC2 sebelum mengubahnya ke jenis instans aslinya.
    - `aws:changeInstanceState`: Memaksa instans Amazon EC2 untuk berhenti sebelum mengubahnya ke jenis instans aslinya jika terjebak dalam keadaan berhenti.
    - `aws:executeAwsApi`: Mengubah instans Amazon EC2 ke jenis aslinya.
    - `aws:sleep`: Menunggu 3 detik setelah mengubah jenis instans untuk konsistensi akhirnya.
    - `aws:changeInstanceState`: Memulai instans Amazon EC2 jika sedang berjalan sebelum mengubah jenis instans.
    - `aws:waitForAwsResourceProperty`: Menunggu instans Amazon EC2 untuk lulus pemeriksaan status.
26. `aws:sleep`: Menunggu sebelum mengakhiri runbook.

## AWSSupport-RestoreEC2InstanceFromSnapshot

### Deskripsi

AWSSupport-RestoreEC2InstanceFromSnapshotRunbook membantu Anda mengidentifikasi dan memulihkan instans Amazon Elastic Compute Cloud (Amazon EC2) dari snapshot Amazon Elastic Block Store (Amazon EBS) yang berfungsi dari volume root.



## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- EndDate

Jenis: String

Deskripsi: (Opsional) Tanggal terakhir Anda ingin otomatisasi mencari snapshot.

- InplaceSwap

Jenis: Boolean

Nilai yang valid: benar/salah

Deskripsi: (Opsional) Jika nilai untuk parameter ini disetel ke `true`, volume yang baru dibuat dari snapshot akan menggantikan volume root yang ada yang dilampirkan ke instans Anda.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans yang ingin Anda pulihkan dari snapshot.

- `LookForInstanceStatusCheck`

Jenis: Boolean

Nilai yang valid: benar/salah

Default: betul

Deskripsi: (Opsional) Jika nilai untuk parameter ini disetel ke `true`, otomatisasi akan memeriksa apakah pemeriksaan status instans gagal pada instance pengujian yang diluncurkan dari snapshot.

- `SkipSnapshotsBy`

Jenis: String

Deskripsi: (Opsional) Interval di mana snapshot dilewati saat mencari snapshot untuk memulihkan instans Anda. Misalnya, jika ada 100 snapshot yang tersedia, dan Anda menentukan nilai 2 untuk parameter ini, maka setiap snapshot ketiga ditinjau.

Default: 0

- `SnapshotId`

Jenis: String

Deskripsi: (Opsional) ID snapshot yang ingin Anda pulihkan instance.

- `StartDate`

Jenis: String

Deskripsi: (Opsional) Tanggal pertama Anda ingin otomatisasi mencari snapshot.

- `TotalSnapshotsToLook`

Jenis: String

Deskripsi: (Opsional) Jumlah snapshot ulasan otomatisasi.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ec2:AttachVolume`
- `ec2:CreateImage`
- `ec2:CreateTags`
- `ec2:CreateVolume`
- `ec2>DeleteTags`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeImages`
- `ec2:DescribeSnapshots`
- `ec2:DescribeVolumes`
- `ec2:DetachVolume`
- `ec2:RunInstances`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `ec2:TerminateInstances`
- `cloudwatch:GetMetricData`

## Langkah Dokumen

1. `aws:executeAwsApi`- Mengumpulkan rincian tentang contoh target.
2. `aws:assertAwsResourceProperty`- Memverifikasi contoh target ada.
3. `aws:assertAwsResourceProperty`- Memverifikasi volume root adalah volume Amazon EBS.
4. `aws:assertAwsResourceProperty`- Memverifikasi bahwa otomatisasi lain belum berjalan yang menargetkan instance ini.
5. `aws:executeAwsApi`- Tag contoh target.
6. `aws:executeAwsApi`- Menciptakan sebuah AMI contoh.

7. `aws:executeAwsApi`- Mengumpulkan detail tentang yang AMI dibuat pada langkah sebelumnya.
8. `aws:waitForAwsResourceProperty`- Menunggu AMI negara untuk menjadi `available` sebelum melanjutkan.
9. `aws:executeScript`- Meluncurkan contoh baru dari yang baru dibuat AMI.
10. `aws:assertAwsResourceProperty`- Memverifikasi negara contoh adalah `available`.
11. `aws:executeAwsApi`- Mengumpulkan detail tentang instance yang baru diluncurkan.
12. `aws:branch`- Cabang berdasarkan apakah Anda memberikan nilai untuk `SnapshotId` parameter.
13. `aws:executeScript`- Mengembalikan daftar snapshot dalam jangka waktu yang ditentukan.
14. `aws:executeAwsApi`- Menghentikan instance.
15. `aws:waitForAwsResourceProperty`- Menunggu status volume menjadi `available`.
16. `aws:waitForAwsResourceProperty`- Menunggu keadaan instance menjadi `stopped`.
17. `aws:executeAwsApi`- Melepaskan volume root.
18. `aws:waitForAwsResourceProperty`- Menunggu volume root terlepas.
19. `aws:executeAwsApi`- Melampirkan volume root baru.
20. `aws:waitForAwsResourceProperty`- Menunggu volume baru dilampirkan.
21. `aws:executeAwsApi`- Mulai contoh.
22. `aws:waitForAwsResourceProperty`- Menunggu keadaan instance menjadi `available`.
23. `aws:waitForAwsResourceProperty`- Menunggu pemeriksaan status sistem dan instance untuk lulus untuk instance.
24. `aws:executeScript`- Menjalankan skrip untuk menemukan snapshot yang dapat digunakan untuk berhasil membuat volume.
25. `aws:executeScript`- Menjalankan skrip untuk memulihkan instance menggunakan volume yang baru dibuat dari snapshot yang diidentifikasi oleh otomatisasi, atau menggunakan volume yang dibuat dari snapshot yang Anda tentukan dalam parameter. `SnapshotId`
26. `aws:executeScript`- Menghapus sumber daya yang dibuat oleh otomatisasi.

Keluaran

`launchCloneInstance.InstanceIds`

`ListSnapshotByDate.FinalSnapshots`

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.bekerjaSnapshot

InstanceRecovery.hasil

## **AWSsupport - SendLogBundleToS3Bucket**

### Deskripsi

AWSsupport-SendLogBundleToS3BucketRunbook mengunggah bundel log yang dihasilkan oleh alat EC2Rescue dari instance target ke bucket S3 yang ditentukan. Runbook menginstal versi spesifik platform EC2Rescue berdasarkan platform instance target. EC2Rescue kemudian digunakan untuk mengumpulkan semua log sistem operasi (OS) yang tersedia.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans terkelola Windows atau Linux yang ingin Anda kumpulkan log.

- S3 BucketName

Jenis: String

Deskripsi: Bucket S3 (Diperlukan) untuk mengunggah log ke.

- S3Path

Jenis: String

Bawaan: `AWSSupport-SendLogBundleToS3Bucket/`

Deskripsi: (Opsional) Jalur S3 untuk log yang dikumpulkan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan agar instans EC2 yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon `AmazonSSMManagedInstanceCore` yang terpasang. Pengguna harus memiliki setidaknya `ssm:StartAutomationExecution` dan `ssm:SendCommand` untuk menjalankan otomatisasi dan mengirim perintah ke instance, ditambah `ssm:GetAutomationExecution` untuk dapat membaca output otomatisasi.

Langkah Dokumen

1. `aws:runCommand`- Instal `EC2Rescue` melalui `AWS-ConfigureAWSPackage`
2. `aws:runCommand`- Jalankan PowerShell skrip untuk mengumpulkan log pemecahan masalah Windows dengan `EC2Rescue`.
3. `aws:runCommand`- Jalankan skrip bash untuk mengumpulkan log pemecahan masalah Linux dengan `EC2rescue`.

Keluaran

`collectAndUploadWindowsLogBundle`.Keluaran

collectAndUploadLinuxLogBundle.Keluaran

## AWSSupport-StartEC2RescueWorkflow

### Deskripsi

AWSSupport-StartEC2RescueWorkflowRunbook menjalankan skrip yang dikodekan base64 yang disediakan (Bash atau Powershell) pada instance pembantu yang dibuat untuk menyelamatkan instans Anda. Volume root instans Anda dilampirkan dan dipasang ke instance helper, juga dikenal sebagai instance EC2Rescue. Jika instans Anda adalah Windows, berikan skrip Powershell. Jika tidak, gunakan Bash. Runbook menetapkan beberapa variabel lingkungan yang dapat Anda gunakan dalam skrip Anda. Variabel lingkungan berisi informasi tentang input yang Anda berikan, serta informasi tentang volume root offline. Volume offline sudah terpasang dan siap digunakan. Misalnya, Anda dapat menyimpan file Konfigurasi Status yang Diinginkan ke volume root Windows offline, atau chroot ke volume root Linux offline dan melakukan remediasi offline.

### [Jalankan Otomasi ini \(konsol\)](#)

#### Important

Instans Amazon EC2 yang dibuat dari Marketplace Amazon Machine Images (AMI) tidak didukung oleh otomatisasi ini.

### Informasi Tambahan

Untuk base64 menyandikan skrip, Anda dapat menggunakan Powershell atau Bash. PowerShell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes([System.IO.File]::ReadAllText('C:\Program Files\Amazon\EC2-Helper\AWSLogs\AWSLogs.ps1')))
```

Bash:

```
base64 PATH_TO_FILE
```

Berikut adalah daftar variabel lingkungan yang dapat Anda gunakan dalam skrip offline Anda, tergantung pada OS target

Windows:

Variabel	Deskripsi	Nilai contoh
\$ ENV:EC2RESCUE_ACCOUNT_ID	{{Global:Account_ID}}	123456789012
\$ ENV:EC2Rescue_Date	{{Global: Tanggal}}	2018-09-07
\$ ENV:EC2Rescue_Date_Time	{{Global:Date_time}}	2018-09-07_18.09.59
\$ENV:EC2Rescue_EC2RW_DIR	EC2Rescue untuk jalur instalasi Windows	C:\Program File\ Amazon\ EC2Rescue
\$ENV:EC2Rescue_EC2RW_DIR	EC2Rescue untuk jalur instalasi Windows	C:\Program File\ Amazon\ EC2Rescue
\$ ENV:EC2RESCUE_EXECUTION_ID	{{Automation: Execution_ID}}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
\$ ENV:EC2RESCUE_OFFLINE_CURRENT_CONTROL_SET	Offline Windows Kontrol Saat Ini Mengatur jalur	HKLM:\AWSTempSystem\ControlSet001
\$ ENV:EC2Rescue_offline_drive	Surat drive Windows offline	D:\
\$ ENV:EC2RESCUE_OFFLINE_EBS_DEVICE	Volume akar offline perangkat EBS	xvdf
\$ ENV:EC2Rescue_offline_kernel_ver	Versi Kernel Windows Offline	6.1.7601.24214
\$ ENV:EC2RESCUE_OFFLINE_OS_ARCHITECTURE	Arsitektur Windows offline	AMD64
\$ ENV:EC2Rescue_OFFLINE_OS_Caption	Keterangan Windows Offline	Pusat Data Windows Server 2008 R2



Variabel	Deskripsi	Nilai contoh
\$ ENV:EC2RESCUE_OFFLINE_OS_TYPE	Jenis OS Windows Offline	Server
\$ ENV:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR	Jalur direktori file Program Windows Offline	D:\Program Berkas
\$ ENV:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	Offline Windows Program file x86 jalur direktori	D:\Program File (x86)
\$ ENV:EC2Rescue_OFFLINE_REGISTRY_DIR	Jalur direktori registri Windows offline	D:\Windows\System32\config
\$ ENV:EC2RESCUE_OFFLINE_SYSTEM_ROOT	Jalur direktori root sistem Windows offline	D:\Windows
\$ ENV:EC2Rescue_Region	{{Global:Wilayah}}	us-west-1
\$ ENV:EC2Rescue_S3_Bucket	{{S3BucketName}}	mybucket
\$ ENV:EC2Rescue_S3_Prefix	{{S3Prefix}}	myprefiks/
\$ ENV:EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	abcdefgh123456789
\$ Script:EC2Rescue_OFFLINE_Windows_Install	Metadata Instalasi Windows Offline	Pelanggan Powershell Obyek

## Linux:

Variabel	Deskripsi	Nilai contoh
EC2RESCUE_ACCOUNT_ID	{{Global:Account_ID}}	123456789012
EC2RESCUE_DATE	{{Global: Tanggal}}	2018-09-07

Variabel	Deskripsi	Nilai contoh
EC2RESCUE_DATE_TIME	{{Global:Date_time}}	2018-09-07_18.09.59
EC2RESCUE_EC2RL_DIR	EC2Rescue untuk jalur instalasi Linux	/usr/lokal/ec2rl-1.1.3
EC2RESCUE_EXECUTION_ID	{{Automation: Execution_ID}}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_DEVICE	Nama perangkat offline	/dev/xvdf1
EC2RESCUE_OFFLINE_EBS_DEVICE	Volume akar offline perangkat EBS	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	Titik pemasangan volume root offline	/mnt/gunung
EC2RESCUE_PYTHON	Versi Python	python2.7
EC2RESCUE_REGION	{{Global:Wilayah}}	us-west-1
EC2RESCUE_S3_BUCKET	{{S3BucketName}}	mybucket
EC2RESCUE_S3_PREFIKS	{{S3Prefix}}	myprefiks/
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	abcdefgh123456789

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

## Parameter

- **AmiPrefix**

Jenis: String

Default: `AWSSupport-EC2Rescue`

Deskripsi: (Opsional) Awalan untuk nama AMI cadangan.

- **AutomationAssumeRole**

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- **CreatePostEC2 RescueBackup**

Jenis: String

Nilai yang valid: benar/salah

Default: salah

Deskripsi: (Opsional) Setel `true` untuk membuat AMI InstanceId setelah menjalankan skrip, sebelum memulainya. AMI akan bertahan setelah otomatisasi selesai. Anda bertanggung jawab untuk mengamankan akses ke AMI, atau menghapusnya.

- **CreatePreEC2 RescueBackup**

Jenis: String

Nilai yang valid: benar/salah

Default: salah

Deskripsi: (Opsional) Atur `true` untuk membuat AMI InstanceId sebelum menjalankan skrip. AMI akan bertahan setelah otomatisasi selesai. Anda bertanggung jawab untuk mengamankan akses ke AMI, atau menghapusnya.

- **EC2 RescueInstanceType**

`AWSSupport-StartEC2RescueWorkflow`

Jenis: String

Nilai yang valid: t2.small | t2.medium | t2.large

Default: t2.small

Deskripsi: (Opsional) Jenis instans EC2 untuk instans EC2Rescue.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans EC2 Anda. PENTING: AWS Systems Manager Otomatisasi menghentikan instance ini. Data yang disimpan dalam volume toko instance akan hilang. Alamat IP publik akan berubah jika Anda tidak menggunakan Elastic IP.

- OfflineScript

Jenis: String

Deskripsi: (Diperlukan) Skrip yang dikodekan Base64 untuk dijalankan melawan instance pembantu. Gunakan Bash jika instance sumber Anda adalah Linux, dan PowerShell jika itu adalah Windows.

- S3 BucketName

Jenis: String

Deskripsi: (Opsional) Nama bucket S3 di akun tempat Anda ingin mengunggah log pemecahan masalah. Pastikan kebijakan bucket tidak memberikan izin baca/tulis yang tidak perlu kepada pihak yang tidak memerlukan akses ke log yang dikumpulkan.

- S3Prefix

Jenis: String

Default: AWSSupport-EC2Rescue

Deskripsi: (Opsional) Awalan untuk log S3.

- SubnetId

Jenis: String

**Bawaan: SelectedInstanceSubnet**

Deskripsi: (Opsional) ID subnet untuk instans EC2Rescue. Secara default, subnet yang sama di mana instance yang disediakan berada digunakan. **PENTING:** Jika Anda menyediakan subnet khusus, subnet harus berada di Availability Zone yang sama denganInstanced, dan harus mengizinkan akses ke titik akhir SSM.

- UniqueId

Jenis: String

Default: {{Automation: execution\_ID}}

Deskripsi: (Opsional) Pengenal unik untuk otomatisasi.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan pengguna yang menjalankan otomatisasi memiliki AmazonSSM AutomationRole IAM dikelola kebijakan terlampir. Selain kebijakan itu, pengguna harus memiliki:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:*:An-AWS-Account-ID:function:AWSSupport-EC2Rescue-*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
```

```

        "arn:aws:s3:::awssupport-ssm.*/*.template",
        "arn:aws:s3:::awssupport-ssm.*/*.zip"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "iam:CreateRole",
      "iam:CreateInstanceProfile",
      "iam:GetRole",
      "iam:GetInstanceProfile",
      "iam:PutRolePolicy",
      "iam:DetachRolePolicy",
      "iam:AttachRolePolicy",
      "iam:PassRole",
      "iam:AddRoleToInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam>DeleteRole",
      "iam>DeleteRolePolicy",
      "iam>DeleteInstanceProfile"
    ],
    "Resource": [
      "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport-EC2Rescue-*",
      "arn:aws:iam::An-AWS-Account-ID:instance-profile/AWSSupport-
EC2Rescue-*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "lambda:CreateFunction",
      "ec2:CreateVpc",
      "ec2:ModifyVpcAttribute",
      "ec2>DeleteVpc",
      "ec2:CreateInternetGateway",
      "ec2:AttachInternetGateway",
      "ec2:DetachInternetGateway",
      "ec2>DeleteInternetGateway",
      "ec2:CreateSubnet",
      "ec2>DeleteSubnet",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:CreateRouteTable",
      "ec2:AssociateRouteTable",

```

```

        "ec2:DisassociateRouteTable",
        "ec2>DeleteRouteTable",
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:Describe*"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

## Langkah Dokumen

1. `aws:executeAwsApi`- Jelaskan contoh yang disediakan
2. `aws:executeAwsApi`- Jelaskan volume root instance yang disediakan
3. `aws:assertAwsResourceProperty`- Periksa jenis perangkat volume root adalah EBS
4. `aws:assertAwsResourceProperty`- Periksa volume root tidak dienkripsi
5. `aws:assertAwsResourceProperty`- Periksa ID subnet yang disediakan
  - a. (Gunakan subnet instance saat ini) - Jika `* SubnetId = SelectedInstanceSubnet *` kemudian jalankan `aws:createStack` untuk menyebarkan tumpukan `EC2Rescue CloudFormation`
  - b. (Buat VPC baru) - If `* SubnetId = CreateNew VPC*` kemudian jalankan `aws:createStack` untuk menyebarkan tumpukan `EC2Rescue CloudFormation`
  - c. (Gunakan subnet khusus) - Dalam semua kasus lain:
    - `aws:assertAwsResourceProperty`- Periksa subnet yang disediakan berada di Availability Zone yang sama dengan instance yang disediakan
    - `aws:createStack`- Menyebarkan tumpukan `CloudFormation EC2Rescue`
6. `aws:invokeLambdaFunction`- Lakukan validasi masukan tambahan
7. `aws:executeAwsApi`- Perbarui `CloudFormation` tumpukan `EC2Rescue` untuk membuat instance helper `EC2Rescue`
8. `aws:waitForAwsResourceProperty`- Tunggu pembaruan `CloudFormation` tumpukan `EC2Rescue` selesai
9. `aws:executeAwsApi`- Jelaskan output `CloudFormation` tumpukan `EC2Rescue` untuk mendapatkan ID contoh pembantu `EC2Rescue`

10. `aws:waitForAwsResourceProperty`- Tunggu instans helper EC2Rescue menjadi instance terkelola
11. `aws:changeInstanceState`- Hentikan contoh yang disediakan
12. `aws:changeInstanceState`- Hentikan contoh yang disediakan
13. `aws:changeInstanceState`- Angkatan menghentikan contoh yang disediakan
14. `aws:assertAwsResourceProperty`- Periksa nilai RescueBackup input CreatePre EC2
- (Buat cadangan pra-EC2Rescue) - Jika \* EC2 = benar\* CreatePre RescueBackup
  - `aws:executeAwsApi`- Buat cadangan AMI dari instance yang disediakan
  - `aws:createTags`- Tag cadangan AMI
15. `aws:runCommand`- Instal EC2Rescue pada contoh pembantu EC2Rescue
16. `aws:executeAwsApi`- Lepaskan volume root dari instance yang disediakan
17. `aws:assertAwsResourceProperty`- Periksa platform instans yang disediakan
- (Instance adalah Windows):
    - `aws:executeAwsApi`- Pasang volume root ke instance helper EC2Rescue sebagai \* xvdf\*
    - `aws:sleep`- Tidur 10 detik
    - `aws:runCommand`- Jalankan skrip offline yang disediakan di Powershell
  - (Instance adalah Linux):
    - `aws:executeAwsApi`- Lampirkan volume root ke instance helper EC2Rescue sebagai \*/dev/sdf\*
    - `aws:sleep`- Tidur 10 detik
    - `aws:runCommand`- Jalankan skrip offline yang disediakan di Bash
18. `aws:changeInstanceState`- Hentikan contoh pembantu EC2Rescue
19. `aws:changeInstanceState`- Paksa menghentikan contoh pembantu EC2Rescue
20. `aws:executeAwsApi`- Lepaskan volume root dari instance helper EC2Rescue
21. `aws:executeAwsApi`- Pasang volume root kembali ke instance yang disediakan
22. `aws:assertAwsResourceProperty`- Periksa nilai RescueBackup input CreatePost EC2
- (Buat cadangan pasca-EC2Rescue) - Jika \* EC2 = benar\* CreatePost RescueBackup
  - `aws:executeAwsApi`- Buat cadangan AMI dari instance yang disediakan



c. `aws:createTags`- Tag cadangan AMI

23.`aws:executeAwsApi`- Kembalikan penghapusan awal pada status terminasi untuk volume root dari instance yang disediakan

24.`aws:changeInstanceState`- Kembalikan keadaan awal dari contoh yang disediakan (berjalan/berhenti)

25.`aws:deleteStack`- Hapus tumpukan CloudFormation EC2Rescue

Keluaran

`runScriptForLinux`.Keluaran

`runScriptForJendela`. Keluaran

`preScriptBackup`.Imageld

`postScriptBackup`.Imageld

## **AWSPremiumSupport-TroubleshootEC2DiskUsage**

Deskripsi

`AWSPremiumSupport-TroubleshootEC2DiskUsageRunbook` membantu Anda menyelidiki dan berpotensi memulihkan masalah dengan penggunaan root instans Amazon Elastic Compute Cloud (Amazon EC2) dan non-root disk. Jika memungkinkan, runbook mencoba untuk memperbaiki masalah dengan memperluas volume dan sistem file-nya. Untuk melakukan tugas-tugas ini, runbook ini mengatur eksekusi beberapa runbook berdasarkan sistem operasi instance yang terpengaruh.

Runbook pertama, `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` atau `AWSPremiumSupport-DiagnoseDiskUsageOnLinux`, menentukan apakah masalah disk dapat dikurangi dengan memperluas volume.

Runbook kedua, `AWSPremiumSupport-ExtendVolumesOnWindows` atau `AWSPremiumSupport-ExtendVolumesOnLinux`, menggunakan output dari runbook pertama untuk menjalankan kode Python yang memodifikasi volume. Setelah volume dimodifikasi, runbook memperluas partisi dan sistem file dari volume yang terpengaruh.

**⚠ Important**

Akses ke `AWSPremiumSupport` - \* runbook memerlukan Langganan Dukungan Perusahaan atau Bisnis. Untuk informasi selengkapnya, lihat [Bandingkan AWS Support Paket](#).

Dokumen ini dibangun bekerja sama dengan AWS Managed Services (AMS). AMS membantu Anda mengelola AWS infrastruktur dengan lebih efisien dan aman. AMS juga menyediakan fleksibilitas operasional, peningkatan keamanan dan kepatuhan, pengoptimalan kapasitas, dan identifikasi penghematan biaya. Untuk informasi selengkapnya, lihat [AWS Managed Services](#).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, jendela

Parameter

- `InstanceId`

Jenis: String

Nilai yang diizinkan: `^i-[a-z0-9]{8,17}$`

Deskripsi: ID (Diperlukan) instans Amazon EC2 Anda.

- `VolumeExpansionEnabled`

Jenis: Boolean

Deskripsi: (Opsional) Tandai untuk mengontrol apakah dokumen akan memperpanjang volume dan partisi yang terpengaruh.

Default: `betul`

- `VolumeExpansionUsageTrigger`

Jenis: String

Deskripsi: (Opsional) Penggunaan minimum ruang partisi yang diperlukan untuk memicu ekstensi (dalam persentase).

Nilai yang diizinkan: `^[0-9]{1,2}$`

Bawaan: 85

- `VolumeExpansionCapSize`

Jenis: String

Deskripsi: (Opsional) Ukuran maksimum volume Amazon Elastic Block Store (Amazon EBS) akan ditingkatkan menjadi (di GiB).

Nilai yang diizinkan: `^[0-9]{1,4}$`

Default: 2048

- `VolumeExpansionGibIncrease`

Jenis: String

Deskripsi: (Opsional) Kenaikan GiB volume. Kenaikan bersih terbesar antara `VolumeExpansionGibIncrease` dan `VolumeExpansionPercentageIncrease` akan digunakan.

Nilai yang diizinkan: `^[0-9]{1,4}$`

Default: 20

- `VolumeExpansionPercentageIncrease`

Jenis: String

Keterangan: (Opsional) Meningkatkan persentase volume. Kenaikan bersih terbesar antara `VolumeExpansionGibIncrease` dan `VolumeExpansionPercentageIncrease` akan digunakan.

Nilai yang diizinkan: `^[0-9]{1,2}$`

Default: 20

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeVolumes`
- `ec2:DescribeVolumesModifications`
- `ec2:ModifyVolume`
- `ec2:DescribeInstances`
- `ec2:CreateImage`
- `ec2:DescribeImages`
- `ec2:DescribeTags`
- `ec2:CreateTags`
- `ec2>DeleteTags`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeAutomationExecutions`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`

Langkah Dokumen

1. `aws:assertAwsResourceProperty`- Periksa apakah instance dikelola oleh Manajer Sistem

2. `aws:executeAwsApi`- Menjelaskan contoh untuk mendapatkan platform.
3. `aws:branch`- Otomatisasi cabang berdasarkan platform instans.
  - a. Jika instance adalah Windows:
    - i. `aws:executeAutomation`- Jalankan `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` runbook untuk mendiagnosis masalah penggunaan disk pada instance.
    - ii. `aws:executeAwsApi`- Mendapat output dari otomatisasi sebelumnya.
    - iii. `aws:branch`- Cabang berdasarkan output diagnostik, dan jika ada volume yang dapat diperluas untuk mengurangi peringatan.
      - A. Tidak ada volume yang perlu diperluas: Akhiri otomatisasi.
      - B. Ada volume yang perlu diperluas:
        - I. `aws:executeAwsApi`- Buat Amazon Machine Image (AMI) dari instance.
        - II. `aws:waitForAwsResourceProperty`- Menunggu AMI negara untuk menjadi `available`
        - III. `aws:executeAutomation`- Jalankan `AWSPremiumSupport-ExtendVolumesOnWindows` runbook untuk melakukan modifikasi volume serta langkah-langkah yang diperlukan dalam sistem operasi (OS) untuk membuat ruang baru tersedia.
  - b. (Platform bukan jendela) Jika instance input bukan Windows:
    - i. `aws:executeAutomation`- Jalankan `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` runbook untuk mendiagnosis masalah penggunaan disk pada instance.
    - ii. `aws:executeAwsApi`- Mendapat output dari otomatisasi sebelumnya.
    - iii. `aws:branch`- Cabang berdasarkan output diagnostik, dan jika ada volume yang dapat diperluas untuk mengurangi peringatan.
      - A. Tidak ada volume yang perlu diperluas: Akhiri otomatisasi.
      - B. Ada volume yang perlu diperluas:
        - I. `aws:executeAwsApi`- Buat AMI contoh.
        - II. `aws:waitForAwsResourceProperty`- Menunggu AMI negara untuk menjadi `available`
        - III. `aws:executeAutomation`- Jalankan `AWSPremiumSupport-ExtendVolumesOnLinux` runbook untuk melakukan modifikasi volume serta langkah-langkah yang diperlukan di OS untuk membuat ruang baru tersedia.

## Keluaran

diagnoseDiskUsageAlertOnWindows.Keluaran

extendVolumesOnWindows.Output

diagnoseDiskUsageAlertOnLinux.Keluaran

extendVolumesOnLinux.Keluaran

BackuPamiLinux. Imageld

BackupamiWindows. Imageld

## **AWSSupport-TroubleshootEC2InstanceConnect**

### Deskripsi

AWSSupport-TroubleshootEC2InstanceConnectotomatisasi membantu menganalisis dan mendeteksi kesalahan yang mencegah koneksi ke instans Elastic Compute Cloud (Amazon EC2) Amazon Elastic Compute Cloud (Amazon EC2) menggunakan Amazon EC2 Instance [Connect](#). Ini mengidentifikasi masalah yang disebabkan oleh Amazon Machine Image (AMI) yang tidak didukung, instalasi atau konfigurasi paket tingkat OS yang hilang, izin AWS Identity and Access Management (IAM) yang hilang, atau masalah konfigurasi jaringan.

### Bagaimana cara kerjanya?

Runbook mengambil ID instans Amazon EC2, nama pengguna, mode koneksi, CIDR IP sumber, port SSH, dan Amazon Resource Name (ARN) untuk peran IAM atau pengguna yang mengalami masalah dengan Amazon EC2 Instance Connect. Kemudian memeriksa [prasyarat](#) untuk menghubungkan ke instans Amazon EC2 menggunakan Amazon EC2 Instance Connect:

- Contohnya berjalan dan dalam keadaan sehat.
- Instans terletak di AWS wilayah yang didukung oleh Amazon EC2 Instance Connect.
- AMI instans didukung oleh Amazon EC2 Instance Connect.
- Instance dapat mencapai Layanan Metadata Instance (IMDSv2).
- Paket Amazon EC2 Instance Connect diinstal dan dikonfigurasi dengan benar di tingkat OS.
- Konfigurasi jaringan (grup keamanan, ACL jaringan, dan aturan tabel rute) memungkinkan koneksi ke instans melalui Amazon EC2 Instance Connect.

- Peran IAM atau pengguna yang digunakan untuk memanfaatkan Amazon EC2 Instance Connect memiliki akses ke tombol push ke instans Amazon EC2.

### Important

- Untuk memeriksa instans AMI, jangkauan IMDSv2, dan penginstalan paket Instans Connect Amazon EC2, instans harus dikelola SSM. Jika tidak, ia melewati langkah-langkah itu. Untuk informasi selengkapnya, lihat [Mengapa instans Amazon EC2 saya tidak ditampilkan sebagai node terkelola](#).
- Pemeriksaan jaringan hanya akan mendeteksi jika grup keamanan dan aturan ACL jaringan memblokir lalu lintas ketika SourceIp CIDR disediakan sebagai parameter input. Jika tidak, itu hanya akan menampilkan aturan terkait SSH.
- Sambungan yang menggunakan [Endpoint Instans Connect Amazon EC2](#) tidak divalidasi di runbook ini.
- Untuk koneksi pribadi, otomatisasi tidak memeriksa apakah klien SSH diinstal pada mesin sumber dan apakah itu dapat mencapai alamat IP pribadi instans.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`

- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`
- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootEC2InstanceConnect](#) dalam AWS Systems Manager konsol.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
  - `InstanceId` (Diperlukan):  
ID instans Amazon EC2 target yang tidak dapat Anda sambungkan menggunakan Amazon EC2 Instance Connect.
  - `AutomationAssumeRole` (Opsional):  
ARN dari peran IAM yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.
  - `Nama Pengguna` (Diperlukan):  
Nama pengguna yang digunakan untuk menyambung ke instans Amazon EC2 menggunakan Amazon EC2 Instance Connect. Ini digunakan untuk mengevaluasi apakah akses IAM diberikan untuk pengguna khusus ini.
  - `EC2 InstanceConnectRoleOrUser` (Diperlukan):  
ARN peran IAM atau pengguna yang memanfaatkan Amazon EC2 Instance Connect untuk menekan tombol ke instans.



- SSHport (Opsional):

Port SSH dikonfigurasi pada instans Amazon EC2. Nilai default-nya adalah 22. Nomor port harus berada di antara 1-65535.

- SourceNetworkType (Opsional):

Metode akses jaringan ke instans Amazon EC2:

- Browser: Anda terhubung dari AWS Management Console.
- Publik: Anda terhubung ke instans yang terletak di subnet publik melalui internet (misalnya, komputer lokal Anda).
- Pribadi: Anda terhubung melalui alamat IP pribadi instans.
- SourceIpCIDR (Opsional):

Sumber CIDR yang menyertakan alamat IP perangkat (seperti komputer lokal Anda) akan Anda log dari menggunakan Amazon EC2 Instance Connect. Contoh: 172.31.48.6/32. Jika tidak ada nilai yang diberikan dengan mode akses publik atau pribadi, runbook tidak akan mengevaluasi apakah grup keamanan instans Amazon EC2 dan aturan ACL jaringan mengizinkan lalu lintas SSH. Ini akan menampilkan aturan terkait SSH sebagai gantinya.

**Input parameters**

**InstanceId**  
(Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.  
 Show interactive instance picker

<p><b>AutomationAssumeRole</b> (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</p> <p><input type="text" value="String"/></p>	<p><b>Username</b> (Required) The username used to connect to the EC2 instance using EC2 Instance Connect. It is used to evaluate if IAM access is granted for this particular user.</p> <p><input type="text" value="String"/></p>
<p><b>EC2InstanceConnectRoleOrUser</b> (Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role or user that is being used to leverage EC2 Instance Connect and push keys to the instance.</p> <p><input type="text" value="String"/></p>	<p><b>SSHPort</b> (Optional) The SSH port configured on the EC2 instance. Default value is '22'. The port number must be between '1-65535'.</p> <p><input type="text" value="22"/></p>
<p><b>SourceNetworkType</b> (Optional) The network access method to the EC2 instance: <b>Browser</b>: you are connecting to the EC2 instance using your browser by clicking the connect button from the console. <b>Public</b>: you are accessing the EC2 instance located in a public subnet over the internet (example: from your local computer). <b>Private</b>: you are connecting to your instance through its private IP address.</p> <p><input type="text" value="Browser"/></p>	<p><b>SourceIpCIDR</b> (Optional) The source CIDR that includes the IP address of the device you will be logging from using EC2 Instance Connect (such as your local computer). Example: 172.31.48.0/20.</p> <p><input type="text" value="None"/></p>

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- AssertInitialState:

Memastikan status instans Amazon EC2 berjalan. Jika tidak, otomatisasi berakhir.

- GetInstanceProperties:

Mendapatkan properti instans Amazon EC2 saat ini (PlatformDetails,, PublicIpAddress VpcId, SubnetId dan MetadataHttpEndpoint).

- GatherInstanceInformationFromSSM:

Mendapat status ping dan detail sistem operasi instans Systems Manager jika instans dikelola SSM.

- CheckIfAWSRegionSupported:

Memeriksa apakah instans Amazon EC2 terletak di wilayah yang didukung Amazon EC2 Instance ConnectAWS.

- BranchOnIfAWSRegionSupported:

Melanjutkan eksekusi jika AWS Wilayah didukung oleh Amazon EC2 Instance Connect. Jika tidak, itu menciptakan output dan keluar dari otomatisasi.

- CheckIfInstanceAMIsSupported:

Memeriksa apakah AMI yang terkait dengan instans didukung oleh Amazon EC2 Instance Connect.

- BranchOnIfInstanceAMIsSupported:

Jika instans AMI didukung, instans akan melakukan pemeriksaan tingkat OS, seperti jangkauan metadata dan instalasi dan konfigurasi paket Amazon EC2 Instance Connect. Jika tidak, ia memeriksa apakah metadata HTTP diaktifkan menggunakan AWS API, lalu melanjutkan ke langkah pemeriksaan jaringan.

- CheckIMDS: ReachabilityFromOs

Menjalankan skrip Bash pada instans Linux Amazon EC2 target untuk memeriksa apakah skrip tersebut dapat mencapai IMDSv2.

- CheckEic: PackageInstallation

Menjalankan skrip Bash pada instans Linux Amazon EC2 target untuk memeriksa apakah paket Amazon EC2 Instance Connect diinstal dan dikonfigurasi dengan benar.

- CheckSSHConfigFromOs:

Menjalankan skrip Bash pada instans Linux Amazon EC2 target untuk memeriksa apakah port SSH yang dikonfigurasi cocok dengan parameter input `SSHport.`

- CheckMetadataHTTPEndpointIsEnabled:

Memeriksa apakah layanan metadata instance HTTP endpoint diaktifkan.

- CheckEic: NetworkAccess

Memeriksa apakah konfigurasi jaringan (grup keamanan, ACL jaringan, dan aturan tabel rute) mengizinkan koneksi ke instans melalui Amazon EC2 Instance Connect.

- CheckIAM: RoleOrUserPermissions

Memeriksa apakah peran IAM atau pengguna yang digunakan untuk memanfaatkan Amazon EC2 Instance Connect memiliki akses ke tombol push ke instans Amazon EC2 menggunakan nama pengguna yang disediakan.

- MakeFinalOutput:

Mengkonsolidasikan output dari semua langkah sebelumnya.

## 7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci:

Eksekusi di mana instance target memiliki semua prasyarat yang diperlukan:

```

▼ Outputs

MakeFinalOutput.ExecutionLogs
Starting the check of EC2 Instance Connect pre-requisites for the instance 'i-██████████'.

### Checking if the AWS region is supported by EC2 Instance Connect ###
SUCCESS: The EC2 instance is located in the AWS region 'eu-west-1' which is one of EC2 Instance Connect supported regions

### Checking if the Amazon Machine Image (AMI) associated to the EC2 instance is supported ###
SUCCESS: The instance AMI 'Ubuntu 22.04' is supported by EC2 Instance Connect

### Checking if Instance Metadata service (IMDSv2) is reachable ###
SUCCESS: Instance metadata is reachable.

### Checking if EC2 Instance Connect package is installed and configured on the instance: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-set-up.html ###
SUCCESS: 'ec2-instance-connect' package is installed
SUCCESS: 'ec2-instance-connect' is properly configured

|
### Checking SSH configuration at the OS-level ###
WARNING: If you configured a firewall in the EC2 instance make sure that it allows SSH traffic from the source ip CIDR
INFO: SSH is configured to listen on port 22.
SUCCESS: The configured SSH port (22) matches the provided input port (22).

### Checking Network configuration requirements to access the instance through EC2 Instance Connect using 'Browser' access mode and port '22' ###
SUCCESS: The instance has a public IPv4 address.
SUCCESS: Subnet subnet-██████████ is public.
SUCCESS: SSH access is allowed by security group id 'sg-██████████'
SUCCESS: 'Inbound' NACL allows connection through EC2 instance connect, using the rule: '100'
SUCCESS: 'Outbound' NACL allows connection through EC2 instance connect, using the rule: '100'
SUCCESS: Network requirements to connect to the instance 'i-██████████' using EC2 instance connect are satisfied

### Checking if the required permissions are granted to the IAM identity 'arn:aws:iam::██████████:role/Admin' used to connect to the instance 'i-██████████' through EC2 Instance Connect with the username 'ubuntu' ###
SUCCESS: The IAM identity 'arn:aws:iam::██████████:role/Admin' includes the 'ec2:DescribeInstances' access permission
SUCCESS: The IAM identity 'arn:aws:iam::██████████:role/Admin' includes the 'ec2:SendSSHPublicKey' access permission

```

Eksekusi di mana AMI dari instans target tidak didukung:

```

▼ Outputs

MakeFinalOutput.ExecutionLogs
Starting the check of EC2 Instance Connect pre-requisites for the instance 'i-██████████'.

### Checking if the AWS region is supported by EC2 Instance Connect ###
SUCCESS: The EC2 instance is located in the AWS region 'eu-west-1' which is one of EC2 Instance Connect supported regions

### Checking if the Amazon Machine Image (AMI) associated to the EC2 instance is supported ###
ERROR: The instance AMI 'SLES 15.5' is not supported by EC2 Instance Connect. Please make sure to use one of the AMIs listed here: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-prerequisites.html#ec2-prereqs-ami:

```

## Referensi

## Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

### AWSdokumentasi layanan

- [Bagaimana cara mengatasi masalah saat terhubung ke instans Amazon EC2 menggunakan Amazon EC2 Instance Connect?](#)

## AWSSupport-TroubleshootRDP

### Deskripsi

AWSSupport-TroubleshootRDPRunbook memungkinkan pengguna untuk memeriksa atau memodifikasi pengaturan umum pada instance target yang dapat memengaruhi koneksi Remote Desktop Protocol (RDP), seperti port RDP, Network Layer Authentication (NLA) dan profil Windows Firewall. Secara opsional, perubahan dapat diterapkan secara offline dengan menghentikan dan memulai instance, jika pengguna secara eksplisit mengizinkan remediasi offline. Secara default, runbook membaca dan mengeluarkan nilai pengaturan.

#### Important

Perubahan pada pengaturan RDP, layanan RDP dan profil Windows Firewall harus ditinjau dengan cermat sebelum menggunakan runbook ini.

### [Jalankan Otomasi ini \(konsol\)](#)

#### Jenis dokumen

#### Otomatisasi

#### Pemilik

#### Amazon

#### Platform

## Windows

### Parameter

- Action

Jenis: String

Nilai yang valid: CheckAll | FixAll | Kustom

Default: Kustom

Deskripsi: (Opsional) [Kustom] Gunakan nilai dari Firewall, RDPServiceStartupType, RDP, RDP ServiceActionPortAction, NLA SettingAction dan RemoteConnections untuk mengelola pengaturan. [CheckAll] Baca nilai-nilai pengaturan tanpa mengubahnya. [FixAll] Kembalikan pengaturan default RDP, dan nonaktifkan Windows Firewall.

- AllowOffline

Jenis: String

Nilai yang valid: benar/salah

Default: salah

Deskripsi: (Opsional) Perbaiki saja - Setel ke true jika Anda mengizinkan remediasi RDP offline jika pemecahan masalah online gagal, atau instans yang disediakan bukan instans terkelola. Catatan: Untuk remediasi offline, SSM Automation menghentikan instans, dan membuat AMI sebelum mencoba operasi apa pun.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- firewall

Jenis: String

Nilai yang valid: Periksa | Nonaktifkan

**Default: Periksa**

Deskripsi: (Opsional) Periksa atau nonaktifkan firewall Windows (semua profil).

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans untuk memecahkan masalah pengaturan RDP dari.

- NLA SettingAction

Jenis: String

Nilai yang valid: Periksa | Nonaktifkan

Default: Periksa

Deskripsi: (Opsional) Periksa atau nonaktifkan Network Layer Authentication (NLA).

- RDP PortAction

Jenis: String

Nilai yang valid: Periksa | Modifikasi

Default: Periksa

Deskripsi: (Opsional) Periksa port saat ini yang digunakan untuk koneksi RDP, atau ubah port RDP kembali ke 3389 dan mulai ulang layanan.

- RDP ServiceAction

Jenis: String

Nilai yang valid: Periksa | Mulai | Mulai Ulang | Mulai Ulang Paksa

Default: Periksa

Deskripsi: (Opsional) Memeriksa, memulai, memulai ulang, atau memaksa-mulai ulang layanan RDP (). TermService

- RDP ServiceStartupType

Jenis: String

Nilai yang valid: Periksa | Otomatis

Default: Periksa

Deskripsi: (Opsional) Periksa atau atur layanan RDP untuk memulai secara otomatis saat Windows melakukan boot.

- RemoteConnections

Jenis: String

Nilai yang valid: Periksa | Aktifkan

Default: Periksa

Deskripsi: (Opsional) Tindakan yang harus dilakukan pada pengaturan fdenytsConnections: Periksa, Aktifkan.

- S3 BucketName

Jenis: String

Deskripsi: (Opsional) Hanya offline - Nama bucket S3 di akun tempat Anda ingin mengunggah log pemecahan masalah. Pastikan kebijakan bucket tidak memberikan izin baca/tulis yang tidak perlu kepada pihak yang tidak memerlukan akses ke log yang dikumpulkan.

- SubnetId

Jenis: String

Bawaan: SelectedInstanceSubnet

Deskripsi: (Opsional) Hanya offline - ID subnet untuk instans EC2Rescue yang digunakan untuk melakukan pemecahan masalah offline. Jika tidak ada ID subnet yang ditentukan, AWS Systems Manager Automation akan membuat VPC baru. PENTING: Subnet harus berada di Availability Zone yang sama dengan InstanceId, dan harus mengizinkan akses ke endpoint SSM.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan agar instans EC2 yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon AmazonSSM ManagedInstanceCore yang terpasang. Untuk remediasi online, pengguna harus memiliki setidaknya `ssm:DescribeInstanceInformation`, `ssm:StartAutomationExecution` dan `ssm:SendCommand` untuk menjalankan otomatisasi dan mengirim perintah ke instance, ditambah `ssm:GetAutomationExecution` untuk dapat membaca output otomatisasi. Untuk remediasi offline, pengguna harus memiliki setidaknya `ssm:DescribeInstanceInformation`, `ssm:ec2:StartAutomationExecution` `DescribeInstances`, plus `ssm:GetAutomationExecution` untuk dapat membaca output otomatisasi. `AWSSupport-TroubleshootRDP` panggilan `AWSSupport-ExecuteEC2Rescue` untuk melakukan remediasi offline - harap tinjau izin `AWSSupport-ExecuteEC2Rescue` untuk memastikan Anda dapat menjalankan otomatisasi dengan sukses.

### Langkah Dokumen

1. `aws:assertAwsResourceProperty`- Periksa apakah instance adalah Windows Server instance
2. `aws:assertAwsResourceProperty`- Periksa apakah instance adalah instance yang dikelola
3. (Pemecahan masalah online) Jika instance adalah instance terkelola, maka:

- a. `aws:assertAwsResourceProperty`- Periksa nilai Aksi yang disediakan

- b. (Cek online) Jika Action = CheckAll, maka:

`aws:runPowerShellScript`- Menjalankan PowerShell skrip untuk mendapatkan status profil Windows Firewall.

`aws:executeAutomation`- Panggilan `AWSSupport-ManageWindowsService` untuk mendapatkan status layanan RDP.

`aws:executeAutomation`- Panggilan `AWSSupport-ManageRDPSettings` untuk mendapatkan pengaturan RDP.

- c. (Perbaiki online) Jika Action = FixAll, maka:

`aws:runPowerShellScript`- Menjalankan PowerShell skrip untuk menonaktifkan semua profil Windows Firewall.

`aws:executeAutomation`- Panggilan `AWSSupport-ManageWindowsService` untuk memulai layanan RDP.

`aws:executeAutomation`- Panggilan `AWSSupport-ManageRDPSettings` untuk mengaktifkan koneksi jarak jauh dan menonaktifkan NLA.

- d. (Manajemen online) Jika Action = Custom, maka:



`aws:runPowerShellScript`- Menjalankan PowerShell script untuk mengelola profil Windows Firewall.

`aws:executeAutomation`- Panggilan `AWSSupport-ManageWindowsService` untuk mengelola layanan RDP.

`aws:executeAutomation`- Panggilan `AWSSupport-ManageRDPSettings` untuk mengelola pengaturan RDP.

4. (Remediasi offline) Jika instance bukan instance terkelola maka:

- a. `aws:assertAwsResourceProperty`- Menegaskan `AllowOffline`= benar
- b. `aws:assertAwsResourceProperty`- Menegaskan Aksi = `FixAll`
- c. `aws:assertAwsResourceProperty`- Menegaskan nilai `SubnetId`

(Gunakan subnet instance yang disediakan) Jika `SubnetId` `SELECTED_INSTANCE_SUBNET`

`aws:executeAwsApi`- Ambil subnet contoh saat ini.

`aws:executeAutomation`- Jalankan `AWSSupport-ExecuteEC2Rescue` dengan subnet contoh yang disediakan.

- d. (Gunakan subnet kustom yang disediakan) Jika tidak `SubnetId` `SELECTED_INSTANCE_SUBNET`

`aws:executeAutomation`- Jalankan `AWSSupport-ExecuteEC2Rescue` dengan `SubnetId` nilai yang diberikan.

Keluaran

`manageFirewallProfiles`.Keluaran

ManajerDP `ServiceSettings` .Output

ManajerDPSettings.output

`checkFirewallProfiles`.Keluaran

`CheckRDP` .Keluaran `ServiceSettings`

`CheckRDPSettings`.output

disableFirewallProfiles.Keluaran

RestoreDefaUltrdp ServiceSettings .Output

RestoreDefaUltrdpSettings.output

Troubleshootrdpoffline.output

Pemecahan OfflineWithSubnetId masalahRDP .Output

## **AWSSupport-TroubleshootSSH**

### Deskripsi

AWSSupport-TroubleshootSSHRunbook menginstal alat Amazon EC2Rescue untuk Linux, dan kemudian menggunakan alat EC2Rescue untuk memeriksa atau mencoba memperbaiki masalah umum yang mencegah koneksi jarak jauh ke mesin Linux melalui SSH. Secara opsional, perubahan dapat diterapkan secara offline dengan menghentikan dan memulai instance, jika pengguna secara eksplisit mengizinkan remediasi offline. Secara default, runbook beroperasi dalam mode read-only.

### [Jalankan Otomasi ini \(konsol\)](#)

Untuk informasi tentang bekerja dengan AWSSupport-TroubleshootSSH runbook, lihat [topik AWSSupport-TroubleshootSSH pemecahan masalah ini dari Dukungan AWS Premium](#).

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- Action

Jenis: String

Nilai yang valid: CheckAll | FixAll

Bawaan: CheckAll

Deskripsi: (Diperlukan) Tentukan apakah akan memeriksa masalah tanpa memperbaikinya atau memeriksa dan memperbaiki masalah yang ditemukan secara otomatis.

- AllowOffline

Jenis: String

Nilai yang valid: benar/salah

Default: salah

Deskripsi: (Opsional) Perbaiki saja - Setel ke true jika Anda mengizinkan remediasi SSH offline jika pemecahan masalah online gagal, atau instance yang disediakan bukan instans terkelola. Catatan: Untuk remediasi offline, SSM Automation menghentikan instans, dan membuat AMI sebelum mencoba operasi apa pun.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans EC2 Anda untuk Linux.

- S3 BucketName

Jenis: String


Deskripsi: (Opsional) Hanya offline - Nama bucket S3 di akun tempat Anda ingin mengunggah log pemecahan masalah. Pastikan kebijakan bucket tidak memberikan izin baca/tulis yang tidak perlu kepada pihak yang tidak memerlukan akses ke log yang dikumpulkan.

- SubnetId

Jenis: String

Bawaan: SelectedInstanceSubnet

Deskripsi: (Opsional) Hanya offline - ID subnet untuk instans EC2Rescue yang digunakan untuk melakukan pemecahan masalah offline. Jika tidak ada ID subnet yang ditentukan, AWS Systems Manager Automation akan membuat VPC baru.

 Important

Subnet harus berada di Availability Zone yang sama dengan InstanceId, dan harus mengizinkan akses ke endpoint SSM.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan agar instans EC2 yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon AmazonSSM ManagedInstanceCore yang terpasang. Untuk remediasi online, pengguna harus memiliki setidaknya ssm:DescribeInstanceInformation, ssm: StartAutomationExecution dan ssm: SendCommand untuk menjalankan otomatisasi dan mengirim perintah ke instance, ditambah ssm: GetAutomationExecution untuk dapat membaca output otomatisasi. Untuk remediasi offline, pengguna harus memiliki setidaknya ssm:DescribeInstanceInformation, ssm:, ec2: StartAutomationExecution DescribeInstances, plus ssm: GetAutomationExecution untuk dapat membaca output otomatisasi. AWSSupport-TroubleshootSSH panggilan AWSSupport-ExecuteEC2Rescue untuk melakukan remediasi offline - harap tinjau izin AWSSupport-ExecuteEC2Rescue untuk memastikan Anda dapat menjalankan otomatisasi dengan sukses.

Langkah Dokumen

1. aws:assertAwsResourceProperty- Periksa apakah instance adalah instance yang dikelola
  - a. (Remediasi online) Jika instance adalah instance terkelola, maka:
    - i. aws:configurePackage- Instal EC2Rescue untuk Linux melalui. AWS-ConfigureAWSPackage
    - ii. aws:runCommand- Jalankan script bash untuk menjalankan EC2Rescue untuk Linux.
  - b. (Remediasi offline) Jika instance bukan instance terkelola maka:

- i. `aws:assertAwsResourceProperty`- Menegaskan `AllowOffline`= benar
- ii. `aws:assertAwsResourceProperty`- Menegaskan Aksi = `FixAll`
- iii. `aws:assertAwsResourceProperty`- Menegaskan nilai `SubnetId`
- iv. (Gunakan subnet instance yang disediakan) Jika `SubnetId SelectedInstanceSubnet` kita menjalankan `aws:executeAutomation AWSSupport-ExecuteEC2Rescue` dengan subnet instance yang disediakan.
- v. (Gunakan subnet kustom yang disediakan) Jika tidak `SubnetId SelectedInstanceSubnet` digunakan `aws:executeAutomation` untuk menjalankan `AWSSupport-ExecuteEC2Rescue` dengan `SubnetId` nilai yang diberikan.

Keluaran

TroubleshootsSH.Output

TroubleshootsShoffline.output

OfflineWithSubnetIdTroubleshootSSH .Output

## **AWSSupport - TroubleshootSUSERegistration**

Deskripsi

`AWSSupport-TroubleshootSUSERegistrationRunbook` membantu Anda mengidentifikasi mengapa mendaftarkan SUSE Linux Enterprise Server instans Amazon Elastic Compute Cloud (Amazon EC2) dengan SUSE Update Infrastructure gagal. Output otomatisasi menyediakan langkah-langkah untuk menyelesaikan, atau membantu Anda memecahkan masalah, masalah. Jika instans melewati semua pemeriksaan selama otomatisasi, instans terdaftar dengan SUSE Update Infrastructure.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

## Platform

### Linux

#### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Amazon Resource Name (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Systems Manager Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Diperlukan) ID instans Amazon EC2 yang ingin Anda pecahkan.

#### Izin IAM yang diperlukan

AutomationAssumeRoleParameter membutuhkan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:ListCommands`

#### Langkah Dokumen

- `aws:assertAwsResourceProperty`- Memeriksa apakah instans Amazon EC2 dikelola oleh AWS Systems Manager.
- `aws:runCommand`- Memeriksa apakah platform instans Amazon EC2 adalah SLES.

- `aws:runCommand`- Memeriksa apakah `cloud-regionsrv-client` versi paket lebih besar dari atau sama dengan versi 9.0.10 yang diperlukan.
- `aws:runCommand`- Memeriksa apakah link simbolis untuk produk dasar rusak, dan perbaikan link itu rusak.
- `aws:runCommand`- Memeriksa apakah file host (`/etc/hosts`) berisi catatan untuk `smt-ec2-susecloud.net`. Otomatisasi menghapus entri duplikat apa pun.
- `aws:runCommand`- Memeriksa apakah `curl` perintah diinstal.
- `aws:runCommand`- Memeriksa apakah instans Amazon EC2 dapat mengakses alamat Instance Metadata Service (IMDS) 169.254.169.254.
- `aws:runCommand`- Memeriksa apakah instans Amazon EC2 memiliki kode penagihan atau kode AWS Marketplace produk.
- `aws:runCommand`- Memeriksa apakah instans Amazon EC2 dapat mencapai setidaknya 1 server regional melalui HTTPS.
- `aws:runCommand`- Memeriksa apakah instans Amazon EC2 dapat mencapai server Subscription Management Tool (SMT) melalui HTTP.
- `aws:runCommand`- Memeriksa apakah instans Amazon EC2 dapat mencapai server Subscription Management Tool (SMT) melalui HTTPS.
- `aws:runCommand`- Memeriksa apakah instans Amazon EC2 dapat mencapai `smt-ec2.susecloud.net` alamat melalui HTTPS.
- `aws:runCommand`- Mendaftarkan instans Amazon EC2 dengan SUSE Update Infrastructure.
- `aws:executeScript`- Mengumpulkan dan output output dari semua langkah sebelumnya.

## AWSSupport-TroubleshootWindowsPerformance

### Deskripsi

Runbook `AWSSupport-TroubleshootWindowsPerformance` membantu memecahkan masalah performa yang sedang berlangsung di instans Windows Amazon Elastic Compute Cloud (Amazon EC2). Runbook menangkap log dari instance target dan menganalisis CPU, memori, disk, dan metrik kinerja jaringan. Secara opsional, otomatisasi dapat menangkap dump proses untuk membantu Anda menentukan potensi penyebab penurunan kinerja. Otomatisasi juga menangkap log peristiwa dan sistem dengan menggunakan [EC2Rescue](#) alat terbaru, jika Anda mengizinkan runbook ini untuk menginstalnya.

## Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Memeriksa instans Amazon EC2 untuk prasyarat.
- Menghasilkan log kinerja di disk root instans Amazon EC2 Windows
- Menyimpan log yang ditangkap di folder `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Jika bucket Amazon Simple Storage Service (Amazon S3) disediakan, dan peran asumsi otomatisasi memiliki izin yang diperlukan, log yang diambil akan diunggah ke bucket Amazon S3.
- Menginstal EC2Rescue alat terbaru ke instans Windows Amazon EC2 untuk menangkap peristiwa dan log sistem jika Anda memilih untuk menginstalnya, tetapi tidak menganalisis dump proses dan log yang ditangkap oleh. EC2Rescue

### Important

- Untuk menjalankan runbook ini, instans Windows Amazon EC2 harus dikelola oleh. AWS Systems Manager Untuk informasi selengkapnya, lihat [Mengapa instans Amazon EC2 saya tidak ditampilkan sebagai node terkelola](#).
- Untuk menjalankan runbook ini, instans Amazon EC2 Windows harus berjalan pada versi Windows 8.1/Windows Server 2012 R2 (6.3) atau yang lebih baru dengan 4.0 atau lebih baru PowerShell . Untuk informasi selengkapnya, lihat [Versi Sistem Operasi Windows](#).
- Untuk pembuatan log kinerja, setidaknya 10 GB ruang kosong pada perangkat root diperlukan. Jika disk root lebih besar dari 100 GB, ruang kosong harus lebih besar dari 10% dari ukuran disk. Jika Anda membuang proses selama eksekusi, ruang kosong harus lebih besar dari 10 GB ditambah ukuran memori total yang dikonsumsi oleh proses ketika proses mengkonsumsi lebih dari 10 GB memori.
- Log yang dihasilkan pada perangkat root tidak dihapus secara otomatis.
- Runbook tidak mencopot pemasangan alat. EC2Rescue Untuk informasi selengkapnya, lihat [Menggunakan EC2Rescue untuk Windows Server](#).
- Ini adalah praktik terbaik untuk menjalankan otomatisasi ini selama dampak kinerja. Anda juga dapat menjalankannya secara berkala menggunakan asosiasi AWS Systems Manager State Manager atau dengan menjadwalkan AWS Systems Manager Pemeliharaan Windows.



## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeInstances`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:GetAutomationExecution`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `s3:ListBucket`
- `s3:GetEncryptionConfiguration`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketPolicyStatus`
- `s3:PutObject`
- `s3:GetBucketAcl`
- `s3:GetAccountPublicAccessBlock`

(Opsional) Peran IAM yang dilampirkan pada profil instans atau pengguna IAM yang dikonfigurasi pada instance memerlukan tindakan berikut untuk mengunggah log ke bucket Amazon S3 yang ditentukan untuk parameter: *LogUploadBucketName*

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootWindowsPerformance](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:

- `AutomationAssumeRole` (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `InstanceId` (Diperlukan):

ID instans Windows Amazon EC2 target tempat Anda ingin menjalankan otomatisasi. Instans harus dikelola oleh Systems Manager untuk menjalankan otomatisasi.

- `CaptureProcessDump` (Opsional):

Jenis dump proses untuk menangkap. Otomatisasi dapat menangkap satu proses dump untuk proses yang berpotensi menyebabkan dampak kinerja di awal otomatisasi. Volume root instance membutuhkan setidaknya 10 GB ruang kosong (lebih besar dari 10% dari ukuran disk ketika ukuran volume root lebih besar dari 100 GB, dan 10 GB ditambah ukuran memori total yang dikonsumsi oleh proses ketika proses mengkonsumsi lebih dari 10 GB memori).

- `LogCaptureDuration` (Opsional):

Jumlah menit, antara 1 dan 15, otomatisasi ini akan menangkap log saat masalah ada. Defaultnya adalah 5.

- **LogUploadBucketName (Opsional):**

Bucket Amazon S3 di akun Anda tempat Anda ingin mengunggah log. Bucket harus dikonfigurasi dengan enkripsi sisi server (SSE), dan kebijakan bucket tidak boleh memberikan izin baca/tulis yang tidak perlu kepada pihak yang tidak memerlukan akses ke log yang diambil. Instans Windows Amazon EC2 harus memiliki akses ke bucket Amazon S3.

- **InstalleC2 RescueTool (Opsional):**

Setel Yes untuk memungkinkan runbook menginstal versi terbaru EC2Rescue alat untuk menangkap Windows Events dan log Sistem. Default-nya adalah No.

- **Pengakuan (Diperlukan):**

Baca detail lengkap tindakan yang dilakukan oleh runbook otomatisasi ini dan jika Anda setuju, ketik `Yes, I understand and acknowledge`.

**Input parameters**

**InstanceId**  
(Required) The ID of the Amazon EC2 Windows instance you want to troubleshoot performance issues.  
 Show interactive instance picker

**AutomationAssumeRole**  
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

**LogCaptureDuration**  
(Optional) The number of minutes this automation should capture logs while the issue is present. Default is '5' minutes. You can specify a value between '1' and up to '15' minutes.

**InstallEC2RescueTool**  
(Optional) Set it to 'True' if you allow the runbook to install the latest version of the 'EC2Rescue' tool to capture the Windows Events and System logs. Default value 'No'.

**CaptureProcessDump**  
(Optional) The process dump type to capture. The automation can capture one process dump for the process which is potentially causing the performance impact in the beginning of the automation. The instance root volume will require to have at least 10 GB free space (greater than 10% of the disk size when the root volume size is bigger than 100 GB and 10GB plus the total memory size consumed by the process when the process consumes more than 10GB memory).

**LogUploadBucketName**  
(Optional) The Amazon S3 bucket in your account to upload the logs to. Please make sure the bucket is configured with server-side encryption (SSE), and the bucket policy does not grant unnecessary read/write permissions to parties that do not need to access the logs. Also please make sure EC2 Windows instance has necessary access to the S3 Bucket.

**Acknowledgement**  
(Required) Please read the complete details of the actions performed by this automation runbook and write 'Yes, I understand and acknowledge' if you acknowledge the steps.

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **CheckConcurrency:**

Memastikan bahwa hanya ada satu eksekusi runbook ini yang menargetkan instance. Jika runbook menemukan eksekusi lain yang menargetkan instance yang sama, ia mengembalikan kesalahan dan berakhir.

- **AssertInstanceIsWindows:**

Menegaskan bahwa instans Amazon EC2 berjalan pada Sistem Operasi Windows. Jika tidak, otomatisasi berakhir.

- **AssertInstanceIsManagedInstance:**

Menegaskan bahwa instans Amazon EC2 dikelola oleh. AWS Systems Manager Jika tidak, otomatisasi berakhir.

- **VerifyPrerequisites:**

Memverifikasi PowerShell versi pada OS instance dan memastikan bahwa instance dapat dihubungkan melalui Systems Manager untuk menjalankan PowerShell perintah. Otomatisasi ini mendukung PowerShell 4.0 dan di atasnya berjalan pada versi Windows 8.1/Server 2012 R2 (6.3) atau yang lebih baru. Jika versinya lebih tua, otomatisasi gagal. Saat Anda memilih untuk mengunggah log ke bucket Amazon S3, otomatisasi ini Memeriksa apakah AWS Alat untuk PowerShell modul tersedia. Jika tidak, otomatisasi berakhir.

- **BranchOnProcessDump:**

Cabang berdasarkan jika Anda mengaturnya untuk menangkap dump proses yang memengaruhi kinerja.

- **CaptureProcessDump:**

Memeriksa apakah instance memiliki cukup ruang untuk menjalankan otomatisasi ini (saat Anda memilih CPU/Memori Tertinggi).

- **CapturePerformanceLogs:**

Memeriksa ruang disk lagi dan menjalankan PowerShell skrip pada instance untuk membuat penghitung perfmon dan memulai Performance Monitor dan Windows Performance Recorder logging. Skrip berhenti setelah yang LogCaptureDuration ditentukan terpenuhi.

- **SummarizePerformanceLogs:**

Merangkum laporan XHTML yang dihasilkan pada langkah sebelumnya,CapturePerformanceLogs, untuk menemukan proses yang bertanggung jawab mengkonsumsi paling banyak WorkingSet 64 (Memori) dan% Processor Time (CPU) ditampilkan sebagai output pada otomatisasi. Ini menghasilkan informasi serupa untuk penggunaan LogicalDisk, Antarmuka Jaringan, Memori, TCPv4, IPv4, dan UDPv4 dan menyimpannya ke dalam folder output. analysis\_output.log

- **BranchOnInstallEC2Rescue:**

Cabang jika Anda mengaturnya untuk menginstal EC2Rescue alat terbaru di instans Amazon EC2.

- **InstallEC2RescueTool:**

Menginstal EC2Rescue alat di OS instance untuk menangkap EC2Rescue log menggunakan `AWS-ConfigureAWSPackage`.

- **RunEC2RescueTool:**

Menjalankan EC2Rescue alat di OS instance untuk menangkap semua log yang dibutuhkan. EC2Rescue menangkap hanya log yang diperlukan untuk menghemat ruang.

- **BranchOnIfS3BucketProvided:**

Cabang berdasarkan masukan pengguna `LogUploadBucketName` untuk melihat apakah ada nama bucket yang tersedia untuk mengunggah log.

- **GetS3BucketPublicStatus:**

Menentukan apakah bucket Amazon S3 disediakan, dan jika demikian, mengonfirmasi bahwa bucket Amazon S3 tidak bersifat publik dan dikonfigurasi dengan SSE.

- **UploadLogResult:**

Mengunggah log ke bucket Amazon S3 yang disediakan. Jika PowerShell versi 5.0 atau lebih tinggi, itu memampatkan log ke arsip ZIP dan mengunggahnya. Ini menghapus file ZIP setelah upload selesai. Jika PowerShell versi di bawah 5.0, itu mengunggah file langsung ke folder.

- **CleanUpLogsOnFailure:**

Membersihkan semua log yang dihasilkan oleh `CapturePerformanceLogs` langkah ketika gagal. `CleanUpLogsOnFailure`Langkah ini mungkin gagal atau batas waktu jika Agen SSM tidak berfungsi dengan benar, atau sistem Windows tidak responsif.

7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci:

Eksekusi di mana instance target memiliki semua prasyarat yang diperlukan.

```

▼ Outputs

CaptureProcessDump.Output
No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output
No output available yet because the step is not successfully executed

CapturePerformanceLogs.Output
The instance has enough space to capture performance logs.
WPR capture process is in 'Stopped' state.
Data Collector Set TroubleshootWindowsPerformance-... was not found.
Attempting to create Performance monitor Data Collector Set TroubleshootWindowsPerformance-...
Data Collector Set TroubleshootWindowsPerformance-... created successfully.
Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance-...
Data Collector Set TroubleshootWindowsPerformance-... started successfully.
Current CPU usage is '54.73%' and Memory usage is '17.15%'
Not both CPU and Memory usage are over 95% at this moment hence continue to capture WPR log.
Starting Windows Performance Recording (WPR) capture process.
Stopping WPR capture process.
WPR capture process is in 'Stopped' state.
The Data Collector Set TroubleshootWindowsPerformance-... is currently generating logs.
The Data Collector Set TroubleshootWindowsPerformance-... has finished generating logs and is currently in 'Stopped' state.
Attempting to delete Data Collector Set TroubleshootWindowsPerformance-...
Data Collector Set TroubleshootWindowsPerformance-... deleted successfully.

[PASSED] Performance logs are captured successfully inside the folder: C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance-...
The captured log files will not be deleted by this automation, please manually delete it after analysis.

RunEC2RescueTool.Output
[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance-..._EC2Rescue_23-05-48.zip'. The latest EC2Rescue tool is installed
by this automation and please manually remove it if you don't need it. Its installed path is C:\Program Files\Amazon\EC2Rescue\EC2RescueCmd.exe.

SummarizePerformanceLogs.Output
Top 5 Processes which consumed most CPU in percentage as below. If you see a percentage higher than 100 that means the process is using more than one CPU core.
Process Counter Min % Max % Avg %
sppsvc Processor 0.00 106.00 9.00
WmiPrvSE#2 Processor 0.00 90.00 2.00
MsMpEng Processor 0.00 38.00 0.75
GenVulObj Processor 0.00 30.00 0.28
svchost#42 Processor 0.00 29.00 0.17

Top 5 Processes which consumed most WorkingSet64 memory as below (in MB):
Process Counter Min MB Max MB Avg MB
MsMpEng WorkingSet 220.00 260.00 236.00
Registry WorkingSet 78.00 193.00 120.00
powershell WorkingSet 90.00 92.00 92.00
LogonUI WorkingSet 43.00 43.00 43.00
dwm WorkingSet 38.00 38.00 38.00
    
```

Eksekusi dimana instance target berada di platform Linux dan eksekusi gagal. Anda akan memilih ID langkah untuk melihat detail kegagalan.

```

▼ Outputs

CapturePerformanceLogs.Output
No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output
No output available yet because the step is not successfully executed

SummarizePerformanceLogs.Output
No output available yet because the step is not successfully executed

VerifyPrerequisites.Output
No output available yet because the step is not successfully executed

CaptureProcessDump.Output
No output available yet because the step is not successfully executed

RunEC2RescueTool.Output
No output available yet because the step is not successfully executed


UploadLogResult.Output
No output available yet because the step is not successfully executed
    
```

Execution status		
Overall status	All executed steps	# Succeeded
🔴 Failed	2	1
# Failed	# Cancelled	# TimedOut
1	0	0

Executed steps (2)							
<input type="text" value="Find Steps"/>							
Step ID	Step #	Step name	Action	Status	Start time	End time	
...	1	CheckConcurrency	aws:executeScript	🟢 Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT	
...	2	AssertInstanceIsWindows	aws:assertAwsResourceProperty	🔴 Failed	Tue, 19 Mar 2024 16:15:00 GMT	Tue, 19 Mar 2024 16:15:01 GMT	

Rincian kegagalan langkah AssertInstanceIsWindows.

**Failure details**

 **Failure message**  
 Step fails when it is Execute/Canceling action. Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows']. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

FailureType	FailureStage
Verification	Invocation
VerificationErrorMessage	
Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows'].	

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

## AWSSupport-TroubleshootWindowsUpdate

### Deskripsi

AWSSupport-TroubleshootWindowsUpdateRunbook digunakan untuk mengidentifikasi masalah yang dapat gagal dalam pembaruan Windows untuk instans Windows Amazon Elastic Compute Cloud (Amazon EC2) Windows.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Memeriksa apakah instans Amazon EC2 target dikelola oleh. AWS Systems Manager
- Memeriksa apakah versi AWS Systems Manager Agen (Agen SSM) dan Windows Server didukung untuk operasi patching Systems Manager.
- Memeriksa ruang disk yang tersedia yang direkomendasikan untuk pembaruan Windows dan jika reboot tertunda. Reboot yang tertunda biasanya menunjukkan bahwa pembaruan sedang tertunda, dan reboot diperlukan sebelum melakukan pembaruan tambahan.
- Mengkonfigurasi pengaturan proxy di tingkat sistem operasi, yang dapat membantu memecahkan masalah konektivitas.

- Melakukan uji konektivitas titik akhir Amazon Simple Storage Service (Amazon S3) dan memanggil [GetDeployablePatchSnapshotForInstance](#) operasi API untuk mengambil snapshot saat ini untuk baseline patch yang digunakan node terkelola.
- Jika koneksi gagal, berikan opsi untuk menjalankan `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook guna menganalisis konektivitas instans ke titik akhir Amazon S3.
- Memvalidasi konfigurasi pembaruan Windows dan menguji Windows Server Update Services (WSUS) (jika ada).

#### Important

- Pengontrol domain Active Directory tidak didukung.
- Windows Server versi 2008 R2 atau versi sebelumnya tidak didukung.
- SSM Agent 1.2.371 atau versi sebelumnya tidak didukung.
- `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook digunakan [VPC Reachability Analyzer](#) untuk menganalisis konektivitas jaringan antara sumber dan titik akhir layanan. Anda dikenakan biaya per analisis yang dijalankan antara sumber dan tujuan. Untuk detail selengkapnya, lihat [Harga Amazon VPC](#).
- `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook tidak tersedia di semua wilayah di mana Systems Manager didukung.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter



## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

### Note

Untuk menjalankan runbook `anakAWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`, tambahkan izin yang tercantum dalam dokumen [ini](#).

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootWindowsUpdate](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
  - AutomationAssumeRole (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId (Diperlukan):

Masukkan ID instans Amazon EC2 di mana pembaruan Windows gagal.

- **RunVpcReachabilityAnalyzer(Opsional):**

Tentukan `true` untuk menjalankan `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` otomatisasi jika masalah jaringan ditentukan oleh pemeriksaan yang diperluas atau jika ID instans yang ditentukan bukan instance terkelola. Untuk informasi lebih lanjut tentang otomatisasi anak ini, lihat [dokumentasi](#). Nilai default-nya adalah `false`.

- **RetainVpcReachabilityAnalysis(Opsional):**

Hanya relevan jika `RunVpcReachabilityAnalyzer` adalah `true`. Tentukan `true` untuk mempertahankan jalur wawasan jaringan dan analisis terkait yang dibuat oleh `ReachabilityAnalyzer`. Secara default, sumber daya tersebut dihapus setelah analisis berhasil. Jika Anda memilih untuk mempertahankan analisis, runbook anak tidak menghapus analisis dan Anda dapat memvisualisasikannya di konsol VPC Amazon. Tautan konsol akan tersedia di output otomatisasi anak. Nilai default `false`.

**Input parameters**

---

**InstanceId**  
(Required) The ID of the Amazon EC2 instance.  
 Show interactive instance picker

**AutomationAssumeRole**  
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

**RunVpcReachabilityAnalyzer**  
(Optional) Specify 'true' to run the 'AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2' automation if a network issue is determined by the extended checks, or if the instance ID specified is not a managed instance. For more information on this child automation, please refer to the documentation above. This parameter defaults to 'false'.

**RetainVpcReachabilityAnalysis**  
(Optional) Only relevant if 'RunVpcReachabilityAnalyzer' is true. Specify 'true' to retain the network insight path and related analyses created by VPC Reachability Analyzer. By default, those resources are deleted after successful analysis. If you choose to retain the analysis, the child runbook does not delete the analysis and you can visualize it in the VPC console. The console link will be available in the child automation output. This parameter defaults to 'false'.

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **getWindowServerAndSSMAgentVersion:**

Memverifikasi bahwa instance target dikelola oleh AWS Systems Manager dan mendapatkan detail tentang versi Agen SSM dan versi Windows.

- **assertIfInstanceIsSsmManaged:**

Memastikan instans Amazon EC2 dikelola oleh AWS Systems Manager (SSM), jika tidak, otomatisasi akan berakhir.

- **CheckProxy:**

Memeriksa semua jenis proxy untuk instance Windows.

- **CheckPrerequisites:**

Mendapat versi Agen SSM dan versi Windows, dan menentukan apakah itu adalah Active Directory Domain Controller (DC). Jika instancenya adalah DC atau SSM Agent atau versi Windows tidak didukung, runbook berhenti.

- **CheckDiskSpace:**

Mendapat dan memvalidasi ruang disk yang tersedia melalui instance Windows jika cukup untuk melakukan pembaruan Windows.

- **CheckPendingReboot:**

Memeriksa reboot yang tertunda melalui instance Windows.

- **CheckS3Connectivity:**

Memeriksa apakah instance dapat mencapai titik akhir Amazon S3 untuk Patchbaseline

- **branchOnRunVpcReachabilityAnalyzer:**

Jika RunVpcReachabilityAnalyzer benar, maka itu cabang otomatisasi untuk menjalankan analisis yang lebih dalam untuk debugging konektivitas Amazon S3.

- **GenerateEndpoints:**

Menghasilkan titik akhir untuk memiliki pemeriksaan konektivitas yang diperluas untuk titik akhir Amazon S3.

- **analyzeAwsEndpointReachabilityFromEC2:**

Memanggil runbook otomatisasi, `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`. untuk memeriksa jangkauan instance yang dipilih ke titik akhir yang diperlukan.

- **CheckWindowsUpdateServices:**

Memeriksa status layanan Pembaruan Windows dan jenis mulai.

- **CheckWindowsUpdateSettings:**

Memeriksa kebijakan Pembaruan Windows yang dikonfigurasi melalui instance Windows.

- **CheckWSUSSettings:**

Memeriksa apakah pembaruan Windows dikonfigurasi dengan WSUS atau Katalog Pembaruan Microsoft dan memverifikasi konektivitas.

- **CheckWUGlobalSettings:**

Memeriksa pengaturan global Pembaruan Windows yang dikonfigurasi melalui instance Windows.

- **GenerateLogs:**

Mengunduh log Pembaruan Windows dan log CBS ke desktop instance dan memeriksa log peristiwa Windows untuk kegagalan.

- **FinalReport:**

Menghasilkan laporan lengkap dari semua langkah.

7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci:

```

FinalReport.Results
"
=====Prerequisites Check=====
Result: ✓ [PASSED]
INFO: The target instance is not an Active Directory Domain Controller.
INFO: The platform 10.0.20348 is supported.
INFO: The SSM Agent version 3.2.1705.0 is supported.

=====Disk Space Check=====
Result: ✓ [PASSED]
INFO: Disk space on drive C: is recommended to run Windows updates.

=====Pending Reboot Check=====
Result: ✓ [PASSED]
INFO: There is no pending reboot.

=====Amazon S3 Connectivity Check=====
Result: ✓ [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

=====AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2=====
Result: ✓ [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

=====Windows Update Services Status=====
Result: ✓ [PASSED]
Getting Services Status and types for Windows Update...
The service 'Application Identity' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Application Identity'
Service 'Application Identity' started successfully
The service 'Background Intelligent Transfer Service' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Background Intelligent Transfer Service'
Service 'Background Intelligent Transfer Service' started successfully
INFO: The service 'Cryptographic Services' status is currently 'Running'
The service 'Windows Installer' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Windows Installer'
Service 'Windows Installer' started successfully
INFO: The service 'Windows Modules Installer' status is currently 'Running'
INFO: The service 'Windows Update' status is currently 'Running'

=====Windows Proxy Settings=====
Result: ✓ [PASSED]
No WinInet Proxy is set on the system
No Winhttp Proxy is set on the system
There is no proxy setting for SSM Agent
System Wide Environment HTTP Proxy is not set.
System Wide Environment HTTPS Proxy is not set.
System Wide Environment NO PROXY is not set.
There is no HTTP Proxy configured at local system account user environment.

=====Windows Update Settings=====
Result: ✓ [PASSED]
INFO: Windows Update (Policies): Never check for updates
INFO: To modify this setting is in Computer Configuration\Administrative Template\Windows Component\Windows
Update\Configure Automatic Updates. For more details please check this document: https://learn.microsoft.com/de-
de/security-updates/windowsupdateservices/18127451

=====Windows Update Global Settings=====
Result: ✓ [PASSED]
Windows Update Client has no restrictions

=====Copy of Windows Update and CBS Logs=====
Result: ✓ [PASSED]
No errors found in Microsoft-Windows-WindowsUpdateClient events.
INFO: Logs copied to the C:\Windows\TEMP\c176a507-d074-4402-8a5b-631dd643f33a folder
"

```

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)

- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

Dokumentasi yang terkait dengan AWS layanan

- Lihat artikel, [Pembaruan Troubleshoot Windows](#), untuk informasi lebih lanjut.

## AWSSupport-UpgradeWindowsAWSDrivers

### Deskripsi

AWSSupport-UpgradeWindowsAWSDriversRunbook memutakhirkan atau memperbaiki penyimpanan dan AWS driver jaringan pada instans EC2 yang ditentukan. Runbook mencoba menginstal versi AWS driver terbaru secara online dengan menghubungi Agen SSM. Jika Agen SSM tidak dapat dihubungi, runbook dapat melakukan instalasi offline AWS driver jika diminta secara eksplisit.

#### Note

Baik peningkatan online dan offline akan membuat AMI sebelum mencoba operasi apa pun, yang akan bertahan setelah otomatisasi selesai. Anda bertanggung jawab untuk mengamankan akses ke AMI, atau menghapusnya. Metode online memulai ulang instance sebagai bagian dari proses pemutakhiran, sedangkan metode offline mengharuskan instans EC2 yang disediakan dihentikan dan kemudian dimulai.

#### Important

Jika instans Anda terhubung AWS Systems Manager menggunakan titik akhir VPC, runbook ini akan gagal kecuali digunakan di Wilayah us-east-1. Runbook ini juga akan gagal pada pengontrol domain. Untuk memperbarui driver AWS PV pada pengontrol domain, lihat [Memutakhirkan Pengontrol Domain \(Peningkatan AWS PV\)](#).

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

## Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AllowOffline

Jenis: String

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Setel ke true jika Anda mengizinkan peningkatan driver offline jika instalasi online tidak dapat dilakukan. Catatan: Metode offline mengharuskan instans EC2 yang disediakan dihentikan dan kemudian dimulai. Data yang disimpan dalam volume penyimpanan instance akan hilang. Alamat IP publik akan berubah jika Anda tidak menggunakan IP Elastis.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ForceUpgrade

Jenis: String

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Hanya offline - Setel ke true jika Anda mengizinkan peningkatan driver offline untuk melanjutkan meskipun instance Anda sudah menginstal driver terbaru.

- InstanceId

Jenis: String


Deskripsi: (Wajib) ID instans EC2 Anda untuk Windows Server.

- SubnetId

Jenis: String

Default: SelectedInstanceSubnet

Deskripsi: (Opsional) Hanya offline - ID subnet untuk instans EC2Rescue yang digunakan untuk melakukan upgrade driver offline. Jika tidak ada subnet ID yang ditentukan, Systems Manager Automation akan membuat VPC baru.

 Important

Subnet harus berada di Availability Zone yang sama dengan InstanceId, dan harus memungkinkan akses ke endpoint SSM.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Instans EC2 yang menerima perintah minimal harus memiliki peran IAM yang mencakup izin untuk ssm: StartAutomationExecution dan ssm: SendCommand untuk menjalankan otomatisasi dan mengirim perintah ke instance, ditambah ssm: GetAutomationExecution untuk dapat membaca output otomatisasi. Anda dapat melampirkan kebijakan terkelola AmazonSSMManagedInstanceCore Amazon ke peran IAM Anda untuk memberikan izin ini. Kami merekomendasikan, bagaimanapun, menggunakan peran IAM Otomasi AmazonSSMAutomationRole untuk tujuan ini. Untuk informasi selengkapnya, lihat [Menggunakan IAM untuk mengonfigurasi peran untuk Otomasi](#).

Jika Anda melakukan upgrade offline, lihat izin yang diperlukan oleh [AWSSupport-StartEC2RescueWorkflow](#).

## Langkah Dokumen

1. aws:assertAwsResourceProperty- Memverifikasi instance input adalah Windows.



2. `aws:assertAwsResourceProperty`- Memverifikasi instance input adalah instance terkelola. Jika demikian, pemutakhiran online dimulai, jika tidak, peningkatan offline dievaluasi.
  - a. (Pemutakhiran online) Jika instance input adalah instance terkelola:
    - i. `aws:createImage`- Membuat cadangan AMI.
    - ii. `aws:createTags`- Menandai cadangan AMI.
    - iii. `aws:runCommand`- Menginstal driver jaringan ENA melalui `AWS-ConfigureAWSPackage`.
    - iv. `aws:runCommand`- Menginstal driver NVMe melalui `AWS-ConfigureAWSPackage`
    - v. `aws:runCommand`- Menginstal driver AWS PV melalui `AWS-ConfigureAWSPackage`.
  - b. (Upgrade offline) Jika instance input bukan instance terkelola:
    - i. `aws:assertAwsResourceProperty`- Memverifikasi `AllowOffline` bendera diatur ke `true`. Jika demikian, peningkatan offline dimulai, jika tidak, otomatisasi berakhir.
    - ii. `aws:changeInstanceState`- Hentikan contoh sumber.
    - iii. `aws:changeInstanceState`- Paksa menghentikan contoh sumber.
    - iv. `aws:createImage`- Buat cadangan AMI dari instance sumber.
    - v. `aws:createTags`- Tandai cadangan AMI dari instance sumber.
    - vi. `aws:executeAwsApi`- Aktifkan ENA untuk contoh
    - vii. `aws:assertAwsResourceProperty`- Tegaskan `ForceUpgrade` benderanya.
    - viii. Paksa pemutakhiran offline) Jika `ForceUpgrade = true` lalu jalankan `aws:executeAutomation` untuk memanggil `AWSSupport-StartEC2RescueWorkflow` dengan skrip pemutakhiran paksa driver. Ini menginstal driver terlepas dari versi saat ini yang diinstal
    - ix. (Upgrade offline) Jika `ForceUpgrade = false` maka jalankan `aws:executeAutomation` untuk memanggil `AWSSupport-StartEC2RescueWorkflow` dengan skrip peningkatan driver.

## Keluaran

`preUpgradeBackup.Imageld`

`preOfflineUpgradeCadangan.Imageld`

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

`upgradeDriversOffline.Keluaran`

`forceUpgradeDriversOffline.Output`

## Amazon ECS

AWS Systems Manager Automation menyediakan runbook standar untuk Amazon Elastic Container Service. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSSupport-CollectECSInstanceLogs](#)
- [AWS-InstallAmazonECSAgent](#)
- [AWS-ECSRunTask](#)
- [AWSSupport-TroubleshootECSContainerInstance](#)
- [AWSSupport-TroubleshootECSTaskFailedToStart](#)
- [AWS-UpdateAmazonECSAgent](#)

## AWSSupport-CollectECSInstanceLogs

Deskripsi

AWSSupport-CollectECSInstanceLogsRunbook mengumpulkan sistem operasi dan file log terkait Amazon Elastic Container Service (Amazon ECS) dari instans Amazon Elastic Compute Cloud (Amazon EC2) untuk membantu Anda memecahkan masalah umum Amazon ECS. Sementara otomatisasi mengumpulkan file log terkait, perubahan dilakukan pada sistem file. Perubahan ini termasuk pembuatan direktori sementara dan direktori log, penyalinan file log ke direktori ini, dan mengompresi file log ke dalam arsip.

Jika Anda menentukan nilai untuk `LogDestination` parameter, otomatisasi akan mengevaluasi status kebijakan bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) yang Anda tentukan. Untuk membantu keamanan log yang dikumpulkan dari instans Amazon EC2 Anda, jika status kebijakan `isPublic` disetel ke `true`, atau jika daftar kontrol akses (ACL) memberikan `READ|WRITE` izin ke grup Amazon S3 All Users yang telah ditentukan

sebelumnya, log tidak akan diunggah. Selain itu, jika bucket yang disediakan tidak tersedia di akun Anda, log tidak diunggah. Untuk informasi selengkapnya tentang grup Amazon S3 yang telah ditentukan sebelumnya, lihat grup [Amazon S3 yang telah ditentukan sebelumnya di Panduan Pengguna](#) Layanan Penyimpanan Sederhana Amazon.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ECS InstanceId

Jenis: String

Deskripsi: (Wajib) ID dari instance yang ingin Anda kumpulkan log. Instance yang Anda tentukan harus dikelola oleh Systems Manager.

- LogDestination

Jenis: String

Deskripsi: (Opsional) Bucket Amazon S3 di Akun AWS untuk mengunggah log yang diarsipkan.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`

Sebaiknya instans Amazon EC2 yang Anda tentukan dalam `ECSInstanceId` parameter memiliki peran IAM dengan kebijakan terkelola `AmazonSSMManagedInstanceCore` Amazon yang dilampirkan. Untuk mengunggah arsip log ke bucket Amazon S3 yang Anda tentukan dalam `LogDestination` parameter, Anda harus menambahkan izin berikut:

- `s3:PutObject`
- `s3:ListBucket`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketAcl`

## Langkah Dokumen

- `assertInstanceIsManaged`- Memverifikasi apakah instance yang Anda tentukan dalam `ECSInstanceId` parameter dikelola oleh Systems Manager.
- `getInstancePlatform`- Mendapat informasi tentang platform sistem operasi (OS) dari instance yang ditentukan dalam `ECSInstanceId` parameter.
- `verifyInstancePlatform`- Cabang otomatisasi berdasarkan platform OS.
- `runLogCollectionScriptOnLinux`- Mengumpulkan sistem operasi dan file log terkait Amazon ECS pada instance Linux dan membuat file arsip di direktori. `/var/log/collectECSlogs`
- `runLogCollectionScriptOnWindows`- Mengumpulkan sistem operasi dan file log terkait Amazon ECS pada instance Windows dan membuat file arsip di direktori. `C:\ProgramData\collectECSlogs`
- `verifyIfS3BucketProvided`- Memverifikasi apakah nilai ditentukan untuk `LogDestination` parameter.
- `runUploadScript`- Cabang langkah otomatisasi berdasarkan platform OS.

- `runUploadScriptOnLinux`- Mengunggah arsip log ke bucket Amazon S3 yang ditentukan dalam parameter dan menghapus file log `LogDestination` yang diarsipkan dari OS.
- `runUploadScriptOnWindows`- Mengunggah arsip log ke bucket Amazon S3 yang ditentukan dalam parameter dan menghapus file log `LogDestination` yang diarsipkan dari OS.

## AWS-InstallAmazonECSAgent

### Deskripsi

AWS-InstallAmazonECSAgentRunbook menginstal agen Amazon Elastic Container Service (Amazon ECS) Elastic Container Service (Amazon ECS) di instans Amazon Elastic Compute Cloud (Amazon EC2) yang Anda tentukan. Runbook ini hanya mendukung instans Amazon Linux dan Amazon Linux 2.

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Linux

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `Instancelds`

Jenis: `StringList`

Deskripsi: (Wajib) ID instans Amazon EC2 yang ingin Anda instal agen Amazon ECS.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`

Langkah Dokumen

`aws:executeScript`- Menginstal agen Amazon ECS pada instans Amazon EC2 yang Anda tentukan dalam parameter. `InstanceIds`

Keluaran

`InstallAmazonAgen ECS`. `SuccessfullInstances` - ID dari contoh di mana instalasi agen Amazon ECS berhasil.

`InstallAmazonAgen ECS`. `FailedInstances` - ID instance di mana instalasi agen Amazon ECS gagal.

`InstallAmazonAgen ECS`. `InProgressInstances` - ID instance tempat pemasangan agen Amazon ECS sedang berlangsung.

## **AWS - ECSRunTask**

Deskripsi

`AWS - ECSRunTaskRunbook` menjalankan tugas Amazon Elastic Container Service (Amazon ECS) yang Anda tentukan.

## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- capacityProviderStrategy

Jenis: String

Deskripsi: (Opsional) Strategi penyedia kapasitas yang digunakan untuk tugas tersebut.

- Klaster

Jenis: String

Deskripsi: (Opsional) Nama pendek atau ARN dari cluster untuk menjalankan tugas Anda. Jika Anda tidak menentukan cluster, cluster default digunakan.

- count

Jenis: String

Deskripsi: (Opsional) Jumlah instantiasi tugas yang ditentukan untuk ditempatkan di klaster Anda. Anda dapat menentukan hingga 10 tugas untuk setiap permintaan.

- Aktifkan ECS ManagedTags

Jenis: Boolean

Deskripsi: (Opsional) Menentukan apakah akan menggunakan tag terkelola Amazon ECS untuk tugas tersebut. Untuk informasi selengkapnya, lihat [Menandai sumber daya Amazon ECS Anda di Panduan](#) Pengembang Layanan Kontainer Elastis Amazon.

- `enableExecuteCommand`

Jenis: Boolean

Deskripsi: (Opsional) Menentukan apakah akan mengaktifkan fungsionalitas perintah eksekusi untuk kontainer dalam tugas ini. Jika benar, ini mengaktifkan fungsionalitas perintah eksekusi pada semua kontainer dalam tugas.

- `grup`

Jenis: String

Deskripsi: (Opsional) Nama kelompok tugas untuk dikaitkan dengan tugas. Nilai default adalah nama keluarga dari definisi tugas. Misalnya, `family:my-family-name`.

- `LaunchType`

Jenis: String

Nilai yang valid: EC2 | FARGATE | EKSTERNAL

Deskripsi: (Opsional) Infrastruktur untuk menjalankan tugas mandiri Anda.

- `networkConfiguration`

Jenis: String

Deskripsi: (Opsional) Konfigurasi jaringan untuk tugas tersebut. Parameter ini diperlukan untuk definisi tugas yang menggunakan mode `awsvpc` jaringan untuk menerima elastic network interface mereka sendiri, dan tidak didukung untuk mode jaringan lainnya.

- `mengesampingkan`

Jenis: String

Deskripsi: (Opsional) Daftar penampungan kontainer dalam format JSON yang menentukan nama kontainer dalam definisi tugas yang ditentukan dan penggantian yang harus diterimanya. Anda dapat mengganti perintah default untuk wadah yang ditentukan dalam definisi tugas atau image



Docker dengan penggantian perintah. Anda juga dapat mengganti variabel lingkungan yang ada yang ditentukan dalam definisi tugas atau gambar Docker pada wadah. Selain itu, Anda dapat menambahkan variabel lingkungan baru dengan penggantian lingkungan.

- Penempatan Kendala

Jenis: String

Deskripsi: (Opsional) Sebuah array objek kendala penempatan untuk digunakan untuk tugas. Anda dapat menentukan hingga 10 kendala untuk setiap tugas termasuk kendala dalam definisi tugas dan yang ditentukan saat runtime.

- Strategi Penempatan

Jenis: String

Deskripsi: (Opsional) Objek strategi penempatan yang akan digunakan untuk tugas. Anda dapat menentukan maksimal 5 aturan strategi untuk setiap tugas.

- platformVersion

Jenis: String

Deskripsi: (Opsional) Versi platform yang digunakan tugas. Versi platform hanya ditentukan untuk tugas yang dihosting di Fargate. Jika versi platform tidak ditentukan, versi LATEST platform akan digunakan.

- propagateTags

Jenis: String

Deskripsi: (Opsional) Menentukan apakah tag menyebar dari definisi tugas ke tugas. Jika tidak ada nilai yang ditentukan, tanda tidak disebar. Tag hanya dapat disebar ke tugas selama pembuatan tugas.

- ReferenceID

Jenis: String

Deskripsi: (Opsional) ID referensi yang akan digunakan untuk tugas. ID referensi dapat memiliki panjang maksimum 1024 karakter.

- dimulaiOleh

Jenis: String

Deskripsi: (Opsional) Tag opsional yang ditentukan saat tugas dimulai. Ini membantu Anda mengidentifikasi tugas mana yang termasuk dalam pekerjaan tertentu dengan memfilter hasil operasi `ListTasks` API. Hingga 36 huruf (huruf besar dan kecil), angka, tanda hubung (-), dan garis bawah (\_) diperbolehkan.

- tag

Jenis: String

Deskripsi: (Opsional) Metadata yang ingin Anda terapkan pada tugas untuk membantu Anda mengkategorikan dan mengatur tugas. Setiap tag terdiri dari kunci dan nilai yang ditentukan pengguna.

- TaskDefinition

Jenis: String

Deskripsi: (Opsional) ARN family dan revision (`family:revision`) atau penuh dari definisi tugas yang akan dijalankan. Jika revisi tidak ditentukan, ACTIVE revisi terbaru akan digunakan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ecs:RunTask`

Langkah Dokumen

`aws:executeScript`- Menjalankan tugas Amazon ECS berdasarkan nilai yang Anda tentukan untuk parameter input runbook.

## **AWSSupport-TroubleshootECSContainerInstance**

Deskripsi

`AWSSupport-TroubleshootECSContainerInstanceRunbook` membantu Anda memecahkan masalah instans Amazon Elastic Compute Cloud (Amazon EC2) yang gagal mendaftar dengan kluster Amazon ECS. Otomatisasi ini meninjau apakah data pengguna untuk instance berisi informasi

klaster yang benar, apakah profil instance berisi izin yang diperlukan, dan masalah konfigurasi jaringan.

**⚠ Important**

Agar berhasil menjalankan otomatisasi ini, status instans Amazon EC2 Anda harus `running`, dan status cluster Amazon ECS harus `ACTIVE`

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `ClusterName`

Jenis: String

Deskripsi: (Wajib) Nama klaster Amazon ECS yang gagal didaftarkan instans.

- `InstanceId`

Jenis: String

Deskripsi: (Wajib) ID instans Amazon EC2 yang ingin Anda pecahkan masalah.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:SimulateCustomPolicy`
- `iam:SimulatePrincipalPolicy`

Langkah Dokumen

AWS:executeScript: Meninjau apakah instans Amazon EC2 memenuhi prasyarat yang diperlukan untuk mendaftar dengan cluster Amazon ECS.

## **AWSSupport-TroubleshootECSTaskFailedToStart**

Deskripsi

AWSSupport-TroubleshootECSTaskFailedToStartRunbook membantu Anda memecahkan masalah mengapa tugas Amazon Elastic Container Service (Amazon ECS) di kluster Amazon ECS gagal dimulai. Anda harus menjalankan runbook ini Wilayah AWS sama dengan tugas Anda yang gagal dimulai. Runbook menganalisis masalah umum berikut yang dapat mencegah tugas dimulai:

- Konektivitas jaringan ke registri kontainer yang dikonfigurasi
- Izin IAM hilang yang diperlukan oleh peran eksekusi tugas
- Konektivitas titik akhir VPC
- Konfigurasi aturan grup keamanan
- AWS Secrets Manager referensi rahasia
- Konfigurasi log

#### Note

Jika analisis menentukan bahwa konektivitas jaringan perlu diuji, fungsi Lambda dan peran IAM yang diperlukan dibuat di akun Anda. Sumber daya ini digunakan untuk mensimulasikan konektivitas jaringan dari tugas Anda yang gagal. Otomatisasi menghapus sumber daya ini ketika mereka tidak lagi diperlukan. Namun, jika otomatisasi gagal menghapus sumber daya, Anda harus melakukannya secara manual.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- **ClusterName**

Jenis: String

Deskripsi: (Wajib) Nama cluster Amazon ECS tempat tugas gagal dimulai.

- **CloudwatchRetentionPeriod**

Jenis: Integer

Deskripsi: (Opsional) Periode retensi, dalam beberapa hari, untuk log fungsi Lambda disimpan di Log Amazon CloudWatch . Ini hanya diperlukan jika analisis menentukan konektivitas jaringan perlu diuji.

Nilai yang valid: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

Bawaan: 30

- **TaskId**

Jenis: String

Deskripsi: (Wajib) ID tugas yang gagal. Gunakan tugas yang terakhir gagal.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudtrail:LookupEvents`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSubnets`

- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ecr:DescribeImages`
- `ecr:GetRepositoryPolicy`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeServices`
- `ecs:DescribeTaskDefinition`
- `ecs:DescribeTasks`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListRoles`
- `iam:PassRole`
- `iam:SimulateCustomPolicy`
- `iam:SimulatePrincipalPolicy`
- `kms:DescribeKey`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:InvokeFunction`
- `lambda:TagResource`
- `logs:DescribeLogGroups`
- `logs:PutRetentionPolicy`
- `secretsmanager:DescribeSecret`
- `ssm:DescribeParameters`
- `sts:GetCallerIdentity`

## Langkah Dokumen

- `aws:executeScript`- Memverifikasi bahwa pengguna atau peran yang memulai otomatisasi memiliki izin IAM yang diperlukan. Jika Anda tidak memiliki izin yang cukup untuk menggunakan runbook ini, izin yang diperlukan yang hilang disertakan dalam output otomatisasi.
- `aws:branch`- Cabang berdasarkan apakah Anda memiliki izin untuk semua tindakan yang diperlukan untuk runbook.
- `aws:executeScript`- Membuat fungsi Lambda di VPC Anda jika analisis menentukan konektivitas jaringan perlu diuji.
- `aws:branch`- Cabang berdasarkan hasil langkah sebelumnya.
- `aws:executeScript`- Menganalisis kemungkinan penyebab kegagalan untuk memulai tugas Anda.
- `aws:executeScript`- Menghapus sumber daya yang dibuat oleh otomatisasi ini.
- `aws:executeScript`- Memformat output otomatisasi untuk mengembalikan hasil analisis ke konsol. Anda dapat meninjau analisis setelah langkah ini sebelum otomatisasi selesai.
- `aws:branch`- Cabang berdasarkan apakah fungsi Lambda dan sumber daya terkait dibuat dan perlu dihapus.
- `aws:sleep`- Tidur selama 30 menit sehingga elastis network interface untuk fungsi Lambda dapat dihapus.
- `aws:executeScript`- Menghapus antarmuka jaringan fungsi Lambda.
- `aws:executeScript`- Memformat output dari langkah penghapusan antarmuka jaringan fungsi Lambda.

## AWS-UpdateAmazonECSAgent

### Deskripsi

AWS-UpdateAmazonECSAgentRunbook memperbarui agen Amazon Elastic Container Service (Amazon ECS) di instans Amazon Elastic Compute Cloud (Amazon EC2) yang Anda tentukan. Runbook ini hanya mendukung instans Amazon Linux dan Amazon Linux 2.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi



## Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ClusterARN

Jenis: StringList

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari klaster Amazon ECS yang terdaftar dengan instans penampung Anda.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeImage
- ec2:DescribeInstance
- ec2:DescribeInstanceAttribute

- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

## Langkah Dokumen

`aws:executeScript`- Memperbarui agen Amazon ECS di cluster Amazon ECS yang Anda tentukan dalam parameter. `ClusterARN`

## Keluaran

`UpdateAmazonAgen ECS`. `UpdatedContainers` - ID instance tempat pembaruan agen Amazon ECS berhasil.

`UpdateAmazonAgen ECS`. `FailedContainers` - ID instance di mana pembaruan agen Amazon ECS gagal.

`UpdateAmazonAgen ECS`. `InProgressContainers` - ID instance tempat pembaruan agen Amazon ECS sedang berlangsung.

## Amazon EFS

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon Elastic File System. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWSSupport-CheckAndMountEFS](#)

## AWSSupport - CheckAndMountEFS

### Deskripsi

`AWSSupport-CheckAndMountEFS` Runbook memverifikasi prasyarat untuk memasang sistem file Amazon Elastic File System (Amazon EFS) dan memasang sistem file di instans Amazon Elastic Compute Cloud (Amazon EC2) yang Anda tentukan. Runbook ini mendukung pemasangan sistem file Amazon EFS Anda dengan nama DNS, atau menggunakan alamat IP target mount.

## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Tindakan

Jenis: String

Nilai yang valid: Periksa | CheckAndMount

Deskripsi: (Wajib) Menentukan apakah runbook memverifikasi prasyarat, atau memverifikasi prasyarat dan memasang sistem file.

- EfsId

Jenis: String

Deskripsi: (Wajib) ID sistem file yang ingin Anda pasang.

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instans Amazon EC2 tempat Anda ingin memasang sistem file.

- **MountOptions**

Jenis: String

Deskripsi: (Opsional) Opsi yang didukung oleh helper mount Amazon EFS yang ingin Anda gunakan saat memasang sistem file. Jika Anda menentukan `tls` opsi, verifikasi stunnel telah ditingkatkan pada instance target.

- **MountPoint**

Jenis: String

Deskripsi: (Opsional) Direktori tempat Anda ingin memasang sistem file. Jika Anda menentukan `Check` nilai untuk `Action` parameter, parameter ini tidak boleh ditentukan.

- **MountTargetIP**

Jenis: String

Deskripsi: (Opsional) Alamat IP target mount. Pemasangan dengan alamat IP berfungsi di lingkungan di mana DNS dinonaktifkan, seperti virtual private cloud (VPC) dengan nama host DNS dinonaktifkan. Selain itu, Anda dapat menggunakan opsi ini jika lingkungan Anda menggunakan penyedia DNS selain Amazon Route 53 (Rute 53).

- **Wilayah**

Jenis: String

Deskripsi: (Wajib) Wilayah AWS Tempat instans Amazon EC2 dan sistem file berada.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeInstanceProperties`
- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:ListDocuments`
- `ssm:StartAutomationExecution`
- `iam:ListRoles`
- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `elasticfilesystem:DescribeFileSystemPolicy`
- `elasticfilesystem:DescribeMountTargets`
- `elasticfilesystem:DescribeMountTargetSecurityGroups`
- `resource-groups:*`

## Langkah Dokumen

- `aws:executeScript`- Mengumpulkan detail tentang instans Amazon EC2 yang Anda tentukan dalam `InstanceId` parameter.
- `aws:executeScript`- Mengumpulkan rincian tentang sistem file yang Anda tentukan dalam `EfsId` parameter.
- `aws:executeScript`- Memverifikasi grup keamanan yang terkait dengan sistem file memungkinkan lalu lintas pada port 2049 dari instans Amazon EC2 yang Anda tentukan dalam parameter. `InstanceId`
- `aws:assertAwsResourceProperty`- Memverifikasi instans Amazon EC2 yang Anda tentukan dalam `InstanceId` parameter dikelola oleh Systems Manager dan statusnya. `Online`
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan untuk `Action` parameter.
- `aws:runCommand`- Memverifikasi prasyarat untuk memasang sistem file yang Anda tentukan dalam parameter. `EfsId`
- `aws:runCommand`- Memverifikasi prasyarat untuk memasang sistem file yang Anda tentukan dalam `EfsId` parameter, dan memasang sistem file pada instans Amazon EC2 yang Anda tentukan dalam parameter. `InstanceId`

# Amazon EKS

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Elastic Kubernetes Service. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWSSupport-CollectEKSIInstanceLogs](#)
- [AWS-CreateEKSClusterWithFargateProfile](#)
- [AWS-CreateEKSClusterWithNodegroup](#)
- [AWS-DeleteEKSCluster](#)
- [AWS-MigrateToNewEKSSelfManagedNodeGroup](#)
- [AWSPremiumSupport-TroubleshootEKSCluster](#)
- [AWSSupport-TroubleshootEKSSWorkerNode](#)
- [AWS-UpdateEKSCluster](#)
- [AWS-UpdateEKSMangedNodeGroup](#)
- [AWS-UpdateEKSSelfManagedLinuxNodeGroups](#)

## AWSSupport-CollectEKSIInstanceLogs

### Deskripsi

AWSSupport-CollectEKSIInstanceLogsRunbook mengumpulkan sistem operasi dan file log terkait Amazon Elastic Kubernetes Service (Amazon EKS) dari instans Amazon Elastic Compute Cloud (Amazon EC2) untuk membantu Anda memecahkan masalah umum. Sementara otomatisasi mengumpulkan file log terkait, perubahan dilakukan pada struktur sistem file termasuk pembuatan direktori sementara, menyalin file log ke direktori sementara, dan mengompresi file log ke dalam arsip. Aktivitas ini dapat mengakibatkan peningkatan CPUUtilization pada instans EC2. Untuk informasi selengkapnya CPUUtilization, lihat [Metrik instans](#) di Panduan CloudWatch Pengguna Amazon.

Jika Anda menentukan nilai untuk LogDestination parameter, otomatisasi akan mengevaluasi status kebijakan bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service

(Amazon S3) yang Anda tentukan. Untuk membantu keamanan log yang dikumpulkan dari instans EC2 Anda, jika status kebijakan `isPublic` disetel ke `true`, atau jika daftar kontrol akses (ACL) memberikan `READ|WRITE` izin ke grup Amazon S3 `All Users` yang telah ditentukan sebelumnya, log tidak akan diunggah. Untuk informasi selengkapnya tentang grup Amazon S3 yang telah ditentukan sebelumnya, lihat grup [Amazon S3 yang telah ditentukan sebelumnya di Panduan Pengguna](#) Layanan Penyimpanan Sederhana Amazon.

#### Note

Otomatisasi ini memerlukan setidaknya 10 persen ruang disk yang tersedia di root volume Amazon Elastic Block Store (Amazon EBS) Elastic Block Store (Amazon EBS) yang terpasang pada instans EC2 Anda. Jika tidak ada cukup ruang disk yang tersedia pada volume root, otomatisasi berhenti.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `EKS InstanceId`

Jenis: String

Deskripsi: (Wajib) ID instans Amazon EKS EC2 tempat Anda ingin mengumpulkan log.

- LogDestination

Jenis: String

Deskripsi: (Opsional) Bucket S3 di akun Anda untuk mengunggah log yang diarsipkan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`

Sebaiknya instans EC2 yang menerima perintah memiliki peran IAM dengan kebijakan terkelola `ManagedInstanceCore Amazon AmazonSSM` yang dilampirkan. Untuk mengunggah arsip log ke bucket S3 yang Anda tentukan dalam `LogDestination` parameter, Anda harus menambahkan `s3:PutObject` izin.

Langkah Dokumen

- `aws:assertAwsResourceProperty`- Mengonfirmasi sistem operasi dari nilai yang ditentukan dalam `EKSInstanceId` parameter adalah Linux.
- `aws:runCommand`- Mengumpulkan sistem operasi dan file log terkait Amazon EKS, mengompresnya menjadi arsip di `/var/log` direktori.
- `aws:branch`- Mengonfirmasi apakah nilai ditentukan untuk `LogDestination` parameter.
- `aws:runCommand`- Mengunggah arsip log ke bucket S3 yang Anda tentukan dalam parameter. `LogDestination`

## AWS-CreateEKSClusterWithFargateProfile

Deskripsi



AWS-CreateEKSClusterWithFargateProfileRunbook membuat cluster Amazon Elastic Kubernetes Service (Amazon EKS) menggunakan file. AWS Fargate

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ClusterName

Jenis: String

Deskripsi: (Wajib) Nama unik untuk cluster.

- ClusterRoleArn

Jenis: String

Deskripsi: (Wajib) ARN dari peran IAM yang memberikan izin bagi control plane Kubernetes untuk melakukan panggilan ke operasi API atas nama Anda. AWS

- FargateProfileName

Jenis: String

Deskripsi: (Wajib) Nama profil Fargate.

- FargateProfileRoleArn

Jenis: String

Deskripsi: (Wajib) ARN dari peran IAM eksekusi Amazon EKS Pod.

- FargateProfileSelectors

Jenis: String

Deskripsi: (Wajib) Penyeleksi untuk mencocokkan pod dengan profil Fargate.

- SubnetIds

Jenis: StringList

Deskripsi: (Wajib) ID subnet yang ingin Anda gunakan untuk kluster Amazon EKS Anda. Amazon EKS membuat antarmuka jaringan elastis di subnet ini untuk komunikasi antara node Anda dan bidang kontrol Kubernetes. Anda harus menentukan setidaknya dua ID subnet.

- EKS EndpointPrivateAccess

Jenis: Boolean

Bawaan: BETUL

Deskripsi: (Opsional) Tetapkan nilai ini `True` untuk mengizinkan akses pribadi untuk titik akhir server Kubernetes API kluster Anda. Jika Anda mengaktifkan akses pribadi, permintaan Kubernetes API dari dalam VPC kluster Anda menggunakan titik akhir VPC pribadi. Jika Anda menonaktifkan akses pribadi dan Anda memiliki node atau AWS Fargate pod di kluster, pastikan itu `publicAccessCidrs` menyertakan blok CIDR yang diperlukan untuk komunikasi dengan node atau pod Fargate.

- EKS EndpointPublicAccess

Jenis: Boolean

Default: Salah

Deskripsi: (Opsional) Tetapkan nilai ini `False` untuk menonaktifkan akses publik ke titik akhir server Kubernetes API kluster Anda. Jika Anda menonaktifkan akses publik, server API Kubernetes kluster Anda hanya dapat menerima permintaan dari dalam VPC tempat ia diluncurkan.

- `PublicAccessCIDR`

Jenis: `StringList`

Deskripsi: (Opsional) CIDR memblokir akses ke titik akhir server API Kubernetes publik kluster Anda. Komunikasi ke titik akhir dari alamat di luar blok CIDR yang Anda tentukan ditolak. Jika Anda telah menonaktifkan akses endpoint pribadi dan Anda memiliki node atau pod Fargate di kluster, pastikan Anda menentukan blok CIDR yang diperlukan.

- `SecurityGroupIds`

Jenis: `StringList`

Deskripsi: (Opsional) Tentukan satu atau beberapa grup keamanan untuk dikaitkan dengan antarmuka jaringan elastis yang dibuat di akun Anda oleh Amazon EKS.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `eks:CreateCluster`
- `eks:CreateFargateProfile`
- `eks:DescribeCluster`
- `eks:DescribeFargateProfile`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

Langkah Dokumen

- `createEksCluster` (aws:) `executeAwsApi` - Membuat cluster Amazon EKS.
- `verifyEksClusterIsActive` (aws: `waitForAwsResourceProperty`) - Memverifikasi status cluster. ACTIVE
- `CreateFargateProfile` (aws: `executeAwsApi`) - Membuat Fargate untuk cluster.
- `VerifyFargateProfileIsActive` (aws: `waitForAwsResourceProperty`) - Memverifikasi status profil Fargate adalah. ACTIVE

## Keluaran

### `CreateEKSCluster.CreateClusterResponse`

Deskripsi: Respons diterima dari panggilan `CreateCluster` API.

### `CreateFargateProfile.CreateFargateProfileResponse`

Deskripsi: Respons diterima dari panggilan `CreateFargateProfile` API.

## **AWS-CreateEKSClusterWithNodegroup**

### Deskripsi

`AWS-CreateEKSClusterWithNodegroupRunbook` membuat cluster Amazon Elastic Kubernetes Service (Amazon EKS) menggunakan grup node untuk kapasitas.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ClusterName

Jenis: String

Deskripsi: (Wajib) Nama unik untuk cluster.

- ClusterRoleArn

Jenis: String

Deskripsi: (Wajib) ARN dari peran IAM yang memberikan izin bagi control plane Kubernetes untuk melakukan panggilan ke operasi API atas nama Anda. AWS

- NodegroupName

Jenis: String

Deskripsi: (Wajib) Nama unik untuk grup simpul.

- NodegroupRoleArn

Jenis: String

Deskripsi: (Wajib) ARN dari peran IAM untuk dikaitkan dengan grup node Anda. Daemon kubelet node pekerja Amazon EKS melakukan panggilan ke AWS API atas nama Anda. Simpul menerima izin untuk panggilan API ini melalui profil instans IAM dan kebijakan terkait. Sebelum Anda dapat memulai node dan mendaftarkannya ke sebuah klaster, Anda harus membuat IAM role untuk node tersebut agar digunakan saat node diluncurkan.

- SubnetIds

Jenis: StringList

Deskripsi: (Wajib) ID subnet yang ingin Anda gunakan untuk klaster Amazon EKS Anda. Amazon EKS membuat antarmuka jaringan elastis di subnet ini untuk komunikasi antara node Anda dan bidang kontrol Kubernetes. Anda harus menentukan setidaknya dua ID subnet.

- `EKS EndpointPrivateAccess`

Jenis: Boolean

Bawaan: `BETUL`

Deskripsi: (Opsional) Tetapkan nilai ini `True` untuk mengizinkan akses pribadi untuk titik akhir server Kubernetes API klaster Anda. Jika Anda mengaktifkan akses pribadi, permintaan Kubernetes API dari dalam VPC klaster Anda menggunakan titik akhir VPC pribadi. Jika Anda menonaktifkan akses pribadi dan Anda memiliki node atau AWS Fargate pod di klaster, pastikan itu `publicAccessCidrs` menyertakan blok CIDR yang diperlukan untuk komunikasi dengan node atau pod Fargate.

- `EKS EndpointPublicAccess`

Jenis: Boolean

Default: Salah

Deskripsi: (Opsional) Tetapkan nilai ini `False` untuk menonaktifkan akses publik ke titik akhir server Kubernetes API klaster Anda. Jika Anda menonaktifkan akses publik, server API Kubernetes klaster Anda hanya dapat menerima permintaan dari dalam VPC tempat ia diluncurkan.

- `PublicAccessCIDR`

Jenis: `StringList`

Deskripsi: (Opsional) CIDR memblokir akses ke titik akhir server API Kubernetes publik klaster Anda. Komunikasi ke titik akhir dari alamat di luar blok CIDR yang Anda tentukan ditolak. Jika Anda telah menonaktifkan akses endpoint pribadi dan Anda memiliki node atau pod Fargate di klaster, pastikan Anda menentukan blok CIDR yang diperlukan.

- `SecurityGroupIds`

Jenis: `StringList`

Deskripsi: (Opsional) Tentukan satu atau beberapa grup keamanan untuk dikaitkan dengan antarmuka jaringan elastis yang dibuat di akun Anda oleh Amazon EKS.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam>ListAttachedRolePolicies`
- `iam:PassRole`

#### Langkah Dokumen

- `createEksCluster (aws:) executeAwsApi` - Membuat cluster Amazon EKS.
- `verifyEks ClusterIsActive (aws: waitForAwsResourceProperty)` - Memverifikasi status cluster. ACTIVE
- `CreateNodegroup (aws:executeAwsApi)` - Membuat grup node untuk cluster.
- `VerifyNodegroupIsActive (aws: waitForAwsResourceProperty)` - Memverifikasi status grup node adalah ACTIVE.

#### Keluaran

- `CreateEKSCluster.CreateClusterResponse`: Tanggapan diterima dari panggilan `CreateCluster` API.
- `CreateNodegroup.CreateNodegroupResponse`: Tanggapan diterima dari panggilan `CreateNodegroup` API.

## AWS-DeleteEKSCluster

### Deskripsi

Runbook ini menghapus sumber daya yang terkait dengan kluster Amazon EKS, termasuk grup node dan profil Fargate. Secara opsional, Anda dapat memilih untuk menghapus semua node yang dikelola sendiri, AWS CloudFormation tumpukan yang digunakan untuk membuat node, dan tumpukan VPC CloudFormation untuk cluster Anda. Untuk informasi selengkapnya tentang menghapus kluster, lihat [Menghapus kluster](#) di Panduan Pengguna Amazon EKS.

### Note

Jika Anda memiliki layanan aktif di kluster yang terkait dengan penyeimbang beban, Anda harus menghapus layanan tersebut sebelum menghapus kluster. Jika tidak, sistem tidak dapat menghapus penyeimbang beban. Gunakan prosedur berikut untuk menemukan dan menghapus layanan sebelum Anda menjalankan `AWS-DeleteEKSCluster` runbook.

Untuk mencari dan menghapus layanan di kluster Anda

1. Instal utilitas baris perintah Kubernetes, `kubectl` Untuk informasi selengkapnya, lihat [Menginstal kubectl di Panduan Pengguna Amazon EKS](#).
2. Jalankan perintah berikut untuk mencantumkan semua layanan yang berjalan di cluster Anda.

```
kubectl get svc --all-namespaces
```

3. Jalankan perintah berikut untuk menghapus layanan apa pun yang memiliki nilai `EXTERNAL-IP` terkait. Layanan ini digawangi oleh penyeimbang beban, dan Anda harus menghapusnya di Kubernetes untuk memungkinkan penyeimbang beban dan sumber daya terkait dilepaskan dengan benar.

```
kubectl delete svc  
service-name
```

Anda sekarang dapat menjalankan `AWS-DeleteEKSCluster` runbook.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi



## Pemilik

Amazon

Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- EKS ClusterName

Jenis: String

Deskripsi: (Wajib) Nama Cluster Amazon EKS yang akan dihapus.

- VPC CloudFormationStack

Jenis: String

Deskripsi: (Opsional) nama AWS CloudFormation tumpukan untuk VPC untuk kluster EKS yang dihapus. Ini menghapus AWS CloudFormation tumpukan untuk VPC dan sumber daya apa pun yang dibuat oleh tumpukan.

- VPC CloudFormationStackRole

Jenis: String

Deskripsi: (Opsional) ARN dari peran IAM yang AWS CloudFormation mengasumsikan untuk menghapus tumpukan VPC. CloudFormation AWS CloudFormation menggunakan kredensi peran untuk melakukan panggilan atas nama Anda.

- SelfManagedNodeStacks

Jenis: String

Deskripsi: (Opsional) Daftar nama AWS CloudFormation tumpukan yang dipisahkan koma untuk node yang dikelola sendiri, Ini akan menghapus AWS CloudFormation tumpukan untuk node yang dikelola sendiri.

- SelfManagedNodeStacksRole

Jenis: String

Deskripsi: (Opsional) ARN dari peran IAM yang AWS CloudFormation mengasumsikan untuk menghapus Tumpukan Node yang dikelola sendiri. AWS CloudFormation menggunakan kredensi peran untuk melakukan panggilan atas nama Anda.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- sts:AssumeRole
- eks:ListNodegroups
- eks>DeleteNodegroup
- eks:ListFargateProfiles
- eks>DeleteFargateProfile
- eks>DeleteCluster
- cfn:DescribeStacks
- cfn>DeleteStack

Langkah Dokumen

- aws:executeScript- DeleteNodeGroups: Temukan dan hapus semua grup node di cluster EKS.
- aws:executeScript- DeleteFargateProfiles: Temukan dan hapus semua profil Fargate di cluster EKS.
- aws:executeScript- DeleteSelfManagedNodes: Hapus semua node yang dikelola sendiri dan CloudFormation tumpukan yang digunakan untuk membuat node.
- aws:executeScript- DeleteEksCluster: Hapus kluster EKS.
- aws:executeScript- DeleteVPCCloudFormationStack: Hapus tumpukan VPC. CloudFormation

# AWS-MigrateToNewEKSSelfManagedNodeGroup

## Deskripsi

AWS-MigrateToNewEKSSelfManagedNodeGroupRunbook membantu Anda membuat grup node Linux Amazon Elastic Kubernetes Service (Amazon EKS) baru untuk memigrasikan aplikasi yang sudah ada. Untuk informasi selengkapnya, lihat [Memigrasi ke grup node baru](#) di Panduan Pengguna Amazon EKS.

## [Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

## Amazon

## Platform

## Linux

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- OldStackName

Jenis: String

Deskripsi: (Wajib) Nama atau ID tumpukan AWS CloudFormation tumpukan Anda yang ada.

- NewStackName

Jenis: String

Deskripsi: (Opsional) Nama AWS CloudFormation tumpukan baru yang dibuat untuk grup node baru Anda. Jika Anda tidak menentukan nilai untuk parameter ini, nama tumpukan dibuat menggunakan format: `NewNodeGroup-ClusterName-AutomationExecutionID`.

- `ClusterControlPlaneSecurityGroup`

Jenis: String

Deskripsi: (Opsional) ID grup keamanan yang ingin digunakan node untuk berkomunikasi dengan bidang kontrol Amazon EKS. Jika Anda tidak menentukan nilai untuk parameter ini, grup keamanan yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- `NodeInstanceType`

Jenis: String

Deskripsi: (Opsional) Jenis instance yang ingin Anda gunakan untuk grup node baru. Jika Anda tidak menentukan nilai untuk parameter ini, jenis instance yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- `NodeGroupName`

Jenis: String

Deskripsi: (Opsional) Nama grup node baru Anda. Jika Anda tidak menentukan nilai untuk parameter ini, nama grup node yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- `NodeAutoScalingGroupDesiredCapacity`

Jenis: String

Deskripsi: (Opsional) Jumlah node yang diinginkan untuk diskalakan saat tumpukan baru Anda dibuat. Angka ini harus lebih besar dari atau sama dengan `NodeAutoScalingGroupMinSize` nilai dan kurang dari atau sama dengan `NodeAutoScalingGroupMaxSize`. Jika Anda tidak menentukan nilai untuk parameter ini, kapasitas yang diinginkan grup node yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- `NodeAutoScalingGroupMaxSize`

Jenis: String

Deskripsi: (Opsional) Jumlah maksimum node yang dapat diskalakan oleh grup node Anda. Jika Anda tidak menentukan nilai untuk parameter ini, ukuran maksimum grup node yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- `NodeAutoScalingGroupMinSize`

Jenis: String

Deskripsi: (Opsional) Jumlah minimum node yang dapat diskalakan oleh grup node Anda. Jika Anda tidak menentukan nilai untuk parameter ini, ukuran minimum grup node yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- `NodeImageId`

Jenis: String

Deskripsi: (Opsional) ID dari Amazon Machine Image (AMI) yang Anda inginkan grup node untuk digunakan.

- `NodeImageIdSSMParam`

Jenis: String

Deskripsi: (Opsional) Parameter Systems Manager publik untuk AMI yang Anda inginkan untuk digunakan oleh grup node.

- `NodeVolumeSize`

Jenis: String

Deskripsi: (Opsional) Ukuran volume root untuk node Anda di GiB. Jika Anda tidak menentukan nilai untuk parameter ini, ukuran volume node yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- `NodeVolumeType`

Jenis: String

Deskripsi: (Opsional) Jenis volume Amazon EBS yang ingin Anda gunakan untuk volume root node Anda. Jika Anda tidak menentukan nilai untuk parameter ini, jenis volume yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- `KeyName`

Jenis: String

Deskripsi: (Opsional) Key pair yang ingin Anda tetapkan ke node Anda. Jika Anda tidak menentukan nilai untuk parameter ini, key pair yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- Subnet

Jenis: StringList

Deskripsi: (Opsional) Daftar ID subnet yang dipisahkan koma yang ingin Anda gunakan untuk grup node baru Anda. Jika Anda tidak menentukan nilai untuk parameter ini, subnet yang ditentukan dalam AWS CloudFormation tumpukan yang ada akan digunakan.

- NonaktifkanIMDSv1

Jenis: Boolean

Deskripsi: (Opsional) Tentukan `true` untuk menonaktifkan Layanan Metadata Instance Versi 1 (IMDSv1). Secara default, node mendukung IMDSv1 dan IMDSv2.

- BootstrapArguments

Jenis: String

Deskripsi: (Opsional) Argumen tambahan yang ingin Anda teruskan ke skrip bootstrap node.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetParameters`
- `autoscaling:CreateAutoScalingGroup`
- `autoscaling:CreateOrUpdateTags`
- `autoscaling>DeleteTags`
- `autoscaling:DescribeAutoScalingGroups`

- `autoscaling:DescribeScalingActivities`
- `autoscaling:DescribeScheduledActions`
- `autoscaling:SetDesiredCapacity`
- `autoscaling:TerminateInstanceInAutoScalingGroup`
- `autoscaling:UpdateAutoScalingGroup`
- `cloudformation:CreateStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateStack`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateLaunchTemplateVersion`
- `ec2:CreateLaunchTemplate`
- `ec2:CreateSecurityGroup`
- `ec2:CreateTags`
- `ec2>DeleteLaunchTemplate`
- `ec2>DeleteSecurityGroup`
- `ec2:DescribeAvailabilityZones`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeInstances`
- `ec2:DescribeKeyPairs`
- `ec2:DescribeLaunchTemplateVersions`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2:RevokeSecurityGroupEgress`

- `ec2:RevokeSecurityGroupIngress`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:PassRole`

### Langkah Dokumen

- `DetermineParameterValuesForNewNodeGroup` (`AWS:executeScript`) - Mengumpulkan nilai parameter yang akan digunakan untuk grup node baru.
- `CreateStack` (`AWS:CreateStack`) - Membuat AWS CloudFormation tumpukan untuk grup node baru.
- `GetNewStackNodeInstanceRole` (`aws:executeAwsApi`) - Mendapat peran instance node.
- `GetNewStackSecurityGroup` (`aws:executeAwsApi`) - Langkah mendapatkan grup keamanan node.
- `AddIngressRulesToNewNodeSecurityGroup` (`aws:executeAwsApi`) - Menambahkan aturan ingress ke grup keamanan yang baru dibuat sehingga dapat menerima lalu lintas dari yang ditetapkan ke grup node Anda sebelumnya.
- `AddIngressRulesToOldNodeSecurityGroup` (`aws:executeAwsApi`) - Menambahkan aturan ingress ke grup keamanan sebelumnya sehingga dapat menerima lalu lintas dari yang ditetapkan ke grup node yang baru Anda buat.
- `VerifyStackComplete` (`aws:assertAwsResourceProperty`) - Memverifikasi status tumpukan baru.  
`CREATE_COMPLETE`

### Keluaran

`DetermineParameterValuesForNewNodeGroup`. `NewStackParameters` - Parameter yang digunakan untuk membuat tumpukan baru.



`GetNewStackNodeInstanceRole`. `NewNodeInstanceRole` - Peran instance node untuk grup node baru.

`GetNewStackSecurityGroup`. `NewNodeSecurityGroup` - ID grup keamanan untuk grup node baru.

`DetermineParameterValuesForNewNodeGroup`. `NewStackName` - Nama AWS CloudFormation tumpukan untuk grup node baru.

`CreateStack`. `StackId` - ID AWS CloudFormation tumpukan untuk grup node baru.

## AWSPremiumSupport-TroubleshootEKSCluster

### Deskripsi

`AWSPremiumSupport-TroubleshootEKSClusterRunbook` mendiagnosis masalah umum dengan kluster Amazon Elastic Kubernetes Service (Amazon EKS), infrastruktur dasar, dan menyediakan langkah-langkah remediasi yang direkomendasikan.

#### Important

Akses ke `AWSPremiumSupport-*` runbook memerlukan Langganan Enterprise atau Business Support. Untuk informasi selengkapnya, lihat [Bandingkan Paket AWS Dukungan](#).

Jika Anda menentukan nilai untuk `S3BucketName` parameter, otomatisasi akan mengevaluasi status kebijakan bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) yang Anda tentukan. Untuk membantu keamanan log yang dikumpulkan dari instans EC2 Anda, jika status kebijakan `isPublic` disetel ke `true`, atau jika daftar kontrol akses (ACL) memberikan `READ|WRITE` izin ke grup Amazon S3 `All Users` yang telah ditentukan sebelumnya, log tidak akan diunggah. Untuk informasi selengkapnya tentang grup Amazon S3 yang telah ditentukan sebelumnya, lihat grup [Amazon S3 yang telah ditentukan sebelumnya di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon](#).

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

## Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ClusterName

Jenis: String

Deskripsi: (Wajib) Nama kluster Amazon EKS yang ingin Anda pecahkan masalah.

- S3 BucketName

Jenis: String

Deskripsi: (Opsional) Nama bucket Amazon S3 pribadi tempat laporan yang dihasilkan oleh runbook harus diunggah.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeInstances
- ec2:DescribeInstanceTypes
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups

- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeVpcs`
- `ec2:DescribeNetworkAcls`
- `iam:GetInstanceProfile`
- `iam:ListInstanceProfiles`
- `iam:ListAttachedRolePolicies`
- `eks:DescribeCluster`
- `eks:ListNodegroups`
- `eks:DescribeNodegroup`
- `autoscaling:DescribeAutoScalingGroups`

Selain itu, kebijakan AWS Identity and Access Management (IAM) yang dilampirkan ke pengguna atau peran yang memulai otomatisasi harus mengizinkan `ssm:GetParameter` operasi ke AWS Systems Manager parameter publik berikut untuk mendapatkan Amazon EKS Amazon Machine Image (AMI) terbaru yang direkomendasikan untuk node pekerja.

- `arn:aws:ssm::parameter/aws/service/eks/optimized-ami/*/amazon-linux-2/recommended/image_id`
- `arn:aws:ssm::parameter/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-EKS_Optimized-*/image_id`
- `arn:aws:ssm::parameter/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-EKS_Optimized-*/image_id`
- `arn:aws:ssm::parameter/aws/service/ami-windows-latest/Windows_Server-1909-English-Core-EKS_Optimized-*/image_id`
- `arn:aws:ssm::parameter/aws/service/eks/optimized-ami/*/amazon-linux-2-gpu/recommended/image_id`

Untuk mengunggah laporan yang dihasilkan oleh runbook ke bucket Amazon S3, izin berikut diperlukan untuk bucket Amazon S3 tertentu yang Anda tentukan.

- `s3:GetBucketPolicyStatus`
- `s3:GetBucketAcl`

- `s3:PutObject`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan detail untuk cluster Amazon EKS yang ditentukan.
- `aws:executeScript`- Mengumpulkan detail instans Amazon Elastic Compute Cloud (Amazon EC2), grup Auto AMI Scaling, s, dan jenis instans grafis GPU Amazon EC2.
- `aws:executeScript`- Mengumpulkan rincian virtual private cloud (VPC), subnet, gateway terjemahan alamat jaringan (NAT), rute subnet, grup keamanan dan daftar kontrol akses jaringan (ACL) dari cluster Amazon EKS.
- `aws:executeScript`- Mengumpulkan rincian profil instans IAM terlampir dan kebijakan peran.
- `aws:executeScript`- Mengumpulkan detail bucket Amazon S3 yang Anda tentukan dalam `S3BucketName` parameter.
- `aws:executeScript`- Mengklasifikasikan subnet VPC Amazon sebagai publik atau pribadi.
- `aws:executeScript`- Memeriksa subnet Amazon VPC untuk tag yang diperlukan sebagai bagian dari kluster Amazon EKS.
- `aws:executeScript`- Memeriksa subnet Amazon VPC untuk tag yang diperlukan untuk subnet Elastic Load Balancing.
- `aws:executeScript`- Memeriksa apakah node pekerja instans Amazon EC2 menggunakan Amazon EKS terbaru yang dioptimalkan s AMI
- `aws:executeScript`- Memeriksa apakah grup keamanan Amazon VPC dilampirkan ke node pekerja untuk tag yang diperlukan.
- `aws:executeScript`- Memeriksa aturan grup keamanan Amazon EKS dan node pekerja Amazon VPC untuk aturan masuk yang direkomendasikan ke cluster Amazon EKS.
- `aws:executeScript`- Memeriksa aturan grup keamanan Amazon EKS dan node pekerja Amazon VPC untuk aturan jalan keluar yang direkomendasikan dari kluster Amazon EKS.
- `aws:executeScript`- Memeriksa konfigurasi ACL jaringan dari subnet Amazon VPC.
- `aws:executeScript`- Memeriksa apakah instance Amazon EC2 node pekerja memiliki kebijakan terkelola yang diperlukan.
- `aws:executeScript`- Memeriksa apakah grup Auto Scaling memiliki tag yang diperlukan untuk penskalaan otomatis cluster.
- `aws:executeScript`- Memeriksa apakah node pekerja instans Amazon EC2 terhubung ke internet.

- `aws:executeScript`- Menghasilkan laporan berdasarkan output dari langkah sebelumnya. Jika nilai ditentukan untuk `S3BucketName` parameter, laporan yang dihasilkan akan diunggah ke bucket Amazon S3.

## AWSSupport-TroubleshootEKSEKWorkerNode

### Deskripsi

`AWSSupport-TroubleshootEKSEKWorkerNodeRunbook` menganalisis node pekerja Amazon Elastic Compute Cloud (Amazon EC2) dan cluster Amazon Elastic Kubernetes Service (Amazon EKS) untuk membantu Anda mengidentifikasi dan memecahkan masalah umum yang mencegah node pekerja bergabung dengan klaster. Panduan keluaran runbook untuk membantu Anda menyelesaikan masalah apa pun yang diidentifikasi.

#### Important

Agar berhasil menjalankan otomatisasi ini, status node pekerja Amazon EC2 Anda harus `running`, dan status klaster Amazon EKS harus `ACTIVE`

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ClusterName

Jenis: String

Deskripsi: (Wajib) Nama cluster Amazon EKS.

- WorkerID

Jenis: String

Deskripsi: (Wajib) ID node pekerja Amazon EC2 yang gagal bergabung dengan cluster.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ec2:DescribeDhcpOptions
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcAttribute
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs

- `eks:DescribeCluster`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam>ListAttachedRolePolicies`
- `ssm:DescribeInstanceInformation`
- `ssm>ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`

### Langkah Dokumen

- `aws:assertAwsResourceProperty`- Mengonfirmasi bahwa kluster Amazon EKS yang Anda tentukan dalam `ClusterName` parameter ada dan dalam ACTIVE keadaan.
- `aws:assertAwsResourceProperty`- Mengonfirmasi bahwa node pekerja Amazon EC2 yang Anda tentukan dalam `WorkerID` parameter ada dan dalam keadaan. `running`
- `aws:executeScript`- Menjalankan skrip Python yang membantu mengidentifikasi kemungkinan penyebab node pekerja gagal bergabung dengan cluster.

## AWS-UpdateEKSCluster

### Deskripsi

AWS-UpdateEKSClusterRunbook membantu Anda memperbarui cluster Amazon Elastic Kubernetes Service (Amazon EKS) ke versi Kubernetes yang ingin Anda gunakan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ClusterName

Jenis: String

Deskripsi: (Wajib) Nama cluster Amazon EKS Anda.

- Versi

Jenis: String

Deskripsi: (Wajib) Versi Kubernetes yang ingin Anda perbarui klaster Anda.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- eks:DescribeUpdate
- eks:UpdateClusterVersion

## Langkah Dokumen

- aws:executeAwsApi- Memperbarui versi Kubernetes yang digunakan oleh cluster Amazon EKS Anda.
- aws:waitForAwsResourceProperty- Menunggu status pembaruan. Successful

## AWS-UpdateEKSMangedNodeGroup

### Deskripsi



AWS-UpdateEKSMangedNodeGroupRunbook membantu Anda memperbarui grup node terkelola Amazon Elastic Kubernetes Service (Amazon EKS). Anda dapat memilih `Version` atau `Configuration` memperbarui.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `ClusterName`

Jenis: String

Deskripsi: (Wajib) Nama cluster yang grup simpulnya ingin Anda perbarui.

- `NodeGroupName`

Jenis: String

Deskripsi: (Wajib) Nama grup node yang akan diperbarui.

- `UpdateType`

Jenis: String

Nilai yang valid: Perbarui Versi Grup Node | Perbarui Konfigurasi Grup Node

## Default: Perbarui Versi Grup Node

Deskripsi: (Wajib) Jenis pembaruan yang ingin Anda lakukan pada grup node.

Parameter berikut hanya berlaku untuk jenis `Version` pembaruan:

- `AMIReleaseVersion`

Jenis: `String`

Deskripsi: (Opsional) Versi Amazon EKS dioptimalkan AMI yang ingin Anda gunakan. Secara default, versi terbaru digunakan.

- `ForceUpgrade`

Jenis: `Boolean`

Deskripsi: (Opsional) Jika benar, pembaruan tidak akan gagal dalam menanggapi pelanggaran anggaran gangguan pod.

- `KubernetesVersion`

Jenis: `String`

Description: (Opsional) Versi Kubernetes untuk memperbarui grup node ke.

- `LaunchTemplateId`

Jenis: `String`

Deskripsi: (Opsional) ID dari template peluncuran.

- `LaunchTemplateName`

Jenis: `String`

Deskripsi: (Opsional) Nama template peluncuran.

- `LaunchTemplateVersion`

Jenis: `String`

Deskripsi: (Opsional) Versi template peluncuran Amazon Elastic Compute Cloud (Amazon EC2). Parameter ini hanya valid jika grup node dibuat dari template peluncuran.

Parameter berikut hanya berlaku untuk jenis `Configuration` pembaruan:

- `AddOrUpdateNodeGroupLabels`

Jenis: `StringMap`

Deskripsi: (Opsional) Label Kubernetes yang ingin Anda tambahkan atau perbarui.

- `AddOrUpdateKubernetesTaintsEffect`

Jenis: `StringList`

Deskripsi: (Opsional) Kubernetes menodai yang ingin Anda tambahkan atau perbarui.

- `MaxUnavailableNodeGroups`

Jenis: `Integer`

Default: 0

Deskripsi: (Opsional) Jumlah maksimum node yang tidak tersedia sekaligus selama pembaruan versi.

- `MaxUnavailablePercentageNodeGroup`

Jenis: `Integer`

Default: 0

Deskripsi: (Opsional) Persentase node yang tidak tersedia selama pembaruan versi.

- `NodeGroupDesiredSize`

Jenis: `Integer`

Default: 0

Deskripsi: (Opsional) Jumlah node yang harus dipertahankan oleh grup node terkelola.

- `NodeGroupMaxSize`

Jenis: `Integer`

Default: 0

Deskripsi: (Opsional) Jumlah maksimum node yang dapat diskalakan oleh grup node terkelola.

- `NodeGroupMinSize`

Jenis: Integer

Default: 0

Deskripsi: (Opsional) Jumlah minimum node yang dapat diskalakan oleh grup node terkelola.

- `RemoveKubernetesTaintsEffect`

Jenis: StringList

Deskripsi: (Opsional) Noda Kubernetes yang ingin Anda hapus.

- `RemoveNodeGroupLabels`

Jenis: StringList

Deskripsi: (Opsional) Daftar label yang dipisahkan koma yang ingin Anda hapus.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

Langkah Dokumen

- `aws:executeScript`- Memperbarui grup node cluster Amazon EKS sesuai dengan nilai yang Anda tentukan untuk parameter input runbook.
- `aws:waitForAwsResourceProperty`- Menunggu status pembaruan cluster. `Successful`

## **AWS-UpdateEKSSelfManagedLinuxNodeGroups**

Deskripsi

`AWS-UpdateEKSSelfManagedLinuxNodeGroupsRunbook` memperbarui grup node terkelola yang dikelola sendiri di klaster Amazon Elastic Kubernetes Service (Amazon EKS) menggunakan tumpukan. `AWS CloudFormation`

Jika klaster Anda menggunakan penskalaan otomatis, sebaiknya skalakan penerapan menjadi dua replika sebelum menggunakan runbook ini.

Untuk menskalakan penerapan ke dua replika

1. Instal utilitas baris perintah Kubernetes, `kubectl` Untuk informasi selengkapnya, silakan lihat [Menginstal kubectl](#) dalam Panduan Pengguna Amazon EKS.
2. Jalankan perintah berikut.

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. Jalankan `AWS-UpdateEKSSelfManagedLinuxNodeGroups` runbook.
4. Skala penerapan kembali ke jumlah replika yang diinginkan dengan menjalankan perintah berikut.

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- **ClusterName**

Jenis: String

Deskripsi: (Wajib) Nama cluster Amazon EKS.

- **NodeGroupName**

Jenis: String

Deskripsi: (Wajib) Nama grup node terkelola.

- **ClusterControlPlaneSecurityGroup**

Jenis: String

Deskripsi: (Wajib) ID grup keamanan pesawat kontrol.

- **NonaktifkanIMDSv1**

Jenis: Boolean

Deskripsi: (Opsional) Menentukan apakah Anda ingin mengizinkan Layanan Metadata Instans Versi 1 (IMDSv1) dan IMDSv2.

- **KeyName**

Jenis: String

Deskripsi: (Opsional) Nama kunci untuk instance.

- **NodeAutoScalingGroupDesiredCapacity**

Jenis: String

Deskripsi: (Opsional) Jumlah node yang harus dipertahankan oleh kelompok node.

- **NodeAutoScalingGroupMaxSize**

Jenis: String

Deskripsi: (Opsional) Jumlah maksimum node yang dapat diskalakan oleh kelompok node.

- **NodeAutoScalingGroupMinSize**

Jenis: String

Deskripsi: (Opsional) Jumlah minimum node yang dapat diskalakan oleh kelompok node.

- `NodeInstanceType`

Jenis: String

Default: `t3.large`

Deskripsi: (Opsional) Jenis instance yang ingin Anda gunakan untuk grup node.

- `NodeImageId`

Jenis: String

Deskripsi: (Opsional) ID dari Amazon Machine Image (AMI) yang Anda inginkan grup node untuk digunakan.

- `NodeImageIdSSMParam`

Jenis: String

Default: `/aws/service/eks/optimized-ami/1.21/amazon-linux-2/merekomendasikan/image_id`

Deskripsi: (Opsional) Parameter Systems Manager publik untuk AMI yang Anda inginkan untuk digunakan oleh grup node.

- `StackName`

Jenis: String

Deskripsi: (Wajib) Nama AWS CloudFormation tumpukan yang digunakan untuk memperbarui grup node.

- `Subnet`

Jenis: String

Deskripsi: (Wajib) Daftar ID yang dipisahkan koma untuk subnet yang ingin digunakan klaster.

- `VpcId`

Jenis: String

Default: Default

Deskripsi: (Diperlukan) Virtual Private Cloud (VPC) tempat klaster Anda digunakan.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- eks:CreateCluster
- eks:CreateNodegroup
- eks>DeleteNodegroup
- eks>DeleteCluster
- eks:DescribeCluster
- eks:DescribeNodegroup
- eks:ListClusters
- eks:ListNodegroups
- eks:UpdateClusterConfig
- eks:UpdateNodegroupConfig

## Langkah Dokumen

- aws:executeScript- Memperbarui grup node cluster Amazon EKS sesuai dengan nilai yang Anda tentukan untuk parameter input runbook.
- aws:waitForAwsResourceProperty- Menunggu status pembaruan AWS CloudFormation tumpukan dikembalikan.

## Elastic Beanstalk

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS Elastic Beanstalk Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWSsupport-CollectElasticBeanstalkLogs](#)
- [AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming](#)
- [AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications](#)



- [AWSSupport-TroubleshootElasticBeanstalk](#)

## AWSSupport-CollectElasticBeanstalkLogs

### Deskripsi

AWSSupport-CollectElasticBeanstalkLogsRunbook mengumpulkan file log AWS Elastic Beanstalk terkait dari instans Amazon Elastic Compute Cloud (Amazon EC2 Windows Server) yang diluncurkan oleh Elastic Beanstalk untuk membantu Anda memecahkan masalah umum. Sementara otomatisasi mengumpulkan file log terkait, perubahan dilakukan pada struktur sistem file termasuk pembuatan direktori sementara, menyalin file log ke direktori sementara, dan mengompresi file log ke dalam arsip. Aktivitas ini dapat meningkatkan CPU Utilization instans Amazon EC2. Untuk informasi selengkapnya CPU Utilization, lihat [Metrik instans](#) di Panduan CloudWatch Pengguna Amazon.

Jika Anda menentukan nilai untuk S3BucketName parameter, otomatisasi akan mengevaluasi status kebijakan bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) yang Anda tentukan. Untuk membantu keamanan log yang dikumpulkan dari instans Amazon EC2 Anda, jika status kebijakan isPublic disetel ke true, atau jika daftar kontrol akses (ACL) memberikan READ | WRITE izin ke grup Amazon S3 All Users yang telah ditentukan sebelumnya, log tidak akan diunggah. Untuk informasi selengkapnya tentang grup Amazon S3 yang telah ditentukan sebelumnya, lihat grup [Amazon S3 yang telah ditentukan sebelumnya di Panduan Pengguna](#) Layanan Penyimpanan Sederhana Amazon.

Jika Anda tidak menentukan nilai untuk S3BucketName parameter, otomatisasi akan mengunggah bundel log ke bucket Elastic Beanstalk Amazon S3 default di tempat Anda menjalankan otomatisasi. Wilayah AWS Direktori diberi nama sesuai dengan struktur berikut, `elasticbeanstalk-region-accountID`. Nilai *region* dan *accountID* akan berbeda berdasarkan Region Akun AWS dan Anda menjalankan otomatisasi di. Bundel log akan disimpan ke `resources/environments/logs/bundle/environmentID/instanceID` direktori. Nilai *EnvironmentID* dan *InstanceID* akan berbeda berdasarkan lingkungan Elastic Beanstalk dan instans Amazon EC2 tempat Anda mengumpulkan log.

Secara default, profil instans AWS Identity and Access Management (IAM) yang dilampirkan ke instans Amazon EC2 dari lingkungan Elastic Beanstalk memiliki izin yang diperlukan untuk mengunggah bundel ke bucket Elastic Beanstalk Amazon S3 default untuk lingkungan Anda. Jika Anda menentukan nilai untuk S3BucketName parameter, profil instance yang dilampirkan ke instans Amazon EC2 harus mengizinkan `s3:GetBucketAc1,,`

s3:GetBucketPolicys3:GetBucketPolicyStatus, dan s3:PutObject tindakan untuk bucket dan path Amazon S3 yang ditentukan.

#### Note

Otomatisasi ini memerlukan setidaknya 500 MB ruang disk yang tersedia pada volume root Amazon Elastic Block Store (Amazon EBS) yang terpasang pada instans Amazon EC2 Anda. Jika tidak ada cukup ruang disk yang tersedia pada volume root, otomatisasi berhenti.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- EnvironmentId

Jenis: String

Deskripsi: (Wajib) ID lingkungan Elastic Beanstalk Anda yang ingin Anda kumpulkan bundel log.

- InstanceId

Jenis: String

(Wajib) ID instans Amazon EC2 di lingkungan Elastic Beanstalk tempat Anda ingin mengumpulkan bundel log.

- S3 BucketName

Jenis: String

(Opsional) Bucket Amazon S3 yang ingin Anda unggah log yang diarsipkan.

- S3 BucketPath

Jenis: String

(Opsional) Jalur bucket Amazon S3 yang ingin Anda unggah bundel log. Parameter ini diabaikan jika Anda tidak menentukan nilai untuk S3BucketName parameter.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`

Langkah Dokumen

- `aws:assertAwsResourceProperty`- Mengonfirmasi instans Amazon EC2 yang Anda tentukan dalam InstanceId parameter dikelola oleh. AWS Systems Manager
- `aws:assertAwsResourceProperty`- Mengonfirmasi instans Amazon EC2 yang Anda tentukan dalam InstanceId parameter adalah sebuah Windows Server instance.
- `aws:runCommand`- Memeriksa apakah instance merupakan bagian dari lingkungan Elastic Beanstalk, jika ada ruang disk yang cukup untuk menggabungkan log, dan apakah bucket Amazon S3 tempat log akan diunggah bersifat publik.

- `aws :runCommand`- Mengumpulkan file log dan mengunggah arsip ke bucket Amazon S3 yang ditentukan dalam `S3BucketName` parameter atau ke bucket default untuk lingkungan Elastic Beanstalk Anda jika nilai tidak ditentukan.

## **AWSConfigRemediation- EnableElasticBeanstalkEnvironmentLogStreaming**

### Deskripsi

`AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreamingRunbook` memungkinkan logging pada lingkungan AWS Elastic Beanstalk (Elastic Beanstalk) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `EnvironmentId`

Jenis: String

Deskripsi: (Wajib) ID lingkungan Elastic Beanstalk yang ingin Anda aktifkan untuk masuk.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

## Langkah Dokumen

- `aws:executeAwsApi`- Memungkinkan logging pada lingkungan Elastic Beanstalk yang Anda tentukan dalam parameter. `EnvironmentId`
- `aws:waitForAwsResourceProperty`- Menunggu status lingkungan berubah menjadi `Ready`.
- `aws:executeScript`- Verifikasi logging telah diaktifkan di lingkungan Elastic Beanstalk.

## **AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications**

### Deskripsi

AWSConfigRemediation-EnableBeanstalkEnvironmentNotificationsRunbook memungkinkan pemberitahuan untuk lingkungan AWS Elastic Beanstalk (Elastic Beanstalk) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `EnvironmentId`

Jenis: String

Deskripsi: (Wajib) ID lingkungan Elastic Beanstalk yang ingin Anda aktifkan notifikasi.

- `TopicArn`

Jenis: String

Deskripsi: (Wajib) ARN dari Amazon Simple Notification Service (Amazon SNS) topik yang ingin Anda kirim notifikasi.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan pemberitahuan untuk lingkungan Elastic Beanstalk yang Anda tentukan dalam parameter. `EnvironmentId`

- `aws:waitForAwsResourceProperty`- Menunggu status lingkungan berubah menjadi `Ready`.
- `aws:executeScript`- Memverifikasi notifikasi telah diaktifkan untuk lingkungan Elastic Beanstalk.

## AWSSupport-TroubleshootElasticBeanstalk

### Deskripsi

`AWSSupport-TroubleshootElasticBeanstalkRunbook` membantu Anda memecahkan masalah alasan potensial mengapa AWS Elastic Beanstalk lingkungan Anda berada dalam keadaan `atauDegraded`. `Severe Otomatisasi` ini memeriksa AWS sumber daya berikut yang terkait dengan lingkungan Elastic Beanstalk Anda:

- Detail konfigurasi untuk load balancer, AWS CloudFormation stack, grup Auto Scaling Amazon EC2, instans Amazon Elastic Compute Cloud (Amazon EC2), dan virtual private cloud (VPC).
- Masalah konfigurasi jaringan dengan aturan grup keamanan terkait, tabel rute, dan daftar kontrol akses jaringan (ACL) yang terkait dengan subnet Anda.
- Memverifikasi konektivitas ke titik akhir Elastic Beanstalk dan akses internet publik.
- Memverifikasi status penyeimbang beban.
- Memverifikasi status instans Amazon EC2.
- Mengambil bundel log dari lingkungan Elastic Beanstalk Anda, dan secara opsional mengunggah file ke. AWS Support

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ApplicationName

Jenis: String

Deskripsi: (Wajib) Nama aplikasi Elastic Beanstalk Anda.

- EnvironmentName

Jenis: String

Deskripsi: (Wajib) Nama lingkungan Elastic Beanstalk Anda.

- AWSS3UploaderLink

Jenis: String

Deskripsi: (Opsional) URL yang diberikan kepada Anda oleh AWS Support untuk mengunggah bundel log dari lingkungan Elastic Beanstalk Anda ke. Opsi ini hanya tersedia untuk pelanggan yang telah membeli AWS Support paket, dan telah membuka kasus Support.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- autoscaling:Describe\*
- cloudformation:Describe\*
- cloudformation:Estimate\*
- cloudformation:Get\*
- cloudformation:List\*
- cloudformation:Validate\*
- cloudwatch:Describe\*



- `cloudwatch:Get*`
- `cloudwatch:List*`
- `ec2:Describe*`
- `elasticbeanstalk:Check*`
- `elasticbeanstalk:Describe*`
- `elasticbeanstalk:List*`
- `elasticbeanstalk:RetrieveEnvironmentInfo*`
- `elasticbeanstalk:RequestEnvironmentInfo*`
- `elasticloadbalancing:Describe*`
- `rds:Describe*`
- `s3:Get*`
- `s3:List*`
- `sns:Get*`
- `sns:List*`

## Langkah Dokumen

- `aws:executeScript`- Memverifikasi prinsipal AWS Identity and Access Management (IAM) yang memulai otomatisasi memiliki izin yang diperlukan untuk melakukan semua tindakan yang ditentukan dalam runbook.
- `aws:branch`- Cabang alur kerja berdasarkan hasil dari langkah sebelumnya.
- `aws:executeScript`- Mengumpulkan informasi tentang lingkungan Elastic Beanstalk termasuk load balancer AWS CloudFormation , stack, grup Auto Scaling, instans Amazon EC2, dan konfigurasi VPC.
- `aws:executeScript`- Memeriksa masalah konektivitas jaringan dengan tabel rute dan ACL yang terkait dengan subnet di VPC Anda.
- `aws:executeScript`- Memeriksa masalah konektivitas jaringan dengan aturan grup keamanan yang terkait dengan instans Amazon EC2 Anda.
- `aws:executeScript`- Memverifikasi pemeriksaan status untuk instans Amazon EC2.
- `aws:executeScript`- Menghasilkan tautan untuk bundel log lingkungan Elastic Beanstalk Anda.
- `aws:executeScript`- Unggah log bundel ke AWS Support.

- `aws:executeScript`- Mengeluarkan laporan item tindakan untuk membantu Anda memecahkan masalah yang mungkin memengaruhi status lingkungan Elastic Beanstalk Anda.

## Penyeimbang Beban Elastis

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Elastic Load Balancing. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSConfigRemediation-DropInvalidHeadersForALB](#)
- [AWS-EnableCLBAccessLogs](#)
- [AWS-EnableCLBConnectionDraining](#)
- [AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing](#)
- [AWSConfigRemediation-EnableELBDeletionProtection](#)
- [AWSConfigRemediation-EnableLoggingForALBAndCLB](#)
- [AWSSupport-TroubleshootCLBConnectivity](#)
- [AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing](#)
- [AWS-UpdateALB DesyncMitigationMode](#)
- [AWS-UpdateCLB DesyncMitigationMode](#)

## **AWSConfigRemediation-DropInvalidHeadersForALB**

### Deskripsi

`AWSConfigRemediation-DropInvalidHeadersForALB` Runbook memungkinkan penyeimbang beban aplikasi yang Anda tentukan untuk menghapus header HTTP dengan header yang tidak valid.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

## Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- LoadBalancerArn

Jenis: String

Deskripsi: (Wajib) Nama Sumber Daya Amazon (ARN) dari penyeimbang beban yang ingin Anda jatuhkan header tidak valid.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

### Langkah Dokumen

- aws:executeAwsApi- Mengaktifkan pengaturan drop header yang tidak valid untuk penyeimbang beban yang Anda tentukan dalam parameter. LoadBalancerArn
- aws:executeScript- Memverifikasi pengaturan drop header yang tidak valid telah diaktifkan pada penyeimbang beban yang Anda tentukan dalam parameter. LoadBalancerArn

# AWS-EnableCLBAccessLogs

## Deskripsi

AWS-EnableCLBAccessLogsRunbook memungkinkan log akses untuk Classic Load Balancer.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- EmitInterval

Jenis: Integer

Nilai yang valid: 5 | 60

Default: 60

Deskripsi: (Opsional) Interval untuk menerbitkan log akses dalam hitungan menit.

- LoadBalancerNames

Jenis: String

Deskripsi: (Wajib) Daftar Classic Load Balancer yang dipisahkan koma yang ingin Anda aktifkan log akses.

- S3 BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket Amazon Simple Storage Service (Amazon S3) tempat log akses disimpan.

- S3 BucketPrefix

Jenis: String

Deskripsi: (Opsional) Hirarki logis yang Anda buat untuk bucket Amazon S3, misalnya. my-bucket-prefix/prod Jika awalan tidak disediakan, log ditempatkan pada tingkat akar bucket.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan log akses untuk Classic Load Balancers yang Anda tentukan dalam parameter. `LoadBalancerNames`

Keluaran

AktifkanCibAccessLogs. `SuccessesLoadBalancers` - Daftar nama penyeimbang beban tempat log akses berhasil diaktifkan.

AktifkanCibAccessLogs. `FailedLoadBalancers` - MapList nama penyeimbang beban di mana mengaktifkan log akses gagal dan alasan kegagalan.

## **AWS-EnableCLBConnectionDraining**

Deskripsi

`AWS-EnableCLBConnectionDrainingRunbook` memungkinkan koneksi menguras pada Classic Load Balancer (CLB) ke nilai batas waktu yang ditentukan. Pengurasan koneksi memungkinkan CLB untuk menyelesaikan permintaan dalam penerbangan yang dibuat untuk instance yang tidak terdaftar atau tidak sehat dengan batas waktu yang ditentukan adalah waktu itu membuat koneksi tetap hidup sebelum melaporkan instance sebagai dideregistrasi. Untuk informasi selengkapnya tentang pengurasan koneksi pada CLB, lihat [Mengonfigurasi pengurasan koneksi untuk Classic Load Balancer Anda di Panduan Pengguna untuk Penyeimbang Beban Klasik](#).

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `LoadBalancerName`

Jenis: String

Deskripsi: (Wajib) Nama penyeimbang beban yang ingin Anda aktifkan koneksi yang terkuras.

- `ConnectionTimeout`

Jenis: Integer

Nilai yang valid: 1-3600

Default: 300

Deskripsi: (Wajib) Nilai batas waktu koneksi untuk penyeimbang beban. Nilai batas waktu dapat diatur antara 1 dan 3600 detik.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Langkah Dokumen

- `ModifyLoadBalancerConnectionDraining` (`aws:executeAwsApi`): Mengaktifkan pengurusan koneksi dan menetapkan nilai batas waktu yang ditentukan untuk penyeimbang beban yang Anda tentukan.
- `VerifyLoadBalancerConnectionDrainingEnabled` (`aws:assertAwsResource Property`): Memverifikasi bahwa pengeringan koneksi diaktifkan untuk penyeimbang beban.
- `VerifyLoadBalancerConnectionDrainingTimeout` (`aws:assertAwsResource Property`): Memverifikasi bahwa nilai batas waktu koneksi untuk penyeimbang beban cocok dengan nilai yang Anda tentukan.

## **AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing**

Deskripsi

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancingRunbook memungkinkan penyeimbangan beban lintas zona untuk Classic Load Balancer (CLB) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `LoadBalancerName`

Jenis: String

Deskripsi: (Wajib) Nama CLB yang ingin Anda aktifkan penyeimbangan beban lintas zona.

## Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan penyeimbangan beban lintas zona untuk CLB yang Anda tentukan dalam parameter. `LoadBalancerName`
- `aws:assertAwsResourceProperty`- Memverifikasi penyeimbangan beban lintas zona telah diaktifkan di CLB.



# AWSConfigRemediation-EnableELBDeletionProtection

## Deskripsi

AWSConfigRemediation-EnableELBDeletionProtectionRunbook memungkinkan perlindungan penghapusan untuk penyeimbang beban elastis (ELB) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- LoadBalancerArn

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari ELB yang ingin Anda aktifkan perlindungan penghapusan.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

### Langkah Dokumen

- `aws:executeScript`- Mengaktifkan perlindungan penghapusan pada ELB yang Anda tentukan dalam parameter. `LoadBalancerArn`

## **AWSConfigRemediation-EnableLoggingForALBAndCLB**

### Deskripsi

AWSConfigRemediation-EnableLoggingForALBAndCLBRunbook memungkinkan logging untuk AWS Application Load Balancer tertentu atau Classic Load Balancer (CLB).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `LoadBalancerId`

Jenis: String

Deskripsi: (Wajib) Nama Classic Load Balancer atau Application Load Balancer ARN.

- S3 BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket Amazon S3.

- S3 BucketPrefix

Jenis: String

Deskripsi: (Opsional) Hirarki logis yang Anda buat untuk bucket Amazon Simple Storage Service (Amazon S3), misalnya. `my-bucket-prefix/prod` Jika awalan tidak disediakan, log ditempatkan pada tingkat akar bucket.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Langkah Dokumen


- `aws:executeScript`- Mengaktifkan dan memverifikasi logging untuk Classic Load Balancer atau Application Load Balancer.

## **AWSSupport-TroubleshootCLBConnectivity**

Deskripsi

`AWSSupport-TroubleshootCLBConnectivityRunbook` membantu Anda memecahkan masalah konektivitas antara instans Classic Load Balancer (CLB) dan Amazon Elastic Compute

Cloud (Amazon EC2). Juga, masalah konektivitas antara klien dan CLB ditinjau. Runbook ini juga meninjau pemeriksaan kesehatan untuk CLB, memverifikasi bahwa praktik terbaik sedang diikuti, dan membuat dasbor pemecahan masalah untuk Anda. Secara opsional, Anda dapat mengunggah output otomatisasi ke bucket Amazon Simple Storage Service (Amazon S3). Namun, runbook ini tidak mendukung pengunggahan output ke bucket S3 yang dapat diakses publik. Sebaiknya buat bucket S3 sementara untuk otomatisasi ini.

 Important

Menggunakan runbook ini mungkin dikenakan biaya untuk dasbor yang dibuat. Untuk informasi selengkapnya, lihat [CloudWatchHarga Amazon](#)

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InvestigationType

Jenis: String

Nilai yang valid: Praktik Terbaik | Masalah Konektivitas | Dasbor Pemecahan Masalah

Deskripsi: (Wajib) Operasi yang Anda inginkan untuk menjalankan runbook.

- LoadBalancerName

Jenis: String

Deskripsi: (Wajib) Nama CLB.

- S3Location

Jenis: String

Deskripsi: (Opsional) Nama bucket S3 yang ingin Anda kirim hasil otomatisasi. Bucket yang dapat diakses publik tidak didukung. Jika bucket S3 Anda menggunakan enkripsi sisi server, pengguna atau peran yang menjalankan otomatisasi ini harus memiliki `kms:GenerateDataKey` izin untuk kunci tersebut. AWS KMS

- S3 LocationPrefix

Jenis: String

Deskripsi: (Opsional) Awalan kunci Amazon S3 (subfolder) yang ingin Anda unggah output otomatisasi. *Output format disimpan dalam format berikut: DOC-EXAMPLE-BUCKET/ S3 LocationPrefix/{{}} \_ {{automation: EXECUTION\_ID InvestigationType}} .txt.*

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeVpcs`

- `ec2:DescribeSubnets`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerPolicies`
- `elasticloadbalancing:DescribeInstanceHealth`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `iam:ListRoles`
- `cloudwatch:PutDashboard`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeInstanceProperties`
- `ssm:GetDocument`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:ListDocuments`
- `ssm:SendCommand`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetPublicAccessBlock`
- `s3:PutObject`

## Langkah Dokumen

- `aws:executeScript`- Memverifikasi bahwa CLB yang Anda tentukan dalam `LoadBalancerName` parameter ada.
- `aws:branch`- Cabang berdasarkan nilai yang ditentukan untuk `InvestigationType` parameter.
- `aws:executeScript`- Melakukan pemeriksaan konektivitas ke CLB.
- `aws:executeScript`- Memverifikasi bahwa konfigurasi CLB mematuhi praktik terbaik Elastic Load Balancing.

- `aws:executeScript`- Membuat CloudWatch dasbor Amazon untuk CLB Anda.
- `aws:executeScript`- Membuat file teks dengan hasil otomatisasi dan mengunggahnya ke bucket Amazon S3 yang Anda tentukan dalam `S3Location` parameter.

Keluaran

`RunBestPractices.Ringkasan`

`RunConnectivityChecks.Ringkasan`

`CreateTroubleshootingDashboard.Keluaran`

`UploadOutputToS3.Keluaran`

## **AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing**

Deskripsi

`AWSConfigRemediation-EnableNLBCrossZoneLoadBalancingRunbook` memungkinkan penyeimbangan beban lintas zona untuk menyeimbangkan beban jaringan (NLB) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `LoadBalancerArn`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari NLB yang ingin Anda aktifkan penyeimbangan beban lintas zona.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan penyeimbangan beban lintas zona untuk NLB yang Anda tentukan dalam parameter. `LoadBalancerArn`
- `aws:executeScript`- Memverifikasi penyeimbangan beban lintas zona telah diaktifkan di NLB.

## AWS-UpdateALB DesyncMitigationMode

Deskripsi

`AWS-UpdateALBDesyncMitigationModeRunbook` akan memperbarui mode mitigasi desync pada Application Load Balancer (ALB) ke mode mitigasi yang ditentukan. Mode mitigasi desync menentukan cara penyeimbang beban menangani permintaan yang mungkin menimbulkan risiko keamanan bagi aplikasi Anda.

[Jalankan Otomasi ini \(konsol\)](#)



## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LoadBalancerArn

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari ALB yang ingin Anda ubah mode mitigasi desync.

- DesyncMitigationMode

Jenis: String

Nilai yang valid: monitor | defensif | paling ketat

Deskripsi: (Wajib) Mode mitigasi yang Anda ingin ALB gunakan. Untuk informasi tentang mode mitigasi desync, lihat Mode mitigasi [desync di Panduan Pengguna untuk Penyeimbang Beban Aplikasi](#).

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

### Langkah Dokumen

- `VerifyLoadBalancerType` (`aws:assertAwsResourceProperty`) - Memverifikasi bahwa nilai yang ditentukan untuk parameter `LoadBalancerArn` input adalah untuk penyeimbang beban aplikasi sebelum melanjutkan ke langkah berikutnya.
- `ModifyLoadBalancerDesyncMode` (`aws:executeAwsApi`) - Memperbarui ALB untuk menggunakan yang ditentukan `DesyncMitigationMode`.
- `VerifyLoadBalancerDesyncMitigationMode` (`AWS:executeScript`) - Memverifikasi bahwa mode mitigasi desync telah diperbarui untuk ALB target.

### Keluaran

`VerifyLoadBalancerDesyncMitigationMode`. `ModificationResult` - Muatan pesan skrip yang memverifikasi modifikasi ALB Anda.

## AWS-UpdateCLB DesyncMitigationMode

### Deskripsi

`AWS-UpdateCLBDesyncMitigationModeRunbook` akan memperbarui mode mitigasi desync pada Classic Load Balancer (CLB) ke mode mitigasi yang ditentukan. Mode mitigasi desync menentukan cara penyeimbang beban menangani permintaan yang mungkin menimbulkan risiko keamanan bagi aplikasi Anda.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

## Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LoadBalancerName

Jenis: String

Deskripsi: (Wajib) Nama CLB yang ingin Anda ubah modus mitigasi desync.

- DesyncMitigationMode

Jenis: String

Nilai yang valid: monitor | defensif | paling ketat

Deskripsi: (Wajib) Mode mitigasi yang Anda ingin CLB gunakan. Untuk informasi tentang mode mitigasi desync, lihat Mode mitigasi [desync di Panduan Pengguna untuk Penyeimbang Beban Aplikasi](#).

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

## Langkah Dokumen

- `ModifyLoadBalancerDesyncMode` (`aws:executeAwsApi`) - Memperbarui CLB untuk menggunakan yang ditentukan `DesyncMitigationMode`.
- `VerifyLoadBalancerDesyncMitigationMode` (`AWS:executeScript`) - Memverifikasi bahwa mode mitigasi desync telah diperbarui untuk CLB target.

## Keluaran

`VerifyLoadBalancerDesyncMitigationMode`. `ModificationResult` - Muatan pesan skrip yang memverifikasi modifikasi ke CLB Anda.

## Amazon EMR

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon EMR. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWSSupport-AnalyzeEMRLogs](#)

## AWSSupport - AnalyzeEMRLogs

### Deskripsi

Runbook ini membantu mengidentifikasi kesalahan saat menjalankan pekerjaan di kluster EMR Amazon. Runbook menganalisis daftar log yang ditentukan pada sistem file dan mencari daftar kata kunci yang telah ditentukan. Entri log ini digunakan untuk membuat CloudWatch peristiwa Amazon Events sehingga Anda dapat mengambil tindakan apa pun yang diperlukan berdasarkan peristiwa. Secara opsional, runbook menerbitkan entri log ke grup CloudWatch log Amazon Logs yang Anda pilih. Runbook ini saat ini mencari kesalahan dan pola berikut dalam file log:

- `container_out_of_memory` - wadah YARN kehabisan memori, menjalankan pekerjaan mungkin gagal.
- `yarn_nodemanager_health`: CORE atau TASK node kehabisan ruang disk dan tidak akan dapat menjalankan tugas.
- `node_state_change`: CORE atau TASK node tidak dapat dijangkau oleh node MASTER.

- `step_failure`: Langkah EMR telah gagal.
- `no_core_nodes_running`: Tidak ada node CORE yang sedang berjalan, cluster tidak sehat.
- `hdfs_missing_blocks`: Ada blok HDFS yang hilang yang dapat menyebabkan hilangnya data.
- `hdfs_high_util`: Pemanfaatan HDFS tinggi, yang dapat mempengaruhi pekerjaan dan kesehatan cluster.
- `instance_controller_restart`: Proses Instance-Controller telah dimulai ulang. Proses ini sangat penting untuk kesehatan cluster.
- `instance_controller_restart_legacy`: Proses Instance-Controller telah dimulai ulang. Proses ini sangat penting untuk kesehatan cluster.
- `high_load`: Rata-rata Beban Tinggi terdeteksi, dapat memengaruhi pelaporan kesehatan node atau mengakibatkan batas waktu atau perlambatan.
- `yarn_node_blacklisted`: CORE atau TASK node telah masuk daftar hitam oleh YARN dari menjalankan tugas.
- `yarn_node_lost`: CORE atau TASK node telah ditandai sebagai LOST oleh YARN, kemungkinan masalah konektivitas.

Contoh yang terkait dengan `ClusterID` yang Anda tentukan harus dikelola oleh AWS Systems Manager. Anda dapat menjalankan otomatisasi ini sekali, menjadwalkan otomatisasi untuk berjalan pada interval waktu tertentu, atau menghapus jadwal yang dibuat sebelumnya oleh otomatisasi. Runbook ini mendukung versi rilis Amazon EMR 5.20 hingga 6.30.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ClusterID

Jenis: String

Deskripsi: (Wajib) ID cluster yang node log Anda ingin menganalisis.

- Operasi

Jenis: String

Nilai yang valid: Jalankan Sekali | Jadwal | Hapus Jadwal

Deskripsi: (Wajib) Operasi untuk melakukan pada cluster.

- IntervalTime

Jenis: String

Nilai yang valid: 5 menit | 10 menit | 15 menit

Deskripsi: (Opsional) Durasi waktu antara menjalankan otomatisasi. Parameter ini hanya berlaku jika Anda menentukan Schedule Operation parameter.

- LogToCloudWatchLogs

Jenis: String

Nilai yang valid: ya | tidak

Deskripsi: (Opsional) Jika Anda menentukan yes nilai parameter ini, otomatisasi membuat grup CloudWatch log Log dengan nama yang ditentukan dalam CloudWatchLogGroup parameter untuk menyimpan entri log yang cocok.

- CloudWatchLogGroup

Jenis: String

Deskripsi: (Opsional) Nama grup CloudWatch log Log tempat Anda ingin menyimpan entri log yang cocok. Parameter ini hanya berlaku jika Anda menentukan `yes LogToCloudWatchLogs` parameter.

- `CreateLogInsightsDashboard`

Jenis: String

Nilai yang valid: ya | tidak

Deskripsi: (Opsional) Jika Anda menentukannya, CloudWatch dasbor dibuat jika belum ada. Parameter ini hanya berlaku jika Anda menentukan `yes LogToCloudWatchLogs` parameter.

- `CreateMetricFilters`

Jenis: String

Nilai yang valid: ya | tidak

Deskripsi: (Opsional) Tentukan `yes` apakah Anda ingin membuat filter metrik untuk grup CloudWatch log Log. Parameter ini hanya berlaku jika Anda menentukan `yes LogToCloudWatchLogs` parameter.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`

- iam:CreateRole
- iam>DeleteRole
- iam:GetRolePolicy
- iam:PutRolePolicy
- iam>DeleteRolePolicy
- iam:passrole
- cloudformation:DescribeStacks
- cloudformation>DeleteStack
- cloudformation>CreateStack
- events>DeleteRule
- events:RemoveTargets
- events:PutTargets
- events:PutRule
- events:DescribeRule
- logs:DescribeLogGroups
- logs>CreateLogGroup
- logs:PutMetricFilter
- cloudwatch:PutDashboard
- elasticmapreduce>ListInstances
- elasticmapreduce:DescribeCluster

## Langkah Dokumen

- aws:executeAwsApi- Mengumpulkan informasi tentang cluster EMR Amazon yang ditentukan dalam ClusterID parameter.
- aws:branch- Cabang berdasarkan masukan.
  - Jika operasi yang disediakan adalah Run Once atauSchedule:
    - aws:assertAwsResourceProperty- Memverifikasi cluster tersedia.
    - aws:executeAwsApi- Mengumpulkan ID dari semua instance yang berjalan di cluster.
    - aws:assertAwsResourceProperty- Memverifikasi Agen SSM berjalan pada semua instance di cluster.



- `aws:branch`- Cabang berdasarkan apakah Anda menentukan untuk menjalankan otomatisasi sekali atau sesuai jadwal.
- Jika operasi yang disediakan adalah `Run Once`:
  - `aws:branch`- Cabang berdasarkan nilai yang ditentukan dalam `LogToCloudWatchLogs` parameter.
  - Jika `LogToCloudWatchLogs` nilainya adalah `yes`:
    - `aws:executeScript`- Memeriksa apakah grup CloudWatch log Log dengan nama yang ditentukan dalam parameter `CloudWatchLogGroup` sudah ada. Jika tidak, grup dibuat dengan nama yang ditentukan.
    - `aws:branch`- Cabang berdasarkan nilai yang ditentukan dalam `CreateMetricFilters` parameter.
    - Jika `CreateMetricFilters` nilainya adalah `yes`:
      - `aws:executeAwsApi`- 12 langkah dijalankan untuk setiap filter metrik
      - `aws:branch`- Cabang berdasarkan nilai yang ditentukan dalam `CreateLogInsightsDashboard` parameter.
      - Jika `CreateLogInsightsDashboard` nilainya adalah `yes`:
        - `aws:executeAwsApi`- Membuat CloudWatch dasbor dengan nama yang sama yang ditentukan dalam `CloudWatchLogGroup` parameter, jika belum ada.
      - Jika `CreateLogInsightsDashboard` nilainya adalah `no`:
        - `aws:runCommand`- Menjalankan skrip shell untuk menemukan pola log pada setiap instance di cluster.
    - Jika `CreateMetricFilters` nilainya adalah `no`:
      - `aws:branch`- Cabang berdasarkan nilai yang ditentukan dalam `CreateLogInsightsDashboard` parameter.
      - Jika `CreateLogInsightsDashboard` nilainya adalah `yes`:
        - `aws:executeAwsApi`- Membuat CloudWatch dasbor dengan nama yang sama yang ditentukan dalam `CloudWatchLogGroup` parameter, jika belum ada.
      - Jika `CreateLogInsightsDashboard` nilainya adalah `no`:
        - `aws:runCommand`- Menjalankan skrip shell untuk menemukan pola log pada setiap instance di cluster.

- Jika `LogToCloudWatchLogs` nilainya adalahno:
  - `aws:executeAwsApi`- Menjalankan skrip shell untuk menemukan pola log pada setiap instance di cluster.
- Jika operasi yang disediakan adalah`Schedule`:
  - `aws:createStack`- Membuat EventBridge acara Amazon yang menargetkan runbook ini.
- Jika operasi yang disediakan adalah`Remove Schedule`:
  - `aws:executeAwsApi`- Memverifikasi jadwal yang ada untuk cluster.
  - `aws:deleteStack`- Menghapus jadwal.

## Keluaran

`GetClusterInformation.ClusterName`

`GetClusterInformation.ClusterState`

`ListingClusterInstances.instanceId`

`CreatingScheduleCloudFormationStack.StackStatus`

`RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus`

`CheckIfLogGroupExists.keluaran`

`FindLogPatternOnEMRNode.CommandId`

## OpenSearch Layanan Amazon

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon OpenSearch Service. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSConfigRemediation-DeleteOpenSearchDomain](#)
- [AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain](#)
- [AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups](#)

- [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#)
- [AWSSupport-TroubleshootOpenSearchHighCPU](#)

## AWSConfigRemediation-DeleteOpenSearchDomain

### Deskripsi

AWSConfigRemediation-DeleteOpenSearchDomainRunbook menghapus domain OpenSearch Layanan Amazon yang diberikan menggunakan API. [DeleteDomain](#)

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- DomainName

Jenis: String

Nilai yang diizinkan:  $(\d{12})?[a-z]{1}[a-z0-9-]{2,28}$

Deskripsi: (Wajib) Nama domain OpenSearch Layanan Amazon yang ingin Anda hapus.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es>DeleteDomain`
- `es:DescribeDomain`

## Langkah Dokumen

- `aws:executeScript`- Menerima nama domain OpenSearch Layanan Amazon sebagai input, menghapusnya, dan memverifikasi penghapusan.

# **AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain**

## Deskripsi

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomainRunbook memungkinkan EnforceHTTPS pada domain OpenSearch Layanan Amazon tertentu menggunakan [UpdateDomainConfig](#) API.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- `DomainName`

Jenis: String

Nilai yang diizinkan: (\ d {12}/)? [a-z] {1} [a-z0-9-] {2,28}

Deskripsi: (Wajib) Nama domain OpenSearch Layanan Amazon yang ingin Anda gunakan untuk menerapkan HTTPS.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

Langkah Dokumen

- aws:executeScript- Mengaktifkan opsi EnforceHTTPS titik akhir pada domain OpenSearch Layanan Amazon yang Anda tentukan dalam DomainName parameter.

## **AWSConfigRemediation- UpdateOpenSearchDomainSecurityGroups**

Deskripsi

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroupsRunbook memperbarui konfigurasi grup keamanan pada domain OpenSearch Layanan Amazon tertentu menggunakan [UpdateDomainConfig](#) API.

**Note**

AWS Grup keamanan hanya dapat diterapkan ke domain OpenSearch Layanan Amazon yang dikonfigurasi untuk Akses Amazon Virtual Private Cloud (VPC), dan bukan ke domain OpenSearch Layanan Amazon yang dikonfigurasi untuk Akses Publik.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- DomainName

Jenis: String

Deskripsi: (Wajib) Nama domain OpenSearch Layanan Amazon yang ingin Anda gunakan untuk memperbarui grup keamanan.

- SecurityGroupList

Jenis: StringList

Deskripsi: (Wajib) ID grup keamanan yang ingin Anda tetapkan ke domain OpenSearch Layanan Amazon.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

## Langkah Dokumen

- `aws:executeScript`- Memperbarui konfigurasi grup keamanan pada domain OpenSearch Layanan Amazon yang Anda tentukan dalam `DomainName` parameter.

# AWSSupport-TroubleshootOpenSearchRedYellowCluster

## Deskripsi

AWSSupport-TroubleshootOpenSearchRedYellowClusterRunbook otomatisasi digunakan untuk mengidentifikasi penyebab status kesehatan kluster [merah](#) atau [kuning](#) dan memandu Anda mengubah cluster kembali menjadi hijau.

## Bagaimana cara kerjanya?

Runbook AWSSupport-TroubleshootOpenSearchRedYellowCluster membantu Anda memecahkan masalah penyebab cluster merah atau kuning dan memberikan langkah selanjutnya untuk mengatasi masalah ini dengan menganalisis konfigurasi cluster dan pemanfaatan sumber daya.

Runbook melakukan langkah-langkah berikut:

- Memanggil [DescribeDomain](#) API terhadap domain target untuk mendapatkan konfigurasi cluster.
- Memeriksa apakah domain OpenSearch Layanan berbasis internet (publik) atau berbasis [Amazon Virtual Private Cloud \(VPC\)](#).
- Membuat AWS Lambda fungsi [berbasis VPC publik atau Amazon](#) tergantung pada konfigurasi cluster. Catatan: Fungsi Lambda berisi kode pemecahan masalah yang menjalankan API

OpenSearch Layanan terhadap kluster untuk menentukan mengapa kluster dalam keadaan merah atau kuning.

- Menghapus fungsi Lambda.
- Menampilkan pemeriksaan yang dilakukan dan langkah-langkah yang disarankan berikutnya untuk menyelesaikan masalah kluster merah atau kuning.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudformation:CreateStack`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `cloudformation>DeleteStack`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:InvokeFunction`
- `lambda:GetFunction`
- `es:DescribeDomain`
- `es:DescribeDomainConfig`
- `ec2:DescribeSecurityGroups`



- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterface`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:AttachNetworkInterface`
- `cloudwatch:GetMetricData`
- `iam:PassRole`

`LambdaExecutionRoleParameter` memerlukan tindakan berikut agar berhasil menggunakan runbook:

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`

Ikhtisar `LambdaExecutionRole` kebijakan:

Berikut ini adalah contoh peran eksekusi fungsi Lambda (AWS Identity and Access Management (IAM)) yang memberikan izin fungsi untuk mengakses AWS layanan dan sumber daya yang diperlukan oleh runbook ini. Untuk informasi selengkapnya, silakan lihat [Peran eksekusi Lambda](#).

#### Note

The `ec2:DescribeNetworkInterfaces`, `ec2:CreateNetworkInterface`, dan hanya `ec2>DeleteNetworkInterface` diperlukan jika kluster OpenSearch Layanan Anda [berbasis Amazon VPC](#) untuk memungkinkan fungsi Lambda membuat dan mengelola antarmuka jaringan VPC Amazon. Untuk informasi selengkapnya, lihat [Menghubungkan jaringan keluar ke sumber daya dalam peran eksekusi Amazon VPC](#) dan [Lambda](#).

```

    {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Action": "es:ESHttpGet",
          "Resource": [
            "arn:<partition>:es:<region>:<account-id>:domain/<domain-
name>/",
            "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cluster/health",
            "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cat/indices",
            "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cat/allocation",
            "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cluster/allocation/explain"
          ]
        },
        {
          "Condition": {
            "ArnLikeIfExists": {
              "ec2:Vpc": "arn:<partition>:ec2:<region>:<account-id>:vpc/
<vpc_id>"
            }
          },
          "Action": [
            "ec2:DeleteNetworkInterface",
            "ec2:CreateNetworkInterface",
            "ec2:DescribeNetworkInterfaces",
            "ec2:UnassignPrivateIpAddresses",
            "ec2:AssignPrivateIpAddresses"
          ],
          "Resource": "*",
          "Effect": "Allow"
        }
      ]
    }
  
```

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport- TroubleshootOpenSearchRedYellowCluster](#) di AWS Systems Manager konsol.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input masukkan yang berikut:

- AutomationAssumeRole (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LambdaExecutionRole (Diperlukan):

ARN dari peran IAM yang akan digunakan Lambda untuk menandatangani permintaan ke kluster Layanan Amazon Anda. OpenSearch

- DomainName (Diperlukan):

Nama domain OpenSearch Layanan dengan status kesehatan kluster merah atau kuning.

- UtilizationThreshold (Opsional):

Persentase ambang batas pemanfaatan yang digunakan untuk membandingkan metrik CPUUtilization dan JVM. MemoryPressure Nilai default adalah 80.

**Input parameters**

**AutomationAssumeRole**  
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Select an existing IAM Role

AutomationAssumeRole  
arn:aws:iam::[redacted]:role/AutomationAssumeRole

**DomainName**  
(Required) The name of the Amazon OpenSearch Service domain is red or yellow status.

opensearch-red-yellow-sample

**LambdaExecutionRole**  
(Required) The ARN of the IAM role that the AWS Lambda will use to sign requests to your Amazon OpenSearch Service cluster.

Select an existing IAM Role

LambdaExecutionRole  
arn:aws:iam::[redacted]:role/LambdaExecutionRole

**UtilizationThreshold**  
(Optional) The utilization threshold in percentage used to compare the `CPUUtilization` and `JVMMemoryPressure` metrics. Default value is `80`.

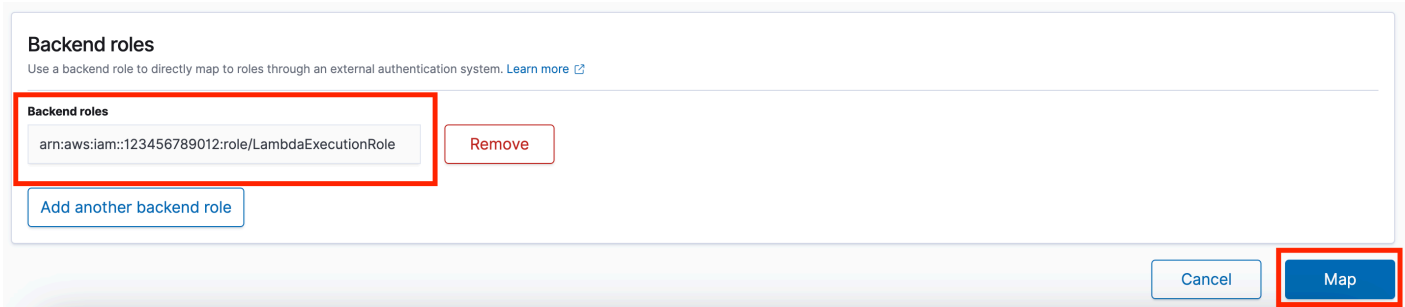
80

4. Jika Anda telah mengaktifkan [kontrol akses berbutir halus](#) pada kluster OpenSearch Service, pastikan bahwa LambdaExecutionRole peran arn dipetakan ke peran dengan setidaknya izin. `cluster_monitor`

**Permissions** Mapped users

**Cluster permissions (1)**  
Cluster permissions specify how users in this role can access the cluster. You can specify permissions using both action groups or single permissions. An action group is a list of single permissions. [Learn more](#)

> • cluster\_monitor



5. Pilih Jalankan.

6. Otomatisasi dimulai.

7. Runbook otomatisasi melakukan langkah-langkah berikut:

- `GetClusterConfiguration`:

Mengambil konfigurasi kluster OpenSearch Layanan.

- `BuatAWSLambdaFunctionStack`:

Membuat fungsi Lambda sementara di akun Anda menggunakan AWS CloudFormation Fungsi Lambda digunakan untuk menjalankan API OpenSearch Layanan.

- `WaitForAWSLambdaFunctionStack`:

Menunggu CloudFormation tumpukan selesai.

- `GetClusterMetricsFromCloudWatch`:

Mendapatkan metrik terkait kluster Amazon CloudWatch `ClusterStatus`, `CPUUtilization`, dan `JVM MemoryPressure` OpenSearch Service serta tanggal pembuatannya.

- `RunOpenSearchAPI`:

Menggunakan fungsi Lambda untuk memanggil API OpenSearch Layanan dan menganalisis data metrik kluster untuk mendiagnosis penyebab status kluster merah atau kuning.

- `HapusAWSLambdaFunctionStack`:

Menghapus fungsi Lambda yang dibuat oleh otomatisasi ini di akun Anda.

8. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci.

- `RootCause`:

Memberikan gambaran umum tentang penyebab yang diidentifikasi untuk kesehatan cluster berada dalam keadaan merah atau kuning.

- **IssueDescription:**

Memberikan detail mengapa cluster dalam keadaan merah atau kuning dan langkah-langkah yang mungkin untuk mengembalikan cluster ke status hijau.

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

### AWS dokumentasi layanan

- Lihat [Pemecahan Masalah Amazon OpenSearch Service](#) untuk informasi selengkapnya

## **AWSsupport-TroubleshootOpenSearchHighCPU**

### Deskripsi

AWSsupport-TroubleshootOpenSearchHighCPURunbook menyediakan solusi otomatis untuk mengumpulkan data diagnostik dari domain OpenSearch Layanan Amazon untuk memecahkan masalah CPU yang [tinggi](#).

### Bagaimana cara kerjanya?

AWSsupport-TroubleshootOpenSearchHighCPURunbook membantu memecahkan masalah pemanfaatan CPU yang tinggi di domain Layanan Amazon. OpenSearch

Runbook melakukan langkah-langkah berikut:

- Menjalankan [DescribeDomain](#) API terhadap domain OpenSearch Layanan Amazon yang disediakan untuk mendapatkan metadata klaster.
- Memeriksa apakah domain OpenSearch Layanan Amazon bersifat publik atau berbasis Amazon VPC dan dengan bantuan AWS CloudFormation, menciptakan fungsi berbasis [AWS Lambda VPC publik atau Amazon](#).

- Fungsi Lambda mengambil data diagnostik dari domain Layanan Amazon OpenSearch .
- Menggunakan mesin AWS Step Functions negara untuk mengatur beberapa eksekusi fungsi Lambda untuk mengumpulkan data yang lebih komprehensif.
- Menyimpan data yang dikumpulkan dalam grup CloudWatch log Amazon selama 24 jam secara default.
- Menghapus sumber daya yang dibuat, kecuali grup CloudWatch log.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudformation:CreateStack`
- `cloudformation:CreateStack`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `cloudformation>DeleteStack`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:InvokeFunction`
- `lambda:GetFunction`
- `lambda:TagResource`
- `es:DescribeDomain`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:AttachNetworkInterface`
- `ec2>DeleteNetworkInterface`

- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:TagResource`
- `states:CreateStateMachine`
- `states>DeleteStateMachine`
- `states:StartExecution`
- `states:TagResource`
- `states:DescribeStateMachine`
- `states:DescribeExecution`
- `iam:PassRole`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam>DeleteRolePolicy`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

`LambdaExecutionRoleParameter` memerlukan tindakan berikut agar berhasil menggunakan runbook:

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Peran eksekusi Lambda memberikan izin fungsi untuk mengakses AWS layanan dan sumber daya yang diperlukan oleh runbook ini. Untuk informasi selengkapnya, silakan lihat [Peran eksekusi Lambda](#).

**Note**

The `ec2:DescribeNetworkInterfaces`, `ec2:CreateNetworkInterface`, dan hanya `ec2:DeleteNetworkInterface` diperlukan jika kluster OpenSearch Layanan Anda [berbasis Amazon VPC](#) untuk memungkinkan fungsi Lambda membuat dan mengelola antarmuka jaringan VPC Amazon. Untuk informasi selengkapnya, lihat [Menghubungkan jaringan keluar ke sumber daya dalam peran eksekusi Amazon VPC](#) dan [Lambda](#).

**Instruksi**

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support- Troubleshoot OpenSearch High CPU](#) di AWS Systems Manager konsol.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input masukkan yang berikut ini:

- `AutomationAssumeRole` (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `DomainName` (Diperlukan):

Nama domain OpenSearch Layanan Amazon yang ingin Anda pecahkan masalah CPU yang tinggi.

- `LambdaExecutionRoleForOpenSearch` (Diperlukan):

ARN dari peran IAM untuk dilampirkan ke fungsi Lambda. Fungsi Lambda menggunakan kredensi dari peran ini untuk menandatangani permintaan ke domain Layanan Amazon. OpenSearch Jika kontrol akses berbutir halus diaktifkan di domain OpenSearch Layanan Amazon, Anda harus memetakan peran ini ke peran backend Dasbor OpenSearch Layanan dengan izin minimum “cluster\_monitor”.

- `DataRetentionDays` (Opsional):

Jumlah hari untuk menyimpan data diagnostik yang dikumpulkan dari domain OpenSearch Layanan Amazon. Secara default, data disimpan selama 24 jam (satu hari). Anda dapat memilih untuk menyimpan data maksimal hingga 30 hari.



- **NumberOfDataSamples (Opsional):**

Jumlah sampel data yang dikumpulkan dari domain OpenSearch Layanan Amazon. Secara default, 5 sampel data dikumpulkan. Anda dapat mengumpulkan hingga 10 sampel dan fungsi Lambda akan dipanggil untuk setiap koleksi sampel.

4. Jika Anda telah mengaktifkan [kontrol akses berbutir halus](#) pada kluster OpenSearch Service, pastikan bahwa `LambdaExecutionRole` peran arn dipetakan ke peran dengan setidaknya izin `cluster_monitor`

5. Pilih Jalankan.

6. Otomatisasi dimulai.

7. Runbook otomatisasi melakukan langkah-langkah berikut:

- **CheckConcurrency:**

Memastikan bahwa hanya ada satu eksekusi runbook ini yang menargetkan domain OpenSearch Layanan Amazon yang ditentukan. Jika runbook menemukan eksekusi lain yang menargetkan nama domain yang sama, ia mengembalikan kesalahan dan berakhir.

- `getDomainConfig`:

Mendapatkan detail konfigurasi untuk domain OpenSearch Layanan target.

- `ProvisionResources`:

Ketentuan sumber daya untuk pengumpulan data menggunakan AWS CloudFormation.

- `waitForStackPenciptaan`:

Menunggu AWS CloudFormation tumpukan selesai.

- `describeStackResources`:

Menjelaskan AWS CloudFormation tumpukan dan mendapatkan ARN dari mesin negara.

- `runStateMachine`:

Memanggil fungsi Lambda pengumpul data satu kali atau beberapa kali dengan menjalankan mesin status Step Functions.

- `describeErrorsFromStackEvents`:

Menjelaskan kesalahan dari AWS CloudFormation tumpukan untuk kesalahan.

- `unstageOpenSearchHighCPUAutomation`:

Menghapus `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation tumpukan.

- `describeErrorsFromStackDeletion`:

Menjelaskan kesalahan yang ditemui saat menghapus AWS CloudFormation tumpukan.

- Status akhir:

Mengembalikan output akhir dari `AWSSupport-TroubleshootOpenSearchHighCPU` runbook.

## 8. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci.

- Status akhir. `FinalOutput`:

Menyediakan grup CloudWatch log tempat data diagnostik disimpan.

```

▼ Outputs
finalStatus:FinalOutput
Hot thread data collection completed. Please check the custom CloudWatch log group /aws/lambda/AWSSupport-HighCPU-df52ba5d-8773-4038-a908-b67ecd9c9d11 for more information.

```

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

### AWS dokumentasi layanan

- Lihat [Pemecahan Masalah Amazon OpenSearch Service](#) untuk informasi selengkapnya

## EventBridge

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon. EventBridge Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-AddOpsItemDedupStringToEventBridgeRule](#)
- [AWS-DisableEventBridgeRule](#)

## AWS-AddOpsItemDedupStringToEventBridgeRule

### Deskripsi

AWS-AddOpsItemDedupStringToEventBridgeRuleRunbook menambahkan string deduplikasi untuk semua yang AWS Systems Manager OpsItems terkait dengan aturan Amazon. EventBridge Runbook tidak menambahkan string deduplikasi ke aturan jika salah satu telah diterapkan. Untuk mempelajari lebih lanjut string deduplikasi dan OpsItems, lihat [Mengurangi duplikat OpsItems di Panduan Pengguna](#).AWS Systems Manager

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `DedupString`

Jenis: String

Deskripsi: (Wajib) String deduplikasi yang ingin Anda tambahkan ke aturan.

- `RuleName`

Jenis: String

Deskripsi: (Wajib) Nama aturan yang ingin Anda tambahkan string deduplikasi.

## Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

## Langkah Dokumen

- `aws:executeScript`- Menambahkan string deduplikasi ke EventBridge aturan yang Anda tentukan dalam parameter. `RuleName`

## AWS-DisableEventBridgeRule

### Deskripsi

AWS-DisableEventBridgeRuleRunbook menonaktifkan EventBridge aturan Amazon yang Anda tentukan. Untuk mempelajari lebih lanjut tentang aturan EventBridge , lihat [aturan Amazon EventBridge di Panduan Pengguna Amazon](#). EventBridge

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux,macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `EventBusName`

Jenis: String

Default: default

Deskripsi: (Opsional) Bus acara yang terkait dengan aturan yang ingin Anda nonaktifkan.

- RuleName

Jenis: String

Deskripsi: (Wajib) Nama aturan yang ingin Anda nonaktifkan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

Langkah Dokumen

- `aws:executeAwsApi`- Menonaktifkan EventBridge aturan yang Anda tentukan dalam RuleName parameter.

## GuardDuty

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon GuardDuty Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSConfigRemediation-CreateGuardDutyDetector](#)

## AWSConfigRemediation-CreateGuardDutyDetector

Deskripsi

AWSConfigRemediation-CreateGuardDutyDetectorRunbook membuat detektor Amazon GuardDuty (GuardDuty) di Wilayah AWS tempat Anda menjalankan otomatisasi.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `guardduty:CreateDetector`
- `guardduty:GetDetector`

Langkah Dokumen

- `aws:executeAwsApi`- Membuat GuardDuty detektor.
- `aws:assertAwsResourceProperty`- Memverifikasi detektor adalah ENABLED. Status

# IAM

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS Identity and Access Management Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWS-AttachIAMToInstance](#)
- [AWS-DeleteIAMInlinePolicy](#)
- [AWSConfigRemediation-DeleteIAMRole](#)
- [AWSConfigRemediation-DeleteIAMUser](#)
- [AWSConfigRemediation-DeleteUnusedIAMGroup](#)
- [AWSConfigRemediation-DeleteUnusedIAMPolicy](#)
- [AWSConfigRemediation-DetachIAMPolicy](#)
- [AWSConfigRemediation-EnableAccountAccessAnalyzer](#)
- [AWSSupport-GrantPermissionsToIAMUser](#)
- [AWSConfigRemediation-RemoveUserPolicies](#)
- [AWSConfigRemediation-ReplaceIAMInlinePolicy](#)
- [AWSConfigRemediation-RevokeUnusedIAMUserCredentials](#)
- [AWSConfigRemediation-SetIAMPasswordPolicy](#)

## **AWS-AttachIAMToInstance**

### Deskripsi

Lampirkan peran AWS Identity and Access Management (IAM) ke instance terkelola.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon



## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- ForceReplace

Jenis: Boolean

Deskripsi: (Opsional) Tandai untuk menentukan apakah akan mengganti profil IAM yang ada atau tidak.

Default: betul

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instance yang ingin Anda tetapkan peran IAM.

- RoleName

Jenis: String

Deskripsi: (Wajib) Nama peran IAM untuk ditambahkan ke instance terkelola.

## Langkah Dokumen

1. `aws:executeAwsApi- DescribeInstanceProfile` - Temukan profil instans IAM yang dilampirkan ke instans EC2.
2. `aws:branch- CheckInstanceProfileAssociations` - Periksa profil instans IAM yang dilampirkan ke instans EC2.
  - a. Jika profil instans IAM dilampirkan dan `ForceReplace` diatur ke `true`:

- i. `aws:executeAwsApi- DisassociatelamInstanceProfile` - Lepaskan profil instans IAM dari instans EC2.
- b. `aws:executeAwsApi- ListInstanceProfilesForRole` - Daftar profil contoh untuk peran IAM yang disediakan.
- c. `aws:branch- CheckInstanceProfileCreated` - Periksa apakah peran IAM yang disediakan memiliki profil instance terkait.
  - i. Jika peran IAM memiliki profil instance terkait:
    - A. `aws:executeAwsApi- Attachiam ProfileToInstance` - Lampirkan peran profil instans IAM ke instans EC2.
  - ii. Jika peran IAM tidak memiliki profil instance terkait:
    - A. `aws:executeAwsApi- CreateInstanceProfileForRole` - Buat peran profil instance untuk peran IAM yang ditentukan.
    - B. `aws:executeAwsApi- AddRoleToInstanceProfile` - Lampirkan peran profil instance ke peran IAM yang ditentukan.
    - C. `aws:executeAwsApi- GetInstanceProfile` - Dapatkan data profil instance untuk peran IAM yang ditentukan.
    - D. `aws:executeAwsApi- Attachiam ProfileToInstanceWithRetry` - Lampirkan peran profil instans IAM ke instans EC2.

## Keluaran

`ProfileToInstanceWithRetryAttachiam. AssociationId`

`GetInstanceProfile.InstanceProfileName`

`GetInstanceProfile.InstanceProfileArn`

`ProfileToInstanceAttachiam. AssociationId`

`ListInstanceProfilesForRole.InstanceProfileName`

`ListInstanceProfilesForRole.InstanceProfileArn`

## **AWS-DeleteIAMInlinePolicy**

### Deskripsi

AWS-DeleteIAMInlinePolicyBuku runbook menghapus semua kebijakan sebaris AWS Identity and Access Management (IAM) yang dilampirkan pada identitas IAM yang Anda tentukan.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- iamArns

Jenis: String

Deskripsi: (Wajib) Daftar ARN yang dipisahkan koma untuk identitas IAM yang ingin Anda hapus kebijakan sebaris. Daftar ini dapat mencakup pengguna, grup, atau peran IAM.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- iam:DeleteGroupPolicy
- iam:DeleteRolePolicy

- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

### Langkah Dokumen

- `aws:executeScript`- Menghapus kebijakan inline IAM yang dilampirkan pada identitas IAM yang ditargetkan.

## **AWSConfigRemediation-DeleteIAMRole**

### Deskripsi

AWSConfigRemediation-DeleteIAMRoleRunbook menghapus peran AWS Identity and Access Management (IAM) yang Anda tentukan. Otomatisasi ini tidak menghapus profil instans yang terkait dengan peran IAM, atau peran terkait layanan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `IamRoleId`

Jenis: String

Deskripsi: (Wajib) ID peran IAM yang ingin Anda hapus.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:GetRole`
- `iam>ListAttachedRolePolicies`
- `iam>ListInstanceProfilesForRole`
- `iam>ListRolePolicies`
- `iam>ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

Langkah Dokumen

- `aws:executeScript`- Mengumpulkan nama peran IAM yang Anda tentukan dalam parameter. `IAMRoleID`
- `aws:executeScript`- Mengumpulkan kebijakan dan profil contoh yang terkait dengan peran IAM.
- `aws:executeScript`- Menghapus kebijakan terlampir.
- `aws:executeScript`- Menghapus peran IAM dan memverifikasi peran telah dihapus.

## **AWSConfigRemediation-DeleteIAMUser**

Deskripsi

`AWSConfigRemediation-DeleteIAMUserRunbook` menghapus pengguna AWS Identity and Access Management (IAM) yang Anda tentukan. Otomatisasi ini menghapus atau melepaskan sumber daya berikut yang terkait dengan pengguna IAM:

- Tombol akses
- Kebijakan terkelola terlampir
- Kredensi Git
- Keanggotaan grup IAM
- Kata sandi pengguna IAM
- Kebijakan inline
- Perangkat otentikasi multi-faktor (MFA)
- Menandatangani sertifikat
- Kunci publik SSH

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `IAM UserId`

**Jenis:** String

**Deskripsi:** (Wajib) ID pengguna IAM yang ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeactivateMFADevice`
- `iam>DeleteAccessKey`
- `iam>DeleteLoginProfile`
- `iam>DeleteServiceSpecificCredential`
- `iam>DeleteSigningCertificate`
- `iam>DeleteSSHPublicKey`
- `iam>DeleteVirtualMFADevice`
- `iam>DeleteUser`
- `iam>DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam:GetUser`
- `iam>ListAttachedUserPolicies`
- `iam>ListAccessKeys`
- `iam>ListGroupsForUser`
- `iam>ListMFADevices`
- `iam>ListServiceSpecificCredentials`
- `iam>ListSigningCertificates`
- `iam>ListSSHPublicKeys`
- `iam>ListUserPolicies`
- `iam>ListUsers`

- `iam:RemoveUserFromGroup`

## Langkah Dokumen

- `aws:executeScript`- Mengumpulkan nama pengguna pengguna IAM yang Anda tentukan dalam parameter. `IAMUserId`
- `aws:executeScript`- Mengumpulkan kunci akses, sertifikat, kredensial, perangkat MFA, dan kunci SSH yang terkait dengan pengguna IAM.
- `aws:executeScript`- Mengumpulkan keanggotaan grup dan kebijakan untuk pengguna IAM.
- `aws:executeScript`- Menghapus kunci akses, sertifikat, kredensial, perangkat MFA, dan kunci SSH yang terkait dengan pengguna IAM.
- `aws:executeScript`- Menghapus keanggotaan grup dan kebijakan untuk pengguna IAM.
- `aws:executeScript`- Menghapus pengguna IAM dan memverifikasi pengguna telah dihapus.

## **AWSConfigRemediation-DeleteUnusedIAMGroup**

### Deskripsi

AWSConfigRemediation-DeleteUnusedIAMGroupRunbook menghapus grup IAM yang tidak berisi pengguna apa pun.

AWSConfigRemediation-DeleteUnusedIAMGroupRunbook menghapus grup IAM yang tidak berisi pengguna apa pun.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows



## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- GroupName

Jenis: String

Deskripsi: (Wajib) Nama grup IAM yang ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam>DeleteGroup
- iam>DeleteGroupPolicy
- iam:DetachGroupPolicy

Langkah Dokumen

- aws:executeScript- Menghapus kebijakan IAM terkelola dan sebaris yang dilampirkan ke grup IAM target, dan kemudian menghapus grup IAM.

## **AWSConfigRemediation-DeleteUnusedIAMPolicy**

Deskripsi

AWSConfigRemediation-DeleteUnusedIAMPolicyRunbook menghapus kebijakan AWS Identity and Access Management (IAM) yang tidak dilampirkan ke pengguna, grup, atau peran apa pun.

## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- IAM ResourceId

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya dari kebijakan IAM yang ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam>DeletePolicy

- `iam:DeletePolicyVersion`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`
- `iam:ListPolicyVersions`

### Langkah Dokumen

- `aws:executeScript`- Menghapus kebijakan yang Anda tentukan dalam `IAMResourceId` parameter, dan memverifikasi kebijakan telah dihapus.

## **AWSConfigRemediation-DetachIAMPolicy**

### Deskripsi

`AWSConfigRemediation-DetachIAMPolicyRunbook` melepaskan kebijakan AWS Identity and Access Management (IAM) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- IAM ResourceId

Jenis: String

Deskripsi: (Wajib) ID kebijakan IAM yang ingin Anda lepaskan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DetachGroupPolicy`
- `iam:DetachRolePolicy`
- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`

Langkah Dokumen

- `aws:executeScript`- Melepaskan kebijakan IAM dari semua sumber daya.

## **AWSConfigRemediation-EnableAccountAccessAnalyzer**

Deskripsi

AWSConfigRemediation-EnableAccountAccessAnalyzerRunbook membuat Access Analyzer AWS Identity and Access Management (IAM) di file Anda. Akun AWS Untuk informasi tentang Access Analyzer, lihat [Menggunakan AWS IAM Access Analyzer di Panduan Pengguna IAM](#).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

## Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AnalyzerName

Jenis: String

Deskripsi: (Wajib) Nama penganalisis yang akan dibuat.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

### Langkah Dokumen

- `aws:executeAwsApi`- Membuat penganalisis akses untuk akun Anda.
- `aws:waitForAwsResourceProperty`- Menunggu status penganalisis akses menjadi `ACTIVE`

- `aws:assertAwsResourceProperty`- Mengonfirmasi status penganalisis akses adalah ACTIVE.

## AWSSupport-GrantPermissionsToIAMUser

### Deskripsi

Runbook ini memberikan izin yang ditentukan ke grup IAM (baru atau yang sudah ada), dan menambahkan pengguna IAM yang ada ke dalamnya. Kebijakan yang dapat Anda pilih: [Billing](#) atau [Support](#). Untuk mengaktifkan akses penagihan untuk IAM, ingatlah untuk juga mengaktifkan pengguna [IAM dan akses pengguna gabungan ke halaman Billing and Cost Management](#).

#### Important

Jika Anda menyediakan grup IAM yang ada, semua pengguna IAM saat ini dalam grup menerima izin baru.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- IAM GroupName

Jenis: String

Default: ExampleSupportAndBillingGroup

Deskripsi: (Wajib) Dapat berupa grup baru atau yang sudah ada. Harus mematuhi [Batas Nama Entitas IAM](#).

- IAM UserName

Jenis: String

Default: ExampleUser

Deskripsi: (Wajib) Harus pengguna yang sudah ada.

- LambdaAssumeRole

Jenis: String

Deskripsi: (Opsional) ARN dari peran yang diasumsikan oleh lambda.

- Izin

Jenis: String

Nilai yang valid: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

Default: SupportAndBillingFullAccess

Deskripsi: (Wajib) Pilih salah satu dari: SupportFullAccess memberikan akses penuh ke pusat Support. BillingFullAccess memberikan akses penuh ke dasbor Penagihan. SupportAndBillingFullAccess memberikan akses penuh ke Pusat Dukungan dan dasbor Penagihan. Info lebih lanjut tentang kebijakan di bawah Detail dokumen.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Izin yang diperlukan tergantung pada bagaimana `AWSSupport-GrantPermissionsToIAMUser` dijalankan

Berjalan sebagai pengguna atau peran yang saat ini masuk

Sebaiknya Anda melampirkan kebijakan terkelola AmazonSSMAutomationRole Amazon, dan izin tambahan berikut untuk dapat membuat fungsi Lambda dan peran IAM untuk diteruskan ke Lambda:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "lambda:InvokeFunction",
                "lambda:CreateFunction",
                "lambda>DeleteFunction",
                "lambda:GetFunction"
            ],
            "Resource":
"arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
            "Effect": "Allow"
        },
        {
            "Effect" : "Allow",
            "Action" : [
                "iam:CreateGroup",
                "iam:AddUserToGroup",
                "iam:ListAttachedGroupPolicies",
                "iam:GetGroup",
                "iam:GetUser"
            ],
            "Resource" : [
                "arn:aws:iam:*:user/*",
                "arn:aws:iam:*:group/*"
            ]
        },
        {
            "Effect" : "Allow",
            "Action" : [
                "iam:AttachGroupPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "ArnEquals": {
                    "iam:PolicyArn": [
                        "arn:aws:iam::aws:policy/job-function/Billing",
                        "arn:aws:iam::aws:policy/AWSSupportAccess"
                    ]
                }
            }
        }
    ]
}
```



```

    ]
  }
},
{
  "Effect" : "Allow",
  "Action" : [
    "iam:ListAccountAliases",
    "iam:GetAccountSummary"
  ],
  "Resource" : "*"
}
]
}

```

### Menggunakan AutomationAssumeRole dan LambdaAssumeRole

Pengguna harus memiliki StartAutomationExecution izin ssm: di runbook, dan iam: pada peran IAM PassRole diteruskan sebagai dan. AutomationAssumeRoleLambdaAssumeRole Berikut adalah izin yang dibutuhkan setiap peran IAM:

#### AutomationAssumeRole

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction"
      ],
      "Resource":
"arn:aws:lambda*:ACCOUNTID:function:AWSSupport-*",
      "Effect": "Allow"
    }
  ]
}

```

#### LambdaAssumeRole

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateGroup",
        "iam:AddUserToGroup",
        "iam:ListAttachedGroupPolicies",
        "iam:GetGroup",
        "iam:GetUser"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/*",
        "arn:aws:iam::*:group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachGroupPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "iam:PolicyArn": [
            "arn:aws:iam::aws:policy/job-function/Billing",
            "arn:aws:iam::aws:policy/AWSSupportAccess"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "iam:GetAccountSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

## Langkah Dokumen

1. `aws:createStack`- Jalankan AWS CloudFormation Template untuk membuat fungsi Lambda.
2. `aws:invokeLambdaFunction`- Jalankan Lambda untuk mengatur izin IAM.
3. `aws:deleteStack`- Hapus CloudFormation Template.

## Keluaran

Configureiam.payload

# AWSConfigRemediation-RemoveUserPolicies

## Deskripsi

AWSConfigRemediation-RemoveUserPolicies Buku runbook menghapus kebijakan sebaris AWS Identity and Access Management (IAM) dan melepaskan kebijakan terkelola apa pun yang dilampirkan pada pengguna yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- iamUserId

Jenis: String

Deskripsi: (Wajib) ID pengguna yang ingin Anda hapus kebijakannya.

- PolicyType

Jenis: String

Nilai yang valid: Semua | Inline | Dikelola

Default: Semua

Deskripsi: (Wajib) Jenis kebijakan IAM yang ingin Anda hapus dari pengguna.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam>DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam>ListAttachedUserPolicies`
- `iam>ListUserPolicies`
- `iam>ListUsers`

Langkah Dokumen

- `aws:executeScript`- Menghapus dan melepaskan kebijakan IAM dari pengguna yang Anda tentukan dalam parameter. `IAMUserID`

## **AWSConfigRemediation-ReplaceIAMInlinePolicy**

Deskripsi

AWSConfigRemediation-ReplaceIAMInlinePolicyRunbook menggantikan kebijakan inline AWS Identity and Access Management (IAM) dengan kebijakan IAM terkelola yang direplikasi. Untuk

kebijakan sebaris yang dilampirkan ke pengguna, grup, atau peran, izin kebijakan sebaris dikloning ke dalam kebijakan IAM terkelola. Kebijakan IAM terkelola ditambahkan ke sumber daya, dan kebijakan inline dihapus. AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- InlinePolicyName

Jenis: StringList

Deskripsi: (Wajib) Kebijakan IAM inline yang ingin Anda ganti.

- ResourceId

Jenis: String

Deskripsi: (Wajib) ID pengguna, grup, atau peran IAM yang kebijakannya ingin Anda ganti.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:AttachGroupPolicy`
- `iam:AttachRolePolicy`
- `iam:AttachUserPolicy`
- `iam:CreatePolicy`
- `iam:CreatePolicyVersion`
- `iam>DeleteGroupPolicy`
- `iam>DeleteRolePolicy`
- `iam>DeleteUserPolicy`
- `iam:GetGroupPolicy`
- `iam:GetRolePolicy`
- `iam:GetUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

#### Langkah Dokumen

- `aws:executeScript`- Ganti kebijakan IAM sebaris dengan kebijakan yang AWS direplikasi pada sumber daya yang Anda tentukan.

## **AWSConfigRemediation-RevokeUnusedIAMUserCredentials**

### Deskripsi

AWSConfigRemediation-RevokeUnusedIAMUserCredentialsRunbook mencabut kata sandi yang tidak digunakan AWS Identity and Access Management (IAM) dan kunci akses aktif. Runbook ini juga menonaktifkan kunci akses kedaluwarsa, dan menghapus profil login yang kedaluwarsa. AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `IAM ResourceId`

Jenis: String

Deskripsi: (Wajib) ID sumber daya IAM yang ingin Anda cabut kredensial yang tidak digunakan.

- `MaxCredentialUsageAge`

Jenis: String

Default: 90

Deskripsi: (Wajib) Jumlah hari di mana kredensi harus digunakan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `config>ListDiscoveredResources`
- `iam>DeleteAccessKey`
- `iam>DeleteLoginProfile`
- `iam:GetAccessKeyLastUsed`
- `iam:GetLoginProfile`
- `iam:GetUser`
- `iam>ListAccessKeys`
- `iam:UpdateAccessKey`

### Langkah Dokumen

- `aws:executeScript`- Mencabut kredensial IAM untuk pengguna yang ditentukan dalam parameter. `IAMResourceId` Kunci akses kedaluwarsa dinonaktifkan, dan profil login yang kedaluwarsa dihapus.

#### Note

Pastikan untuk mengonfigurasi `MaxCredentialUsageAge` parameter tindakan remediasi ini agar sesuai dengan `maxAccessKeyAge` parameter AWS Config aturan yang Anda gunakan untuk memicu tindakan ini: [access-keys-rotated](#).

## AWSConfigRemediation-SetIAMPASSWORDPolicy

### Deskripsi

`AWSConfigRemediation-SetIAMPASSWORDPolicyRunbook` menetapkan kebijakan kata sandi pengguna AWS Identity and Access Management (IAM) untuk Anda. Akun AWS

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi



## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- AllowUsersToChangePassword

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika diatur ke `true`, semua pengguna IAM di Anda Akun AWS dapat menggunakan AWS Management Console untuk mengubah kata sandi mereka.

- HardExpiry

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika disetel ke `true`, pengguna IAM dicegah untuk mengatur ulang kata sandi mereka setelah kata sandi mereka kedaluwarsa.

- MaxPasswordAge

Jenis: Integer

Default: 0

Deskripsi: (Opsional) Jumlah hari kata sandi pengguna IAM valid.

- MinimumPasswordLength

Jenis: Integer

Default: 6

Deskripsi: (Opsional) Jumlah minimum karakter kata sandi pengguna IAM dapat.

- PasswordReusePrevention

Jenis: Integer

Default: 0

Deskripsi: (Opsional) Jumlah kata sandi sebelumnya yang dicegah oleh pengguna IAM untuk digunakan kembali.

- RequireLowercaseCharacters

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika disetel ke `true`, kata sandi pengguna IAM harus berisi karakter huruf kecil dari alfabet Latin dasar ISO (a sampai z).

- RequireNumbers

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika diatur ke `true`, kata sandi pengguna IAM harus berisi karakter numerik (0-9).

- RequireSymbols

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika diatur ke `true`, kata sandi pengguna IAM harus berisi karakter non-alfanumerik (! @ # \$ % ^ \* ( ) \_ + - = [ ] { } | ').

- RequireUppercaseCharacters

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika diatur ketruue, kata sandi pengguna IAM harus berisi karakter huruf besar dari alfabet Latin dasar ISO (A sampai Z).

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

Langkah Dokumen

- `aws:executeScript`- Menetapkan kebijakan kata sandi pengguna IAM berdasarkan nilai yang Anda tentukan untuk parameter runbook untuk Anda. Akun AWS

## Amazon Kinesis Data Streams

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Kinesis Data Streams. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWS-EnableKinesisStreamEncryption](#)

### **AWS-EnableKinesisStreamEncryption**

Deskripsi

AWS-EnableKinesisStreamEncryptionRunbook memungkinkan enkripsi pada Amazon Kinesis Data Streams (Kinesis Data Streams). Aplikasi produser yang menulis ke aliran terenkripsi akan

mengalami kesalahan jika mereka tidak memiliki akses ke kunci AWS Key Management Service (AWS KMS).

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- KinesisStreamName

Jenis: String

Deskripsi: (Wajib) Nama aliran yang ingin Anda aktifkan enkripsi.

- KeyId

Jenis: String

Default: alias/aws/kinesis

Deskripsi: (Wajib) AWS KMS Kunci yang dikelola pelanggan yang ingin Anda gunakan untuk enkripsi. Nilai ini dapat berupa pengidentifikasi unik global, ARN untuk alias atau kunci, atau nama alias yang diawali dengan "alias/". Anda juga dapat menggunakan kunci yang AWS dikelola dengan menggunakan nilai default untuk parameter.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

## Langkah Dokumen

- `VerifyKinesisStreamStatus` (`aws: waitforAwsResource Properti`) - Memeriksa status Kinesis Data Streams.
- `EnableKinesisStreamEncryption` (`aws:executeAwsApi`) - Mengaktifkan enkripsi untuk Kinesis Data Streams.
- `VerifyKinesisStreamUpdateComplete` (`aws: waitForAwsResourceProperty`) - Menunggu status Kinesis Data Streams kembali ke. ACTIVE
- `VerifyKinesisStreamEncryption` (`aws: assertAwsResource Properti`) - Memverifikasi enkripsi diaktifkan untuk Kinesis Data Streams.

## AWS KMS

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS Key Management Service Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSConfigRemediation-CancelKeyDeletion](#)
- [AWSConfigRemediation-EnableKeyRotation](#)

## **AWSConfigRemediation-CancelKeyDeletion**

### Deskripsi

AWSConfigRemediation-CancelKeyDeletionRunbook membatalkan penghapusan AWS Key Management Service (AWS KMS) kunci terkelola pelanggan yang Anda tentukan.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- KeyId

Jenis: String

Deskripsi: (Wajib) ID kunci terkelola pelanggan yang ingin Anda batalkan penghapusan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:CancelKeyDeletion
- kms:DescribeKey

## Langkah Dokumen

- `aws:executeAwsApi`- Membatalkan penghapusan untuk kunci terkelola pelanggan yang Anda tentukan dalam parameter. `KeyId`
- `aws:assertAwsResourceProperty`- Mengonfirmasi penghapusan kunci dinonaktifkan pada kunci yang dikelola pelanggan Anda.

## **AWSConfigRemediation-EnableKeyRotation**

### Deskripsi

`AWSConfigRemediation-EnableKeyRotationRunbook` memungkinkan rotasi kunci otomatis untuk kunci yang dikelola pelanggan simetris AWS Key Management Service (AWS KMS).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `KeyId`

Jenis: String

Deskripsi: (Wajib) ID kunci terkelola pelanggan yang ingin Anda aktifkan rotasi kunci otomatis.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan rotasi kunci otomatis pada kunci terkelola pelanggan yang Anda tentukan dalam `KeyId` parameter.
- `aws:assertAwsResourceProperty`- Mengonfirmasi bahwa rotasi kunci otomatis diaktifkan pada kunci yang dikelola pelanggan Anda.

## Lambda

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS Lambda Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing](#)
- [AWSConfigRemediation-DeleteLambdaFunction](#)
- [AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK](#)
- [AWSConfigRemediation-MoveLambdaToVPC](#)
- [AWSSupport-RemediateLambdaS3Event](#)
- [AWSSupport-TroubleshootLambdaInternetAccess](#)
- [AWSSupport-TroubleshootLambdaS3Event](#)

## **AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing**

### Deskripsi



AWSConfigRemediation-ConfigureLambdaFunctionXRayTracingRunbook memungkinkan penelusuran AWS X-Ray langsung pada AWS Lambda fungsi yang Anda tentukan dalam parameter.

FunctionName

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- FunctionName

Jenis: String

Deskripsi: (Wajib) Nama atau ARN dari fungsi Lambda untuk mengaktifkan penelusuran.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `lambda:UpdateFunctionConfiguration`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan penelusuran X-Ray pada fungsi Lambda yang Anda tentukan dalam `FunctionName` parameter.
- `aws:assertAwsResourceProperty`- Memverifikasi bahwa penelusuran X-Ray telah diaktifkan pada fungsi Lambda.

## Keluaran

`UpdateLambdaConfig.UpdateFunctionConfigurationResponse` - Respon dari panggilan `UpdateFunctionConfiguration` API.

## **AWSConfigRemediation-DeleteLambdaFunction**

### Deskripsi

`AWSConfigRemediation-DeleteLambdaFunction` runbook menghapus AWS Lambda fungsi yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `LambdaFunctionName`

Jenis: String

Deskripsi: (Wajib) Nama fungsi Lambda yang ingin Anda hapus.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

Langkah Dokumen

- `aws:executeAwsApi`- Menghapus fungsi Lambda yang ditentukan dalam `LambdaFunctionName` parameter.
- `aws:executeScript`- Memverifikasi fungsi Lambda telah dihapus.

## **AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK**

Deskripsi

`AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMKRunbook` mengenkripsi, pada saat lain, variabel lingkungan untuk fungsi (AWS Lambda Lambda) yang Anda tentukan menggunakan kunci yang dikelola pelanggan AWS Key Management Service (AWS KMS). Runbook ini hanya boleh digunakan sebagai baseline untuk memastikan bahwa variabel lingkungan fungsi Lambda Anda dienkripsi sesuai dengan praktik terbaik keamanan minimum yang direkomendasikan. Kami merekomendasikan mengenkripsi beberapa fungsi dengan kunci terkelola pelanggan yang berbeda.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

## Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `FunctionName`

Jenis: String

Deskripsi: (Wajib) Nama atau ARN dari fungsi Lambda yang variabel lingkungannya ingin Anda enkripsi.

- `KMS KeyArn`

Jenis: String

Deskripsi: (Wajib) ARN kunci terkelola AWS KMS pelanggan yang ingin Anda gunakan untuk mengenkripsi variabel lingkungan fungsi Lambda Anda.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

## Langkah Dokumen

- `aws:waitForAwsResourceProperty`- Menunggu `LastUpdateStatus` properti menjadi `Successful`.
- `aws:executeAwsApi`- Mengenkripsi variabel lingkungan untuk fungsi Lambda yang Anda tentukan dalam `FunctionName` parameter menggunakan kunci terkelola AWS KMS pelanggan yang Anda tentukan dalam parameter. `KMSKeyArn`
- `aws:assertAwsResourceProperty`- Mengonfirmasi enkripsi diaktifkan pada variabel lingkungan untuk fungsi Lambda Anda.

## AWSConfigRemediation-MoveLambdaToVPC

### Deskripsi

`AWSConfigRemediation-MoveLambdaToVPC` Runbook memindahkan fungsi AWS Lambda (Lambda) ke Amazon Virtual Private Cloud (Amazon VPC).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `FunctionName`

Jenis: String

Deskripsi: (Wajib) Nama fungsi Lambda untuk pindah ke VPC Amazon.

- `SecurityGroupIds`

Jenis: String

Deskripsi: (Wajib) ID grup keamanan yang ingin Anda tetapkan ke antarmuka jaringan elastis (ENI) yang terkait dengan fungsi Lambda Anda.

- `SubnetIds`

Jenis: String

Deskripsi: (Wajib) ID subnet yang ingin Anda buat antarmuka jaringan elastis (ENI) yang terkait dengan fungsi Lambda Anda.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

### Langkah Dokumen

- `aws:executeAwsApi`- Memperbarui konfigurasi Amazon VPC untuk fungsi Lambda yang Anda tentukan dalam parameter. `FunctionName`
- `aws:waitForAwsResourceProperty`- Menunggu `LastUpdateStatus` fungsi Lambda. `successful`
- `aws:executeScript`- Memverifikasi fungsi Lambda konfigurasi Amazon VPC telah berhasil diperbarui.

# AWSSupport-RemediateLambdaS3Event

## Deskripsi

AWSSupport-TroubleshootLambdaS3EventRunbook menyediakan solusi otomatis untuk prosedur yang diuraikan dalam artikel Pusat AWS Pengetahuan [Mengapa pemberitahuan peristiwa Amazon S3 saya tidak memicu fungsi Lambda saya?](#) dan [Mengapa saya mendapatkan kesalahan “Tidak dapat memvalidasi konfigurasi tujuan berikut” saat membuat pemberitahuan acara Amazon S3 untuk memicu fungsi Lambda saya?](#) Runbook ini membantu Anda mengidentifikasi dan memulihkan mengapa pemberitahuan peristiwa Amazon Simple Storage Service (Amazon S3) gagal memicu fungsi yang Anda tentukan. AWS Lambda [Jika keluaran runbook menyarankan untuk memvalidasi dan mengonfigurasi konkurensi fungsi Lambda Anda, lihat Pemanggilan asinkron dan Penskalaan fungsi.AWS Lambda](#)

### Note

Kesalahan “Tidak dapat memvalidasi konfigurasi tujuan berikut” juga dapat terjadi karena Simple Notification Service Amazon (Amazon SNS) yang salah dan Amazon Simple Queue Service (Amazon SQS) konfigurasi acara Amazon S3. Runbook ini hanya memeriksa konfigurasi fungsi Lambda. Jika setelah menggunakan runbook, Anda masih menerima kesalahan “Tidak dapat memvalidasi konfigurasi tujuan berikut”, harap tinjau konfigurasi acara Amazon SNS dan Amazon SQS Amazon S3 yang ada.

## [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LambdaFunctionArn

Jenis: String

Deskripsi: (Wajib) ARN dari fungsi Lambda.

- S3 BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket Amazon S3 yang notifikasi kejadiannya memicu fungsi Lambda.

- Tindakan

Jenis: String

Nilai yang valid: Memecahkan masalah | Remediate

Deskripsi: (Wajib) Tindakan yang Anda ingin runbook lakukan. TroubleshootOpsi ini membantu mengidentifikasi masalah apa pun, tetapi tidak melakukan tindakan mutasi apa pun untuk menyelesaikan masalah. RemediateOpsi ini membantu mengidentifikasi dan mencoba menyelesaikan masalah untuk Anda.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetDocument
- ssm:ListDocuments
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions



- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

## Langkah Dokumen

- `aws:branch`- Cabang berdasarkan input yang ditentukan untuk `Action` parameter.

Jika nilai yang ditentukan adalah `Troubleshoot`:

- `aws:executeAutomation`- Menjalankan `AWSSupport-TroubleshootLambdaS3Event` runbook.
- `aws:executeAwsApi`- Memeriksa output dari `AWSSupport-TroubleshootLambdaS3Event` runbook yang berjalan pada langkah sebelumnya.

Jika nilai yang ditentukan adalah `Remediate`:

- `aws:executeScript`- Menjalankan skrip untuk memperbaiki masalah yang diuraikan dalam [Mengapa pemberitahuan peristiwa Amazon S3 saya tidak memicu fungsi Lambda saya?](#) dan [Mengapa saya mendapatkan kesalahan “Tidak dapat memvalidasi konfigurasi tujuan berikut” saat membuat pemberitahuan acara Amazon S3 untuk memicu fungsi Lambda saya?](#) Artikel Pusat Pengetahuan.

## Keluaran

`Checkout.output`

`RemediateLambdas3Event.output`

## **AWSSupport-TroubleshootLambdaInternetAccess**

### Deskripsi

`AWSSupport-TroubleshootLambdaInternetAccessRunbook` membantu Anda memecahkan masalah akses internet untuk AWS Lambda fungsi yang diluncurkan ke Amazon Virtual Private Cloud (Amazon VPC). Sumber daya seperti rute subnet, aturan grup keamanan, dan aturan daftar kontrol akses jaringan (ACL) ditinjau untuk mengonfirmasi akses internet keluar diizinkan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- FunctionName

Jenis: String

Deskripsi: (Wajib) Nama fungsi Lambda yang ingin Anda pecahkan masalah akses internet.

- destinationIp

Jenis: String

Deskripsi: (Wajib) Alamat IP tujuan yang ingin Anda buat koneksi keluar.

- destinationPort

Jenis: String

Standar: 443

Deskripsi: (Opsional) Port tujuan yang ingin Anda buat koneksi keluar.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

### Langkah Dokumen

- `aws:executeScript`- Memverifikasi konfigurasi berbagai sumber daya di VPC Anda tempat fungsi Lambda diluncurkan.
- `aws:branch`- Cabang berdasarkan apakah fungsi Lambda yang ditentukan ada dalam VPC atau tidak.
- `aws:executeScript`- Meninjau rute tabel rute untuk subnet tempat fungsi Lambda diluncurkan, dan memverifikasi bahwa rute ke gateway terjemahan alamat jaringan (NAT), dan gateway internet hadir. Mengonfirmasi bahwa fungsi Lambda tidak ada dalam subnet publik.
- `aws:executeScript`- Memverifikasi grup keamanan yang terkait dengan fungsi Lambda memungkinkan akses internet keluar berdasarkan nilai yang ditentukan untuk `destinationIp` dan parameter. `destinationPort`
- `aws:executeScript`- Memverifikasi aturan ACL yang terkait dengan subnet fungsi Lambda dan gateway NAT memungkinkan akses internet keluar berdasarkan nilai yang ditentukan untuk dan parameter. `destinationIp` `destinationPort`

### Keluaran

`CheckVPC.vpc` - ID VPC tempat fungsi Lambda Anda diluncurkan.

`CheckVPC.subnet` - ID subnet tempat fungsi Lambda Anda diluncurkan.

`CheckVPC.SecurityGroups` - Grup keamanan yang terkait dengan fungsi Lambda.

`Checknacl.nacl` - Pesan analisis dengan nama sumber daya. `LambdaIp` mengacu pada alamat IP pribadi dari elastic network interface untuk fungsi Lambda Anda. `LambdaIpRulesObjek` hanya dihasilkan untuk subnet yang memiliki rute ke gateway NAT. Konten berikut adalah contoh dari output.

```
{
  "subnet-1234567890":{
    "NACL":"acl-1234567890",
    "destinationIp_Egress":"Allowed",
    "destinationIp_Ingress":"notAllowed",
    "Analysis":"This NACL has an allow rule for Egress traffic but there is no
Ingress rule. Please allow the destination IP / destination port in Ingress rule",
    "LambdaIpRules":{
      "{LambdaIp}":{
        "Egress":"notAllowed",
        "Ingress":"notAllowed",
        "Analysis":"This is a NAT subnet NACL. It does not have ingress or egress
rule allowed in it for Lambda's corresponding private ip {LambdaIp} Please allow this
IP in your egress and ingress NACL rules"
      }
    }
  },
  "subnet-0987654321":{
    "NACL":"acl-0987654321",
    "destinationIp_Egress":"Allowed",
    "destinationIp_Ingress":"notAllowed",
    "Analysis":"This NACL has an allow rule for Egress traffic but there is no
Ingress rule. Please allow the destination IP / destination port in Ingress rule"
  }
}
```

checkSecurityGroups.secgrps - Analisis untuk grup keamanan yang terkait dengan fungsi Lambda Anda. Konten berikut adalah contoh dari output.

```
{
  "sg-123456789":{
    "Status":"Allowed",
    "Analysis":"This security group has allowed destintion IP and port in its
outbuond rule."
  }
}
```

CheckSubnet.subnets - Analisis untuk subnet di VPC Anda yang terkait dengan fungsi Lambda Anda. Konten berikut adalah contoh dari output.

```
{
  "subnet-0c4ee6cdexample15":{
```

```
"Route":{
  "DestinationCidrBlock":"8.8.8.0/26",
  "NatGatewayId":"nat-00f0example69fdec",
  "Origin":"CreateRoute",
  "State":"active"
},
"Analysis":"This Route Table has an active NAT gateway path. Also, The NAT
gateway is launched in public subnet",
"RouteTable":"rtb-0b1fexample16961b"
}
}
```

## AWSSupport-TroubleshootLambdaS3Event

### Deskripsi

AWSSupport-TroubleshootLambdaS3EventRunbook menyediakan solusi otomatis untuk prosedur yang diuraikan dalam artikel Pusat AWS Pengetahuan [Mengapa pemberitahuan peristiwa Amazon S3 saya tidak memicu fungsi Lambda saya?](#) dan [Mengapa saya mendapatkan kesalahan “Tidak dapat memvalidasi konfigurasi tujuan berikut” saat membuat pemberitahuan acara Amazon S3 untuk memicu fungsi Lambda saya?](#) Runbook ini membantu Anda mengidentifikasi mengapa pemberitahuan peristiwa Amazon Simple Storage Service (Amazon S3) gagal memicu fungsi yang Anda tentukan. AWS Lambda [Jika keluaran runbook menyarankan untuk memvalidasi dan mengonfigurasi konkurensi fungsi Lambda Anda, lihat Pemanggilan asinkron dan Penskalaan fungsi.AWS Lambda](#)

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LambdaFunctionArn

Jenis: String

Deskripsi: (Wajib) ARN dari fungsi Lambda yang dipicu oleh notifikasi peristiwa Amazon S3.

- S3 BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket Amazon S3 yang notifikasi kejadiannya memicu fungsi Lambda.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

Langkah Dokumen

- `aws:executeScript`- Menjalankan skrip untuk memvalidasi pengaturan konfigurasi untuk pemberitahuan acara Amazon S3. Memvalidasi kebijakan IAM berbasis sumber daya untuk fungsi Lambda Anda, dan menghasilkan perintah AWS CLI() untuk menambahkan izin AWS Command Line Interface yang diperlukan jika izin yang diperlukan tidak ada dari kebijakan. Memvalidasi kebijakan sumber daya fungsi Lambda lainnya yang merupakan bagian dari pemberitahuan peristiwa untuk bucket S3 yang sama dan menghasilkan perintah AWS CLI sebagai output jika izin yang diperlukan tidak ada.

Keluaran

Lambdas3Event.output

## Amazon Managed Workflows for Apache Airflow (MWAA)

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Alur Kerja Terkelola Amazon untuk Apache Airflow. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSSupport-TroubleshootMWAAEnvironmentCreation](#)

### AWSSupport-TroubleshootMWAAEnvironmentCreation

Deskripsi

AWSSupport-TroubleshootMWAAEnvironmentCreationRunbook menyediakan informasi untuk men-debug Amazon Managed Workflows untuk masalah pembuatan lingkungan Apache Airflow (Amazon MWAA), dan melakukan pemeriksaan bersama dengan alasan yang didokumentasikan dengan upaya terbaik untuk membantu mengidentifikasi kegagalan.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Mengambil detail lingkungan Amazon MWAA.
- Memverifikasi izin peran eksekusi.
- Memeriksa apakah lingkungan memiliki izin untuk menggunakan AWS KMS kunci yang disediakan untuk logging, dan apakah grup CloudWatch log yang diperlukan ada.
- Mem-parsing log dalam grup log yang disediakan untuk menemukan kesalahan apa pun.
- Memeriksa konfigurasi jaringan untuk memverifikasi apakah lingkungan Amazon MWAA memiliki akses ke titik akhir yang diperlukan.
- Menghasilkan laporan dengan temuan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

## Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `airflow:GetEnvironment`
- `cloudtrail:LookupEvents`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `iam:GetPolicy`
- `iam:GetPolicyVersion`
- `iam:GetRolePolicy`
- `iam>ListAttachedRolePolicies`
- `iam>ListRolePolicies`
- `iam:SimulateCustomPolicy`
- `kms:GetKeyPolicy`
- `kms>ListAliases`
- `logs:DescribeLogGroups`
- `logs:FilterLogEvents`



- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetPublicAccessBlock`
- `s3control:GetPublicAccessBlock`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootMWAAEnvironmentCreation](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
  - `AutomationAssumeRole` (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `EnvironmentName` (Diperlukan):

Nama lingkungan Amazon MWAA yang ingin Anda evaluasi.

The screenshot shows the 'Input parameters' section of the AWS Systems Manager console. It contains two input fields:

- AutomationAssumeRole**: (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. This field has a dropdown menu and a clear button.
- EnvironmentName**: (Required) Name of the MWAA environment you wish to evaluate. This field is a text input box with a 'String' label.

4. Pilih Jalankan.
5. Otomatisasi dimulai.
6. Dokumen melakukan langkah-langkah berikut:

- **GetMWAAEnvironmentDetails:**

Mengambil detail lingkungan Amazon MWAA. Jika langkah ini gagal, proses otomatisasi akan berhenti dan ditampilkan sebagai `Failed`.

- **CheckIAMPermissionsOnExecutionRole:**

Memverifikasi bahwa peran eksekusi memiliki izin yang diperlukan untuk sumber daya Amazon MWAA, Amazon S3, Log CloudWatch, dan CloudWatch Amazon SQS. Jika mendeteksi kunci terkelola pelanggan AWS Key Management Service (AWS KMS), otomatisasi memvalidasi izin kunci yang diperlukan. Langkah ini menggunakan `iam:SimulateCustomPolicy` API untuk memastikan apakah peran eksekusi otomatisasi memenuhi semua izin yang diperlukan.

- **CheckKMSPolicyOnKMSKey:**

Memeriksa apakah kebijakan AWS KMS kunci memungkinkan lingkungan Amazon MWAA menggunakan kunci untuk mengenkripsi CloudWatch Log. Jika AWS KMS kuncinya AWS-managed, otomatisasi melewati pemeriksaan ini.

- **CheckIfRequiredLogGroupsExists:**

Memeriksa apakah ada grup CloudWatch log yang diperlukan untuk lingkungan Amazon MWAA. Jika tidak, otomatisasi CloudTrail memeriksa `CreateLogGroup` dan `DeleteLogGroup` acara. Langkah ini juga memeriksa `CreateLogGroup` acara.

- **BranchOnLogGroupsFindings:**

Cabang berdasarkan keberadaan grup CloudWatch log yang terkait dengan lingkungan Amazon MWAA. Jika setidaknya ada satu grup log, otomatisasi menguraikannya untuk menemukan kesalahan. Jika tidak ada grup log, otomatisasi melewati langkah berikutnya.

- **CheckForErrorsInLogGroups:**

Mem-parsing grup CloudWatch log untuk menemukan kesalahan.

- **GetRequiredEndpointsDetails:**

Mengambil titik akhir layanan yang digunakan oleh lingkungan Amazon MWAA.

- **CheckNetworkConfiguration:**

Memverifikasi bahwa konfigurasi jaringan lingkungan Amazon MWAA memenuhi persyaratan, termasuk pemeriksaan pada grup keamanan, ACL jaringan, subnet, dan konfigurasi tabel rute.

- **CheckEndpointsConnectivity:**

Memanggil otomatisasi `AWSsupport-ConnectivityTroubleshooter` anak untuk memvalidasi konektivitas Amazon MWAA ke titik akhir yang diperlukan.

- **CheckS3BlockPublicAccess:**

Memeriksa apakah bucket Amazon S3 lingkungan Amazon MWAAs `Public Access` telah diaktifkan dan juga meninjau keseluruhan pengaturan Akses Publik Blok Amazon S3 akun.

- **GenerateReport:**

Mengumpulkan informasi dari otomatisasi dan mencetak hasil atau output dari setiap langkah.

7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci:

- Memeriksa izin peran eksekusi lingkungan Amazon MWAAs:

Memverifikasi apakah peran eksekusi memiliki izin yang diperlukan untuk sumber daya Amazon MWAAs, Amazon S3, Log CloudWatch, dan CloudWatch Amazon SQS. Jika AWS KMS kunci yang Dikelola Pelanggan terdeteksi, otomatisasi memvalidasi izin kunci yang diperlukan.

- Memeriksa kebijakan AWS KMS kunci lingkungan Amazon MWAAs:

Memverifikasi apakah peran eksekusi memiliki izin yang diperlukan untuk sumber daya Amazon MWAAs, Amazon S3, Log CloudWatch, CloudWatch dan Amazon SQS. Selain itu, jika AWS KMS kunci yang Dikelola Pelanggan terdeteksi, otomatisasi akan memeriksa izin kunci yang diperlukan.

- Memeriksa grup CloudWatch log lingkungan Amazon MWAAs:

Memeriksa apakah Grup CloudWatch Log yang diperlukan untuk lingkungan Amazon MWAAs ada. Jika tidak, otomatisasi kemudian CloudTrail memeriksa lokasi `CreateLogGroup` dan `DeleteLogGroup` acara.

- Memeriksa Tabel Rute lingkungan Amazon MWAAs:

Memeriksa apakah tabel rute VPC Amazon di lingkungan Amazon MWAAs dikonfigurasi dengan benar.

- Memeriksa Grup Keamanan lingkungan Amazon MWAAs:

Memeriksa apakah lingkungan Amazon MWAAs Grup keamanan Amazon VPC dikonfigurasi dengan benar.

- Memeriksa ACL Jaringan lingkungan Amazon MWAAs:

Memeriksa apakah grup keamanan Amazon VPC di lingkungan Amazon MWAAs dikonfigurasi dengan benar.

- Memeriksa Subnet lingkungan Amazon MWAAs:

Memverifikasi apakah subnet lingkungan Amazon MWAAs bersifat pribadi.

- Memeriksa lingkungan Amazon MWAA memerlukan konektivitas titik akhir:

Memverifikasi apakah lingkungan Amazon MWAA dapat mengakses titik akhir yang diperlukan. Untuk tujuan ini, otomatisasi memanggil `AWSSupport-ConnectivityTroubleshooter` otomatisasi.

- Memeriksa lingkungan Amazon MWAA Amazon S3 bucket:

Memeriksa apakah bucket Amazon S3 lingkungan Amazon MWAA Block Public Access telah diaktifkan dan juga meninjau pengaturan Akses Publik Blok Amazon S3 akun.

- Memeriksa kesalahan grup CloudWatch log lingkungan Amazon MWAA:

Mem-parsing grup CloudWatch log yang ada di lingkungan Amazon MWAA untuk menemukan kesalahan.

#### ▼ Outputs

```

GenerateReport.AutomationReport
Troubleshooting report for MWAA environment

🔗 The automation found no issues with the MWAA environment configuration ✓

🔗 Checking the MWAA environment execution role permissions
All the required permissions for the MWAA environment execution role are in place ✓

🔗 Checking the MWAA environment KMS key policy
KMS key is an AWS managed key ✓

🔗 Checking the MWAA environment CloudWatch logs groups
The number of CloudWatch log groups found is 5 and the number of enabled log groups for the MWAA environment [REDACTED] is 5. This suggests that all log groups were created successfully ✓

🔗 Checking the MWAA environment Route Tables
NAT GW [REDACTED] has Internet route: subnet: [REDACTED] > nat- [REDACTED] -> igw [REDACTED] ✓
NAT GW [REDACTED] has Internet route: subnet: [REDACTED] > nat- [REDACTED] -> igw [REDACTED] ✓

🔗 Checking the MWAA environment Security Groups
Security group [REDACTED] has self-referencing rules for all traffic. ✓

🔗 Checking the MWAA environment Network ACLs
NACL: [REDACTED] allows port 5432 on egress ✓ and allows port 5432 on ingress ✓

🔗 Checking the MWAA environment Subnets
Subnet: subnet- [REDACTED] is private ✓
Subnet: subnet- [REDACTED] is private ✓

🔗 Checking the MWAA environment required endpoints connectivity

✓ Testing connectivity with sqs.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and sqs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the sqs.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

✓ Testing connectivity with api.ecr.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and api.ecr.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.ecr.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

✓ Testing connectivity with monitoring.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and monitoring.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the monitoring.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

✓ Testing connectivity with kms.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and kms.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the kms.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

✓ Testing connectivity with s3.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and s3.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the s3.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and env.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and env.airflow.eu-west-1.amazonaws.com on port 5432 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

✓ Testing connectivity with api.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and api.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

✓ Testing connectivity with logs.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and logs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the logs.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

✓ Testing connectivity with ops.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [REDACTED] and ops.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the ops.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[REDACTED]?region=eu-west-1

🔗 Checking the MWAA environment S3 bucket
Environment's S3 bucket and/or account block public access ✓

🔗 Checking the MWAA environment CloudWatch logs groups errors
Parsed log group [REDACTED] DIAGProcessing - no errors found ✓
Parsed log group [REDACTED] Scheduler - no errors found ✓
Parsed log group [REDACTED] Task - no errors found ✓
Parsed log group [REDACTED] WebServer - no errors found ✓
Parsed log group [REDACTED] Worker - no errors found ✓

```

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

## Neptune

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon Neptune. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-EnableNeptuneDbAuditLogsToCloudWatch](#)
- [AWS-EnableNeptuneDbBackupRetentionPeriod](#)
- [AWS-EnableNeptuneClusterDeletionProtection](#)

## AWS - EnableNeptuneDbAuditLogsToCloudWatch

### Deskripsi

AWS-EnableNeptuneDbAuditLogsToCloudWatchRunbook membantu Anda mengirim log audit untuk klaster DB Amazon Neptune ke Amazon Logs. CloudWatch

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DbClusterResourceId

Jenis: String

Deskripsi: (Wajib) ID sumber daya cluster DB Neptunus yang ingin Anda aktifkan log audit.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

## Langkah Dokumen

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Mengembalikan ID cluster DB Neptunus.
- VerifyNeptuneDbEngine (aws:assertAwsResource Properti) - Memverifikasi jenis mesin Neptunus DB adalah. neptune
- EnableNeptuneDbAuditLogs (aws:executeAwsApi) - Mengaktifkan log audit untuk cluster DB Neptunus untuk dikirim Log. CloudWatch
- VerifyNeptuneDbStatus (aws:waitAwsResource Property) - Memverifikasi status cluster DB Neptunus adalah. available

- `VerifyNeptuneDbAuditLogs (AWS:ExecuteScript)` - Memverifikasi bahwa log audit berhasil dikonfigurasi untuk dikirim ke Log. CloudWatch

## AWS - EnableNeptuneDbBackupRetentionPeriod

### Deskripsi

`AWS-EnableNeptuneDbBackupRetentionPeriodRunbook` membantu Anda mengaktifkan pencadangan otomatis dengan periode retensi cadangan antara 7 dan 35 hari untuk cluster DB Amazon Neptunus.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `DbClusterResourceId`

Jenis: String

Deskripsi: (Wajib) ID sumber daya dari cluster DB Neptunus yang ingin Anda aktifkan pencadangan.

- `BackupRetentionPeriod`

Jenis: Integer

Nilai yang valid: 7-35

Deskripsi: (Wajib) Jumlah hari cadangan dipertahankan.

- PreferredBackupWindow

Jenis: String

Deskripsi: (Opsional) Jangka waktu harian minimal 30 menit saat pencadangan dilakukan. Nilai harus dalam Universal Time Coordinated (UTC) dan gunakan format: hh24:mm-hh24:mm Periode retensi cadangan tidak dapat bertentangan dengan jendela pemeliharaan yang diinginkan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

Langkah Dokumen

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Mengembalikan ID cluster DB Neptunus.
- VerifyNeptuneDbEngine (aws:assertAwsResource Properti) - Memverifikasi jenis mesin Neptunus DB adalah. neptune
- VerifyNeptuneDbStatus (aws:waitAwsResource Properti) - Memverifikasi status cluster DB Neptunus adalah. available
- ModifyNeptuneDbRetentionPeriod (aws:executeAwsApi) - Mengatur periode retensi untuk cluster DB Neptunus.
- VerifyNeptuneDbBackupsEnabled (AWS: ExecuteScript) - Memverifikasi periode retensi dan jendela cadangan berhasil ditetapkan.



# AWS-EnableNeptuneClusterDeletionProtection

## Deskripsi

AWS-EnableNeptuneClusterDeletionProtectionRunbook memungkinkan perlindungan penghapusan untuk cluster Amazon Neptunus yang Anda tentukan.

## Jenis dokumen

## Otomatisasi

## Pemilik

## Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DbClusterResourceId

Jenis: String

Deskripsi: (Wajib) ID cluster Neptunus yang ingin Anda aktifkan perlindungan penghapusan.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`

- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

### Langkah Dokumen

- `GetNeptuneDbClusterIdentifier` (`aws:executeAwsApi`) - Mengembalikan ID cluster DB Neptunus.
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`) - Memverifikasi jenis mesin dari cluster DB yang ditentukan. `neptune`
- `VerifyNeptuneStatus` (`aws:waitForAwsResourceProperty`) - Memverifikasi bahwa status cluster adalah `available`.
- `EnableNeptuneDbDeletionProtection` (`aws:executeAwsApi`) - Mengaktifkan perlindungan penghapusan pada cluster DB Neptunus.
- `VerifyNeptuneDbDeletionProtection` (`aws:assertAwsResourceProperty`) - Memverifikasi perlindungan penghapusan diaktifkan pada cluster DB.

### Keluaran

- `EnableNeptuneDbDeletionProtection`. `EnableNeptuneDbDeletionProtectionResponse` - Output dari operasi API.

## Amazon RDS

AWS Systems Manager Automation menyediakan runbook standar untuk Amazon Relational Database Service. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-CreateEncryptedRdsSnapshot](#)
- [AWS-CreateRdsSnapshot](#)
- [AWSConfigRemediation-DeleteRDSCluster](#)
- [AWSConfigRemediation-DeleteRDSClusterSnapshot](#)

- [AWSConfigRemediation-DeleteRDSInstance](#)
- [AWSConfigRemediation-DeleteRDSInstanceSnapshot](#)
- [AWSConfigRemediation-DisablePublicAccessToRDSInstance](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance](#)
- [AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance](#)
- [AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS](#)
- [AWSConfigRemediation-EnableMultiAZOnRDSInstance](#)
- [AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance](#)
- [AWSConfigRemediation-EnableRDSClusterDeletionProtection](#)
- [AWSConfigRemediation-EnableRDSInstanceBackup](#)
- [AWSConfigRemediation-EnableRDSInstanceDeletionProtection](#)
- [AWSConfigRemediation-ModifyRDSInstancePortNumber](#)
- [AWSSupport-ModifyRDSSnapshotPermission](#)
- [AWSPremiumSupport-PostgreSQLWorkloadReview](#)
- [AWS-RebootRdsInstance](#)
- [AWSSupport-ShareRDSSnapshot](#)
- [AWS-StartRdsInstance](#)
- [AWS-StartStopAuroraCluster](#)
- [AWS-StopRdsInstance](#)
- [AWSSupport-TroubleshootConnectivityToRDS](#)
- [AWSSupport-TroubleshootRDSIAMAuthentication](#)
- [AWSSupport-ValidateRdsNetworkConfiguration](#)

## **AWS-CreateEncryptedRdsSnapshot**

### Deskripsi

AWS-CreateEncryptedRdsSnapshotRunbook membuat snapshot terenkripsi dari instans Amazon Relational Database Service (Amazon RDS) yang tidak terenkripsi.

## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DB InstanceIdentifier

Jenis: String

Deskripsi: (Wajib) ID instans Amazon RDS yang ingin Anda buat snapshot.

- DB SnapshotIdentifier

Jenis: String

Deskripsi: (Opsional) Template nama untuk snapshot Amazon RDS. Template nama default adalah *DB InstanceIdentifier -yyyymmddhhmmss*.

- TerenkripsiDB SnapshotIdentifier

Jenis: String

Deskripsi: (Opsional) Nama untuk snapshot terenkripsi. Nama default adalah nilai yang Anda tentukan untuk DBSnapshotIdentifier parameter yang ditambahkan. -encrypted

- InstanceTags

Jenis: String

Deskripsi: (Opsional) Tag untuk ditambahkan ke instans DB. (Contoh: key=tagkey1, value = tagValue1; key=tagkey2, value = tagValue2) '

- KmsKeyId

Jenis: String

Default: alias/aws/rds

Deskripsi: (Opsional) ARN, ID kunci, atau alias kunci dari kunci terkelola pelanggan yang ingin Anda gunakan untuk mengenkripsi snapshot.

- SnapshotTags

Jenis: String

Deskripsi: (Opsional) Tag untuk ditambahkan ke snapshot. (Contoh: key=tagkey1, value = tagValue1; key=tagkey2, value = tagValue2) '

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- rds:AddTagsToResource
- rds:CopyDBSnapshot
- rds>CreateDBSnapshot
- rds>DeleteDBSnapshot
- rds:DescribeDBSnapshots

Langkah Dokumen

- aws:executeScript- Membuat snapshot dari instans DB yang Anda tentukan dalam DBInstanceIdentifier parameter.
- aws:executeScript- Memverifikasi snapshot yang dibuat pada langkah sebelumnya ada dan sedang. available

- `aws:executeScript`- Menyalin snapshot yang dibuat sebelumnya ke snapshot terenkripsi.
- `aws:executeScript`- Memverifikasi snapshot terenkripsi yang dibuat pada langkah sebelumnya ada.

Keluaran

`CopyRdsSnapshotToEncryptedRdsSnapshot`. `EncryptedSnapshotId` - ID snapshot Amazon RDS terenkripsi.

## AWS-CreateRdsSnapshot

Deskripsi

Buat snapshot Amazon Relational Database Service (Amazon RDS) untuk instans Amazon RDS.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `DB InstanceIdentifier`

Jenis: String

Deskripsi: (Wajib) InstanceId ID DB dari Instans RDS untuk membuat Snapshot dari.

- DB SnapshotIdentifier

Jenis: String

Deskripsi: (Opsional) SnapshotIdentifier ID DB snapshot RDS yang akan dibuat.

- InstanceTags

Jenis: String

Deskripsi: (Opsional) Tag untuk membuat misalnya.

- SnapshotTags

Jenis: String

Deskripsi: (Opsional) Tag yang akan dibuat untuk snapshot.

Langkah Dokumen

CreatordsSnapshot — Membuat snapshot RDS dan mengembalikan ID snapshot.

VerifyRDSnapshot — Memeriksa apakah snapshot yang dibuat pada langkah sebelumnya ada.

Keluaran

CreatordsSnapshot. SnapshotId — ID snapshot yang dibuat.

## **AWSConfigRemediation-DeleteRDSCluster**

Deskripsi

AWSConfigRemediation-DeleteRDSClusterRunbook menghapus kluster Amazon Relational Database Service (Amazon RDS) yang Anda tentukan. AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

## Otomatisasi

### Pemilik

### Amazon

### Platform

### Basis Data

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- DB ClusterId

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk cluster DB yang ingin Anda aktifkan perlindungan penghapusan.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds>DeleteDBCluster
- rds>DeleteDBInstance
- rds:DescribeDBClusters

### Langkah Dokumen



- `aws:executeScript`- Menghapus cluster DB yang Anda tentukan dalam `DBClusterId` parameter.

## AWSConfigRemediation-DeleteRDSClusterSnapshot

### Deskripsi

AWSConfigRemediation-DeleteRDSClusterSnapshotRunbook menghapus snapshot cluster Amazon Relational Database Service (Amazon RDS) yang diberikan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `DB ClusterSnapshotId`

Jenis: String

Deskripsi: (Diperlukan) Pengidentifikasi snapshot kluster Amazon RDS yang akan dihapus.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

### Langkah Dokumen

- `aws:branch`- Memeriksa apakah snapshot cluster dalam `available` keadaan. Jika tidak tersedia, alirannya berakhir.
- `aws:executeAwsApi`- Menghapus snapshot kluster Amazon RDS yang diberikan menggunakan pengidentifikasi snapshot cluster database (DB).
- `aws:executeScript`- Memverifikasi bahwa snapshot cluster Amazon RDS yang diberikan telah dihapus.

## AWSConfigRemediation-DeleteRDSInstance

### Deskripsi

AWSConfigRemediation-DeleteRDSInstanceRunbook menghapus instans Amazon Relational Database Service (Amazon RDS) yang Anda tentukan. Ketika Anda menghapus instance database (DB), semua backup otomatis untuk instance tersebut dihapus dan tidak dapat dipulihkan. Snapshot DB manual tidak dihapus. Jika instans DB yang ingin Anda hapus ada di `failed`, `incompatible-network`, atau `incompatible-restore` status, Anda harus mengatur `SkipFinalSnapshot` parameternya `true`.

#### Note

Jika instans DB yang ingin Anda hapus ada di cluster DB Amazon Aurora, runbook tidak akan menghapus instans DB jika itu adalah replika baca dan satu-satunya instance di cluster DB.

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

## Otomatisasi

### Pemilik

Amazon

### Platform

### Basis Data

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- DbResourceId

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda hapus.

- SkipFinalSnapshot

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika disetel ke `true`, snapshot akhir tidak dibuat sebelum instans DB dihapus.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBInstance`
- `rds:DescribeDBInstances`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan nama instans DB dari nilai yang Anda tentukan dalam `DbiResourceId` parameter.
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan dalam `SkipFinalSnapshot` parameter.
- `aws:executeAwsApi`- Menghapus instans DB yang Anda tentukan dalam `DbiResourceId` parameter.
- `aws:executeAwsApi`- Menghapus instans DB yang Anda tentukan dalam `DbiResourceId` parameter setelah snapshot akhir dibuat.
- `aws:assertAwsResourceProperty`- Memverifikasi instans DB telah dihapus.

## **AWSConfigRemediation-DeleteRDSInstanceSnapshot**

### Deskripsi

`AWSConfigRemediation-DeleteRDSInstanceSnapshotRunbook` menghapus snapshot instans Amazon Relational Database Service (Amazon RDS) yang Anda tentukan. Hanya snapshot di `available` negara bagian yang dihapus. Runbook ini tidak mendukung penghapusan snapshot dari instance database Amazon Aurora.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- DbSnapshotId

Jenis: String

Deskripsi: (Wajib) ID snapshot yang ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan status snapshot yang ditentukan dalam parameter. DbSnapshotId
- `aws:assertAwsResourceProperty`- Mengonfirmasi status snapshot adalah `available`.
- `aws:executeAwsApi`- Menghapus snapshot yang ditentukan dalam parameter. DbSnapshotId
- `aws:executeScript`- Memverifikasi snapshot telah dihapus.

## **AWSConfigRemediation-DisablePublicAccessToRDSInstance**

Deskripsi

AWSConfigRemediation-DisablePublicAccessToRDSInstanceRunbook menonaktifkan aksesibilitas publik untuk instans database (DB) Amazon Relational Database Service (Amazon RDS) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Basis Data

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- DbiResourceId

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda nonaktifkan aksesibilitas publik.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

### Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan pengidentifikasi instans DB dari pengidentifikasi sumber daya instans DB.
- `aws:assertAwsResourceProperty`- Memverifikasi instans DB dalam keadaan. AVAILABLE
- `aws:executeAwsApi`- Menonaktifkan aksesibilitas publik pada instans DB Anda.
- `aws:waitForAwsResourceProperty`- Menunggu instans DB berubah ke MODIFYING status.
- `aws:waitForAwsResourceProperty`- Menunggu instans DB berubah ke AVAILABLE status.
- `aws:assertAwsResourceProperty`- Mengonfirmasi aksesibilitas publik dinonaktifkan pada instans DB.

## **AWSConfigRemediation- EnableCopyTagsToSnapshotOnRDSCluster**

### Deskripsi

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSClusterRunbook mengaktifkan CopyTagsToSnapshot pengaturan pada kluster Amazon Relational Database Service (Amazon RDS) yang Anda tentukan. Mengaktifkan pengaturan ini menyalin semua tag dari cluster DB ke snapshot dari cluster DB. Defaultnya bukan untuk menyalinnya. AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `ApplyImmediately`

Jenis: Boolean

## Bawaan: salah

Deskripsi: (Opsional) Jika Anda menentukan `true` parameter ini, modifikasi dalam permintaan ini dan modifikasi yang tertunda diterapkan secara asinkron sesegera mungkin, terlepas dari `PreferredMaintenanceWindow` pengaturan untuk cluster DB.

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `DbClusterResourceId`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk cluster DB yang ingin Anda aktifkan `CopyTagsToSnapshot` pengaturannya.

## Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan pengidentifikasi cluster DB dari pengidentifikasi sumber daya cluster DB.
- `aws:assertAwsResourceProperty`- Mengonfirmasi cluster DB dalam `AVAILABLE` keadaan.
- `aws:executeAwsApi`- Mengaktifkan `CopyTagsToSnapshot` pengaturan pada cluster DB Anda.



- `aws:assertAwsResourceProperty`- Mengonfirmasi `CopyTagsToSnapshot` pengaturan diaktifkan pada cluster DB Anda.

## **AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance**

### Deskripsi

`AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstanceRunbook` mengaktifkan `CopyTagsToSnapshot` pengaturan pada instans Amazon Relational Database Service (Amazon RDS) yang Anda tentukan. Mengaktifkan pengaturan ini menyalin semua tag dari instans DB ke snapshot dari instans DB. Defaultnya bukan untuk menyalinnya. AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `ApplyImmediately`

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika Anda menentukan `true` parameter ini, modifikasi dalam permintaan ini dan modifikasi yang tertunda diterapkan secara asinkron sesegera mungkin, terlepas dari `PreferredMaintenanceWindow` pengaturan untuk instans DB.

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `DbiResourceId`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda aktifkan `CopyTagsToSnapshot` pengaturannya.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan pengidentifikasi instans DB dari pengidentifikasi sumber daya instans DB.
- `aws:assertAwsResourceProperty`- Mengonfirmasi instans DB dalam AVAILABLE keadaan.
- `aws:executeAwsApi`- Mengaktifkan `CopyTagsToSnapshot` pengaturan pada instans DB Anda.
- `aws:assertAwsResourceProperty`- Mengonfirmasi `CopyTagsToSnapshot` pengaturan diaktifkan pada instans DB Anda.

## **AWSConfigRemediation- EnableEnhancedMonitoringOnRDSInstance**

Deskripsi

`AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstanceRunbook` memungkinkan Enhanced Monitoring pada instans database Amazon RDS yang Anda tentukan. Untuk informasi tentang Pemantauan yang Ditingkatkan, lihat [Pemantauan yang Ditingkatkan](#) di Panduan Pengguna Amazon RDS.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `MonitoringInterval`

Jenis: Integer

Nilai yang valid: 1 | 5 | 10 | 15 | 30 | 60

Deskripsi: (Wajib) Interval dalam hitungan detik saat metrik Pemantauan yang Ditingkatkan dikumpulkan dari instans DB.

- `MonitoringRoleArn`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran IAM yang memungkinkan Amazon RDS mengirim metrik Pemantauan yang Ditingkatkan ke Log Amazon. CloudWatch

- ResourceId

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda aktifkan Enhanced Monitoring.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan pengidentifikasi instans DB dari pengidentifikasi sumber daya instans DB.
- `aws:assertAwsResourceProperty`- Mengonfirmasi Instans DB dalam AVAILABLE keadaan.
- `aws:executeAwsApi`- Mengaktifkan Pemantauan yang Ditingkatkan pada instans DB Anda.
- `aws:executeScript`- Mengonfirmasi bahwa Enhanced Monitoring diaktifkan pada instans DB Anda.

## **AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS**

Deskripsi

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSRunbook mengaktifkan AutoMinorVersionUpgrade pengaturan pada instance database Amazon RDS yang Anda tentukan. Mengaktifkan pengaturan ini berarti bahwa upgrade versi minor diterapkan secara otomatis ke instans DB selama jendela pemeliharaan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

## Otomatisasi

### Pemilik

Amazon

### Platform

### Basis Data

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `DbiResourceId`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda `AutoMinorVersionUpgrade` setelah.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

### Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan pengidentifikasi instans DB dari pengidentifikasi sumber daya instans DB.

- `aws:assertAwsResourceProperty`- Mengonfirmasi Instans DB dalam AVAILABLE keadaan.
- `aws:executeAwsApi`- Mengaktifkan `AutoMinorVersionUpgrade` pengaturan pada instans DB Anda.
- `aws:executeScript`- Mengonfirmasi bahwa `AutoMinorVersionUpgrade` pengaturan diaktifkan pada instans DB Anda.

## AWSConfigRemediation-EnableMultiAZOnRDSInstance

### Deskripsi

AWSConfigRemediation-EnableMultiAZOnRDSInstanceRunbook mengubah instans database (DB) Amazon Relational Database Service (Amazon RDS) Anda menjadi penerapan Multi-AZ. Mengubah pengaturan ini tidak mengakibatkan pemadaman listrik. Perubahan diterapkan selama jendela pemeliharaan berikutnya kecuali Anda menyetel `ApplyImmediately` parameternya `true`.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `ApplyImmediately`

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika Anda menentukan `true` parameter ini, modifikasi dalam permintaan ini dan modifikasi yang tertunda diterapkan secara asinkron sesegera mungkin, terlepas dari `PreferredMaintenanceWindow` pengaturan untuk instans DB.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- DbiResourceId

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi Wilayah AWS-unik dan tidak dapat diubah untuk instans DB untuk mengaktifkan pengaturan. MultiAZ

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- rds:DescribeDBInstances
- rds:ModifyDBInstance
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

Langkah Dokumen

- aws:executeAwsApi- Mengambil nama instans DB menggunakan nilai yang disediakan dalam DBInstanceId parameter.
- aws:executeAwsApi- Memverifikasi DBInstanceStatus adalahavailable.
- aws:branch- Memeriksa MultiAZ apakah sudah diatur ke true pada instans DB yang Anda tentukan dalam DbiResourceId parameter.
- aws:executeAwsApi- Mengubah MultiAZ pengaturan ke true instans DB yang Anda tentukan dalam DbiResourceId parameter.
- aws:assertAwsResourceProperty- Memverifikasi MultiAZ diatur ke true pada instans DB yang Anda tentukan dalam DbiResourceId parameter.

# AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

## Deskripsi

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstanceRunbook mengaktifkan Performance Insights pada instans Amazon RDS DB yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

## Basis Data

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- DbiResourceId

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda aktifkan Performance Insights.

- PerformanceInsightsKMS KeyId

Jenis: String



Default: `alias/aws/rds`

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN), ID kunci, atau alias kunci kunci AWS Key Management Service (AWS KMS) kunci terkelola pelanggan yang Anda inginkan Performance Insights gunakan untuk mengenkripsi semua data yang berpotensi sensitif. Jika Anda memasukkan alias kunci untuk parameter ini, awali nilai dengan `alias/`. Jika Anda tidak menentukan nilai untuk parameter ini, Kunci yang dikelola AWS digunakan.

- `PerformanceInsightsRetentionPeriod`

Jenis: Integer

Nilai yang valid: 7-731

Default: 7

Deskripsi: (Opsional) Jumlah hari Anda ingin menyimpan data Performance Insights.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan pengidentifikasi instans DB dari pengidentifikasi sumber daya instans DB.
- `aws:assertAwsResourceProperty`- Mengonfirmasi status instans DB adalah `available`.
- `aws:executeAwsApi`- Mengumpulkan ARN dari kunci yang dikelola pelanggan AWS KMS yang ditentukan dalam `PerformanceInsightsKMSKeyId` parameter.

- `aws:branch`- Memeriksa apakah nilai sudah ditetapkan ke `PerformanceInsightsKMSKeyId` properti instance DB.
- `aws:executeAwsApi`- Mengaktifkan Performance Insights pada instans DB yang Anda tentukan dalam parameter. `DbiResourceId`
- `aws:assertAwsResourceProperty`- Mengonfirmasi nilai yang ditentukan untuk `PerformanceInsightsKMSKeyId` parameter yang digunakan untuk mengaktifkan enkripsi untuk Performance Insights pada instans DB.
- `aws:assertAwsResourceProperty`- Mengonfirmasi Performance Insights diaktifkan pada instans DB.

## **AWSConfigRemediation-EnableRDSClusterDeletionProtection**

### Deskripsi

AWSConfigRemediation-EnableRDSClusterDeletionProtectionRunbook memungkinkan perlindungan penghapusan pada kluster Amazon Relational Database Service (Amazon RDS) yang Anda tentukan. AWS Config harus diaktifkan di Wilayah AWS tempat Anda menjalankan otomatisasi ini.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- ClusterId

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk cluster DB yang ingin Anda aktifkan perlindungan penghapusan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan nama cluster DB dari pengidentifikasi sumber daya cluster DB.
- `aws:assertAwsResourceProperty`- Memverifikasi status cluster DB adalah `available`.
- `aws:executeAwsApi`- Mengaktifkan perlindungan penghapusan pada cluster DB yang Anda tentukan dalam parameter. `ClusterId`
- `aws:assertAwsResourceProperty`- Memverifikasi perlindungan penghapusan telah diaktifkan pada cluster DB.

## **AWSConfigRemediation-EnableRDSInstanceBackup**

Deskripsi

`AWSConfigRemediation-EnableRDSInstanceBackup` memungkinkan pencadangan untuk instans database Amazon Relational Database Service (Amazon RDS) yang Anda tentukan. Runbook ini tidak mendukung pengaktifan cadangan untuk instance database Amazon Aurora.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `ApplyImmediately`

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika Anda menentukan `true` parameter ini, modifikasi dalam permintaan ini dan modifikasi yang tertunda diterapkan secara asinkron sesegera mungkin, terlepas dari `PreferredMaintenanceWindow` pengaturan untuk instans DB.

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `BackupRetentionPeriod`

Jenis: Integer

Nilai yang valid: 1-35

Deskripsi: (Wajib) Jumlah hari cadangan dipertahankan.

- `DbiResourceId`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda aktifkan pencadangan.

- `PreferredBackupWindow`

Jenis: String

Deskripsi: (Opsional) Rentang waktu harian (dalam UTC) selama pencadangan dibuat.

Batasan:

- Harus dalam format `hh24:mi-hh24:mi`
- Harus dalam Waktu Universal Terkoordinasi (UTC)
- Tidak boleh bertentangan dengan pemeliharaan jendela yang diinginkan
- Harus setidaknya 30 menit

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Langkah Dokumen

- `aws:executeScript`- Mengumpulkan pengidentifikasi instans DB dari pengidentifikasi sumber daya instans DB. Mengaktifkan backup untuk instans DB Anda. Mengonfirmasi backup diaktifkan pada instans DB.

## **AWSConfigRemediation-EnableRDSInstanceDeletionProtection**

Deskripsi

AWSConfigRemediation-EnableRDSInstanceDeletionProtectionRunbook memungkinkan perlindungan penghapusan pada instance database Amazon RDS yang Anda tentukan.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- ApplyImmediately

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika Anda menentukan `true` parameter ini, modifikasi dalam permintaan ini dan modifikasi yang tertunda diterapkan secara asinkron sesegera mungkin, terlepas dari `PreferredMaintenanceWindow` pengaturan untuk instans DB.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- DbInstanceResourceId

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda aktifkan perlindungan penghapusan.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan pengidentifikasi instans DB dari pengidentifikasi sumber daya instans DB.
- `aws:executeAwsApi`- Mengaktifkan perlindungan penghapusan pada instans DB Anda.
- `aws:assertAwsResourceProperty`- Mengonfirmasi perlindungan penghapusan diaktifkan pada instans DB.

# AWSConfigRemediation-ModifyRDSInstancePortNumber

## Deskripsi

AWSConfigRemediation-ModifyRDSInstancePortNumberRunbook memodifikasi nomor port tempat instans Amazon Relational Database Service (Amazon RDS) menerima koneksi. Menjalankan otomatisasi ini akan me-restart database.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

## Basis Data

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `PortNumber`

Jenis: String

Deskripsi: (Opsional) Nomor port yang Anda inginkan instans DB untuk menerima koneksi.

- `RDSDB InstanceResourceId`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang nomor port masuknya ingin Anda ubah.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

### Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan pengidentifikasi instans DB dari pengidentifikasi sumber daya instans DB.
- `aws:assertAwsResourceProperty`- Mengonfirmasi Instans DB dalam AVAILABLE keadaan.



- `aws:executeAwsApi`- Memodifikasi nomor port masuk tempat instans DB Anda menerima koneksi.
- `aws:waitForAwsResourceProperty`- Menunggu Instans DB berada dalam MODIFYING keadaan.
- `aws:waitForAwsResourceProperty`- Menunggu Instans DB berada dalam AVAILABLE keadaan.

## AWSSupport-ModifyRDSSnapshotPermission

### Deskripsi

AWSSupport-ModifyRDSSnapshotPermissionRunbook membantu Anda mengubah izin untuk beberapa snapshot Amazon Relational Database Service (Amazon RDS). Menggunakan runbook ini, Anda dapat membuat snapshot `Public` atau `Private` dan membagikannya dengan yang lain. Akun AWS Snapshot yang dienkripsi dengan kunci KMS default tidak dapat dibagikan dengan akun lain menggunakan runbook ini.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan

tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `AccountIds`

Jenis: `StringList`

Default: tidak ada

Deskripsi: (Opsional) ID akun yang ingin Anda bagikan snapshot. Parameter ini diperlukan jika Anda memasukkan No nilai `Private` parameter.

- `AccountPermissionOperation`

Jenis: `String`

Nilai yang valid: `tambahkan` | `hapus`

Default: tidak ada

Deskripsi: (Opsional) Jenis operasi yang harus dilakukan.

- `Privat`

Jenis: `String`

Nilai yang valid: `Ya` | `Tidak`

Deskripsi: (Wajib) Masukkan No nilai jika Anda ingin berbagi snapshot dengan akun tertentu.

- `SnapshotIdentifiers`

Jenis: `StringList`

Deskripsi: (Wajib) Nama-nama snapshot Amazon RDS yang izinnnya ingin Anda ubah.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`

- `rds:ModifyDBSnapshotAttribute`

## Langkah Dokumen

1. `aws:executeScript`- Memverifikasi ID snapshot yang disediakan dalam parameter. `SnapshotIdentifiers` Setelah memverifikasi ID, skrip memeriksa snapshot terenkripsi dan mengeluarkan daftar jika ada yang ditemukan.
2. `aws:branch`- Cabang otomatisasi berdasarkan nilai yang Anda masukkan untuk `Private` parameter.
3. `aws:executeScript`- Memodifikasi izin snapshot yang ditentukan untuk membagikannya dengan akun yang ditentukan.
4. `aws:executeScript`- Memodifikasi izin snapshot untuk mengubahnya dari ke. `Public` `Private`

## Keluaran

`ValidateSnapshots.EncryptedSnapshots`

`SharewithOtherAccounts.Hasil`

`MakePrivate.Hasil`

`MakePrivate.Commands`

## **AWSPremiumSupport-PostgreSQLWorkloadReview**

### Deskripsi

`AWSPremiumSupport-PostgreSQLWorkloadReviewRunbook` menangkap beberapa snapshot statistik penggunaan database PostgreSQL Amazon Relational Database Service (Amazon RDS) Anda. Statistik yang diambil diperlukan untuk ahli [Layanan AWS Support Proaktif](#) untuk melakukan tinjauan operasional. Statistik dikumpulkan menggunakan satu set skrip SQL dan shell kustom. Skrip ini diunduh ke instans Amazon Elastic Compute Cloud (Amazon EC2) sementara Akun AWS di instans Anda yang dibuat oleh runbook ini. Runbook mengharuskan Anda untuk memberikan kredensial menggunakan AWS Secrets Manager rahasia yang berisi pasangan nilai kunci nama pengguna dan kata sandi. Nama pengguna harus memiliki izin untuk menanyakan tampilan dan fungsi statistik PostgreSQL standar.

Runbook ini secara otomatis membuat AWS sumber daya berikut dalam Akun AWS menggunakan AWS CloudFormation tumpukan. Anda dapat memantau pembuatan tumpukan menggunakan AWS CloudFormation konsol.

- Virtual private cloud (VPC) dan instans Amazon EC2 diluncurkan di subnet pribadi VPC dengan konektivitas opsional ke internet menggunakan gateway NAT.
- Peran AWS Identity and Access Management (IAM) yang dilampirkan ke instans Amazon EC2 sementara dengan izin untuk mengambil nilai rahasia Secrets Manager. Peran ini juga memberikan izin untuk mengunggah file ke bucket Amazon Simple Storage Service (Amazon S3) pilihan Anda, dan secara opsional ke kasing. AWS Support
- Koneksi peering VPC untuk memungkinkan konektivitas antara instans DB Anda dan instans Amazon EC2 sementara.
- Systems Manager, Secrets Manager, dan endpoint Amazon S3 VPC yang dilampirkan ke VPC sementara.
- Jendela pemeliharaan dengan tugas terdaftar yang secara berkala memulai dan menghentikan instans Amazon EC2 sementara, menjalankan skrip pengumpulan data, dan mengunggah file ke bucket Amazon S3. Peran IAM juga dibuat untuk jendela pemeliharaan yang menyediakan izin untuk melakukan tugas terdaftar.

Saat runbook selesai, AWS CloudFormation tumpukan yang digunakan untuk membuat AWS sumber daya yang diperlukan akan dihapus dan laporan diunggah ke bucket Amazon S3 pilihan Anda, dan secara opsional merupakan kasus. AWS Support

#### Note

Secara default, volume root Amazon EBS dari instans Amazon EC2 sementara dipertahankan. Anda dapat mengganti opsi ini dengan menyetel `EbsVolumeDeleteOnTermination` parameter ke `true`.

#### Prasyarat

- Langganan Enterprise Support Runbook ini dan Diagnostik dan Ulasan Beban Kerja Layanan Proaktif memerlukan Langganan Dukungan Perusahaan. Sebelum menggunakan runbook ini, hubungi Technical Account Manager (TAM) atau Specialist TAM (STAM) Anda untuk mendapatkan petunjuk. Untuk informasi selengkapnya, lihat [Layanan AWS Support Proaktif](#).

- Akun dan Wilayah AWS Pastikan Anda belum mencapai jumlah maksimum instans Amazon EC2 atau VPC yang dapat Anda buat di akun dan Wilayah tempat Anda menggunakan runbook ini. Jika Anda perlu meminta kenaikan batas, lihat [formulir peningkatan batas Layanan](#).
- Konfigurasi basis data
  1. Basis data yang Anda tentukan dalam `DatabaseName` parameter harus memiliki `pg_stat_statements` ekstensi yang dikonfigurasi. Jika Anda belum mengkonfigurasi `pg_stat_statements` atau `shared_preload_libraries`, maka Anda harus mengedit nilai di Grup Parameter DB dan menerapkan perubahan. Perubahan pada parameter `shared_preload_libraries` mengharuskan Anda untuk me-reboot instans DB Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan grup parameter](#). Menambahkan `pg_stat_statements` ke `shared_preload_libraries` akan menambah beberapa overhead kinerja. Namun, ini berguna untuk melacak kinerja pernyataan individu. Untuk informasi selengkapnya tentang `pg_stat_statements` ekstensi, lihat dokumentasi [PostgreSQL](#). Jika Anda tidak mengonfigurasi `pg_stat_statements` ekstensi atau jika ekstensi tidak ada dalam database yang digunakan untuk pengumpulan statistik, analisis tingkat pernyataan tidak akan disajikan dalam tinjauan operasional.
  2. Pastikan bahwa `track_counts` dan `track_activities` parameter tidak dimatikan. Jika parameter ini dimatikan di Grup Parameter DB, tidak ada statistik yang berarti yang akan tersedia. Mengubah parameter ini akan mengharuskan Anda untuk me-reboot instans DB Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan parameter pada instans Amazon RDS for PostgreSQL DB](#).
  3. Jika `track_io_timing` parameter dimatikan, statistik level I/O tidak akan dimasukkan dalam tinjauan operasional. Mengubah `track_io_timing` akan mengharuskan Anda untuk me-reboot instans DB Anda dan akan dikenakan overhead kinerja tambahan tergantung pada beban kerja instans DB. Terlepas dari overhead kinerja untuk beban kerja kritis, parameter ini memberikan informasi berguna terkait waktu I/O per kueri.

Penagihan dan tagihan Anda Akun AWS akan dikenakan biaya untuk biaya yang terkait dengan instans Amazon EC2 sementara, volume Amazon EBS terkait, gateway NAT, dan data yang ditransfer saat otomatisasi ini berjalan. Secara default, runbook ini membuat instance `t3.micro` Amazon Linux 2 untuk mengumpulkan statistik. Runbook memulai dan menghentikan instance di antara langkah-langkah untuk mengurangi biaya.

Keamanan dan tata kelola data Runbook ini mengumpulkan statistik dengan menanyakan tampilan dan fungsi statistik [PostgreSQL](#). Pastikan kredensial yang disediakan dalam `SecretId` parameter hanya mengizinkan izin hanya-baca ke tampilan dan fungsi statistik. Sebagai bagian dari otomatisasi,

skrip koleksi diunggah ke bucket Amazon S3 Anda dan dapat ditemukan di. `s3://DOC-EXAMPLE-BUCKET/automation execution id/queries/`

Skrip ini mengumpulkan data yang digunakan oleh AWS Spesialis untuk meninjau indikator kinerja utama pada tingkat objek. Skrip mengumpulkan informasi seperti nama tabel, nama skema, dan nama indeks. Jika salah satu dari informasi ini berisi informasi sensitif seperti indikator pendapatan, nama pengguna, alamat email, atau informasi identitas pribadi lainnya, maka kami sarankan Anda menghentikan peninjauan beban kerja ini. Hubungi AWS TAM Anda untuk mendiskusikan pendekatan alternatif untuk tinjauan beban kerja.

Pastikan Anda memiliki persetujuan dan izin yang diperlukan untuk berbagi statistik dan metadata yang dikumpulkan oleh otomatisasi ini. AWS

Pertimbangan keamanan Jika Anda menyetel `UpdateRdsSecurityGroup` parameter nyayes, runbook akan memperbarui grup keamanan yang terkait dengan instans DB Anda untuk mengizinkan lalu lintas masuk dari alamat IP pribadi instans Amazon EC2 sementara.

Jika Anda menyetel `UpdateRdsRouteTable` parameter nyayes, runbook akan memperbarui tabel rute yang terkait dengan subnet yang dijalankan instans DB Anda untuk mengizinkan lalu lintas ke instans Amazon EC2 sementara melalui koneksi peering VPC.

Pembuatan pengguna Untuk mengizinkan skrip koleksi terhubung ke database Amazon RDS Anda, Anda harus menyiapkan pengguna dengan izin untuk membaca tampilan statistik. Maka Anda harus menyimpan kredensialnya di Secrets Manager. Kami merekomendasikan untuk membuat pengguna khusus baru untuk otomatisasi ini. Membuat pengguna terpisah memungkinkan Anda untuk mengaudit dan melacak aktivitas yang dilakukan oleh otomatisasi ini.

1. Buat pengguna baru.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. Pastikan bahwa pengguna ini hanya dapat membuat koneksi read-only.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. Tetapkan batas tingkat pengguna.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET work_mem=4096;"
```

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET statement_timeout=10000;"
```

```
psql -h <database_connection_endpoint> -p <database_port>
-U <admin_user> -c "ALTER USER <user_name> SET
idle_in_transaction_session_timeout=60000;"
```

4. Berikan `pg_monitor` izin kepada pengguna baru sehingga dapat mengakses statistik DB. (`pg_monitor` Perannya adalah anggota `pg_read_all_settings`, `pg_read_all_stats`, dan `pg_stat_scan_table`.)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

Izin ditambahkan ke profil instans Amazon EC2 sementara oleh Otomatisasi Systems Manager ini. Izin berikut ditambahkan ke peran IAM yang terkait dengan instans Amazon EC2 sementara. Kebijakan `AmazonSSMManagedInstanceCore` terkelola juga dikaitkan dengan peran IAM untuk memungkinkan instans Amazon EC2 dikelola oleh Systems Manager.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/automation execution id/*",
```

```

    "Effect": "Allow"
  },
  {
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:region:account id:secret:secret id",
    "Effect": "Allow"
  },
  {
    "Action": [
      "support:AddAttachmentsToSet",
      "support:AddCommunicationToCase",
      "support:DescribeCases"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
]
}

```

Izin ditambahkan ke jendela pemeliharaan sementara oleh Otomatisasi Systems Manager ini. Izin berikut secara otomatis ditambahkan ke peran IAM yang terkait dengan tugas Pemeliharaan Windows. Tugas Pemeliharaan Windows dimulai, berhenti, dan mengirim perintah ke instans Amazon EC2 sementara.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:GetAutomationExecution",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation",
        "ssm:GetCalendarState",
        "ssm:CancelCommand",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {

```



```

    "Action": [
      "ssm:SendCommand",
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ssm:StartAutomationExecution"
    ],
    "Resource": [
      "arn:aws:ec2:region:account id:instance/temporary instance id",
      "arn:aws:ssm:*:*:document/AWS-RunShellScript",
      "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:$DEFAULT",
      "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:$DEFAULT"
    ],
    "Effect": "Allow"
  },
  {
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "ssm.amazonaws.com"
      }
    },
    "Action": "iam:PassRole",
    "Resource": "*",
    "Effect": "Allow"
  }
]
}

```

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DB InstanceIdentifier

Jenis: String

Deskripsi: (Wajib) ID instans DB Anda.

- DatabaseName

Jenis: String

Deskripsi: (Wajib) Nama database yang dihosting pada instans DB Anda.

- SecretId

Jenis: String

Deskripsi: (Wajib) ARN rahasia Secrets Manager Anda yang berisi pasangan nilai kunci nama pengguna dan kata sandi. AWS CloudFormation Tumpukan membuat kebijakan IAM dengan izin untuk `GetSecretValue` operasi ke ARN ini. Kredensyal digunakan untuk memungkinkan instance sementara untuk mengumpulkan statistik database. Hubungi TAM atau STAM Anda untuk mendiskusikan izin minimum yang diperlukan.

- Akui

Jenis: String

Deskripsi: (Wajib) Masukkan **yes** jika Anda mengakui bahwa runbook ini akan membuat sumber daya sementara di akun Anda untuk mengumpulkan statistik dari instans DB Anda. Sebaiknya hubungi TAM atau STAM Anda sebelum menjalankan otomatisasi ini.

- SupportCase

Jenis: String

Deskripsi: (Opsional) Nomor AWS Support kasus yang disediakan oleh TAM atau STAM Anda. Jika disediakan, buku runbook memperbarui kasus dan melampirkan

data yang dikumpulkan. Opsi ini memerlukan instans Amazon EC2 sementara untuk memiliki konektivitas internet untuk mengakses titik akhir AWS Support API. Anda harus mengatur `AllowVpcInternetAccess` parameter ke `true`. Subjek kasus harus berisi frasa `AWSPremiumSupport-PostgreSQLWorkloadReview`.

- `S3 BucketName`

Jenis: String

Deskripsi: (Wajib) Nama bucket Amazon S3 di akun tempat Anda ingin mengunggah data yang dikumpulkan oleh otomatisasi. Pastikan kebijakan bucket tidak memberikan izin baca atau tulis yang tidak perlu kepada kepala sekolah yang tidak memerlukan akses ke konten bucket. Kami merekomendasikan untuk membuat bucket Amazon S3 sementara baru untuk tujuan otomatisasi ini. Runbook memberikan izin untuk operasi `s3:PutObject` API ke peran IAM yang dilampirkan ke instans Amazon EC2 sementara. File yang diunggah akan ditemukan di `s3://bucket name/automation execution id/`.

- `InstanceType`

Jenis: String

Deskripsi: (Opsional) Jenis instans Amazon EC2 sementara yang akan menjalankan skrip SQL dan shell kustom.

Nilai yang valid: `t2.micro` | `t2.small` | `t2.medium` | `t2.large` | `t3.micro` | `t3.small` | `t3.medium` | `t3.large`

Default: `t3.micro`

- `VpcCidr`

Jenis: String

Deskripsi: (Opsional) Rentang alamat IP dalam notasi CIDR untuk VPC baru (misalnya, `172.31.0.0/16`). Pastikan Anda memilih CIDR yang tidak tumpang tindih atau cocok dengan VPC yang ada dengan konektivitas ke instans DB Anda. VPC terkecil yang dapat Anda buat menggunakan subnet mask `/28`, dan VPC terbesar menggunakan subnet mask `/16`.

Standar: `172.31.0.0/16`

- `StackResourcesNamePrefix`

Jenis: String

Deskripsi: (Opsional) Awalan dan tag nama sumber daya AWS CloudFormation tumpukan.

Runbook membuat sumber daya AWS CloudFormation tumpukan menggunakan awalan ini sebagai bagian dari nama dan tag yang diterapkan ke sumber daya. Struktur untuk pasangan nilai kunci tag adalah. *StackResourcesNamePrefix*:`{{automation:EXECUTION_ID}}`

Default: `AWSPostgreSQLWorkloadReview`

- Jadwal

Jenis: String

Deskripsi: (Opsional) Jadwal jendela pemeliharaan. Menentukan seberapa sering jendela pemeliharaan menjalankan tugas. Nilai defaultnya adalah setiap1 hour.

Nilai yang valid: 15 menit | 30 menit | 1 jam | 2 jam | 4 jam | 6 jam | 12 jam | 1 hari | 2 hari | 4 hari

Default: 1 jam

- Durasi

Jenis: Integer

Deskripsi: (Opsional) Durasi maksimum, dalam hitungan menit, Anda ingin mengizinkan otomatisasi berjalan. Durasi maksimum yang didukung adalah 8.640 menit (6 hari). Nilai default adalah 4.320 menit (3 hari).

Nilai yang valid: 30-8640

Standar: 4320

- UpdateRdsRouteTable

Jenis: String

Deskripsi: (Opsional) Jika disetel ke `true`, buku runbook akan memperbarui tabel rute yang terkait dengan subnet yang dijalankan instans DB Anda. Rute IPv4 ditambahkan untuk merutekan lalu lintas ke alamat IPV4 pribadi instans Amazon EC2 sementara melalui koneksi peering VPC yang baru dibuat.

Nilai yang valid: benar/salah

Bawaan: salah

- AllowVpcInternetAccess

Jenis: String

Deskripsi: (Opsional) Jika disetel ke `true`, runbook akan membuat gateway NAT untuk menyediakan konektivitas internet ke instans Amazon EC2 sementara untuk berkomunikasi dengan AWS Support titik akhir API. Anda dapat membiarkan parameter ini `false` seolah-olah Anda hanya ingin runbook mengunggah output ke bucket Amazon S3 Anda.

Nilai yang valid: benar/salah

Bawaan: salah

- UpdateRdsSecurityGroup

Jenis: String

Deskripsi: (Opsional) Jika disetel ke `true`, runbook akan memperbarui grup keamanan yang terkait dengan instans DB Anda untuk mengizinkan lalu lintas dari alamat IP pribadi instans sementara.

Nilai yang valid: `false` | `true`

Bawaan: salah

- EbsVolumeDeleteOnTermination

Jenis: String

Deskripsi: (Opsional) Jika disetel ke `true`, volume root instans Amazon EC2 sementara akan dihapus setelah runbook selesai dan menghapus tumpukan. AWS CloudFormation

Nilai yang valid: `false` | `true`

Bawaan: salah

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudformation:CreateStack`

- `cloudformation>DeleteStack`

- `cloudformation:DescribeStackEvents`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateStack`
- `ec2:AcceptVpcPeeringConnection`
- `ec2:AllocateAddress`
- `ec2:AssociateRouteTable`
- `ec2:AssociateVpcCidrBlock`
- `ec2:AttachInternetGateway`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateEgressOnlyInternetGateway`
- `ec2:CreateInternetGateway`
- `ec2:CreateNatGateway`
- `ec2:CreateRoute`
- `ec2:CreateRouteTable`
- `ec2:CreateSecurityGroup`
- `ec2:CreateSubnet`
- `ec2:CreateTags`
- `ec2:CreateVpc`
- `ec2:CreateVpcEndpoint`
- `ec2:CreateVpcPeeringConnection`
- `ec2>DeleteEgressOnlyInternetGateway`
- `ec2>DeleteInternetGateway`
- `ec2>DeleteNatGateway`
- `ec2>DeleteRoute`
- `ec2>DeleteRouteTable`
- `ec2>DeleteSecurityGroup`

- ec2:DeleteSubnet
- ec2:DeleteTags
- ec2:DeleteVpc
- ec2:DeleteVpcEndpoints
- ec2:DescribeAddresses
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInternetGateways
- ec2:DescribeNatGateways
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DetachInternetGateway
- ec2:DisassociateRouteTable
- ec2:DisassociateVpcCidrBlock
- ec2:ModifySubnetAttribute
- ec2:ModifyVpcAttribute
- ec2:RebootInstances
- ec2:ReleaseAddress
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress
- ec2:StartInstances
- ec2:StopInstances

- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam>DeleteInstanceProfile`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:GetRolePolicy`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `iam:RemoveRoleFromInstanceProfile`
- `iam:TagPolicy`
- `iam:TagRole`
- `rds:DescribeDBInstances`
- `s3:GetAccountPublicAccessBlock`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:ListBucket`
- `ssm:AddTagsToResource`
- `ssm:CancelMaintenanceWindowExecution`
- `ssm:CreateDocument`
- `ssm:CreateMaintenanceWindow`



- `ssm:DeleteDocument`
- `ssm:DeleteMaintenanceWindow`
- `ssm:DeregisterTaskFromMaintenanceWindow`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeDocument`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeMaintenanceWindowExecutions`
- `ssm:GetCalendarState`
- `ssm:GetDocument`
- `ssm:GetMaintenanceWindowExecution`
- `ssm:GetParameters`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:ListTagsForResource`
- `ssm:RegisterTaskWithMaintenanceWindow`
- `ssm:RemoveTagsFromResource`
- `ssm:SendCommand`
- `support:AddAttachmentsToSet`
- `support:AddCommunicationToCase`
- `support:DescribeCases`

## Langkah Dokumen

1. `aws:assertAwsResourceProperty`- Mengonfirmasi instans DB dalam `available` keadaan.
2. `aws:executeAwsApi`- Mengumpulkan rincian tentang instans DB.
3. `aws:executeScript`- Memeriksa apakah bucket Amazon S3 yang ditentukan dalam `S3BucketName` mengizinkan izin akses baca atau tulis anonim, atau publik.
4. `aws:executeScript`- Mendapatkan konten AWS CloudFormation template dari lampiran Runbook Otomasi yang digunakan untuk membuat AWS sumber daya sementara di Anda Akun AWS.

5. `aws:createStack`- Menciptakan sumber daya AWS CloudFormation tumpukan.
6. `aws:waitForAwsResourceProperty`- Menunggu sampai instans Amazon EC2 yang dibuat oleh template AWS CloudFormation berjalan.
7. `aws:executeAwsApi`- Mendapatkan ID untuk instans Amazon EC2 sementara dan koneksi peering VPC yang dibuat oleh. AWS CloudFormation
8. `aws:executeAwsApi`- Mendapatkan alamat IP untuk instans Amazon EC2 sementara untuk mengonfigurasi konektivitas dengan instans DB Anda.
9. `aws:executeAwsApi`- Menandai volume Amazon EBS yang dilampirkan ke instans Amazon EC2 sementara.
10. `aws:waitForAwsResourceProperty`- Menunggu hingga instans Amazon EC2 sementara melewati pemeriksaan status.
11. `aws:waitForAwsResourceProperty`- Menunggu hingga instans Amazon EC2 sementara dikelola oleh Systems Manager. Jika langkah ini habis atau gagal, maka runbook me-reboot instance.
  - a. `aws:executeAwsApi`- Mem-boot ulang instans Amazon EC2 sementara jika langkah sebelumnya gagal atau habis waktu.
  - b. `aws:waitForAwsResourceProperty`- Menunggu hingga instans Amazon EC2 sementara dikelola oleh Systems Manager setelah reboot.
12. `aws:runCommand`- Menginstal persyaratan aplikasi kolektor metadata pada instans Amazon EC2 sementara.
13. `aws:runCommand`- Mengonfigurasi akses ke instans DB Anda dengan membuat file konfigurasi pada instans Amazon EC2 sementara.
14. `aws:executeAwsApi`- Membuat jendela pemeliharaan untuk menjalankan aplikasi kolektor metadata secara berkala menggunakan Run Command. Jendela pemeliharaan memulai dan menghentikan instance di antara perintah.
15. `aws:waitForAwsResourceProperty`- Menunggu sampai jendela pemeliharaan yang dibuat oleh AWS CloudFormation template siap.
16. `aws:executeAwsApi`- Mendapat ID untuk jendela pemeliharaan dan mengubah kalender yang dibuat oleh AWS CloudFormation.
17. `aws:sleep`- Menunggu hingga tanggal akhir jendela pemeliharaan.
18. `aws:executeAwsApi`- Mematikan jendela pemeliharaan.
19. `aws:executeScript`- Mendapatkan hasil tugas yang dijalankan selama jendela pemeliharaan.

20. `aws:waitForAwsResourceProperty`- Menunggu jendela pemeliharaan untuk menyelesaikan tugas terakhir sebelum melanjutkan.
21. `aws:branch`- Cabang alur kerja berdasarkan apakah Anda memberikan nilai untuk `SupportCase` parameter.
- `aws:changeInstanceState`- Memulai instans Amazon EC2 sementara dan menunggu pemeriksaan status lulus sebelum mengunggah laporan.
  - `aws:waitForAwsResourceProperty`- Menunggu hingga instans Amazon EC2 sementara dikelola oleh Systems Manager. Jika batas waktu langkah ini atau gagal, maka runbook me-reboot instance.
    - `aws:executeAwsApi`- Mem-boot ulang instans Amazon EC2 sementara jika langkah sebelumnya gagal atau habis waktu.
    - `aws:waitForAwsResourceProperty`- Menunggu hingga instans Amazon EC2 sementara dikelola oleh Systems Manager setelah reboot.
  - `aws:runCommand`- Melampirkan laporan metadata ke AWS Support kasus jika Anda memberikan nilai untuk parameter. `SupportCase` Skrip mengompres dan membagi laporan menjadi file 5 MB. Jumlah maksimum file yang dilampirkan skrip ke AWS Support kasing adalah 12.
22. `aws:changeInstanceState`- Menghentikan instans Amazon EC2 sementara jika AWS CloudFormation tumpukan gagal dihapus.
23. `aws:executeAwsApi`- Menjelaskan peristiwa AWS CloudFormation tumpukan jika runbook gagal membuat atau memperbarui AWS CloudFormation tumpukan.
24. `aws:waitForAwsResourceProperty`- Menunggu sampai AWS CloudFormation tumpukan berada dalam status terminal sebelum menghapus.
25. `aws:executeAwsApi`- Menghapus AWS CloudFormation tumpukan tidak termasuk jendela pemeliharaan. Volume Amazon EBS root yang terkait dengan instans Amazon EC2 sementara dipertahankan jika nilai parameter `EbsVolumeDeleteOnTermination` disetel ke `false`

## AWS-RebootRdsInstance

### Deskripsi

AWS-`RebootRdsInstance` Runbook me-reboot instans DB Amazon Relational Database Service (Amazon RDS) jika belum reboot.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Basis Data

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instans Amazon RDS DB yang ingin Anda reboot.

### Langkah Dokumen

RebootInstance - Reboot instance DB jika belum me-reboot.

WaitForAvailableState - Menunggu instans DB untuk menyelesaikan proses reboot.

### Keluaran

Otomatisasi ini tidak memiliki output.

## **AWSsupport - ShareRDSSnapshot**

### Deskripsi

AWSSupport-ShareRDSnapshotRunbook menyediakan solusi otomatis untuk prosedur yang diuraikan dalam artikel Pusat Pengetahuan [Bagaimana cara membagikan snapshot Amazon RDS DB terenkripsi dengan akun](#) lain? Jika snapshot Amazon Relational Database Service (Amazon RDS) dienkripsi menggunakan Kunci yang dikelola AWS default, Anda tidak dapat membagikan snapshot tersebut. Dalam hal ini, Anda harus menyalin snapshot menggunakan kunci yang dikelola pelanggan, dan kemudian membagikan snapshot dengan akun target. Otomatisasi ini melakukan langkah-langkah ini menggunakan nilai yang Anda tentukan dalam SnapshotName parameter, atau snapshot terbaru yang ditemukan untuk instans atau cluster Amazon RDS DB yang dipilih.

#### Note

Jika Anda tidak menentukan nilai untuk KMSKey parameter, otomatisasi akan membuat kunci terkelola AWS KMS pelanggan baru di akun Anda yang digunakan untuk mengenkripsi snapshot.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AccountIds

Jenis: StringList

Deskripsi: (Wajib) Daftar ID akun yang dipisahkan koma untuk berbagi snapshot.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Basis Data

Jenis: String

Deskripsi: (Wajib) Nama instans Amazon RDS DB atau cluster yang snapshotnya ingin Anda bagikan. Parameter ini opsional jika Anda menentukan nilai untuk SnapshotName parameter.

- KMSKey

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) lengkap dari kunci terkelola AWS KMS pelanggan yang digunakan untuk mengenkripsi snapshot.

- SnapshotName

Jenis: String

Deskripsi: (Opsional) ID cluster DB atau snapshot instance yang ingin Anda gunakan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:DescribeDBSnapshots`
- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

Ini AutomationAssumeRole membutuhkan tindakan berikut untuk berhasil memulai runbook untuk cluster DB.

- `ssm:StartAutomationExecution`

- `rds:DescribeDBClusters`
- `rds:DescribeDBClusterSnapshots`
- `rds:CopyDBClusterSnapshot`
- `rds:ModifyDBClusterSnapshotAttribute`

Peran IAM yang digunakan untuk menjalankan otomatisasi harus ditambahkan sebagai pengguna kunci untuk menggunakan kunci KMS yang ditentukan dalam parameter. `ARNKmsKey` Untuk informasi tentang menambahkan pengguna kunci ke kunci KMS, lihat [Mengubah kebijakan kunci](#) di Panduan AWS Key Management Service Pengembang.

Ini `AutomationAssumeRole` membutuhkan tindakan tambahan berikut untuk berhasil memulai runbook jika Anda tidak menentukan nilai untuk `KMSKey` parameter.

- `kms:CreateKey`
- `kms:ScheduleKeyDeletion`

#### Langkah Dokumen

1. `aws:executeScript`- Memeriksa apakah nilai disediakan untuk `KMSKey` parameter, dan membuat kunci yang dikelola AWS KMS pelanggan jika tidak ada nilai yang ditemukan.
2. `aws:branch`- Memeriksa apakah nilai disediakan untuk `SnapshotName` parameter, dan cabang yang sesuai.
3. `aws:executeAwsApi`- Memeriksa apakah snapshot yang disediakan berasal dari instance DB.
4. `aws:executeScript`- Memformat `SnapshotName` parameter menggantikan titik dua dengan tanda hubung.
5. `aws:executeAwsApi`- Menyalin snapshot menggunakan yang ditentukan `KMSKey`.
6. `aws:waitForAwsResourceProperty`- Menunggu operasi snapshot salin selesai.
7. `aws:executeAwsApi`- Berbagi snapshot baru dengan yang `AccountIds` ditentukan.
8. `aws:executeAwsApi`- Memeriksa apakah snapshot yang disediakan berasal dari cluster DB.
9. `aws:executeScript`- Memformat `SnapshotName` parameter menggantikan titik dua dengan tanda hubung.
10. `aws:executeAwsApi`- Menyalin snapshot menggunakan yang ditentukan `KMSKey`.
11. `aws:waitForAwsResourceProperty`- Menunggu operasi snapshot salin selesai.

12. `aws:executeAwsApi`- Berbagi snapshot baru dengan yang AccountIds ditentukan.
13. `aws:executeAwsApi`- Memeriksa apakah nilai yang disediakan untuk Database parameter adalah instance DB.
14. `aws:executeAwsApi`- Memeriksa apakah nilai yang disediakan untuk Database parameter adalah cluster DB.
15. `aws:executeAwsApi`- Mengambil daftar snapshot untuk yang ditentukan. Database
16. `aws:executeScript`- Menentukan snapshot terbaru yang tersedia dari daftar yang dirakit pada langkah sebelumnya.
17. `aws:executeAwsApi`- Menyalin snapshot instance DB menggunakan yang ditentukanKMSKey.
18. `aws:waitForAwsResourceProperty`- Menunggu operasi snapshot salin selesai.
19. `aws:executeAwsApi`- Berbagi snapshot baru dengan yang AccountIds ditentukan.
20. `aws:executeAwsApi`- Mengambil daftar snapshot untuk yang ditentukan. Database
21. `aws:executeScript`- Menentukan snapshot terbaru yang tersedia dari daftar yang dirakit pada langkah sebelumnya.
22. `aws:executeAwsApi`- Menyalin snapshot instance DB menggunakan yang ditentukanKMSKey.
23. `aws:waitForAwsResourceProperty`- Menunggu operasi snapshot salin selesai.
24. `aws:executeAwsApi`- Berbagi snapshot baru dengan yang AccountIds ditentukan.
25. `aws:executeScript`- Menghapus kunci yang dikelola AWS KMS pelanggan yang dibuat oleh otomatisasi jika Anda tidak menentukan nilai untuk KMSKey parameter dan otomatisasi gagal.

## AWS-StartRdsInstance

### Deskripsi

Mulai instans Amazon Relational Database Service (Amazon RDS).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon



## Platform

## Basis Data

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instans Amazon RDS untuk memulai.

## AWS-StartStopAuroraCluster

### Deskripsi

Runbook ini memulai atau menghentikan cluster Amazon Aurora.

#### Note

Untuk memulai cluster itu harus dalam `stopped` status. Untuk menghentikan cluster itu harus dalam `available` status. Runbook ini tidak dapat digunakan untuk memulai atau menghentikan cluster yang merupakan cluster Aurora Tanpa Server, cluster multi-master Aurora, bagian dari database global Aurora, atau cluster yang menggunakan kueri paralel Aurora.

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

## Pemilik

Amazon

Platform

Basis Data

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `ClusterName`

Jenis: String

Deskripsi: (Wajib) Nama cluster Aurora yang ingin Anda hentikan atau mulai.

- Tindakan

Jenis: String

Nilai yang valid: Mulai | Berhenti

Default: Mulai

Deskripsi: (Wajib) Nama cluster Aurora yang ingin Anda hentikan atau mulai.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `rds:DescribeDBClusters`
- `rds:StartDBCluster`
- `rds:StopDBCluster`

## Langkah Dokumen

- `aws:executeScript`- Memulai atau menghentikan cluster berdasarkan nilai yang Anda tentukan untuk.

## Keluaran

`StartStopAuroraCluster.ClusterName` - Nama cluster Aurora

`StartStopAuroraCluster.CurrentStatus` - Status cluster Aurora saat ini

`StartStopAuroraCluster.Message` - Detail otomatisasi

## AWS-StopRdsInstance

### Deskripsi

Hentikan instans Amazon Relational Database Service (Amazon RDS).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

### Basis Data

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan

tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instans Amazon RDS untuk berhenti.

## **AWSSupport-TroubleshootConnectivityToRDS**

### Deskripsi

AWSSupport-TroubleshootConnectivityToRDSRunbook mendiagnosis masalah konektivitas antara instans EC2 dan instance Amazon Relational Database Service. Otomatisasi memastikan instans DB tersedia, dan kemudian memeriksa aturan grup keamanan terkait, daftar kontrol akses jaringan (ACL jaringan), dan tabel rute untuk potensi masalah konektivitas.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `DB InstanceIdentifier`

Jenis: String

Deskripsi: (Wajib) ID instans DB untuk menguji konektivitas ke.

- `SourceInstance`

Jenis: String

Pola yang diizinkan: `^i- [a-z0-9] {8,17} $`

Deskripsi: (Wajib) ID instans EC2 untuk menguji konektivitas dari.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

Langkah Dokumen

- `aws:assertAwsResourceProperty`- Mengonfirmasi status instans DB adalah `available`.
- `aws:executeAwsApi`- Mendapat informasi tentang instans DB.
- `aws:executeAwsApi`- Mendapat informasi tentang ACL jaringan instans DB.
- `aws:executeAwsApi`- Mendapat contoh DB subnet CIDR.
- `aws:executeAwsApi`- Mendapat informasi tentang instans EC2.
- `aws:executeAwsApi`- Mendapat informasi tentang ACL jaringan instans EC2.
- `aws:executeAwsApi`- Mendapat informasi tentang kelompok keamanan yang terkait dengan instans EC2.

- `aws:executeAwsApi`- Mendapat informasi tentang kelompok keamanan yang terkait dengan instans DB.
- `aws:executeAwsApi`- Mendapat informasi tentang tabel rute yang terkait dengan instans EC2.
- `aws:executeAwsApi`- Mendapat informasi tentang tabel rute utama yang terkait dengan Amazon VPC untuk instans EC2.
- `aws:executeAwsApi`- Mendapat informasi tentang tabel rute yang terkait dengan instans DB.
- `aws:executeAwsApi`- Mendapat informasi tentang tabel rute utama yang terkait dengan Amazon VPC untuk instans DB.
- `aws:executeScript`- Mengevaluasi aturan kelompok keamanan.
- `aws:executeScript`- Mengevaluasi ACL jaringan.
- `aws:executeScript`- Mengevaluasi tabel rute.
- `aws:sleep`- Mengakhiri otomatisasi.

## Keluaran

`InstancePropertiesGetRDS.DB InstanceIdentifier` - Instans DB yang digunakan dalam otomatisasi.

`InstancePropertiesGetRDS.DB InstanceStatus` - Status saat ini dari `DBInstance`.

`evalSecurityGroupAturan. SecurityGroupEvaluation` - Hasil dari membandingkan aturan grup `SourceInstance` keamanan dengan aturan grup keamanan instans DB.

`evalNetworkAclAturan. NetworkAclEvaluation` - Hasil dari membandingkan ACL `SourceInstance` jaringan dengan ACL jaringan instance DB.

`evalRouteTableEntri. RouteTableEvaluation` - Hasil dari membandingkan tabel `SourceInstance` rute dengan rute instans DB.

## **AWSsupport-TroubleshootRDSIAMAuthentication**

### Deskripsi

`AWSsupport-TroubleshootRDSIAMAuthentication` ini membantu memecahkan masalah AWS Identity and Access Management (IAM) otentikasi untuk Amazon RDS untuk PostgreSQL, Amazon RDS untuk MySQL, Amazon RDS untuk MariaDB, Amazon Aurora PostgreSQL, dan Amazon Aurora MySQL instans. Gunakan runbook ini untuk memverifikasi konfigurasi yang diperlukan untuk autentikasi IAM dengan instans Amazon RDS atau Aurora Cluster.

Ini juga menyediakan langkah-langkah untuk memperbaiki masalah konektivitas ke Amazon RDS Instance atau Aurora Cluster.

**⚠ Important**

Runbook ini tidak mendukung Amazon RDS for Oracle atau Amazon RDS untuk Microsoft SQL Server.

**⚠ Important**

Jika Instans Amazon EC2 sumber disediakan dan Database target adalah Amazon RDS, otomatisasi akan `AWSSupport-TroubleshootConnectivityToRDS` dipanggil untuk memecahkan masalah konektivitas TCP. Output juga menyediakan perintah yang dapat Anda jalankan di instans Amazon EC2 atau mesin sumber untuk terhubung ke instans Amazon RDS menggunakan autentikasi IAM.

Bagaimana cara kerjanya?

Runbook ini terdiri dari enam langkah:

- Langkah 1: `ValidateInputs`: Memvalidasi input ke otomatisasi.
- Langkah 2: `branchOnSource EC2Disediakan`: Memverifikasi apakah ID Instans Amazon EC2 sumber disediakan dalam parameter input.
- Langkah 3: `ValidaterdsConnectivity`: Memvalidasi konektivitas Amazon RDS dari sumber instans Amazon EC2 jika disediakan.
- Langkah 4: `ValidaterdSiamAuthentication`: Memvalidasi jika fitur Autentikasi IAM diaktifkan.
- Langkah 5: `Validatelampolicies`: Memverifikasi apakah izin IAM yang diperlukan ada di pengguna/ peran IAM yang disediakan.
- Langkah 6: `GenerateReport`: Menghasilkan laporan hasil dari langkah-langkah yang dieksekusi sebelumnya.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

## Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- RDType

Jenis: String

Deskripsi: (Wajib): Pilih jenis database relasional yang Anda coba sambungkan dan autentikasi.

Nilai yang Diizinkan: Amazon RDS atau Amazon Aurora Cluster.

- DB InstanceIdentifier

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi Instance Basis Data Amazon RDS target atau Cluster Basis Data Aurora.

Pola yang Diizinkan:  $^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$$

Karakter Maks: 63

- SourceEc2 InstanceIdentifier

Tipe: `AWS::EC2::Instance::Id`

Deskripsi: (Opsional) ID Instans Amazon EC2 jika Anda terhubung ke Instans Basis Data Amazon RDS dari Instans Amazon EC2 yang berjalan di akun dan wilayah yang sama. Jangan tentukan



parameter ini jika sumbernya bukan instans Amazon EC2 atau jika jenis Amazon RDS target adalah Cluster Basis Data Aurora.

Default: ""

- DBIAM RoleName

Jenis: String

Deskripsi: (Opsional) Nama peran IAM yang digunakan untuk otentikasi berbasis IAM. Berikan hanya jika parameter tidak DBIAMUserName disediakan, jika tidak biarkan kosong. Entah DBIAMRoleName atau DBIAMUserName harus disediakan.

Pola yang Diizinkan: `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

Karakter Maks: 64

Default: ""

- DBIAM UserName

Jenis: String

Deskripsi: (Opsional) Nama pengguna IAM yang digunakan untuk otentikasi berbasis IAM. Berikan hanya jika DBIAMRoleName parameter tidak disediakan, jika tidak biarkan kosong. Entah DBIAMRoleName atau DBIAMUserName harus disediakan.

Pola yang Diizinkan: `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

Karakter Maks: 64

Default: ""

- DB UserName

Jenis: String

Deskripsi: (Opsional) Nama pengguna database dipetakan ke peran/pengguna IAM untuk otentikasi berbasis IAM dalam database. Opsi default \* mengevaluasi apakah `rds-db:connect` izin diizinkan untuk semua pengguna di Database.

Pola yang Diizinkan: `^[a-zA-Z0-9+=, .@*__-]{1,64}$`

**Karakter Maks: 64**

Default: \*

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- iam:GetPolicy
- iam:GetRole
- iam:GetUser
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies
- iam:SimulatePrincipalPolicy
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

Instruksi

1. Arahkan ke [AWSSupport-TroubleShootrdSiamAuthentication](#) di Konsol. AWS Systems Manager
2. Pilih Jalankan Otomasi
3. Untuk parameter input, masukkan yang berikut ini:
  - AutomationAssumeRole (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- RDS`type` (Diperlukan):

Pilih jenis Amazon RDS yang Anda coba sambungkan dan autentikasi. Pilih dari dua nilai yang diizinkan: Amazon RDS atau Amazon Aurora Cluster.

- DB `InstanceIdentifier` (Diperlukan):

Masukkan pengenal Instans Database Amazon RDS target atau Cluster Aurora yang Anda coba sambungkan dan gunakan kredensial IAM untuk autentikasi.

- SourceEc2 `InstanceIdentifier` (Opsional):

Berikan ID Instans Amazon EC2 jika Anda terhubung ke Instans Basis Data Amazon RDS dari Instans Amazon EC2 yang ada di akun dan wilayah yang sama. Biarkan kosong jika sumbernya bukan Amazon EC2 atau jika jenis Amazon RDS target adalah Aurora Cluster.

- DBIAM `RoleName` (Opsional):

Masukkan nama Peran IAM yang digunakan untuk otentikasi berbasis IAM. Berikan hanya jika tidak DBIAM`UserName` disediakan; jika tidak, biarkan kosong. Entah DBIAM`RoleName` atau DBIAM`UserName` harus disediakan.

- DBIAM `UserName` (Opsional):

Masukkan Pengguna IAM yang digunakan untuk otentikasi berbasis IAM. Berikan hanya jika tidak DBIAM`RoleName` disediakan, jika tidak, biarkan kosong. Entah DBIAM`RoleName` atau DBIAM`UserName` harus disediakan.

- DB `UserName` (Opsional):

Masukkan pengguna database yang dipetakan ke peran/pengguna IAM untuk otentikasi berbasis IAM dalam database. Opsi default \* digunakan untuk mengevaluasi; tidak ada yang disediakan di bidang ini.

### Input parameters

**SourceEc2InstanceIdentifier**  
(Optional) The Amazon EC2 Instance ID if you are connecting to the RDS DB instance from an EC2 instance running in the same account and region. Do not specify this parameter if the source is not an EC2 instance or if the target RDS type is an Aurora DB cluster.

Show interactive instance picker

↻

Name	Instance ID	State	Availability zone	Platform
There are no managed Instances in this account.				

We recommend using [Quick Setup](#) to configure your Instances for Systems Manager.

After configuring your Instances for Systems Manager, the Instances will be displayed here in a few minutes.

**AutomationAssumeRole**  
(Optional) The Amazon Resource Name (ARN) of the role that allows the Automation runbook to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your current IAM user permissions context to execute this runbook.

**RDSInstanceIdentifier**  
(Required) The identifier of the target Amazon RDS DB instance or Amazon Aurora DB cluster.

**DBIAMRoleName**  
(Optional) The IAM role name used for IAM-based authentication. Provide only if the parameter `DBIAMRoleName` is not provided, otherwise leave it empty. Either `DBIAMRoleName` or `DBIAMUserName` must be provided.

**RDSType**  
(Required) The type of Relational Database.

**DBIAMUserName**  
(Optional) The IAM user name used for IAM-based authentication. Provide only if the `DBIAMRoleName` parameter is not provided, otherwise leave it empty. Either `DBIAMRoleName` or `DBIAMUserName` must be provided.

**DBUserName**  
(Optional) The database user name mapped to an IAM role/user for IAM-based authentication within the database. The default option "" evaluates if the `rds-db:connect` permission is allowed for all users in the DB.

4. Pilih Jalankan.

5. Perhatikan bahwa otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- Langkah 1: ValidateInputs:

Memvalidasi input ke otomatisasi - SourceEC2InstanceIdentifier (opsional), DBInstanceIdentifier atau ClusterID, dan DBIAMRoleName atau DBIAMUserName. Ini memverifikasi apakah parameter input yang dimasukkan ada di akun dan wilayah Anda. Ini juga memverifikasi apakah pengguna memasukkan salah satu parameter IAM (misalnya, DBIAMRoleName atau DBIAMUserName). Selain itu, ia melakukan verifikasi lain, seperti jika Database yang disebutkan dalam status Tersedia.

- Langkah 2: branchOnSource EC2disediakan:

Memverifikasi apakah Sumber Amazon EC2 disediakan dalam parameter input dan Database adalah Amazon RDS. Jika ya, lanjutkan ke langkah 3. Jika tidak, ia melewati langkah 3, yaitu validasi Konektivitas Amazon EC2-Aman RDS dan melanjutkan ke langkah 4.

- Langkah 3: ValidaterdsConnectivity:

Jika Sumber Amazon EC2 disediakan dalam parameter input dan Database adalah Amazon RDS, langkah 2 memulai langkah 3. Pada langkah ini, otomatisasi AWSSupport-TroubleshootConnectivityToRDS akan dipanggil untuk memvalidasi konektivitas

Amazon RDS dari sumber Amazon EC2. Runbook otomatisasi anak `AWSSupport-TroubleshootConnectivityToRDS` memverifikasi apakah konfigurasi jaringan yang diperlukan (Amazon Virtual Private Cloud [Amazon VPC], Grup Keamanan, Daftar Kontrol Akses Jaringan [NACL], ketersediaan Amazon RDS) tersedia sehingga Anda dapat terhubung dari instans Amazon EC2 ke instans Amazon RDS.

- Langkah 4: `ValidateRDSSIAMAuthentication`:

Memvalidasi jika fitur Autentikasi IAM diaktifkan pada instans Amazon RDS atau Aurora Cluster.

- Langkah 5: `ValidateIAMPolicies`:

Memverifikasi jika izin IAM yang diperlukan ada di pengguna/peran IAM yang diteruskan untuk mengaktifkan kredensial IAM untuk mengautentikasi ke instans Amazon RDS untuk Pengguna Database yang ditentukan (jika ada).

- Langkah 6: `GenerateReport`:

Memperoleh semua informasi dari langkah sebelumnya dan mencetak hasil atau output dari setiap langkah. Ini juga mencantumkan langkah-langkah untuk merujuk dan melakukan, untuk terhubung ke instans Amazon RDS menggunakan kredensial IAM.

## 7. Saat otomatisasi selesai, tinjau bagian Output untuk hasil terperinci:

- Memeriksa izin Pengguna/Peran IAM untuk terhubung ke Database:

Memverifikasi jika izin IAM yang diperlukan ada di pengguna/peran IAM yang diteruskan untuk mengaktifkan kredensial IAM untuk mengautentikasi ke Instans Amazon RDS untuk Pengguna Database yang ditentukan (jika ada).

- Memeriksa Atribut Autentikasi Berbasis IAM untuk Database:

Memverifikasi jika fitur autentikasi IAM diaktifkan untuk Amazon RDS Database/Aurora Cluster yang ditentukan.

- Memeriksa Konektivitas dari Instans Amazon EC2 ke Instans Amazon RDS:

Memverifikasi apakah konfigurasi jaringan yang diperlukan (Amazon VPC, Grup Keamanan, NACL, ketersediaan Amazon RDS) sudah tersedia sehingga Anda dapat terhubung dari instans Amazon EC2 ke Instans Amazon RDS.

- Langkah selanjutnya:

Daftar perintah dan langkah untuk merujuk dan melakukan, untuk menyambung ke Instans Amazon RDS menggunakan kredensial IAM.

**Outputs**

ScriptExecutionId

Ze1d[REDACTED]ba4

Output

[Troubleshooting Results]

```

1. Checking the IAM user/role permissions to connect to database:
  ✓ [PASSED]: Found permission 'rds-db:connect' for the resource 'a[REDACTED]-db1'.

2. Checking IAM-based authentication attribute for the database:
  ✓ [PASSED]: IAM-based authentication attribute is enabled for the database 'a[REDACTED]-db1'.

3. Checking connectivity from the EC2 instance to RDS instance:
  ✓ [SKIPPED]: No Source EC2 instance provided.
Run these commands to troubleshoot connectivity to your aurora-mysql DB instance:
$ telnet a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com 3306
$ nc -vz a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com 3306

[Next Steps]

1. Verify if the database user exists and have the required permissions to connect to the database using IAM authentication:
- Connect to DB a[REDACTED]-db1 using admin/master db user.
- Run the following query/command in your database:
  SELECT user, plugin, host from mysql.user WHERE user LIKE '%<name of the DB user>%';
- From the output, verify if the user has the AWSAuthenticationPlugin.

2. Download the SSL bundle and connect to aurora-mysql database using IAM authentication by running the following commands:
$ wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
$ export DBPASS=$(aws rds generate-db-auth-token --hostname a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com --port 3306 --region us-[REDACTED]-2 --username <name of the DB user>)'
mysql --host=a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com --port=3306 --ssl-ca=global-bundle.pem --enable-cleartext-plugin --user=<name of the DB user> --password=$DBPASS

Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html

```

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

## AWSSupport-ValidateRdsNetworkConfiguration

### Deskripsi

AWSSupport-ValidateRdsNetworkConfigurationotomatisasi membantu menghindari status jaringan yang tidak kompatibel untuk Amazon Relational Database Service (Amazon RDS) /Amazon Aurora/Amazon DocumentDB yang ada sebelum Anda melakukan atau mengoperasikannya. ModifyDBInstance StartDBInstance Jika instance sudah dalam status jaringan yang tidak kompatibel, runbook akan memberikan alasannya.

### Bagaimana cara kerjanya?

Runbook ini menentukan apakah instans database Amazon RDS Anda akan masuk ke status jaringan yang tidak kompatibel, atau jika memiliki, tentukan alasannya dalam status jaringan yang tidak kompatibel.

Runbook melakukan pemeriksaan berikut terhadap instance database Amazon RDS Anda:

- Kuota Amazon Elastic Network Interface (ENI) per wilayah.
- Semua subnet dalam database Subnet Group ada.
- Ada cukup alamat IP gratis yang tersedia untuk subnet.
- (Untuk instans Amazon RDS yang dapat diakses publik) Pengaturan atribut VPC (dan).  
`enableDnsSupport enableDnsHostnames`

**⚠ Important**

Saat menggunakan dokumen ini terhadap kluster Amazon Aurora /Amazon DocumentDB, pastikan Anda menggunakannya sebagai gantinya. `DBInstanceIdentifier` `ClusterIdentifier` Jika tidak, dokumen akan gagal pada langkah pertama.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis data

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `rds:DescribeDBInstances`
- `servicequotas:GetServiceQuota`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeVpcAttribute`

- `ec2:DescribeSubnets`

Kebijakan sampel:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ValidateRdsNetwork",
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "servicequotas:GetServiceQuota",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets"
      ],
      "Resource": [
        "arn:aws:rds:{Region}:{Account}:db:{DbInstanceName}"
      ]
    }
  ]
}
```

### Instruksi

1. Arahkan ke [AWSSupport- ValidateRdsNetworkConfiguration](#) di AWS Systems Manager Konsol.
2. Pilih Jalankan Otomasi
3. Untuk parameter input, masukkan yang berikut ini:

- AutomationAssumeRole (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DB InstanceIdentifier (Diperlukan):

Masukkan Pengenal Instans Layanan Amazon Relational Database Service.



**Input parameters**

**AutomationAssumeRole**  
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Select an existing IAM Role

AutomationAssumeRoleSSM

**DBInstanceIdentifier**  
(Required) The Amazon Aurora or Amazon DocumentDB instance identifier.

my-rds-instance-01

#### 4. Pilih Jalankan.

#### 5. Perhatikan bahwa otomatisasi dimulai.

#### 6. Dokumen melakukan langkah-langkah berikut:

- Langkah 1: `assertRdsState`:

Memeriksa apakah pengidentifikasi instance yang disediakan ada dan memiliki salah satu status berikut: `available`, `stopped`, atau `incompatible-network`.

- Langkah 2: `gatherRdsInformation`:

Mengumpulkan informasi yang diperlukan tentang instans Amazon RDS untuk digunakan nanti dalam otomatisasi.

- Langkah 3: `checkEniQuota`:

Memeriksa kuota Amazon ENI yang tersedia saat ini untuk wilayah tersebut.

- Langkah 4: `validateVpcAttributes`:

Memvalidasi bahwa parameter DNS (`enableDnsSupport` dan `enableDnsHostnames`) dari VPC Amazon disetel ke `true` (atau tidak jika instans Amazon RDS). `PubliclyAccessible`

- Langkah 5: `validateSubnetAttributes`:

Memvalidasi keberadaan subnet di `DBSubnetGroup` dan memeriksa IP yang tersedia untuk setiap subnet.

- Langkah 6: `GenerateReport`:

Memperoleh semua informasi dari langkah sebelumnya dan mencetak hasil atau output dari setiap langkah. Ini juga mencantumkan langkah-langkah untuk merujuk dan melakukan, untuk terhubung ke instans Amazon RDS menggunakan kredensial IAM.

#### 7. Saat otomatisasi selesai, tinjau bagian Output untuk hasil terperinci:

Instans Amazon RDS dengan konfigurasi jaringan yang valid:

## ▼ Outputs

generateReport.Report

```
# AWS RDS Network Configuration Checks: aws-rds-01rr (available)
## ✅ No Issue(s) Found
```

```
### [Troubleshooting Results]
```

```
1. Checking ENI Quota for region the RDS Instance is in:
```

```
✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4997) is sufficient at the moment.
```

```
2. Checking VPC Attribute ('enableDnsHostname' & 'enableDnsSupport') settings:
```

```
✅ [PASSED] : [PASSED] Value for both VPC attributes ('enableDnsHostnames' and 'enableDnsSupport') is set to 'true'.
```

```
3. Checking if subnets required for RDS exists or not:
```

```
✅ [PASSED] : All subnets in 'ap-south-1b' availability zone exists.
```

```
4. Checking if Available IPs are sufficient per subnets that are required:
```

```
✅ [PASSED] : There are sufficient available IPs in 'ap-south-1b' availability zone.
```

```
5. Checking if other Availability zone satisfy Check No# 3 & 4:
```

```
* Availability Zone: ap-south-1c
```

```
  i. Subnet Existence Check: ✅ [PASSED]
```

```
  ii. Available IP Check: ✅ [PASSED]
```

```
* Availability Zone: ap-south-1a
```

```
  i. Subnet Existence Check: ✅ [PASSED]
```

```
  ii. Available IP Check: ✅ [PASSED]
```

```
### [Next Steps]
```

```
✅ All the checks has passed so the RDS Network configuration is correct.
```

```
Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
```

```
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.
```

Instans Amazon RDS dengan konfigurasi jaringan yang salah ( enableDnsHostnames atribut VPC disetel ke false):

## ▼ Outputs

```

generateReport.Report
# AWS RDS Network Configuration Checks: test-fail-sazrds-vpcattr (stopped)
### 🚫 Issue(s) Found!!!

### [Troubleshooting Results]
1. Checking ENI Quota for region the RDS Instance is in:
   ✔️ [PASSED] : Quota for Elastic Network Interface (ENIs) (4996) is sufficient at the moment.

2. Checking VPC Attribute ('enableDnsHostname' & 'enableDnsSupport') settings:
   ❌ [FAILED] : Value for 'enableDnsHostnames' VPC Attribute is 'false'.

3. Checking if subnets required for RDS exists or not:
   ✔️ [PASSED] : All subnets in 'ap-south-1b' availability zone exists.

4. Checking if Available IPs are sufficient per subnets that are required:
   ⚠️ [WARNING] : There are sufficient available IPs in 'ap-south-1b' availability zone, but it is recommended to have more than 9 IPs.

5. Checking if other Availability zone satisfy Check No# 3 & 4:
   * Availability Zone: ap-south-1a
     i. Subnet Existence Check: ✔️ [PASSED]
     ii. Available IP Check: ⚠️ [WARNING]

### [Next Steps]
o Please set the value of 'enableDnsHostnames' VPC attribute to 'true'.
  [+] View and update DNS attributes for your VPC: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-updating
o Please free up some IPs before performing Modify/Stop operation on the instance.
  [+] Learn why a subnet in your VPC has insufficient IP addresses : https://repost.aws/knowledge-center/subnet-insufficient-ips

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.

```

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

### AWSdokumentasi layanan

- [Bagaimana cara mengatasi masalah dengan database Amazon RDS yang berada dalam status jaringan yang tidak kompatibel?](#)
- [Bagaimana cara mengatasi masalah dengan instance Amazon DocumentDB yang berada dalam status jaringan yang tidak kompatibel?](#)

# Amazon Redshift

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Redshift. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWSConfigRemediation-DeleteRedshiftCluster](#)
- [AWSConfigRemediation-DisablePublicAccessToRedshiftCluster](#)
- [AWSConfigRemediation-EnableRedshiftClusterAuditLogging](#)
- [AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot](#)
- [AWSConfigRemediation-EnableRedshiftClusterEncryption](#)
- [AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting](#)
- [AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster](#)
- [AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings](#)
- [AWSConfigRemediation-ModifyRedshiftClusterNodeType](#)

## **AWSConfigRemediation-DeleteRedshiftCluster**

### Deskripsi

AWSConfigRemediation-DeleteRedshiftClusterRunbook menghapus cluster Amazon Redshift yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

## Basis Data

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `ClusterIdentifier`

Jenis: String

Deskripsi: (Wajib) ID cluster Amazon Redshift yang ingin Anda hapus.

- `SkipFinalClusterSnapshot`

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika disetel ke `false`, otomatisasi akan membuat snapshot sebelum menghapus klaster Amazon Redshift. Jika disetel ke `true`, snapshot klaster akhir tidak dibuat.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift>DeleteCluster`
- `redshift:DescribeClusters`

### Langkah Dokumen

- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan untuk `SkipFinalClusterSnapshot` parameter.

- `aws:executeAwsApi`- Menghapus cluster Amazon Redshift yang ditentukan dalam `ClusterIdentifier` parameter.
- `aws:assertAwsResourceProperty`- Memverifikasi cluster Amazon Redshift telah dihapus.

## **AWSConfigRemediation-DisablePublicAccessToRedshiftCluster**

### Deskripsi

AWSConfigRemediation-DisablePublicAccessToRedshiftClusterRunbook menonaktifkan aksesibilitas publik untuk klaster Amazon Redshift yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `ClusterIdentifier`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda nonaktifkan aksesibilitas publik.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

## Langkah Dokumen

- `aws:executeAwsApi`- Menonaktifkan aksesibilitas publik untuk cluster yang ditentukan dalam parameter. `ClusterIdentifier`
- `aws:waitForAwsResourceProperty`- Menunggu status cluster berubah menjadi `available`.
- `aws:assertAwsResourceProperty`- Mengonfirmasi pengaturan aksesibilitas publik dinonaktifkan di cluster.

# **AWSConfigRemediation-EnableRedshiftClusterAuditLogging**

## Deskripsi

AWSConfigRemediation-EnableRedshiftClusterAuditLoggingRunbook memungkinkan pencatatan audit untuk kluster Amazon Redshift yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `BucketName`

Jenis: String

Deskripsi: (Wajib) Nama bucket Amazon Simple Storage Service (Amazon S3) Simple Storage S3 yang ingin Anda unggah log.

- `ClusterIdentifier`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda aktifkan log audit.

- `S3 KeyPrefix`

Jenis: String

Deskripsi: (Opsional) Awalan kunci Amazon S3 (subfolder) yang ingin Anda unggah log.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

Langkah Dokumen



- `aws:branch`- Cabang berdasarkan apakah nilai ditentukan untuk `S3KeyPrefix` parameter.
- `aws:executeAwsApi`- Memungkinkan audit logging pada cluster yang ditentukan dalam `ClusterIdentifier` parameter.
- `aws:assertAwsResourceProperty`- Verifikasi audit logging diaktifkan pada cluster.

## **AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot**

### Deskripsi

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshotRunbook memungkinkan snapshot otomatis untuk cluster Amazon Redshift yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Basis Data

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `AutomatedSnapshotRetentionPeriod`

Jenis: Integer

Nilai yang valid: 1-35

Deskripsi: (Wajib) Jumlah hari snapshot otomatis dipertahankan.

- `ClusterIdentifier`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda aktifkan snapshot otomatis.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan snapshot otomatisasi pada cluster yang ditentukan dalam `ClusterIdentifier` parameter.
- `aws:waitForAwsResourceProperty`- Menunggu status cluster berubah menjadi `available`.
- `aws:executeScript`- Mengonfirmasi snapshot otomatis diaktifkan di cluster.

## **AWSConfigRemediation-EnableRedshiftClusterEncryption**

Deskripsi

`AWSConfigRemediation-EnableRedshiftClusterEncryptionRunbook` mengaktifkan enkripsi pada klaster Amazon Redshift yang Anda tentukan menggunakan kunci AWS Key Management Service terkelola pelanggan AWS KMS(). Runbook ini hanya boleh digunakan sebagai baseline untuk memastikan bahwa klaster Amazon Redshift Anda dienkripsi sesuai dengan praktik terbaik keamanan minimum yang disarankan. Kami merekomendasikan mengenkripsi beberapa cluster dengan kunci terkelola pelanggan yang berbeda. Runbook ini tidak dapat mengubah kunci

terkelola AWS KMS pelanggan yang digunakan pada kluster yang sudah dienkripsi. Untuk mengubah kunci terkelola AWS KMS pelanggan yang digunakan untuk mengenkripsi cluster, Anda harus terlebih dahulu menonaktifkan enkripsi pada cluster.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- ClusterIdentifier

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda aktifkan enkripsi.

- KmsKeyArn

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari kunci terkelola AWS KMS pelanggan yang ingin Anda gunakan untuk mengenkripsi data kluster.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

#### Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan enkripsi pada cluster Amazon Redshift yang ditentukan dalam parameter. `ClusterIdentifier`
- `aws:assertAwsResourceProperty`- Memverifikasi enkripsi telah diaktifkan pada cluster.

## **AWSConfigRemediation- EnableRedshiftClusterEnhancedVPCRouting**

### Deskripsi

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRoutingRunbook memungkinkan perutean virtual private cloud (VPC) yang disempurnakan untuk cluster Amazon Redshift yang Anda tentukan. Untuk informasi tentang perutean VPC yang disempurnakan, lihat Perutean [VPC Amazon Redshift yang disempurnakan di Panduan Manajemen Pergeseran Merah Amazon](#).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `ClusterIdentifier`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda aktifkan perutean VPC yang disempurnakan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan peningkatan routing VPC pada cluster yang ditentukan dalam parameter. `ClusterIdentifier`
- `assertAwsResourceProperty`- Mengonfirmasi peningkatan routing VPC diaktifkan pada cluster.

## **AWSConfigRemediation- EnforceSSLOnlyConnectionsToRedshiftCluster**

Deskripsi

`AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` Runbook memerlukan koneksi masuk untuk menggunakan SSL untuk cluster Amazon Redshift yang Anda tentukan.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `ClusterIdentifier`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda aktifkan perutean VPC yang disempurnakan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`

- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

### Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan rincian parameter dari cluster yang ditentukan dalam `ClusterIdentifier` parameter.
- `aws:executeAwsApi`- Mengaktifkan `require_ssl` pengaturan pada cluster yang ditentukan dalam `ClusterIdentifier` parameter.
- `aws:assertAwsResourceProperty`- Mengonfirmasi `require_ssl` pengaturan diaktifkan pada cluster.
- `aws:executeScript`- Memverifikasi `require_ssl` pengaturan untuk cluster.

## **AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings**

### Deskripsi

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettingsRunbook memodifikasi pengaturan pemeliharaan untuk klaster Amazon Redshift yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- `AllowVersionUpgrade`

Jenis: Boolean

Deskripsi: (Diperlukan) Jika disetel ke `true`, upgrade versi mayor diterapkan secara otomatis ke cluster selama jendela pemeliharaan.

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `AutomatedSnapshotRetentionPeriod`

Jenis: Integer

Nilai yang valid: 1-35

Deskripsi: (Wajib) Jumlah hari snapshot otomatis dipertahankan.

- `ClusterIdentifier`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda aktifkan perutean VPC yang disempurnakan.

- `PreferredMaintenanceWindow`

Jenis: String

Deskripsi: (Wajib) Rentang waktu mingguan (dalam UTC) selama pemeliharaan sistem dapat terjadi.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`



## Langkah Dokumen

- `aws:executeAwsApi`- Memodifikasi pengaturan pemeliharaan untuk cluster yang ditentukan dalam `ClusterIdentifier` parameter.
- `aws:assertAwsResourceProperty`- Mengonfirmasi pengaturan pemeliharaan yang dimodifikasi telah dikonfigurasi untuk cluster.

## **AWSConfigRemediation-ModifyRedshiftClusterNodeType**

### Deskripsi

AWSConfigRemediation-ModifyRedshiftClusterNodeTypeRunbook memodifikasi jenis node dan jumlah node untuk klaster Amazon Redshift yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Basis Data

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `Klasik`

Jenis: Boolean

Deskripsi: (Opsional) Jika disetel ke `true`, operasi pengubahan ukuran menggunakan proses pengubahan ukuran klasik.

- `ClusterIdentifier`

Jenis: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang tipe simpulnya ingin Anda modifikasi.

- `ClusterType`

Jenis: String

Nilai yang valid: simpul tunggal | multi-node

Deskripsi: (Wajib) Jenis cluster yang ingin Anda tetapkan ke cluster Anda.

- `NodeType`

Jenis: String

Nilai yang valid: `ds2.xlarge` | `ds2.8xlarge` | `dc1.large` | `dc1.8xlarge` | `dc2.large` | `dc2.8xlarge` | `ra3.4xlarge` | `ra3.16xlarge`

Deskripsi: (Wajib) Jenis node yang ingin Anda tetapkan ke cluster Anda.

- `NumberOfNodes`

Jenis: Integer

Nilai yang valid: 2-100

Deskripsi: (Opsional) Jumlah node yang ingin Anda tetapkan ke cluster Anda. Jika cluster Anda adalah `single-node` tipe, jangan tentukan nilai untuk parameter ini.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`

- `redshift:ResizeCluster`

### Langkah Dokumen

- `aws:executeScript`- Memodifikasi tipe node dan jumlah node untuk cluster yang ditentukan dalam `ClusterIdentifier` parameter.

## Amazon S3

AWS Systems Manager Automation menyediakan runbook standar untuk Amazon Simple Storage Service. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-ArchiveS3BucketToIntelligentTiering](#)
- [AWS-ConfigureS3BucketLogging](#)
- [AWS-ConfigureS3BucketVersioning](#)
- [AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock](#)
- [AWSConfigRemediation-ConfigureS3PublicAccessBlock](#)
- [AWS-CreateS3PolicyToExpireMultipartUploads](#)
- [AWS-DisableS3BucketPublicReadWrite](#)
- [AWS-EnableS3BucketEncryption](#)
- [AWS-EnableS3BucketKeys](#)
- [AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy](#)
- [AWSConfigRemediation-RestrictBucketSSLRequestsOnly](#)
- [AWSSupport-TroubleshootS3PublicRead](#)

## AWS-ArchiveS3BucketToIntelligentTiering

### Deskripsi

`AWS-ArchiveS3BucketToIntelligentTieringRunbook` membuat, atau menggantikan, konfigurasi tingkatan cerdas untuk bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) yang Anda tentukan.

## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket S3 yang ingin Anda buat konfigurasi tiering cerdas.

- ConfigurationId

Jenis: String

Deskripsi: (Wajib) ID untuk konfigurasi tingkatan cerdas. Ini bisa berupa ID konfigurasi baru, atau ID dari konfigurasi yang ada.

- NumberOfDaysToArchive

Jenis: String

Nilai yang valid: 90-730

Deskripsi: (Wajib) Jumlah hari berturut-turut setelah objek di bucket Anda memenuhi syarat untuk dialihkan ke tingkat Akses Arsip.

- `NumberOfDaysToDeepArchive`

Jenis: String

Nilai yang valid: 180-730

Deskripsi: (Wajib) Jumlah hari berturut-turut setelah objek di bucket Anda memenuhi syarat untuk dialihkan ke tingkat Akses Arsip Dalam.

- `S3Prefix`

Jenis: String

Deskripsi: (Opsional) Awalan nama kunci dari objek yang ingin Anda terapkan konfigurasinya.

- `Tag`

Jenis: MapList

Deskripsi: (Opsional) Metadata ditetapkan ke objek yang ingin Anda terapkan konfigurasi. Tag terdiri dari kunci dan nilai yang ditentukan pengguna.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

Langkah Dokumen

- `PutBucketIntelligentTieringConfiguration` (AWS:executeScript) - Membuat atau memperbarui konfigurasi Intelligent-Tiering Amazon S3 untuk bucket yang ditentukan.

- `VerifyBucketIntelligentTieringConfiguration`(aws: assertAwsResource Property) - Memverifikasi Konfigurasi Cerdas Bucket S3 diterapkan ke bucket yang ditentukan.

## AWS-ConfigureS3BucketLogging

### Deskripsi

Aktifkan logging pada bucket Amazon Simple Storage Service (Amazon S3).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `BucketName`

Jenis: String

Deskripsi: (Wajib) Nama Bucket Amazon S3 yang ingin Anda konfigurasi logging.

- `GrantedPermission`

Jenis: String

Nilai yang valid: FULL\_CONTROL | BACA | TULIS

Deskripsi: (Wajib) Izin pencatatan yang diberikan kepada penerima hibah untuk bucket.

- GranteeEmailAddress

Jenis: String

(Opsional) Alamat email penerima hibah.

- GranteeId

Jenis: String

Deskripsi: (Opsional) ID pengguna kanonik penerima hibah.

- GranteeType

Jenis: String

Nilai yang valid: CanonicalUser | AmazonCustomerByEmail | Grup

Keterangan: (Wajib) Jenis penerima hibah.

- GranteeUri

Jenis: String

Deskripsi: (Opsional) URI dari kelompok penerima hibah.

- TargetBucket

Jenis: String

Deskripsi: (Wajib) Menentukan bucket tempat Anda ingin Amazon S3 menyimpan log akses server. Anda dapat mengirimkan log Anda ke ember apa pun yang Anda miliki. Anda juga dapat mengonfigurasi beberapa bucket untuk mengirimkan lognya ke bucket target yang sama. Dalam hal ini Anda harus memilih yang berbeda TargetPrefix untuk setiap bucket sumber sehingga file log yang dikirim dapat dibedakan dengan kunci.

- TargetPrefix

Jenis: String

Default: /

Deskripsi: (Opsional) Menentukan awalan untuk kunci di mana file log akan disimpan.

## AWS-ConfigureS3BucketVersioning

### Deskripsi

Konfigurasi pembuatan versi untuk bucket Amazon Simple Storage Service (Amazon S3).

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket Amazon S3 yang ingin Anda konfigurasi untuk pembuatan versi.

- VersioningState

Jenis: String



Nilai yang valid: Diaktifkan | Ditangguhkan

Default: Diaktifkan

Deskripsi: (Opsional) Diterapkan ke `VersioningConfiguration` .`Status`. Saat disetel ke 'Diaktifkan', proses ini memungkinkan pembuatan versi untuk objek di bucket, semua objek yang ditambahkan ke bucket menerima ID versi unik. Saat disetel ke `Suspended`, proses ini menonaktifkan pembuatan versi untuk objek di ember. Semua objek yang ditambahkan ke bucket menerima ID `versinull`.

## AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Deskripsi

`AWSConfigRemediation-ConfigureS3BucketPublicAccessBlockRunbook` mengonfigurasi setelan blok akses publik Amazon Simple Storage Service (Amazon S3) untuk bucket Amazon S3 berdasarkan nilai yang Anda tentukan dalam parameter runbook.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- **BlockPublicAcls**

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Jika disetel ke `true`, Amazon S3 memblokir daftar kontrol akses publik (ACL) untuk bucket S3, dan objek yang disimpan dalam bucket S3 yang Anda tentukan dalam parameter.

BucketName

- **BlockPublicPolicy**

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Jika disetel ke `true`, Amazon S3 memblokir kebijakan bucket publik untuk bucket S3 yang Anda tentukan dalam parameter. BucketName

- **BucketName**

Jenis: String

Deskripsi: (Wajib) Nama bucket S3 yang ingin Anda konfigurasi.

- **IgnorePublicAcls**

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Jika disetel ke `true`, Amazon S3 mengabaikan semua ACL publik untuk bucket S3 yang Anda tentukan dalam parameter. BucketName

- **RestrictPublicBuckets**

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Jika disetel ke `true`, Amazon S3 membatasi kebijakan bucket publik untuk bucket S3 yang Anda tentukan dalam parameter. BucketName

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

#### Langkah Dokumen

- `aws:executeAwsApi`- Membuat atau memodifikasi `PublicAccessBlock` konfigurasi untuk bucket S3 yang ditentukan dalam parameter. `BucketName`
- `aws:executeScript`- Mengembalikan `PublicAccessBlock` konfigurasi untuk bucket S3 yang ditentukan dalam `BucketName` parameter, dan memverifikasi perubahan berhasil dibuat berdasarkan nilai yang ditentukan dalam parameter runbook.

## **AWSConfigRemediation-ConfigureS3PublicAccessBlock**

### Deskripsi

`AWSConfigRemediation-ConfigureS3PublicAccessBlockRunbook` mengonfigurasi setelan blok akses publik Akun AWS Amazon Simple Storage Service (Amazon S3) Simple Storage S3) berdasarkan nilai yang Anda tentukan dalam parameter runbook.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

## Linux, macOS, Windows

### Parameter

- AccountId

Jenis: String

Deskripsi: (Wajib) ID pemilik Akun AWS bucket S3 yang Anda konfigurasi.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- BlockPublicAcls

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Jika disetel ke `true`, Amazon S3 memblokir daftar kontrol akses publik (ACL) untuk bucket S3 yang dimiliki oleh yang Akun AWS Anda tentukan dalam parameter. AccountId

- BlockPublicPolicy

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Jika disetel ke `true`, Amazon S3 memblokir kebijakan bucket publik untuk bucket S3 yang dimiliki oleh yang Akun AWS Anda tentukan dalam parameter. AccountId

- IgnorePublicAcls

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Jika disetel ke `true`, Amazon S3 mengabaikan semua ACL publik untuk bucket S3 yang dimiliki oleh yang Anda tentukan dalam Akun AWS parameter. AccountId

- RestrictPublicBuckets

Jenis: Boolean

Default: betul

Deskripsi: (Opsional) Jika disetel ke `true`, Amazon S3 membatasi kebijakan bucket publik untuk bucket S3 yang dimiliki oleh yang Akun AWS Anda tentukan dalam parameter. `AccountId`

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

Langkah Dokumen

- `aws:executeAwsApi`- Membuat atau memodifikasi `PublicAccessBlock` konfigurasi untuk yang Akun AWS ditentukan dalam `AccountId` parameter.
- `aws:executeScript`- Mengembalikan `PublicAccessBlock` konfigurasi untuk yang Akun AWS ditentukan dalam `AccountId` parameter, dan memverifikasi perubahan berhasil dibuat berdasarkan nilai yang ditentukan dalam parameter runbook.

## AWS-CreateS3PolicyToExpireMultipartUploads

Deskripsi

`AWS-CreateS3PolicyToExpireMultipartUploadsRunbook` membuat kebijakan siklus hidup untuk bucket tertentu yang kedaluwarsa unggahan multi-bagian yang tidak lengkap yang sedang berlangsung setelah beberapa hari yang ditentukan. Runbook ini menggabungkan kebijakan siklus hidup baru dengan kebijakan bucket siklus hidup yang sudah ada yang sudah ada.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

## Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket S3 yang ingin Anda konfigurasi.

- DaysUntilExpire

Jenis: Integer

Deskripsi: (Wajib) Jumlah hari Amazon S3 menunggu sebelum menghapus semua bagian unggahan secara permanen.

- RuleId

Jenis: String

Deskripsi: (Wajib) ID yang digunakan untuk mengidentifikasi aturan bucket siklus hidup. Ini harus menjadi nilai yang unik.

- S3Prefix

Jenis: String

Deskripsi: (Opsional) Awalan nama kunci dari objek yang ingin Anda terapkan konfigurasinya.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

## Langkah Dokumen

- `ConfigureExpireMultipartUploads (AWS:executeScript)` - Mengkonfigurasi kebijakan siklus hidup untuk bucket.
- `VerifyExpireMultipartUploads (AWS:executeScript)` - Memverifikasi kebijakan siklus hidup telah dikonfigurasi untuk bucket.

## Keluaran

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

# AWS-DisableS3BucketPublicReadWrite

## Deskripsi

Gunakan Amazon Simple Storage Service (Amazon Block Public Access S3) untuk menonaktifkan akses baca dan tulis untuk bucket S3 publik. Untuk informasi selengkapnya, lihat [Menggunakan Amazon S3 Blokir Akses Publik](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

## [Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- S3 BucketName

Jenis: String

Deskripsi: (Wajib) Bucket S3 di mana Anda ingin membatasi akses.

## **AWS-EnableS3BucketEncryption**

Deskripsi

Mengonfigurasi enkripsi default untuk bucket Amazon Simple Storage Service (Amazon S3).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter



- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket S3 tempat Anda ingin mengenkripsi konten.

- Algoritma SSE

Jenis: String

Standar: AES256

Deskripsi: (Opsional) Algoritma enkripsi sisi server yang akan digunakan untuk enkripsi default.

## AWS-EnableS3BucketKeys

### Deskripsi

AWS-EnableS3BucketKeysRunbook mengaktifkan Kunci Bucket di bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) yang Anda tentukan. Kunci tingkat bucket ini membuat kunci data untuk objek baru selama siklus hidupnya. Jika Anda tidak menentukan nilai untuk KmsKeyId parameter, enkripsi sisi server menggunakan kunci terkelola Amazon S3 (SSE-S3) akan digunakan untuk konfigurasi enkripsi default.

#### Note

Kunci Bucket Amazon S3 tidak didukung untuk enkripsi sisi server dua lapis dengan AWS Key Management Service kunci () (DSSE-KMS).AWS KMS

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

## Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `BucketName`

Jenis: String

Deskripsi: (Wajib) Nama bucket S3 yang ingin Anda aktifkan Kunci Bucket.

- `KMS KeyId`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN), ID kunci, atau alias kunci dari AWS Key Management Service (AWS KMS) kunci terkelola pelanggan yang ingin Anda gunakan untuk enkripsi sisi server.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`

- `s3:PutEncryptionConfiguration`

### Langkah Dokumen

- `ChooseEncryptionType` (`aws:branch`) - Mengevaluasi nilai yang diberikan untuk `KmsKeyId` parameter untuk menentukan apakah SSE-S3 (AES256) atau SSE-KMS akan digunakan.
- `PutBucketKeysKMS` (`aws:executeAwsApi`) - Menyetel `BucketKeyEnabled` properti ke `true` bucket S3 yang ditentukan menggunakan yang ditentukan. `KmsKeyId`
- `PutBucketKeysAES256` (`aws:executeAwsApi`) - Menyetel `BucketKeyEnabled` properti ke `true` bucket S3 yang ditentukan dengan enkripsi AES256.
- `verifyS3 BucketKeysEnabled` (`aws:assertAwsResource Property`) - Memverifikasi bahwa Kunci Bucket diaktifkan pada bucket S3 target.

## **AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy**

### Deskripsi

`AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicyRunbook` menghapus pernyataan kebijakan utama yang memiliki wildcard (`Principal: *atauPrincipal: "AWS": *`) untuk Allow tindakan dari kebijakan bucket Amazon Simple Storage Service (Amazon S3). Pernyataan kebijakan dengan kondisi juga dihapus.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket Amazon S3 yang kebijakannya ingin Anda ubah.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

Langkah Dokumen

- `aws:executeScript`- Memodifikasi kebijakan bucket dan memverifikasi pernyataan kebijakan utama dengan wildcard telah dihapus dari bucket Amazon S3 yang Anda tentukan dalam parameter. BucketName

## **AWSConfigRemediation-RestrictBucketSSLRequestsOnly**

Deskripsi

AWSConfigRemediation-RestrictBucketSSLRequestsOnlyRunbook membuat pernyataan kebijakan bucket Amazon Simple Storage Service (Amazon S3) yang secara eksplisit menolak permintaan HTTP ke bucket Amazon S3 yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- BucketName

Jenis: String

Deskripsi: (Wajib) Nama bucket S3 yang ingin Anda tolak permintaan HTTP.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:DeleteBucketPolicy
- s3:GetBucketPolicy
- s3:PutEncryptionConfiguration
- s3:PutBucketPolicy

### Langkah Dokumen

- `aws:executeScript`- Membuat kebijakan bucket untuk bucket S3 yang ditentukan dalam `BucketName` parameter yang secara eksplisit menolak permintaan HTTP.

## AWSSupport-TroubleshootS3PublicRead

### Deskripsi

AWSSupport-TroubleshootS3PublicReadRunbook mendiagnosis masalah saat membaca objek dari bucket Simple Storage Service (Amazon S3) publik yang Anda tentukan dalam parameter. `S3BucketName` Subset pengaturan juga dianalisis untuk objek di bucket S3.

[Jalankan Otomasi ini \(konsol\)](#)

### Batasan

- Otomatisasi ini tidak memeriksa titik akses yang memungkinkan akses publik ke objek.
- Otomatisasi ini tidak mengevaluasi kunci kondisi dalam kebijakan bucket S3.
- Jika Anda menggunakan AWS Organizations, otomatisasi ini tidak mengevaluasi kebijakan kontrol layanan untuk mengonfirmasi bahwa akses ke Amazon S3 diizinkan.

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan

tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `CloudWatchLogGroupName`

Jenis: String

Deskripsi: (Opsional) Grup CloudWatch log Amazon Logs tempat Anda ingin mengirim output otomatisasi. Jika grup log tidak ditemukan yang cocok dengan nilai yang Anda tentukan, otomatisasi akan membuat grup log menggunakan nilai parameter ini. Periode retensi untuk grup log yang dibuat oleh otomatisasi ini adalah 14 hari.

- `CloudWatchLogStreamName`

Jenis: String

Deskripsi: (Opsional) Aliran CloudWatch log log tempat Anda ingin mengirim output otomatisasi. Jika aliran log tidak ditemukan yang cocok dengan nilai yang Anda tentukan, otomatisasi akan membuat aliran log menggunakan nilai parameter ini. Jika Anda tidak menentukan nilai untuk parameter ini, otomatisasi akan menggunakan `ExecutionId` untuk nama aliran log.

- `HttpGet`

Jenis: Boolean

Nilai yang valid: benar/salah

Default: betul

Deskripsi: (Opsional) Jika parameter ini diatur `true`, otomatisasi membuat permintaan HTTP sebagian ke objek yang `S3BucketName` Anda tentukan. Hanya byte pertama dari objek yang dikembalikan menggunakan header `Range` HTTP.

- `IgnoreBlockPublicAccess`

Jenis: Boolean

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Jika parameter ini disetel `true`, otomatisasi mengabaikan pengaturan blok akses publik dari bucket S3 yang Anda tentukan dalam parameter. `S3BucketName` Mengubah parameter ini dari nilai default tidak disarankan.

- **MaxObjects**

Jenis: Integer

Nilai yang valid: 1-25

Default: 5

Deskripsi: (Opsional) Jumlah objek yang akan dianalisis dalam bucket S3 yang Anda tentukan dalam S3BucketName parameter.

- **S3 BucketName**

Jenis: String

Deskripsi: (Wajib) Nama bucket S3 untuk memecahkan masalah.

- **S3 PrefixName**

Jenis: String

Deskripsi: (Opsional) Awalan nama kunci dari objek yang ingin Anda analisis di bucket S3 Anda. Untuk informasi selengkapnya, lihat [Kunci objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

- **StartAfter**

Jenis: String

Deskripsi: (Opsional) Nama kunci objek tempat Anda ingin otomatisasi mulai menganalisis objek di bucket S3 Anda.

- **ResourcePartition**

Tipe: String

Nilai yang valid: aws | aws-us-gov | aws-cn

Default: aws

Deskripsi: (Wajib) Partisi tempat bucket S3 Anda berada.

- **Bertele-tele**

Jenis: Boolean



Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Untuk mengembalikan informasi yang lebih rinci selama otomatisasi, atur parameter ini ke `true`. Hanya pesan peringatan dan kesalahan yang akan dikembalikan jika parameter diatur ke `false`.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

`logs:PutLogEvents` Izin `logs:CreateLogGroup` `logs:CreateLogStream`, dan hanya diperlukan jika Anda ingin otomatisasi mengirim data CloudWatch log ke Log.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:SimulateCustomPolicy",
        "iam:GetContextKeysForCustomPolicy",
        "s3:ListAllMyBuckets",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",
      "Effect": "Allow"
    }
  ]
}
```

```
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPolicy",
        "s3:GetBucketAcl"
      ],
      "Resource": "arn:aws:s3:::awsexamplebucket1",
      "Effect": "Allow"
    }
  ]
}
```

## Langkah Dokumen

- `aws:assertAwsResourceProperty`- Mengonfirmasi bucket S3 ada, dan dapat diakses.
- `aws:executeScript`- Mengembalikan lokasi bucket S3 dan ID pengguna kanonik Anda.
- `aws:executeScript`- Mengembalikan pengaturan blok akses publik untuk akun Anda dan bucket S3.
- `aws:assertAwsResourceProperty`- Mengonfirmasi pembayar bucket S3 diatur ke `BucketOwner` Jika `Requester Pays` diaktifkan pada bucket S3, otomatisasi berakhir.
- `aws:executeScript`- Mengembalikan status kebijakan bucket S3 dan menentukan apakah dianggap publik. Untuk informasi selengkapnya tentang bucket S3 publik, lihat [Arti “publik”](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
- `aws:executeAwsApi`- Mengembalikan kebijakan bucket S3.
- `aws:executeAwsApi`- Mengembalikan semua kunci konteks yang ditemukan dalam kebijakan bucket S3.
- `aws:assertAwsResourceProperty`- Mengonfirmasi apakah ada penolakan eksplisit dalam kebijakan bucket S3 untuk tindakan `GetObject` API.
- `aws:executeAwsApi`- Mengembalikan daftar kontrol akses (ACL) untuk bucket S3.
- `aws:executeScript`- Membuat grup CloudWatch log Log dan aliran log jika Anda menentukan nilai untuk `CloudWatchLogGroupName` parameter.

- `aws:executeScript`- Berdasarkan nilai yang Anda tentukan dalam parameter input runbook, mengevaluasi apakah setelah bucket S3 yang dikumpulkan selama otomatisasi mencegah objek diakses oleh publik. Skrip ini melakukan fungsi-fungsi berikut:
  - Mengevaluasi pengaturan blok akses publik
  - Mengembalikan objek dari bucket S3 Anda berdasarkan nilai yang Anda tentukan dalam `MaxObjects`, `S3PrefixName`, dan `StartAfter` parameter.
  - Mengembalikan kebijakan bucket S3 untuk mensimulasikan kebijakan IAM khusus untuk objek yang dikembalikan dari bucket S3 Anda.
  - Melakukan permintaan HTTP sebagian ke objek yang dikembalikan jika `HttpGet` parameter diatur `true`. Hanya byte pertama dari objek yang dikembalikan menggunakan header `Range HTTP`.
  - Memeriksa nama kunci objek yang dikembalikan untuk mengonfirmasi apakah itu berakhir dengan satu atau dua periode. Nama kunci objek yang berakhir dengan periode tidak dapat diunduh dari konsol Amazon S3.
  - Memeriksa apakah pemilik objek yang dikembalikan cocok dengan pemilik bucket S3.
  - Memeriksa apakah ACL objek memberikan `READ` atau `FULL_CONTROL` izin kepada pengguna anonim.
  - Mengembalikan tag yang terkait dengan objek.
  - Menggunakan kebijakan IAM yang disimulasikan untuk mengonfirmasi apakah ada penolakan eksplisit untuk objek ini dalam kebijakan bucket S3 untuk tindakan API. `GetObject`
  - Mengembalikan metadata objek untuk mengkonfirmasi bahwa kelas penyimpanan didukung.
  - Memeriksa setelah enkripsi sisi server objek untuk mengonfirmasi apakah objek dienkripsi menggunakan kunci yang dikelola pelanggan AWS Key Management Service (AWS KMS).

Keluaran

```
AnalyzeObjects.ember
```

```
AnalyzeObjects.objek
```

## SageMaker

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon SageMaker Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWS-DisableSageMakerNotebookRootAccess](#)

# AWS-DisableSageMakerNotebookRootAccess

## Deskripsi

AWS-DisableSageMakerNotebookRootAccessRunbook menonaktifkan akses root pada instance SageMaker notebook Amazon. Selama otomatisasi, instance notebook dihentikan untuk membuat perubahan yang diperlukan. SageMaker Instans notebook studio tidak didukung.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- NotebookInstanceName

Jenis: String

Deskripsi: (Wajib) Nama instance SageMaker notebook untuk menonaktifkan akses root pada.

- `StartInstanceAfterUpdate`

Jenis: Boolean

Default: `betul`

Deskripsi: (Opsional) Menentukan apakah instance notebook dimulai setelah menonaktifkan akses root. Pengaturan default untuk parameter ini adalah `true`. Jika disetel ke `true`, instance dimulai setelah akses root dinonaktifkan. Jika disetel ke `false`, instance dibiarkan dalam `stopped` status setelah akses root dinonaktifkan.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

### Langkah Dokumen

- `CheckNotebookInstanceStatus` (`aws:executeAwsApi`): Memeriksa status saat ini dari instance notebook.
- `StopOrUpdateNotebookInstance` (`aws:branch`): Cabang berdasarkan status instance notebook.
- `StopNotebookInstance` (`aws:executeAwsApi`): Memulai instance jika statusnya `stopped`.
- `WaitForInstanceToStop` (`aws:waitForAwsResourceProperty`): Memverifikasi instancinya `stopped`
- `UpdateNotebookInstance` (`aws:executeAwsApi`): Menonaktifkan akses root pada instance notebook.
- `WaitForNotebookUpdate` (`aws:waitForAwsResourceProperty`): Memverifikasi akses root telah dinonaktifkan dan instance memiliki `stopped` status.

- `ChooseInstanceStart` (`aws:branch`): Cabang berdasarkan apakah instance harus dimulai.
- `StartNotebookInstance` (`aws:executeAwsApi`): Memulai instance notebook.
- `VerifyNotebookInstanceStatus` (`aws:waitAwsResourceProperty`): Memverifikasi apakah instance `available` sebelum menonaktifkan akses root.
- `VerifyNotebookInstanceRootAccess` (`aws:assertAwsResourceProperty`): Memverifikasi setelah akses root instance notebook berhasil dinonaktifkan.

## Secrets Manager

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS Secrets Manager Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSConfigRemediation-DeleteSecret](#)
- [AWSConfigRemediation-RotateSecret](#)

## AWSConfigRemediation-DeleteSecret

### Deskripsi

`AWSConfigRemediation-DeleteSecretRunbook` menghapus rahasia dan semua versi yang disimpan di dalamnya. AWS Secrets Manager Anda dapat secara opsional menentukan jendela pemulihan di mana Anda dapat mengembalikan rahasia. Jika Anda tidak menentukan nilai untuk `RecoveryWindowInDays` parameter, operasi default menjadi 30 hari.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `RecoveryWindowInDays`

Jenis: Integer

Nilai yang valid: 7-30

Bawaan: 30

Deskripsi: (Opsional) Jumlah hari yang Anda dapat mengembalikan rahasia.

- `SecretId`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari rahasia yang ingin Anda hapus.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager>DeleteSecret`
- `secretsmanager:DescribeSecret`

## Langkah Dokumen

- `aws:executeAwsApi`- Menghapus rahasia yang Anda tentukan dalam `SecretId` parameter.

- `aws:executeScript`- Memverifikasi rahasia telah dijadwalkan untuk dihapus.

## AWSConfigRemediation-RotateSecret

### Deskripsi

AWSConfigRemediation-RotateSecretRunbook memutar rahasia yang disimpan di. AWS Secrets Manager

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `RotationInterval`

Jenis: Interval

Nilai yang valid: 1-365

Deskripsi: (Wajib) Jumlah hari antara rotasi rahasia.

- `RotationLambdaArn`



Jenis: String

Deskripsi: (Wajib) Nama Sumber Daya Amazon (ARN) dari AWS Lambda function yang dapat memutar rahasia.

- SecretId

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari rahasia yang ingin Anda putar.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

Langkah Dokumen

- `aws:executeAwsApi`- Memutar rahasia yang Anda tentukan dalam SecretId parameter.
- `aws:executeScript`- Verifikasi rotasi telah diaktifkan pada rahasia.

## Security Hub

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS Security Hub Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSConfigRemediation-EnableSecurityHub](#)

# AWSConfigRemediation-EnableSecurityHub

## Deskripsi

AWSConfigRemediation-EnableSecurityHubRunbook memungkinkan AWS Security Hub (Security Hub) untuk Akun AWS dan di Wilayah AWS mana Anda menjalankan otomatisasi. Untuk informasi tentang Security Hub, lihat [Apa itu AWS Security Hub?](#) dalam AWS Security Hub User Guide.

## [Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- EnableDefaultStandards

Jenis: Boolean

Default: betul

Deskripsi: (Diperlukan) Jika disetel ke `true`, standar keamanan default yang ditetapkan oleh Security Hub akan diaktifkan.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- securityhub:DescribeHub
- securityhub:EnableSecurityHub
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

### Langkah Dokumen

- aws:executeAwsApi- Mengaktifkan Security Hub di akun saat ini dan Wilayah.
- aws:executeAwsApi- Memverifikasi bahwa Security Hub telah diaktifkan.

## AWS Shield

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS Shield Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSPremiumSupport-DDoSResiliencyAssessment](#)

## AWSPremiumSupport-DDoSResiliencyAssessment

### Deskripsi

Runbook AWS Systems Manager otomatisasi membantu Anda memeriksa kerentanan DDoS dan konfigurasi sumber daya sesuai dengan AWS Shield Advanced perlindungan untuk Anda. AWSPremiumSupport-DDoSResiliencyAssessment Akun AWS Ini menyediakan laporan pengaturan konfigurasi untuk sumber daya yang rentan terhadap serangan Distributed Denial of Service (DDoS). Ini digunakan untuk mengumpulkan, menganalisis, dan menilai sumber daya berikut: Amazon Route 53, Amazon Load Balancers, CloudFront distribusi Amazon, AWS Global Accelerator dan IP AWS Elastis untuk pengaturan konfigurasinya sesuai dengan praktik terbaik yang direkomendasikan untuk Perlindungan. AWS Shield Advanced Laporan konfigurasi akhir tersedia di bucket Amazon S3 pilihan Anda sebagai file HTML.

## Bagaimana cara kerjanya?

Runbook ini berisi serangkaian pemeriksaan untuk berbagai jenis sumber daya yang diaktifkan untuk akses publik dan jika mereka memiliki perlindungan yang dikonfigurasi sesuai rekomendasi di Whitepaper Praktik [Terbaik AWS DDoS](#). Runbook melakukan hal berikut:

- Memeriksa apakah langganan AWS Shield Advanced diaktifkan.
- Jika diaktifkan, ia menemukan apakah ada sumber daya yang dilindungi Shield Advanced.
- Ia menemukan semua sumber daya global dan regional di Akun AWS dan memeriksa apakah ini dilindungi oleh Shield.
- Ini memerlukan parameter Jenis Sumber Daya untuk penilaian, nama bucket Amazon S3, dan ID Akun AWS bucket Amazon S3 (S3). BucketOwner
- Ini mengembalikan temuan sebagai laporan HTML yang disimpan di bucket Amazon S3 yang disediakan.

Parameter input `AssessmentType` memutuskan apakah pemeriksaan pada semua sumber daya akan dilakukan. Secara default, runbook memeriksa semua jenis sumber daya. Jika hanya `GlobalResources` atau `RegionalResources` parameter yang dipilih, runbook hanya melakukan pemeriksaan pada jenis sumber daya yang dipilih.

### Important

- Akses ke `AWSPremiumSupport` - \* runbook memerlukan langganan Enterprise atau Business Support. Untuk informasi selengkapnya, lihat [Bandingkan AWS Support Paket](#).
- Runbook ini membutuhkan ACTIVE [AWS Shield Advanced langganan](#).

## [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

## Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- AssessmentType

Jenis: String

Deskripsi: (Opsional) Menentukan jenis sumber daya yang akan dievaluasi untuk penilaian ketahanan DDoS. Secara default, runbook akan mengevaluasi sumber daya global dan regional. Untuk sumber daya regional, runbook menjelaskan semua penyeimbang beban Application (ALB) dan Network (NLB) serta semua grup Auto Scaling di /region Anda. Akun AWS

Nilai yang valid: ['Global Resources', 'Regional Resources', 'Global and Regional Resources']

Default: Sumber Daya Global dan Regional

- S3 BucketName

Tipe: AWS::S3::Bucket::Name

Deskripsi: (Wajib) Nama bucket Amazon S3 tempat laporan akan diunggah.

Pola yang Diizinkan: `^[0-9a-z][a-z0-9\-\.\.]{3,63}$`

- S3 BucketOwnerAccount

Jenis: String

Deskripsi: (Opsional) Akun AWS Yang memiliki ember Amazon S3. Harap tentukan parameter ini jika bucket Amazon S3 milik yang berbeda Akun AWS, jika tidak, Anda dapat membiarkan parameter ini kosong.

Pola yang Diizinkan: `^$|^[0-9]{12,13}$`

- S3 BucketOwnerRoleArn

Tipe: `AWS::IAM::Role::Arn`

Deskripsi: (Opsional) ARN peran IAM dengan izin untuk menjelaskan bucket Amazon S3 dan Akun AWS memblokir konfigurasi akses publik jika bucket berbeda. Akun AWS Jika parameter ini tidak ditentukan, runbook menggunakan `AutomationAssumeRole` atau pengguna IAM yang memulai runbook ini (jika tidak `AutomationAssumeRole` ditentukan). Silakan lihat bagian izin yang diperlukan di deskripsi buku runbook.

Pola yang Diizinkan: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam:[0-9]{12,13}:role/.*$`

- S3 BucketPrefix

Jenis: String

Deskripsi: (Opsional) Awalan untuk jalur di dalam Amazon S3 untuk menyimpan hasil.

Pola yang Diizinkan: `^[a-zA-Z0-9][-. /a-zA-Z0-9]{0,255}$|^$`

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `autoscaling:DescribeAutoScalingGroups`
- `cloudfront:ListDistributions`
- `ec2:DescribeAddresses`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeInstances`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeTargetGroups`
- `globalaccelerator:ListAccelerators`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `route53:ListHostedZones`

- `route53:GetHealthCheck`
- `shield:ListProtections`
- `shield:GetSubscriptionState`
- `shield:DescribeSubscription`
- `shield:DescribeEmergencyContactSettings`
- `shield:DescribeDRTAccess`
- `waf:GetWebACL`
- `waf:GetRateBasedRule`
- `wafv2:GetWebACL`
- `wafv2:GetWebACLForResource`
- `waf-regional:GetWebACLForResource`
- `waf-regional:GetWebACL`
- `s3:ListBucket`
- `s3:GetBucketAcl`
- `s3:GetBucketLocation`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketEncryption`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutObject`

### Contoh Kebijakan IAM untuk Otomasi Asumsikan Peran

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": "*"
    }
  ]
}
```

```
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketAcl",
      "s3:GetBucketLocation",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetBucketPolicyStatus",
      "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::<bucket-name>",
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::<bucket-name>/*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "autoscaling:DescribeAutoScalingGroups",
      "cloudfront:ListDistributions",
      "ec2:DescribeInstances",
      "ec2:DescribeAddresses",
      "ec2:DescribeNetworkAcls",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTargetGroups",
      "globalaccelerator:ListAccelerators",
      "iam:GetRole",
      "iam:ListAttachedRolePolicies",
      "route53:ListHostedZones",
      "route53:GetHealthCheck",
      "shield:ListProtections",
      "shield:GetSubscriptionState",
      "shield:DescribeSubscription",
      "shield:DescribeEmergencyContactSettings",
      "shield:DescribeDRTAccess",
      "waf:GetWebACL",
      "waf:GetRateBasedRule",
      "wafv2:GetWebACL",
      "wafv2:GetWebACLForResource",
```



```

        "waf-regional:GetWebACLForResource",
        "waf-regional:GetWebACL"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::123456789012:role/
<AutomationAssumeRole-Name>",
    "Effect": "Allow"
  }
]
}

```

## Instruksi

1. Arahkan ke [AWSPremiumSupport-DDoS ResiliencyAssessment](#) di Konsol. AWS Systems Manager
2. Pilih Jalankan Otomasi
3. Untuk parameter input, masukkan yang berikut ini:

- AutomationAssumeRole (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- AssessmentType (Opsional):

Menentukan jenis sumber daya untuk mengevaluasi penilaian ketahanan DDoS. Secara default, runbook mengevaluasi sumber daya global dan regional.

- S3 BucketName (Diperlukan):

Nama bucket Amazon S3 untuk menyimpan laporan penilaian dalam format HTML.

- S3 BucketOwner (Opsional):

Akun AWSID bucket Amazon S3 untuk verifikasi kepemilikan. Akun AWSID diperlukan jika laporan perlu dipublikasikan ke bucket Amazon S3 lintas akun dan opsional jika bucket Amazon S3 sama dengan inisiasi otomatisasi. Akun AWS

- S3 BucketPrefix (Opsional):

Awalan apa pun untuk jalur di dalam Amazon S3 untuk menyimpan hasilnya.

**Input parameters**

<p><b>AutomationAssumeRole</b>  <small>(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</small></p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <small>Select an existing IAM Role</small> </div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <small>ssm-admin</small> <span style="float: right;">✕</span>  <small>arn:aws:iam::[redacted]:role/ssm-admin</small> </div> <div style="text-align: right; margin-top: 5px;">↻</div> <p><b>S3BucketName</b>  <small>(Required) The name of the Amazon S3 bucket to save the assessment report in HTML format.</small></p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <small>Select an existing S3 Bucket</small> </div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <small>[redacted]</small> <span style="float: right;">✕</span> </div> <div style="text-align: right; margin-top: 5px;">↻</div> <p><b>S3BucketPrefix</b>  <small>(Optional) Any prefix for the path inside Amazon S3 for storing the results. Example path with prefix: S3://&lt;BucketName&gt;/&lt;Prefix&gt;</small></p> <div style="border: 1px solid #ccc; padding: 2px;"> <small>String</small> </div>	<p><b>ResourceType</b>  <small>(Required) Determines the type of resources to be evaluated for DDoS resiliency assessment. By default, the runbook will evaluate both global and regional resources.</small></p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <small>Global and Regional Resources</small> </div> <p><b>S3BucketOwner</b>  <small>(Required) The Account ID of the Amazon S3 bucket for ownership verification.</small></p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <small>[redacted]</small> </div>
--	---

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- CheckShieldAdvancedState:

Memeriksa apakah bucket Amazon S3 yang ditentukan dalam "S3BucketName" memungkinkan izin akses baca atau tulis anonim, atau publik, apakah bucket mengaktifkan enkripsi saat istirahat, dan jika Akun AWS ID yang disediakan di "S3BucketOwner" adalah pemilik bucket Amazon S3.

- S3BucketSecurityChecks:

Memeriksa apakah bucket Amazon S3 yang ditentukan dalam "S3BucketName" memungkinkan izin akses baca atau tulis anonim, atau publik, apakah bucket mengaktifkan enkripsi saat istirahat, dan jika Akun AWS ID yang disediakan di "S3BucketOwner" adalah pemilik bucket Amazon S3.

- BranchOnShieldAdvancedStatus:

Cabang mendokumentasikan langkah-langkah berdasarkan status AWS Shield Advanced Langganan dan/atau status Kepemilikan Bucket Amazon S3.

- ShieldAdvancedConfigurationReview:

Ulasan konfigurasi Shield Advanced untuk memastikan detail minimum yang diperlukan ada. Misalnya: Tim IAM Access for AWS Shield Response Team (SRT), Detail Daftar Kontak, dan Status Keterlibatan Proaktif SRT.

- `ListShieldAdvancedProtections`:

Daftar Sumber Daya yang Dilindungi Shield dan membuat grup sumber daya yang dilindungi untuk setiap layanan.

- `BranchOnResourceTypeAndCount`:

Cabang mendokumentasikan langkah-langkah berdasarkan nilai parameter Jenis Sumber Daya dan jumlah sumber daya global yang dilindungi Shield.

- `ReviewGlobalResources`:

Meninjau sumber daya Global yang dilindungi Shield Advanced seperti Zona yang Dihosting Route 53, CloudFront Distribusi, dan Akselerator Global.

- `BranchOnResourceType`:

Cabang mendokumentasikan langkah-langkah berdasarkan pilihan jenis Sumber Daya, jika Global, Regional, atau keduanya.

- `ReviewRegionalResources`:

Meninjau sumber daya Regional yang dilindungi Shield Advanced seperti Application Load Balancers, Network Load Balancer, Classic Load Balancers, Amazon Elastic Compute Cloud (Amazon EC2) Instans (IP Elastis).

- `SendReportToS3`:

Mengunggah detail Laporan Penilaian DDoS ke bucket Amazon S3.

## 7. Setelah selesai, URI untuk file HTML laporan penilaian disediakan di bucket Amazon S3:

Tautan Konsol S3 dan URI Amazon S3 untuk Laporan tentang keberhasilan eksekusi runbook

**▼ Outputs**

SendReportToS3.AssessmentReportS3ConsoleUrl  
[https://s3.console.aws.amazon.com/s3/object/ddos-readiness-review?region=us-east-1&prefix=ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24\\_04.08.37.html](https://s3.console.aws.amazon.com/s3/object/ddos-readiness-review?region=us-east-1&prefix=ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html)

SendReportToS3.AssessmentReportS3Uri  
[S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24\\_04.08.37.html](S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html)

---

**Execution status**

Overall status	All executed steps	# Succeeded
Success	9	9
# Failed	# Cancelled	# TimedOut
0	0	0

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

### AWSdokumentasi layanan

- [AWS Shield Advanced](#)

## Amazon SNS

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon Simple Notification Service. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-EnableSNSTopicDeliveryStatusLogging](#)
- [AWSConfigRemediation-EncryptSNSTopic](#)
- [AWS-PublishSNSNotification](#)

## AWS-EnableSNSTopicDeliveryStatusLogging

### Deskripsi

`AWS-EnableSNSTopicDeliveryStatusLoggingRunbook` mengonfigurasi pencatatan status pengiriman untuk titik akhir HTTP Amazon Data Firehose, LambdaPlatform application, atau Amazon Simple Queue Service (Amazon SQS). Ini memungkinkan Amazon SNS untuk mencatat peringatan yang gagal dan persentase sampel pemberitahuan peringatan yang berhasil ke Amazon CloudWatch. Jika pencatatan status pengiriman sudah dikonfigurasi untuk topik, buku runbook akan menggantikan konfigurasi yang ada dengan nilai baru yang Anda tentukan untuk parameter input.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `EndpointType`

Jenis: String

Nilai valid:

- HTTP
- Firehose
- Lambda
- Aplikasi

- SQS

Deskripsi: (Wajib) Jenis titik akhir topik Amazon SNS yang ingin Anda log pesan pemberitahuan status pengiriman.

- TopicArn

Jenis: String

Deskripsi: (Wajib) ARN dari topik Amazon SNS yang ingin Anda konfigurasi pencatatan status pengiriman.

- SuccessFeedbackRoleArn

Jenis: String

Deskripsi: (Wajib) ARN dari peran IAM yang digunakan Amazon SNS untuk mengirim log agar pesan notifikasi berhasil. CloudWatch

- SuccessFeedbackSampleRate

Jenis: String

Nilai yang valid: 0-100

Deskripsi: (Wajib) Persentase pesan yang berhasil diambil sampel untuk topik Amazon SNS yang ditentukan.

- FailureFeedbackRoleArn

Jenis: String

Deskripsi: (Wajib) ARN dari peran IAM yang digunakan Amazon SNS untuk mengirim log untuk pesan pemberitahuan kegagalan. CloudWatch

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`

- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

### Langkah Dokumen

- `aws:executeAwsApi`- Menerapkan nilai untuk `SuccessFeedbackRoleArn` parameter ke topik Amazon SNS.
- `aws:executeAwsApi`- Menerapkan nilai untuk `SuccessFeedbackSampleRate` parameter ke topik Amazon SNS.
- `aws:executeAwsApi`- Menerapkan nilai untuk `FailureFeedbackRoleArn` parameter ke topik Amazon SNS.
- `aws:executeScript`- Mengonfirmasi pencatatan status pengiriman diaktifkan pada topik Amazon SNS.

### Keluaran

`VerifyDeliveryStatusLoggingEnabled`. `GetTopicAttributesResponse` - Respon dari operasi `GetTopicAttributes` API.

`VerifyDeliveryStatusLoggingEnabled`. `VerifyDeliveryStatusLoggingEnabled` - Pesan yang menunjukkan keberhasilan verifikasi pencatatan status pengiriman.

## **AWSConfigRemediation-EncryptSNSTopic**

### Deskripsi

`AWSConfigRemediation-EncryptSNSTopicRunbook` mengaktifkan enkripsi pada topik Amazon Simple Notification Service (Amazon SNS) yang Anda tentukan menggunakan kunci yang dikelola pelanggan AWS Key Management Service (AWS KMS). Runbook ini hanya boleh digunakan sebagai baseline untuk memastikan bahwa topik Amazon SNS Anda dienkripsi sesuai dengan praktik terbaik keamanan minimum yang disarankan. Sebaiknya enkripsi beberapa topik dengan kunci terkelola pelanggan yang berbeda.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `KmsKeyArn`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari kunci terkelola AWS KMS pelanggan yang ingin Anda gunakan untuk mengenkripsi topik Amazon SNS.

- `TopicArn`

Jenis: String

Deskripsi: (Wajib) ARN dari topik Amazon SNS yang ingin Anda enkripsi.

## Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

## Langkah Dokumen



- `aws:executeAwsApi`- Mengenkripsi topik Amazon SNS yang Anda tentukan dalam parameter. `TopicArn`
- `aws:assertAwsResourceProperty`- Mengonfirmasi enkripsi diaktifkan pada topik Amazon SNS.

## AWS-PublishSNSNotification

### Deskripsi

Publikasikan pemberitahuan ke Amazon SNS.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `Pesan`

Jenis: String

Deskripsi: (Wajib) Pesan untuk disertakan dalam notifikasi SNS.

- `TopicArn`

Jenis: String

Deskripsi: (Wajib) ARN dari topik SNS untuk mempublikasikan notifikasi ke.

## Amazon SQS

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Simple Queue Service (Amazon SQS). Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWS-EnableSQSEncryption](#)

## AWS-EnableSQSEncryption

Deskripsi

AWS-EnableSQSEncryptionRunbook memungkinkan enkripsi saat istirahat untuk antrian Amazon Simple Queue Service (Amazon SQS). Antrian Amazon SQS dapat dienkripsi dengan kunci terkelola Amazon SQS (SSE-SQS), atau dengan () kunci terkelola (SSE-KMS). AWS Key Management Service AWS KMS Kunci yang Anda tetapkan ke antrian harus memiliki kebijakan kunci yang menyertakan izin untuk semua kepala sekolah yang berwenang untuk menggunakan antrean. Dengan enkripsi diaktifkan, anonim SendMessage dan ReceiveMessage permintaan ke antrian terenkripsi ditolak.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- QueueUrl

Jenis: String

Deskripsi: (Wajib) URL antrian Amazon SQS yang ingin Anda aktifkan enkripsi.

- KmsKeyId

Jenis: String

Deskripsi: (Opsional) AWS KMS Kunci yang digunakan untuk enkripsi. Nilai ini dapat berupa pengidentifikasi unik global, ARN untuk alias atau kunci, atau nama alias yang diawali dengan "alias/". Anda juga dapat menggunakan kunci yang AWS dikelola dengan menentukan alias aws/sqs.

- KmsDataKeyReusePeriodSeconds

Jenis: String

Nilai yang valid: 60-86400

Default: 300

Deskripsi: (Opsional) Lamanya waktu, dalam hitungan detik, antrian Amazon SQS dapat menggunakan kembali kunci data untuk mengenkripsi atau mendekripsi pesan sebelum menelepon lagi. AWS KMS

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

### Langkah Dokumen

- `SelectKeyType` (`aws:branch`): Cabang berdasarkan kunci yang ditentukan.
- `PutAttributeSseKms` (`aws:executeAwsApi`) - Memperbarui antrian Amazon SQS untuk menggunakan AWS KMS kunci yang ditentukan untuk enkripsi.
- `PutAttributeSseSqs` (`aws:executeAwsApi`) - Memperbarui antrian Amazon SQS untuk menggunakan kunci default untuk enkripsi.
- `VerifySqsEncryptionKms` (`aws:assertAwsResource Properti`) - Memverifikasi enkripsi diaktifkan pada antrean Amazon SQS.
- `VerifySqsEncryptionDefault` (`aws:assertAwsResource Properti`) - Memverifikasi enkripsi diaktifkan pada antrean Amazon SQS.

## Step Functions

AWS Systems Manager Automation menyediakan runbook standar untuk AWS Step Functions (Step Functions). Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-EnableStepFunctionsStateMachineLogging](#)

## AWS-EnableStepFunctionsStateMachineLogging

### Deskripsi

`AWS-EnableStepFunctionsStateMachineLoggingRunbook` mengaktifkan atau memperbarui pencatatan pada mesin AWS Step Functions status yang Anda tentukan. Tingkat logging minimum harus diatur ke `ALL`, `ERROR`, atau `FATAL`.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Tingkat

Jenis: String

Nilai yang valid: SEMUA | KESALAHAN | FATAL

Deskripsi: (Wajib) URL antrian Amazon SQS yang ingin Anda aktifkan enkripsi.

- LogGroupArn

Jenis: String

Deskripsi: (Diperlukan) ARN dari grup CloudWatch log Amazon Logs yang ingin Anda kirim log mesin status.

- StateMachineArn

Jenis: String

Deskripsi: (Wajib) ARN dari mesin status yang Anda inginkan aktifkan masuk.

- IncludeExecutionData

Jenis: Boolean

Default: Salah

Deskripsi: (Opsional) Menentukan apakah data eksekusi disertakan dalam log.

- `TracingConfiguration`

Jenis: Boolean

Default: Salah

Deskripsi: (Opsional) Menentukan apakah AWS X-Ray penelusuran diaktifkan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `states:DescribeStateMachine`
- `states:UpdateStateMachine`

Langkah Dokumen

- `EnableStepFunctionsStateMachineLogging` (`aws:executeAwsApi`)- Memperbarui mesin negara yang ditentukan dengan konfigurasi logging yang ditentukan.
- `VerifyStepFunctionsStateMachineLoggingEnabled` (`aws:assertAwsResourceProperty`)- Memverifikasi logging diaktifkan untuk mesin status tertentu.

Keluaran

- `EnableStepFunctionsStateMachineLogging.Response` - Respon dari panggilan `UpdateStateMachine` API.

# Systems Manager

AWS Systems Manager Automation menyediakan runbook standar untuk Systems Manager. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWS-BulkDeleteAssociation](#)
- [AWS-BulkEditOpsItems](#)
- [AWS-BulkResolveOpsItems](#)
- [AWS-ConfigureMaintenanceWindows](#)
- [AWS-CreateManagedLinuxInstance](#)
- [AWS-CreateManagedWindowsInstance](#)
- [AWSConfigRemediation-EnableCWLoggingForSessionManager](#)
- [AWS-ExportOpsDataToS3](#)
- [AWS-ExportPatchReportToS3](#)
- [AWS-SetupInventory](#)
- [AWS-SetupManagedInstance](#)
- [AWS-SetupManagedRoleOnEC2Instance](#)
- [AWSSupport-TroubleshootManagedInstance](#)
- [AWSSupport-TroubleshootPatchManagerLinux](#)
- [AWSSupport-TroubleshootSessionManager](#)

## AWS-BulkDeleteAssociation

### Deskripsi

`AWS-BulkDeleteAssociation`Runbook membantu Anda menghapus hingga 50 asosiasi Systems Manager State Manager sekaligus.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

## Pemilik

Amazon

Platform

Linux, macOS, Windows

## Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `AssociationIds`

Jenis: StringList

Deskripsi: (Wajib) Daftar ID yang dipisahkan koma dari asosiasi yang ingin Anda hapus.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:DeleteAssociation`

Langkah Dokumen

- `aws:executeScript`- Menghapus asosiasi yang Anda tentukan dalam `AssociationIds` parameter.

## **AWS-BulkEditOpsItems**

Deskripsi



AWS-BulkEditOpsItemsRunbook membantu Anda mengedit status, tingkat keparahan, kategori, atau prioritas. AWS Systems Manager OpsItems Otomatisasi ini dapat mengedit maksimal 50 OpsItems sekaligus.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Kategori

Jenis: String

Nilai valid:

- Ketersediaan
- Biaya
- Tidak ada perubahan
- Performa
- Pemulihan
- Keamanan

Default: Tidak ada perubahan

Deskripsi: (Opsional) Kategori baru yang ingin Anda tentukan untuk diedit. OpsItems

- OpsItemIds

Jenis: StringList

Deskripsi: (Wajib) Daftar OpsItems ID yang dipisahkan koma yang ingin Anda edit (misalnya, OI-XXXXXXXXXX, OI-XXXXXXXXXX).

- Prioritas

Jenis: String

Nilai valid:

- Tidak ada perubahan
- 1
- 2
- 3
- 4
- 5

Default: Tidak ada perubahan

Deskripsi: (Opsional) Pentingnya diedit OpsItems dalam kaitannya dengan yang lain OpsItems dalam sistem.

- Kepelikan

Jenis: String

Nilai valid:

- Tidak ada perubahan
- 1
- 2
- 3
- 4

Default: Tidak ada perubahan

Deskripsi: (Opsional) Tingkat keparahan yang diedit. OpsItems

- WaitTimeBetweenEditsInSecs

Jenis: String

Nilai yang valid: 0.0-2.0

Default: 0.8

Deskripsi: (Opsional) Waktu otomatisasi menunggu antara memanggil UpdateOpsItems operasi.

- Status

Jenis: String

Nilai valid:

- InProgress
- Tidak ada perubahan
- Buka
- Diselesaikan

Default: Tidak ada perubahan

Deskripsi: (Opsional) Status baru yang diedit. OpsItems

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

Langkah Dokumen

- `aws:executeScript`- Mengedit yang OpsItems Anda tentukan dalam `OpsItemIds` parameter berdasarkan nilai yang Anda tentukan untuk `Category`, `PrioritySeverity`, dan `Status` parameter.

## AWS-BulkResolveOpsItems

### Deskripsi

`AWS-BulkResolveOpsItemsRunbook` menyelesaikan yang cocok dengan filter AWS Systems Manager OpsItems yang Anda tentukan. Anda juga dapat menentukan `OpsItemId` untuk ditambahkan ke diselesaikan OpsItems menggunakan `OpsInsightsId` parameter. Jika Anda menentukan nilai untuk `S3BucketName` parameter, ringkasan hasil akan dikirim ke bucket Amazon Simple Storage Service (Amazon S3). Untuk menerima pemberitahuan setelah ringkasan hasil dikirim ke bucket Amazon S3, tentukan nilai untuk parameter tersebut `SnsTopicArn`. Otomatisasi ini akan menyelesaikan maksimum 1.000 OpsItems sekaligus.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Filter

Jenis: String

Deskripsi: (Wajib) Pasangan kunci-nilai filter untuk mengembalikan yang ingin OpsItems Anda selesaikan. Misalnya, [{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]. Untuk mempelajari lebih lanjut tentang opsi yang tersedia untuk memfilter OpsItems respons, lihat [OpsItemFilters](#) di Referensi AWS Systems Manager API.

- OpsInsightId

Jenis: String

Deskripsi: (Opsional) Pengidentifikasi sumber daya terkait yang ingin Anda tambahkan untuk diselesaikan OpsItems.

- S3 BucketName

Jenis: String

Deskripsi: (Opsional) Nama bucket Amazon S3 yang ingin Anda kirim ringkasan hasilnya.

- SnsMessage

Jenis: String

Deskripsi: (Opsional) Pemberitahuan yang Anda inginkan untuk dikirim oleh Amazon Simple Notification Service (Amazon SNS) saat otomatisasi selesai.

- SnsTopicArn

Jenis: String

Deskripsi: (Opsional) ARN topik Amazon SNS yang ingin Anda beri tahu saat ringkasan hasil telah dikirim ke Amazon S3.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- s3:GetBucketAcl

- s3:PutObject

- `sns:Publish`
- `ssm:DescribeOpsItems`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

### Langkah Dokumen

- `aws:executeScript`- Mengumpulkan dan menyelesaikan OpsItems berdasarkan filter yang Anda tentukan. Jika Anda menentukan nilai untuk `OpsInsightId` parameter, nilai ditambahkan sebagai sumber daya terkait.
- `aws:executeScript`- Jika Anda menentukan nilai untuk `S3BucketName` parameter, ringkasan hasil kemudian dikirim ke bucket Amazon S3.
- `aws:executeScript`- Jika Anda menentukan nilai untuk `SnsTopicArn` parameter, pemberitahuan dikirim ke topik Amazon SNS setelah ringkasan hasil dikirim ke Amazon S3 termasuk `SnsMessage` nilai parameter jika ditentukan.

## AWS-ConfigureMaintenanceWindows

### Deskripsi

AWS-ConfigureMaintenanceWindowsRunbook membantu Anda mengaktifkan atau menonaktifkan beberapa jendela pemeliharaan Systems Manager.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- MaintenanceWindows

Jenis: StringList

Deskripsi: (Wajib) Daftar ID yang dipisahkan koma dari jendela pemeliharaan yang ingin Anda aktifkan atau nonaktifkan.

- MaintenanceWindowsStatus

Jenis: String

Nilai yang valid: "Benar" | "Salah"

Default: "Salah"

Deskripsi: (Wajib) Menentukan apakah jendela pemeliharaan diaktifkan atau dinonaktifkan. Tentukan "True" untuk mengaktifkan jendela pemeliharaan, dan "False" untuk menonaktifkannya.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:GetMaintenanceWindow
- ssm:UpdateMaintenanceWindow

## Langkah Dokumen

- aws:executeScript- Mengumpulkan status jendela pemeliharaan yang Anda tentukan dalam MaintenanceWindows parameter, dan mengaktifkan atau menonaktifkan jendela pemeliharaan.

# AWS-CreateManagedLinuxInstance

## Deskripsi

Buat instans EC2 untuk Linux yang dikonfigurasi untuk Systems Manager.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

## Amazon

## Platform

## Linux

## Parameter

- Amild

Jenis: String

Deskripsi: (Wajib) AMI ID yang akan digunakan untuk meluncurkan instance.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- GroupName

Jenis: String

Default: SSM SecurityGroupForLinuxInstances

Deskripsi: (Diperlukan) Nama grup keamanan untuk dibuat.

- HttpTokens



Jenis: String

Nilai yang valid: opsional | diperlukan

Default: opsional

Deskripsi: (Opsional) IMDSv2 menggunakan sesi yang didukung token. Tetapkan penggunaan token HTTP ke `optional` atau `required` untuk menentukan apakah IMDSv2 adalah opsional atau wajib.

- InstanceType

Jenis: String

Default: t2.medium

Deskripsi: (Wajib) Jenis instance yang akan diluncurkan. Defaultnya adalah t2.medium.

- KeyPairName

Jenis: String

Deskripsi: (Wajib) Pasangan kunci yang akan digunakan saat membuat instance.

- RemoteAccessCidr

Jenis: String

Default 0.0.0.0/0

Deskripsi: (Wajib) Membuat grup Keamanan dengan port untuk SSH (Rentang port 22) terbuka untuk IP yang ditentukan oleh CIDR (default adalah 0.0.0.0/0). Jika grup keamanan sudah ada, itu tidak akan diubah dan aturan tidak akan diubah.

- RoleName

Jenis: String

Default: SSM ManagedInstanceProfileRole

Deskripsi: (Diperlukan) Nama peran untuk membuat.

- StackName

Jenis: String

Default: `CreateManagedInstanceStack {{Automation:Execution_ID}}`

Deskripsi: (Opsional) Tentukan nama tumpukan yang digunakan oleh runbook ini

- SubnetId

Jenis: String

Default: Default

Deskripsi: (Wajib) Instance baru akan digunakan ke subnet ini atau di subnet default jika tidak ditentukan.

- VpcId

Jenis: String

Default: Default

Deskripsi: (Wajib) Instans baru akan diterapkan ke Amazon Virtual Private Cloud (Amazon VPC) ini atau di VPC Amazon default jika tidak ditentukan.

## AWS-CreateManagedWindowsInstance

Deskripsi

Buat instans EC2 untuk Windows Server yang dikonfigurasi untuk Systems Manager.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter

## Parameter

- **Amild**

Jenis: String

Default: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

Deskripsi: (Wajib) AMI ID yang akan digunakan untuk meluncurkan instance.

- **AutomationAssumeRole**

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- **GroupName**

Jenis: String

Default: `SSM SecurityGroupForLinuxInstances`

Deskripsi: (Diperlukan) Nama grup keamanan untuk dibuat.

- **HttpTokens**

Jenis: String

Nilai yang valid: `opsional` | `diperlukan`

Default: `opsional`

Deskripsi: (Opsional) IMDSv2 menggunakan sesi yang didukung token. Tetapkan penggunaan token HTTP ke `optional` atau `required` untuk menentukan apakah IMDSv2 adalah opsional atau wajib.

- **InstanceType**

Jenis: String

Default: `t2.medium`

Deskripsi: (Wajib) Jenis instance yang akan diluncurkan. Defaultnya adalah t2.medium.

- KeyPairName

Jenis: String

Deskripsi: (Wajib) Pasangan kunci yang akan digunakan saat membuat instance.

- RemoteAccessCidr

Jenis: String

Default 0.0.0.0/0

Deskripsi: (Wajib) Membuat grup keamanan dengan port untuk RDP (Rentang port 3389) terbuka untuk IP yang ditentukan oleh CIDR (default adalah 0.0.0.0/0). Jika grup keamanan sudah ada, itu tidak akan diubah dan aturan tidak akan diubah.

- RoleName

Jenis: String

Default: SSM ManagedInstanceProfileRole

Deskripsi: (Diperlukan) Nama peran untuk membuat.

- StackName

Jenis: String

Default: CreateManagedInstanceStack {{Automation:Execution\_ID}}

Deskripsi: (Opsional) Tentukan nama tumpukan yang digunakan oleh runbook ini

- SubnetId

Jenis: String

Default: Default

Deskripsi: (Wajib) Instance baru akan digunakan ke subnet ini atau di subnet default jika tidak ditentukan.

- VpcId

Jenis: String

Default: Default

Deskripsi: (Wajib) Instans baru akan diterapkan ke Amazon Virtual Private Cloud (Amazon VPC) ini atau di VPC Amazon default jika tidak ditentukan.

## **AWSConfigRemediation-EnableCWLoggingForSessionManager**

Deskripsi

AWSConfigRemediation-EnableCWLoggingForSessionManagerRunbook memungkinkan AWS Systems Manager sesi Session Manager (Session Manager) untuk menyimpan log keluaran ke grup log Amazon CloudWatch (CloudWatch).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- DestinationLogGroup

Jenis: String

Deskripsi: (Wajib) Nama grup CloudWatch log.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:UpdateDocument`
- `ssm:CreateDocument`
- `ssm:UpdateDefaultDocumentVersion`
- `ssm:DescribeDocument`

## Langkah Dokumen

- `aws:executeScript`- Menerima grup CloudWatch log untuk memperbarui dokumen yang menyimpan preferensi log keluaran sesi Manajer Sesi, atau membuatnya jika tidak ada.

## AWS - ExportOpsDataToS3

### Deskripsi

Runbook ini mengambil daftar OpsData ringkasan di AWS Systems Manager Explorer dan mengekspornya ke objek di bucket Amazon Simple Storage Service (Amazon S3) yang ditentukan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- columnFields

Jenis: StringList

Deskripsi: (Wajib) Kolom kolom untuk menulis ke file output.

- saringan

Jenis: String

Deskripsi: (Opsional) Filter untuk getOpsSummary permintaan.

- resultAttribute

Jenis: String

Deskripsi: (Opsional) Atribut hasil untuk getOpsSummary permintaan.

- s3 BucketName

Jenis: String

Deskripsi: (Wajib) Bucket S3 tempat Anda ingin mengunduh file output.

- snsSuccessMessage

Jenis: String

Deskripsi: (Opsional) Pesan untuk dikirim saat runbook selesai.

- snsTopicArn

Jenis: String

Deskripsi: (Wajib) Amazon Simple Notification Service (Amazon SNS) topik ARN untuk memberi

- syncName

Jenis: String

Deskripsi: (Opsional) Nama sinkronisasi data sumber daya.

## Langkah Dokumen

getOpsSummaryLangkah - Mengambil hingga 5.000 ringkasan operasi untuk diekspor dalam file CSV sekarang.

## Keluaran

OpsData objek — Jika runbook berjalan dengan sukses, Anda akan menemukan OpsData objek yang diekspor di bucket S3 target Anda.

# AWS-ExportPatchReportToS3

## Deskripsi

Runbook ini mengambil daftar data ringkasan tambalan dan detail tambalan di AWS Systems Manager Patch Manager dan mengekspornya ke file.csv dalam bucket Amazon Simple Storage Service (Amazon S3) yang ditentukan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

## Amazon

## Platform

Linux, macOS, Windows

## Parameter

- assumeRole

Jenis: String



Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang menjalankan dokumen ini.

- s3 BucketName

Jenis: String

Deskripsi: (Wajib) Bucket S3 tempat Anda ingin mengunduh file output.

- snsTopicArn

Jenis: String

Deskripsi: (Opsional) Tema Amazon Simple Notification Service (Amazon SNS) Nama Sumber Daya Amazon (ARN) untuk memberi tahu kapan unduhan selesai.

- snsSuccessMessage

Jenis: String

Deskripsi: (Opsional) Teks pesan yang akan dikirim saat runbook selesai.

- sasaran

Jenis: String

Deskripsi: (Wajib) ID instans atau karakter wildcard (\*) untuk menunjukkan apakah akan melaporkan data patch untuk instance tertentu atau untuk semua instance.

## Langkah Dokumen

ExportReportStep — Tindakan untuk langkah ini tergantung pada nilai `targets` parameter. Jika `targets` dalam format `instanceids=*`, langkah mengambil hingga 10.000 ringkasan patch untuk instance di akun Anda dan mengeksport data ke `file.csv`.

Jika `targets` dalam format `instanceids=<instance-id>`, langkah mengambil ringkasan tambalan dan semua tambalan untuk instance yang ditentukan di akun Anda dan mengeksportnya ke `file.csv`.

## Keluaran

PatchSummary/Patches object - Jika runbook berjalan dengan sukses, objek laporan patch yang diekspor diunduh ke bucket S3 target Anda.

## AWS-SetupInventory

### Deskripsi

Buat asosiasi Inventaris Systems Manager untuk satu atau beberapa instance terkelola. Sistem mengumpulkan metadata dari instans Anda sesuai dengan jadwal dalam asosiasi. Untuk informasi selengkapnya, lihat [AWS Systems Manager Inventaris](#).

### [Jalankan Otomasi ini \(konsol\)](#)

#### Jenis dokumen

#### Otomatisasi

#### Pemilik

#### Amazon

#### Platform

Linux, macOS, Windows

#### Parameter

- Aplikasi

Jenis: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan metadata tentang aplikasi yang diinstal.

- AssociatedDocName

Jenis: String

Default: AWS-GatherSoftwareInventory

Deskripsi: (Opsional) Nama runbook yang digunakan untuk mengumpulkan Inventaris dari instance terkelola.

- AssociationName

Jenis: String

Deskripsi: (Opsional) Nama untuk asosiasi Inventaris yang akan ditetapkan ke instance.

- AssocWaitTime

Jenis: String

Default: PT5M

Deskripsi: (Opsional) Jumlah waktu pengumpulan Inventaris harus berhenti sejenak ketika waktu mulai asosiasi Inventaris tercapai. Waktu menggunakan format ISO 8601.

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- AwsComponents

Jenis: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan metadata untuk AWS Komponen seperti. amazon-ssm-agent

- CustomInventory

Jenis: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan metadata inventaris khusus.

- Berkas

Jenis: String

Deskripsi: (Opsional) Kumpulkan metadata tentang file pada instans Anda. Untuk informasi selengkapnya tentang cara mengumpulkan data Inventaris jenis ini, lihat [Bekerja dengan file dan](#)

[inventaris registri Windows](#). Membutuhkan SSmagent versi 2.2.64.0 atau yang lebih baru. Contoh Linux: [{"Path":"/usr/bin", "Pattern":["aws\*", "\*ssm\*"], "Recursive":false}, {"Path":"/var/log", "Pattern":["amazon\*.\*"], "Recursive":true, "DirScanLimit":1000}] Windows example: [{"Path":"%PROGRAMFILES%", "Pattern":["\*.exe"], "Recursive":true}]

- InstanceDetailedInformation

Jenis: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan informasi tambahan tentang instance, termasuk model CPU, kecepatan, dan jumlah inti, untuk beberapa nama.

- InstanceIds

Jenis: String

Default: \*

Deskripsi: (Diperlukan) instans EC2 yang ingin Anda inventarisasi.

- LambdaAssumeRole

Jenis: String

Deskripsi: (Opsional) ARN peran yang memungkinkan Lambda yang dibuat oleh Otomasi untuk melakukan tindakan atas nama Anda. Jika tidak ditentukan peran sementara akan dibuat untuk menjalankan fungsi Lambda.

- NetworkConfig

Jenis: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan metadata tentang konfigurasi jaringan.

- Keluaran3 BucketName

Jenis: String

Deskripsi: (Opsional) Nama bucket Amazon S3 tempat Anda ingin menulis data log Inventaris.

- Keluaran3 KeyPrefix

Jenis: String

Deskripsi: (Opsional) Sebuah key prefix Amazon S3 (subfolder) tempat Anda ingin menulis data log Inventaris.

- Keluaran3wilayah

Jenis: String

Deskripsi: (Opsional) Nama Wilayah AWS tempat Amazon S3 ada.

- Jadwal

Jenis: String

Default: cron (0 \*/30 \* \* \*? \*)

Deskripsi: (Opsional) Ekspresi cron untuk jadwal asosiasi Inventaris. Defaultnya adalah setiap 30 menit.

- Layanan

Jenis: String

Default: Diaktifkan

Deskripsi: (Opsional, hanya OS Windows, memerlukan SSMagent versi 2.2.64.0 ke atas) Kumpulkan data untuk konfigurasi layanan.

- WindowsRegistry

Jenis: String

Deskripsi: (Opsional) Kumpulkan metadata tentang kunci Microsoft Windows Registry. Untuk informasi selengkapnya tentang cara mengumpulkan data Inventaris jenis ini, lihat [Bekerja dengan file dan inventaris registri Windows](#). Membutuhkan SSM Agent versi 2.2.64.0 atau yang lebih baru. Contoh: [{"Path" : "HKEY\_CURRENT\_CONFIG\ System", "Recursive" : true}, {"Path" : "HKEY\_LOCAL\_MACHINE\ SOFTWARE\ Amazon\ ", " " : [" amination "]}] MachinelImage ValueNames

- WindowsRoles

Jenis: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan informasi tentang peran Windows pada instance. Hanya berlaku untuk sistem operasi Windows. Membutuhkan SSMagent versi 2.2.64.0 atau yang lebih baru.

- WindowsUpdates

Jenis: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan data tentang semua Pembaruan Windows pada instance.

## AWS-SetupManagedInstance

Deskripsi

Konfigurasi instance dengan peran AWS Identity and Access Management (IAM) untuk akses Systems Manager.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan

tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instans EC2 untuk dikonfigurasi

- LambdaAssumeRole

Jenis: String

Deskripsi: (Opsional) ARN peran yang memungkinkan Lambda yang dibuat oleh Otomasi untuk melakukan tindakan atas nama Anda. Jika tidak ditentukan peran sementara akan dibuat untuk menjalankan fungsi Lambda.

- RoleName

Jenis: String

Default: SSM RoleForManagedInstance

Deskripsi: (Opsional) Nama peran IAM untuk instans EC2. Jika peran ini tidak ada, itu akan dibuat. Saat menentukan nilai ini, verifikasi bahwa peran tersebut berisi Kebijakan Terkelola ManagedInstanceCoreAmazonSSM.

## AWS-SetupManagedRoleOnEC2Instance

Deskripsi

Konfigurasi instance dengan peran IAM RoleForManagedInstance terkelola SSM untuk akses Systems Manager.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instans EC2 untuk dikonfigurasi

- LambdaAssumeRole

Jenis: String

Deskripsi: (Opsional) ARN peran yang memungkinkan Lambda yang dibuat oleh Otomasi untuk melakukan tindakan atas nama Anda. Jika tidak ditentukan peran sementara akan dibuat untuk menjalankan fungsi Lambda.

- RoleName

Jenis: String

Default: SSM RoleForManagedInstance

Deskripsi: (Opsional) Nama peran IAM untuk instans EC2. Jika peran ini tidak ada, itu akan dibuat. Saat menentukan nilai ini, verifikasi bahwa peran tersebut berisi Kebijakan Terkelola ManagedInstanceCoreAmazonSSM.

## **AWSsupport-TroubleshootManagedInstance**

### Deskripsi



AWSSupport-TroubleshootManagedInstanceRunbook membantu Anda menentukan mengapa instans Amazon Elastic Compute Cloud (Amazon EC2) tidak melaporkan seperti yang dikelola oleh AWS Systems Manager. Buku runbook ini meninjau konfigurasi VPC untuk instance termasuk aturan grup keamanan, titik akhir VPC, aturan daftar kontrol akses jaringan (ACL), dan tabel rute. Ini juga mengonfirmasi profil instance AWS Identity and Access Management (IAM) yang berisi izin yang diperlukan dilampirkan ke instance.

 Important

Runbook otomatisasi ini tidak mengevaluasi aturan IPv6.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instans Amazon EC2 yang tidak melaporkan seperti yang dikelola oleh Systems Manager.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeInstanceProperties`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:StartAutomationExecution`
- `iam:ListRoles`
- `iam:GetInstanceProfile`
- `iam:ListAttachedRolePolicies`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcEndpoints`

## Langkah Dokumen

- `aws:executeScript`- PingStatus Mengumpulkan contoh.
- `aws:branch`- Cabang berdasarkan apakah instans sudah melaporkan seperti yang dikelola oleh Systems Manager.
- `aws:executeAwsApi`- Mengumpulkan rincian tentang instance termasuk konfigurasi VPC.
- `aws:executeScript`- Jika berlaku, kumpulkan detail tambahan terkait titik akhir VPC yang telah digunakan untuk digunakan dengan Systems Manager, dan mengonfirmasi grup keamanan yang dilampirkan pada titik akhir VPC memungkinkan lalu lintas masuk pada port TCP 443 dari instance.

- `aws:executeScript`- Memeriksa apakah tabel rute memungkinkan lalu lintas ke titik akhir VPC atau titik akhir Systems Manager publik.
- `aws:executeScript`- Memeriksa apakah aturan ACL jaringan mengizinkan lalu lintas ke titik akhir VPC atau titik akhir Systems Manager publik.
- `aws:executeScript`- Memeriksa apakah lalu lintas keluar ke titik akhir VPC atau titik akhir Systems Manager publik diizinkan oleh grup keamanan yang terkait dengan instance.
- `aws:executeScript`- Memeriksa apakah profil instance yang dilampirkan pada instance menyertakan kebijakan terkelola yang memberikan izin yang diperlukan.
- `aws:branch`- Cabang berdasarkan sistem operasi instance.
- `aws:executeScript`- Menyediakan referensi ke skrip `ssmagent-toolkit-linux` shell.
- `aws:executeScript`- Menyediakan referensi ke `ssmagent-toolkit-windows` PowerShell skrip.
- `aws:executeScript`- Menghasilkan output akhir untuk otomatisasi.
- `aws:executeScript`- Jika instance adalah `Online`, mengembalikan bahwa instance sudah dikelola oleh Systems Manager. `PingStatus`

## **AWSSupport-TroubleshootPatchManagerLinux**

### Deskripsi

`AWSSupport-TroubleshootPatchManagerLinuxRunbook` memecahkan masalah umum yang dapat menyebabkan kegagalan patch pada node terkelola berbasis Linux menggunakan kemampuan "Patch Manager". AWS Systems Manager Tujuan utama dari runbook ini adalah untuk mengidentifikasi akar penyebab kegagalan perintah patch dan menyarankan rencana remediasi.

### Bagaimana cara kerjanya?

`AWSSupport-TroubleshootPatchManagerLinuxRunbook` mempertimbangkan ID instance/ID perintah pasangan yang disediakan oleh Anda untuk pemecahan masalah. Jika tidak ada Command ID yang disediakan, ia memilih perintah patch gagal terbaru dalam 30 hari terakhir pada instance yang disediakan. Setelah memeriksa status perintah, pemenuhan prasyarat, dan distribusi OS, runbook mengunduh dan menjalankan paket penganalisis log. Outputnya mencakup akar masalah serta tindakan yang diperlukan untuk memperbaiki masalah.

### Jenis Dokumen

### Otomatisasi

## Pemilik

Amazon

## Platform

- Amazon Linux 2 dan 2023
- Red Hat Enterprise Linux 8.X dan 9.X
- Centos 8.X dan 9.X
- SUSE 15.X

## Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

## Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootPatchManagerLinux](#) dalam AWS Systems Manager konsol.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:

- **InstanceId (Diperlukan):**

Gunakan pemilih instans interaktif untuk memilih ID Node Terkelola SSM Berbasis Linux (Amazon Elastic Compute Cloud (Amazon EC2) atau server Hybrid Activated) yang gagal dilakukan oleh perintah patch, atau masukkan ID instans SSM Managed secara manual.

- **AutomationAssumeRole (Opsional):**

Masukkan ARN peran IAM yang memungkinkan Otomasi melakukan tindakan atas nama Anda. Jika peran tidak ditentukan, Automation menggunakan izin pengguna yang memulai runbook ini.

- **RunCommandId (Opsional):**

Masukkan ID Perintah Jalankan Gagal AWS-RunPatchBaseline dokumen. Jika Anda tidak memberikan Command ID, runbook akan mencari perintah patch gagal terbaru dalam 30 hari terakhir pada instance yang dipilih.

**Input parameters**

---

**InstanceId**  
(Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.  
 Show interactive instance picker

i-0[REDACTED]

---

<p><b>AutomationAssumeRole</b>  <small>(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</small></p> <p>Choose an option ▼ <input type="button" value="↺"/></p>	<p><b>RunCommandId</b>  <small>(Optional) Failed Run Command ID of AWS-RunPatchBaseline. If not provided, we look for the latest unsuccessful execution of AWS-RunPatchBaseline for the instance and evaluate it. To confirm the command ID, look under Command History tab in the Run Command Console under AWS Systems Manager.</small></p> <p>42[REDACTED]e</p>
---	--

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **CheckConcurrency:**

Memastikan bahwa hanya ada satu eksekusi runbook ini yang menargetkan instance yang sama. Jika runbook menemukan eksekusi lain dalam proses yang menargetkan instance yang sama, ia mengembalikan kesalahan dan berakhir.

- **ValidateCommandID:**

Memvalidasi jika ID Perintah yang disediakan, sebagai parameter input, dieksekusi untuk Dokumen AWS-RunPatchBaseline SSM. Jika tidak ada Command ID yang diberikan, runbook akan mempertimbangkan eksekusi gagal terbaru AWS-RunPatchBaseline dalam 30 hari terakhir pada instance yang dipilih.

- **BranchOnCommandStatus:**

Mengonfirmasi bahwa status perintah yang diberikan gagal. Jika tidak, runbook mengakhiri eksekusi dan menghasilkan laporan yang menyatakan bahwa perintah yang disediakan berhasil dijalankan.

- **VerifyPrerequisites:**

Mengonfirmasi bahwa Prasyarat yang disebutkan di atas terpenuhi.

- **GetPlatformDetails:**

Mengambil distribusi dan versi Sistem Operasi (OS).

- **GetDownloadURL:**

Mengambil URL unduhan untuk paket PatchManager Log Analyzer.

- **EvaluatePatchManagerLogs:**

Mengunduh dan mengeksekusi paket python PatchManager Log Analyzer pada instance untuk mengevaluasi file log.

- **GenerateReport:**

Menghasilkan laporan akhir dari eksekusi runbook yang mencakup masalah yang diidentifikasi dan solusi yang disarankan.

## 7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci:

```

▼ Outputs
GenerateReport.output
Starting 'python3 main.py i-0[REDACTED] 3e016680-82f4-45f4-845c-aa4685b4fab Ubuntu 22.04'

TROUBLESHOOTING RESULTS
=====
[PROBLEM] :
The error found in the log file at /var/lib/amazon/ssm/i-0[REDACTED]/document/orchestration/3e016680-82f4-45f4-845c-aa4685b4fab/awssrunShellScript/PatchLinux/stdout is :
Unable to download payload: https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz.failed to run commands: exit status 156

[SOLUTION] :
Here are some suggestions to troubleshoot the issue:

Possible reasons for the above error are :
1. Network connectivity issue while accessing the s3 service endpoint from the instance to download the payload.
2. Instance doesn't have the required permissions to access the specified Amazon Simple Storage Service (Amazon S3) bucket.
3. No space left on the Instance.

To resolve this, ensure network connectivity to S3 endpoint from the instance. For more details, see information about required access to S3 buckets for Patch Manager in https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent-minimum-s3-permissions.

For testing purpose, try to manually access the above payload URL using curl or wget from within Instance. Command to run:

curl https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz --output payload.tar.gz

```

## Referensi

## Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

## AWSSupport-TroubleshootSessionManager

### Deskripsi

AWSSupport-TroubleshootSessionManagerRunbook membantu Anda memecahkan masalah umum yang mencegah Anda terhubung ke instans Amazon Elastic Compute Cloud (Amazon EC2) yang dikelola menggunakan Session Manager. Session Manager adalah kemampuan AWS Systems Manager. Runbook ini memeriksa hal-hal berikut:

- Memeriksa apakah instans berjalan dan melaporkan seperti yang dikelola oleh Systems Manager.
- Menjalankan AWSSupport-TroubleshootManagedInstance runbook jika instance tidak melaporkan seperti yang dikelola oleh Systems Manager.
- Memeriksa versi Agen SSM yang diinstal pada instance.
- Memeriksa apakah profil instans yang berisi kebijakan direkomendasikan AWS Identity and Access Management (IAM) untuk Pengelola Sesi dilampirkan ke instans Amazon EC2.
- Mengumpulkan log Agen SSM dari instance.
- Menganalisis preferensi Manajer Sesi Anda.
- Menjalankan AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 runbook untuk menganalisis konektivitas instans ke titik akhir untuk Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3), dan Amazon CloudWatch Logs (Log). CloudWatch

### Pertimbangan-pertimbangan

- Node terkelola hibrida tidak didukung.
- Runbook ini hanya memeriksa apakah kebijakan IAM terkelola yang direkomendasikan dilampirkan ke profil instance. Itu tidak menganalisis IAM atau AWS KMS izin yang terkandung dalam profil instans Anda.

**⚠ Important**

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2Runbook menggunakan [VPC Reachability Analyzer](#) untuk menganalisis konektivitas jaringan antara sumber dan titik akhir layanan. Anda dikenakan biaya per analisis yang dijalankan antara sumber dan tujuan. Untuk detail selengkapnya, lihat [Harga Amazon VPC](#).

**Jalankan Otomasi ini (konsol)**

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instans Amazon EC2 yang tidak dapat Anda sambungkan menggunakan Pengelola Sesi.

- SessionPreferenceDocument

Jenis: String



Default: SSM- SessionManagerRunShell

Deskripsi: (Opsional) Nama dokumen preferensi sesi Anda. Jika Anda tidak menentukan dokumen preferensi sesi kustom saat memulai sesi, gunakan nilai default.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ec2:CreateNetworkInsightsPath
- ec2>DeleteNetworkInsightsAnalysis
- ec2>DeleteNetworkInsightsPath
- ec2:StartNetworkInsightsAnalysis
- tiros:CreateQuery
- ec2:DescribeAvailabilityZones
- ec2:DescribeCustomerGateways
- ec2:DescribeDhcpOptions
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- 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:DescribeVpcAttribute`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcEndpointServiceConfigurations`
- `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`
- `iam:GetInstanceProfile`
- `iam>ListAttachedRolePolicies`
- `iam>ListRoles`
- `iam:PassRole`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:GetAutomationExecution`

- `ssm:GetDocument`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`
- `tiros:GetQueryAnswer`
- `tiros:GetQueryExplanation`

## Langkah Dokumen

1. `aws:waitForAwsResourceProperty`: Menunggu hingga 6 menit agar instans target Anda lulus pemeriksaan status.
2. `aws:executeScript`: Mem-parsing dokumen preferensi sesi.
3. `aws:executeAwsApi`: Mendapat ARN dari profil instance yang dilampirkan ke instance Anda.
4. `aws:executeAwsApi`: Memeriksa apakah instans Anda melaporkan seperti yang dikelola oleh Systems Manager.
5. `aws:branch`: Cabang berdasarkan apakah instans Anda melaporkan seperti yang dikelola oleh Systems Manager.
6. `aws:executeScript`: Memeriksa apakah Agen SSM yang diinstal pada instans Anda mendukung Session Manager.
7. `aws:branch`: Cabang berdasarkan platform instans Anda untuk mengumpulkan `ssm-cli` log.
8. `aws:runCommand`: Mengumpulkan log output dari `ssm-cli` dari Linux atau macOS instance.
9. `aws:runCommand`: Mengumpulkan log output dari `ssm-cli` dari sebuah Windows instance.
10. `aws:executeScript`: Mem-parsing `ssm-cli` log.
11. `aws:executeScript`: Memeriksa apakah kebijakan IAM yang direkomendasikan dilampirkan ke profil instance.
12. `aws:branch`: Menentukan apakah akan mengevaluasi konektivitas `ssmmessages` titik akhir berdasarkan `ssm-cli` log.
13. `aws:executeAutomation`: Mengevaluasi apakah instance dapat terhubung ke titik `ssmmessages` akhir.
14. `aws:branch`: Menentukan apakah akan mengevaluasi konektivitas titik akhir Amazon S3 berdasarkan `ssm-cli` log dan preferensi sesi Anda.

15. `aws:executeAutomation`: Mengevaluasi apakah instans dapat terhubung ke titik akhir Amazon S3.
16. `aws:branch`: Menentukan apakah akan mengevaluasi konektivitas AWS KMS titik akhir berdasarkan `ssm-cli` log dan preferensi sesi Anda.
17. `aws:executeAutomation`: Mengevaluasi apakah instance dapat terhubung ke titik AWS KMS akhir.
18. `aws:branch`: Menentukan apakah akan mengevaluasi CloudWatch konektivitas titik akhir `ssm-cli` Log berdasarkan log dan preferensi sesi Anda.
19. `aws:executeAutomation`: Mengevaluasi apakah instance dapat terhubung ke titik akhir CloudWatch Log.
20. `aws:executeAutomation`: Menjalankan `AWSSupport-TroubleshootManagedInstance` runbook.
21. `aws:executeScript`: Mengkompilasi output dari langkah-langkah sebelumnya dan mengeluarkan laporan.

## Ouput

- `generateReport.EvalReport`- Hasil pemeriksaan yang dilakukan oleh runbook dalam teks biasa.

## Pihak ketiga

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk produk dan layanan pihak ketiga. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWS-CreateJiraIssue](#)
- [AWS-CreateServiceNowIncident](#)
- [AWS-RunPacker](#)

## AWS-CreateJiraIssue

### Deskripsi

Buat masalah di Jira.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AssigneeName

Jenis: String

Deskripsi: (Opsional) Nama pengguna orang yang menjadi masalah harus ditetapkan.

- DueDate

Jenis: String

Deskripsi: (Opsional) Tanggal jatuh tempo untuk masalah dalam yyyy-mm-dd format.

- IssueDescription

Jenis: String

Deskripsi: (Wajib) Penjelasan rinci tentang masalah ini.

- IssueSummary

Jenis: String

Deskripsi: (Wajib) Ringkasan singkat tentang masalah ini.

- IssueTypeName

Jenis: String

Deskripsi: (Wajib) Nama jenis masalah yang ingin Anda buat (misalnya, Tugas, Sub-tugas, Bug, dll.).

- JiraURL

Jenis: String

Deskripsi: (Wajib) Url dari contoh Jira.

- JiraUsername

Jenis: String

Deskripsi: (Wajib) Nama pengguna yang akan dibuat dengan masalah tersebut.

- PriorityName

Jenis: String

Deskripsi: (Opsional) Nama prioritas masalah.

- ProjectKey

Jenis: String

Deskripsi: (Wajib) Kunci proyek yang harus dibuat masalah.

- SSM ParameterName

Jenis: String

Deskripsi: (Wajib) Nama Parameter SSM terenkripsi yang berisi kunci API atau kata sandi untuk pengguna Jira.

## Langkah Dokumen

`aws:createStack`- Buat CloudFormation tumpukan untuk membuat peran dan fungsi Lambda IAM.

`aws:invokeLambdaFunction`- Memanggil fungsi Lambda untuk membuat masalah Jira

`aws:deleteStack`- Hapus CloudFormation tumpukan yang dibuat.

## Keluaran

Issueld: ID masalah Jira yang baru dibuat

# AWS-CreateServiceNowIncident

## Deskripsi

Buat insiden di tabel ServiceNow insiden.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

## Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Kategori

Jenis: String

Deskripsi: (Opsional) Kategori insiden.

Nilai yang valid: Tidak Ada | Permintaan/Bantuan | Perangkat Lunak | Perangkat Keras | Jaringan | Database

Nilai Default: Tidak ada

- Deskripsi

Jenis: String

Deskripsi: (Wajib) Penjelasan rinci tentang insiden tersebut.

- Dampak

Jenis: String

Deskripsi: (Opsional) Efek suatu insiden terhadap bisnis.

Nilai yang valid: Tinggi | Sedang | Rendah

Nilai Default: Rendah

- ServiceNowInstanceUsername

Jenis: String

Deskripsi: (Wajib) Nama pengguna yang akan dibuat dengan insiden tersebut.

- ServiceNowInstancePassword

Jenis: String

Deskripsi: (Wajib) Nama Parameter SSM terenkripsi yang berisi kata sandi untuk pengguna.  
ServiceNow

- ServiceNowInstanceURL

Jenis: String

Deskripsi: (Wajib) URL dari ServiceNow contoh

- ShortDescription

Jenis: String

Deskripsi: (Wajib) Deskripsi singkat tentang insiden tersebut.

- Subkategori

Jenis: String

Keterangan: (Opsional) Subkategori insiden.

Nilai yang valid: Tidak Ada | Antivirus | Email | Aplikasi Internal | Sistem Operasi | CPU | Disk |  
Keyboard | Perangkat Keras | Memori | Monitor | Mouse | DHCP | DNS | Alamat IP | VPN | Nirkabel  
| DB2 | MS SQL Server | Oracle



Nilai Default: Tidak ada

## Langkah Dokumen

Push\_incident — Mendorong informasi insiden ke. ServiceNow

## Keluaran

Push\_incident.incidentid — ID insiden yang dibuat.

# AWS-RunPacker

## Deskripsi

Runbook ini menggunakan alat HashiCorp [Packer](#) untuk memvalidasi, memperbaiki, atau membangun template packer yang digunakan untuk membuat gambar mesin. Runbook ini menggunakan Packer v1.7.2.

### Note

Jika Anda menentukan `vpc_id` nilai, Anda juga harus menentukan `subnet_id` nilai subnet publik. Kecuali Anda memodifikasi atribut pengalamatan publik IPv4 subnet Anda, Anda juga harus menyetel ke `true`. `associate_public_ip_address`

## [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Kekuatan

Jenis: Boolean

Deskripsi: Opsi Packer untuk memaksa pembuat berjalan saat artefak dari build sebelumnya mencegah build berjalan.

- Mode

Jenis: String

Deskripsi: Mode, atau perintah, di mana untuk menggunakan Packer saat memvalidasi terhadap template. Pilihan termasuk `Build`, `Validate`, dan `Fix`.

- `TemplateFileName`

Jenis: String

Deskripsi: Nama, atau kunci, dari file template di bucket S3.

- `Template3 BucketName`

Jenis: String

Deskripsi: Nama bucket S3 yang berisi template packer.

## Langkah Dokumen

`RunPackerProcessTemplate` — Menjalankan mode yang dipilih terhadap template menggunakan alat Packer.

## Keluaran

`RunPackerProcessTemplate.output` — Stdout dari alat Packer.

`RunPackerProcessTemplate.fixed_template_key` — Nama template yang disimpan dalam bucket S3 untuk digunakan hanya ketika berjalan dalam mode “Fix”.

RunPackerProcessTemplate.s3\_bucket — Nama bucket S3 yang berisi template tetap untuk digunakan hanya saat berjalan dalam mode “Fix”.

## Amazon VPC

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Virtual Private Cloud. Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWS-CloseSecurityGroup](#)
- [AWSSupport-ConfigureDNSQueryLogging](#)
- [AWSSupport-ConfigureTrafficMirroring](#)
- [AWSSupport-ConnectivityTroubleshooter](#)
- [AWSSupport-TroubleshootVPN](#)
- [AWSConfigRemediation-DeleteEgressOnlyInternetGateway](#)
- [AWSConfigRemediation-DeleteUnusedENI](#)
- [AWSConfigRemediation-DeleteUnusedSecurityGroup](#)
- [AWSConfigRemediation-DeleteUnusedVPCNetworkACL](#)
- [AWSConfigRemediation-DeleteVPCFlowLog](#)
- [AWSConfigRemediation-DetachAndDeleteInternetGateway](#)
- [AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway](#)
- [AWS-DisableIncomingSSHOnPort22](#)
- [AWS-DisablePublicAccessForSecurityGroup](#)
- [AWSConfigRemediation-DisableSubnetAutoAssignPublicIP](#)
- [AWSSupport-EnableVPCFlowLogs](#)
- [AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch](#)
- [AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket](#)
- [AWS-ReleaseElasticIP](#)
- [AWS-RemoveNetworkACLUnrestrictedSSHRDP](#)
- [AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules](#)
- [AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules](#)

- [AWSSupport-SetupIPMonitoringFromVPC](#)
- [AWSSupport-TerminateIPMonitoringFromVPC](#)

## AWS - CloseSecurityGroup

### Deskripsi

Runbook ini menghapus semua aturan masuk dan keluar dari grup keamanan yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- SecurityGroupId

Jenis: String

Deskripsi: (Wajib) ID grup keamanan yang ingin Anda tutup.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

#### Langkah Dokumen

- aws:executeScript- Menghapus semua aturan masuk dan keluar dari grup keamanan yang Anda tentukan dalam parameter. SecurityGroupId

## AWSSupport-ConfigureDNSQueryLogging

### Deskripsi

AWSSupport-ConfigureDNSQueryLoggingRunbook mengonfigurasi pencatatan untuk kueri DNS yang berasal dari cloud pribadi virtual (VPC) Anda atau untuk zona yang dihosting Amazon Route 53. Anda dapat memilih untuk mempublikasikan log kueri ke Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3), atau Amazon Data Firehose. Untuk informasi selengkapnya tentang pencatatan kueri dan log kueri penyelesaian, lihat Pencatatan kueri [DNS Publik dan pencatatan kueri Resolver](#).

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LogDestinationArn

Jenis: String

Deskripsi: (Opsional) ARN dari grup CloudWatch Log, bucket Amazon S3, atau aliran Firehose yang ingin Anda kirim log kueri. Perhatikan bahwa pencatatan kueri DNS publik Route 53 hanya mendukung grup CloudWatch Log. Jika Anda tidak menentukan nilai untuk parameter ini, otomatisasi akan membuat grup CloudWatch Log dengan format `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID }`, dan kebijakan sumber daya IAM untuk mempublikasikan log kueri. Grup CloudWatch Log yang dibuat oleh otomatisasi memiliki periode retensi 14 hari.

- QueryLogType

Jenis: String

Deskripsi: (Opsional) Jenis kueri yang ingin Anda log.

Nilai yang valid: Publik | Resolver/Pribadi

Default: Publik

- ResourceId

Jenis: String

Deskripsi: (Wajib) ID sumber daya yang pertanyaannya ingin Anda log. Jika Anda menentukan `Public QueryLogType` parameter, sumber daya harus ID dari zona host pribadi Route 53. Jika Anda menentukan `Resolver/Private QueryLogType` parameter, sumber daya harus berupa ID VPC.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeVpcs`
- `firehose:ListTagsForDeliveryStream`
- `firehose:PutRecord`
- `firehose:PutRecordBatch`
- `firehose:TagDeliveryStream`
- `iam:AttachRolePolicy`
- `iam:CreatePolicy`
- `iam:CreateRole`
- `iam:CreateServiceLinkedRole`
- `iam>DeletePolicy`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:GetPolicy`
- `iam:GetRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `iam:TagRole`
- `iam:UpdateRole`
- `logs:CreateLogDelivery`
- `logs:CreateLogGroup`
- `logs>DeleteLogDelivery`
- `logs>DeleteLogGroup`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:DescribeResourcePolicies`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:PutRetentionPolicy`

- `logs:UpdateLogDelivery`
- `route53:CreateQueryLoggingConfig`
- `route53>DeleteQueryLoggingConfig`
- `route53:GetHostedZone`
- `route53resolver:AssociateResolverQueryLogConfig`
- `route53resolver:CreateResolverQueryLogConfig`
- `route53resolver>DeleteResolverQueryLogConfig`
- `s3:GetBucketAcl`

### Langkah Dokumen

- `aws:executeScript`- Memverifikasi sumber daya yang Anda tentukan untuk `ResourceId` parameter yang ada, dan memeriksa apakah jenis sumber daya cocok dengan `QueryLogType` opsi yang diperlukan.
- `aws:executeScript`- Memverifikasi bahwa nilai yang Anda tentukan untuk `LogDestinationArn` parameter cocok dengan yang diperlukan `QueryLogType`.
- `aws:executeScript`- Memverifikasi izin yang diperlukan untuk Route 53 untuk mempublikasikan log ke grup CloudWatch log Log, dan membuat kebijakan sumber daya IAM yang diperlukan jika tidak ada.
- `aws:executeScript`- Mengaktifkan pencatatan query DNS pada tujuan yang dipilih.

## AWSSupport-ConfigureTrafficMirroring

### Deskripsi

`AWSSupport-ConfigureTrafficMirroringRunbook` mengonfigurasi pencerminan lalu lintas untuk membantu Anda memecahkan masalah konektivitas antara penyeimbang beban dan instans Amazon Elastic Compute Cloud (Amazon EC2). Pencerminan lalu lintas menyalin lalu lintas masuk dan keluar dari antarmuka jaringan yang dilampirkan ke instance Anda. Untuk mengonfigurasi pencerminan lalu lintas, buku runbook ini membuat target, filter, dan sesi yang diperlukan. Secara default, runbook mengonfigurasi mirroring untuk semua lalu lintas masuk dan keluar untuk semua protokol kecuali Amazon DNS. Jika Anda ingin mencerminkan lalu lintas dari sumber dan tujuan tertentu, Anda dapat mengubah aturan masuk dan keluar setelah otomatisasi selesai.

[Jalankan Otomasi ini \(konsol\)](#)



## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- SourceENI

Jenis: String

Deskripsi: (Diperlukan) Elastic network interface yang ingin Anda konfigurasi untuk mirroring lalu lintas.

- Target

Jenis: String

Deskripsi: (Wajib) Tujuan untuk lalu lintas cermin. Anda harus menentukan ID antarmuka jaringan, Network Load Balancer, atau titik akhir Gateway Load Balancer. Jika Anda menentukan Network Load Balancer, harus ada pendengar UDP pada port 4789.

- SessionNumber

Jenis: String

Nilai yang valid: 1-32766

Deskripsi: (Wajib) Jumlah sesi cermin yang ingin Anda gunakan.

## Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:CreateTrafficMirrorTarget`
- `ec2:CreateTrafficMirrorFilter`
- `ec2:CreateTrafficMirrorFilterRule`
- `ec2:CreateTrafficMirrorSession`
- `ec2>DeleteTrafficMirrorSession`
- `ec2>DeleteTrafficMirrorFilter`
- `ec2>DeleteTrafficMirrorSession`
- `ec2>DeleteTrafficMirrorFilterRule`
- `iam:ListRoles`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`

## Langkah Dokumen

- `aws:executeScript`- Menjalankan skrip untuk membuat target.
- `aws:executeAwsApi`- Membuat aturan filter.
- `aws:executeAwsApi`- Membuat aturan filter cermin untuk semua lalu lintas masuk.
- `aws:executeAwsApi`- Membuat aturan filter cermin untuk semua lalu lintas keluar.
- `aws:executeAwsApi`- Membuat sesi cermin lalu lintas.
- `aws:executeAwsApi`- Menghapus filter jika pembuatan filter atau sesi gagal.
- `aws:executeAwsApi`- Menghapus target jika pembuatan filter atau sesi gagal.

## Keluaran

`CreateFilter.FilterId`

`CreateSession.SessionId`

`CreateTarget.targetIdOutput`

# AWSSupport-ConnectivityTroubleshooter

## Deskripsi

AWSSupport-ConnectivityTroubleshooterRunbook mendiagnosis masalah konektivitas antara yang berikut:

- AWS sumber daya dalam Amazon Virtual Private Cloud (Amazon VPC)
- AWS sumber daya di VPC Amazon yang berbeda dalam hal yang sama Wilayah AWS yang terhubung menggunakan peering VPC
- AWS sumber daya di VPC Amazon dan sumber daya internet menggunakan gateway internet
- AWS sumber daya di VPC Amazon dan sumber daya internet menggunakan gateway terjemahan alamat jaringan (NAT)

## [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DestinasiIP

Jenis: String

Deskripsi: (Wajib) Alamat IPv4 dari sumber daya yang ingin Anda sambungkan.

- DestinationPort

Jenis: String

Default: betul

Deskripsi: (Wajib) Nomor port yang ingin Anda sambungkan pada sumber daya tujuan.

- DestinationVpc

Jenis: String

Default: Semua

Deskripsi: (Opsional) ID VPC Amazon yang ingin Anda uji konektivitas.

- SourceIP

Jenis: String

Deskripsi: (Wajib) Alamat IPv4 pribadi AWS sumber daya di VPC Amazon Anda yang ingin Anda uji konektivitas.

- SourcePortRange

Jenis: String

Deskripsi: (Opsional) Rentang port yang digunakan oleh AWS sumber daya di VPC Amazon yang ingin Anda uji konektivitas.

- SourceVpc

Jenis: String

Default: Semua

Deskripsi: (Opsional) ID VPC Amazon yang ingin Anda uji konektivitas.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcPeeringConnections`

## Langkah Dokumen

- `aws:executeScript`- Mengumpulkan detail tentang AWS sumber daya yang Anda tentukan dalam `SourceIP` parameter.
- `aws:executeScript`- Menentukan tujuan lalu lintas jaringan dari AWS sumber daya menggunakan rute yang dikumpulkan dari langkah sebelumnya.
- `aws:branch`- Cabang berdasarkan tujuan lalu lintas jaringan.
- `aws:executeAwsApi`- Mengumpulkan detail tentang sumber daya tujuan.
- `aws:executeScript`- Mengonfirmasi bahwa ID yang dikembalikan untuk VPC Amazon tujuan cocok dengan nilai yang ditentukan, jika ada, dalam parameter. `DestinationVpc`
- `aws:executeAwsApi`- Mengumpulkan aturan kelompok keamanan untuk sumber dan sumber daya tujuan.
- `aws:executeScript`- Mengonfirmasi apakah aturan grup keamanan memungkinkan lalu lintas yang diperlukan antara sumber dan sumber daya tujuan.
- `aws:executeAwsApi`- Mengumpulkan daftar kontrol akses jaringan (NACL) yang terkait dengan subnet untuk sumber daya sumber dan tujuan.
- `aws:executeScript`- Mengonfirmasi apakah NACL memungkinkan lalu lintas yang diperlukan antara sumber dan sumber daya tujuan.
- `aws:executeScript`- Mengonfirmasi apakah sumber memiliki alamat IP publik yang terkait dengan sumber daya, jika tujuan rute adalah gateway internet.
- `aws:executeAwsApi`- Mengumpulkan aturan kelompok keamanan untuk sumber daya sumber.
- `aws:executeScript`- Mengonfirmasi apakah aturan grup keamanan mengizinkan lalu lintas yang diperlukan dari sumber ke sumber daya tujuan.
- `aws:executeAwsApi`- Mengumpulkan NACL yang terkait dengan subnet untuk sumber daya sumber.

- `aws:executeScript`- Mengonfirmasi apakah NACL memungkinkan lalu lintas yang dibutuhkan dari sumber daya sumber.
- `aws:executeAwsApi`- Mengumpulkan rincian tentang gateway NAT.
- `aws:executeAwsApi`- Mengumpulkan NACL yang terkait dengan subnet untuk gateway NAT.
- `aws:executeScript`- Mengonfirmasi apakah NACL mengizinkan lalu lintas yang diperlukan dari subnet untuk gateway NAT.
- `aws:executeScript`- Mengumpulkan rute yang terkait dengan subnet untuk gateway NAT.
- `aws:executeScript`- Mengonfirmasi apakah gateway NAT memiliki rute ke gateway internet.
- `aws:executeAwsApi`- Mengumpulkan detail tentang koneksi peering VPC.
- `aws:executeScript`- Mengonfirmasi kedua VPC berada di Wilayah yang sama dan bahwa ID yang dikembalikan untuk VPC tujuan cocok dengan nilai yang ditentukan, jika ada, dalam `DestinationVpc` parameter.
- `aws:executeAwsApi`- Mengembalikan subnet dari sumber daya tujuan.
- `aws:executeScript`- Mengumpulkan rute yang terkait dengan subnet untuk VPC yang diintip.
- `aws:executeScript`- Mengonfirmasi apakah VPC peered memiliki rute ke koneksi peering.
- `aws:executeScript`- Mengonfirmasi apakah lalu lintas diizinkan dari sumber daya sumber jika tujuan tidak didukung oleh otomatisasi.

## AWSSupport-TroubleshootVPN

### Deskripsi

`AWSSupport-TroubleshootVPNRunbook` membantu Anda melacak dan menyelesaikan kesalahan dalam AWS Site-to-Site VPN koneksi. Otomatisasi mencakup beberapa pemeriksaan otomatis yang dirancang untuk melacak IKEv1 atau IKEv2 kesalahan yang terkait dengan terowongan AWS Site-to-Site VPN koneksi. Otomatisasi mencoba mencocokkan kesalahan tertentu dan resolusi yang sesuai membentuk daftar masalah umum.

Catatan: Otomatisasi ini tidak memperbaiki kesalahan. Ini berjalan untuk rentang waktu yang disebutkan dan memindai grup log untuk kesalahan dalam [grup CloudWatch log VPN](#).

### Bagaimana cara kerjanya?

Runbook menjalankan validasi parameter untuk mengonfirmasi apakah grup CloudWatch log Amazon yang disertakan dalam parameter input ada, jika ada aliran log di grup log yang sesuai

dengan logging terowongan VPN, jika ada id koneksi VPN, dan jika alamat IP Tunnel ada. Itu membuat panggilan API Logs Insights pada grup CloudWatch log Anda yang dikonfigurasi untuk logging VPN.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LogGroupName

Jenis: String

Deskripsi: (Diperlukan) Nama grup CloudWatch log Amazon yang dikonfigurasi untuk pencatatan AWS Site-to-Site VPN koneksi

Pola yang Diizinkan: `^[\\.\\-\\_/#A-Za-z0-9]{1,512}`

- VpnConnectionId

Jenis: String

Deskripsi: (Wajib) Id AWS Site-to-Site VPN koneksi yang akan dipecahkan masalah.

Pola yang Diizinkan: `^vpn-[0-9a-f]{8,17}$`

- TunnelIpAddress

Jenis: String

Deskripsi: (Wajib) Alamat IPv4 nomor terowongan 1 yang terkait dengan alamat Anda. AWS Site-to-Site VPN

Pola yang Diizinkan: `^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}$`

- TunnelbiPAddress

Jenis: String

Deskripsi: (Opsional) Alamat IPv4 nomor terowongan 2 yang terkait dengan alamat Anda. AWS Site-to-Site VPN

Pola yang Diizinkan: `^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}|^$`

- IKEVersion

Jenis: String

Deskripsi: (Wajib) Pilih Versi IKE yang Anda gunakan. Nilai yang diizinkan: IKEv1, IKEv2

Nilai yang valid: ['IKEv1', 'IKEv2']

- StartTimeinEpoch

Tipe: String

Deskripsi: (Opsional) Waktu mulai untuk analisis log. Anda dapat menggunakan StartTimeinEpoch/EndTimeinEpoch atau LookBackPeriod untuk analisis log

Pola yang Diizinkan: `^\d{10}|^$`

- EndTimeinEpoch

Jenis: String

Deskripsi: (Opsional) Waktu akhir untuk analisis log. Anda dapat menggunakan StartTimeinEpoch/EndTimeinEpoch atau LookBackPeriod untuk analisis log. Jika diberikan keduanya StartTimeinEpoch/EndTimeinEpoch dan LookBackPeriod kemudian LookBackPeriod diutamakan

Pola yang Diizinkan: `^\d{10}|^$`



- LookBackPeriod

Jenis: String

Deskripsi: (Opsional) Dua digit waktu dalam beberapa jam untuk melihat ke belakang untuk analisis log. Rentang yang valid: 01 - 99. Nilai ini diutamakan jika Anda juga memberi dan StartTimeinEpoch EndTime

Pola yang Diizinkan:  $^(\backslash d?[1-9] | [1-9]0) | ^\$$

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- logs:DescribeLogGroups
- logs:GetQueryResults
- logs:DescribeLogStreams
- logs:StartQuery
- ec2:DescribeVpnConnections

### Instruksi

Catatan: Otomatisasi ini berfungsi pada grup CloudWatch log yang dikonfigurasi untuk logging terowongan VPN Anda, ketika format Output logging adalah JSON.

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootVPN](#) di konsol. AWS Systems Manager
2. Untuk parameter input masukkan yang berikut ini:

- AutomationAssumeRole (Opsional):

Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- LogGroupName (Diperlukan):

Nama grup CloudWatch log Amazon akan divalidasi. Ini harus grup CloudWatch log yang dikonfigurasi untuk VPN untuk mengirim log ke.

- `VpnConnectionId` (Diperlukan):

Id AWS Site-to-Site VPN koneksi yang grup lognya dilacak untuk kesalahan VPN.

- `TunnelaipAddress` (Diperlukan):

Terowongan Alamat IP yang terkait dengan AWS Site-to-Site VPN koneksi Anda.

- `Tunnelbipaddress` (Opsional):

Alamat IP terowongan B yang terkait dengan AWS Site-to-Site VPN koneksi Anda.

- `IKEVersion` (Diperlukan):

Pilih IKEVersion yang Anda gunakan. Nilai yang diizinkan: IKEv1, IKEv2.

- `StartTimeinEpoch` (Opsional):

Awal rentang waktu untuk meminta kesalahan. Rentang ini inklusif, sehingga waktu mulai yang ditentukan termasuk dalam kueri. Ditentukan sebagai waktu epoch, jumlah detik sejak 1 Januari 1970, 00:00:00 UTC.

- `EndTimeinEpoch` (Opsional):

Akhir rentang waktu untuk meminta kesalahan. Rentang ini inklusif, sehingga waktu akhir yang ditentukan disertakan dalam kueri. Ditentukan sebagai waktu epoch, jumlah detik sejak 1 Januari 1970, 00:00:00 UTC.

- `LookBackPeriod` (Diperlukan):

Waktu dalam beberapa jam untuk melihat kembali ke kueri untuk kesalahan.

Catatan: Konfigurasi `StartTimeinEpoch`, `EndTimeinEpoch`, atau `LookBackPeriod` untuk memperbaiki rentang waktu untuk analisis log. Berikan angka dua digit dalam jam untuk memeriksa kesalahan di masa lalu dari waktu mulai otomatisasi. Atau, jika kesalahan di masa lalu dalam rentang waktu tertentu, sertakan `StartTimeinEpoch` dan `EndTimeinEpoch`, alih-alih `LookBackPeriod`.

Input parameters	
<b>AutomationAssumeRole</b> <small>(Optional) The ARN of the role that allows Automation to perform the actions on your behalf.</small> <input type="text" value="Choose an option"/>	<b>LogGroupName</b> <small>(Required) The Amazon CloudWatch log group name to be validated. This must be the CloudWatch log group which is destined for VPN logs</small> <input type="text" value="vpnlog"/>
<b>VpnConnectionId</b> <small>(Required) The AWS Site-to-Site VPN connection id to be validated.</small> <input type="text" value="vpn-123abc456xyz"/>	<b>Tunnel1IPAddress</b> <small>(Required) The tunnel number 1 IP address associated with your AWS Site-to-Site VPN to be validated.</small> <input type="text" value="1.1.1.1"/>
<b>Tunnel2IPAddress</b> <small>(Optional) The tunnel number 2 IP address associated with your AWS Site-to-Site VPN to be validated.</small> <input type="text" value="String"/>	<b>IKEVersion</b> <small>(Required) Select what IKE Version you are using. Allowed values : IKEv1, IKEv2 or both</small> <input type="text" value="IKEv1"/>
<b>StartTimeEpoch</b> <small>(Optional) Start time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis</small> <input type="text" value="String"/>	<b>EndTimeEpoch</b> <small>(Optional) End time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis</small> <input type="text" value="String"/>
<b>LookBackPeriod</b> <small>(Required) Time in hours to look back for log analysis</small> <input type="text" value="05"/>	

### 3. Pilih Jalankan.

### 4. Otomatisasi dimulai.

### 5. Runbook otomatisasi melakukan langkah-langkah berikut:

- **ParameterValidasi:**

Menjalankan serangkaian validasi pada parameter input yang termasuk dalam otomatisasi.

- **branchOnValidationOfLogGroup:**

Memeriksa apakah grup log yang disebutkan dalam parameter valid. Jika tidak valid, ini menghentikan inisiasi langkah-langkah otomatisasi lebih lanjut.

- **branchOnValidationOfLogStream:**

Memeriksa apakah aliran log ada di grup CloudWatch log yang disertakan. Jika tidak valid, ini menghentikan inisiasi langkah-langkah otomatisasi lebih lanjut.

- **branchOnValidationOfVpnConnectionId:**

Memeriksa apakah id Koneksi VPN yang termasuk dalam parameter valid. Jika tidak valid, ini menghentikan inisiasi langkah-langkah otomatisasi lebih lanjut.

- **branchOnValidationOfVpnIp:**

Memeriksa apakah alamat IP Tunnel yang disebutkan dalam parameter valid atau tidak. Jika tidak valid maka itu menghentikan eksekusi lebih lanjut dari langkah-langkah otomatisasi.

- **TraceError:**

Membuat panggilan API wawasan log di grup CloudWatch log yang disertakan dan mencari kesalahan yang terkait dengan IKEv1/IKEv2 bersama dengan resolusi yang disarankan terkait.

### 6. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci.

```

▼ Outputs
parameterValidation.LogGroupName
LogGroupValid
parameterValidation.VpnConnection
validVpnConnection
traceErrorTunnel1IKEV2
["IKEV2ErrorCount":0]
traceErrorTunnel2IKEV2
["IKEV2ErrorCount":0]
traceErrorTunnel1IKEV1
{"Error related to : AWS tunnel received DELETE for Phase 2 SA"}
Please treat below as Potential resolution of this error :
AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent Delete_SA message for Phase 2. When AWS receives Delete_SA for Phase 2 from CGW it deletes the Phase 2 of SPI mentioned in Delete_SA request.
Possible reason of CGW sending Delete_SA message can be due to any configurational changes made in CGW side
Next Steps:
* Check IPsec logs on the CGW Device to verify if you are able to see information pertaining to this issue.
References:
["1] Tunnel stability issues during a rekey: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-fix-ikev2-tunnel-instability-rekey/
["2] Phase 2 Troubleshooting: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-phase-2-ipsec/
", "Error related to : AWS tunnel received DELETE for IKE_SA from CGW"}
Please treat below as Potential resolution of this error :
AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent the Delete_SA message for Parent/IKE_SA. When AWS receives Delete_SA from CGW, it honours the message and brings down the VPN tunnel.
There can be various reasons for CGW sending Delete_SA message like :
* A reset to clear active SAs has been performed on the CGW side
* IKE SA has been timed out
* Configurational changes have been made on CGW
Next Steps:
* Review your VPN device idle timeout settings using information from your device vendor. When there is no traffic through a VPN tunnel for the duration of your vendor-specific VPN idle time, the IPsec session terminates. For more information on tunnel inactivity and instability refer to this documentation ["1]
* Check logs on your CGW device to verify if you are able to see information pertaining to this issue.
References:
["1] Tunnel inactivity or instability: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-instability-inactivity/
", "Error related to : No proposal chosen"}
Please treat below as Potential resolution of this error :
AWS CloudWatch monitoring has detected that IKE Phase 2 parameters (such as encryption algorithm, hashing algorithm and DH group) configured on Customer Gateway (CGW) device and AWS VPN endpoint do not match or the CGW is using parameters that are not supported by the AWS VPN.
Next Steps:
* Verify that the Phase 2 parameters (Integrity algorithm, Encryption algorithm and DH group) being proposed by CGW are matching with those configured on AWS side. If you are using default settings on AWS side then verify that parameters being proposed are supported by AWS VPN. To Find list of parameters supported by
* If you want to modify the parameters on the AWS VPN side you can follow below steps:
Step 1: Open the Amazon VPC console at https://console.aws.amazon.com/vpc/
Step 2: In the navigation pane, choose Site-to-Site VPN Connections.
Step 3: Select the Site-to-Site VPN connection, and choose Actions, Modify VPN Tunnel Options.
Step 4: For VPN Tunnel Outside IP Address, choose the tunnel endpoint IP of the VPN tunnel that you are modifying options for.
Step 5: Choose or enter new values for the tunnel options.
Step 6: Choose Save.

```

## Referensi

### Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

### AWSdokumentasi layanan

- [Isi log VPN Site-to-Site](#)

## AWSConfigRemediation-DeleteEgressOnlyInternetGateway

### Deskripsi

AWSConfigRemediation-DeleteEgressOnlyInternetGatewayRunbook menghapus gateway internet khusus egress yang Anda tentukan.

### [Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- EgressOnlyInternetGatewayId

Jenis: String

Deskripsi: (Wajib) ID gateway internet khusus egress yang ingin Anda hapus.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2>DeleteEgressOnlyInternetGateway
- ec2:DescribeEgressOnlyInternetGateways

### Langkah Dokumen

- aws:executeScript- Menghapus gateway internet egress-only yang ditentukan dalam parameter. EgressOnlyInternetGatewayId

- `aws:executeScript`- Memverifikasi gateway internet khusus egres telah dihapus.

## AWSConfigRemediation-DeleteUnusedENI

### Deskripsi

AWSConfigRemediation-DeleteUnusedENIRunbook menghapus elastic network interface (ENI) yang memiliki status lampiran. `detached`

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `NetworkInterfaceId`

Jenis: String

Deskripsi: (Wajib) ID ENI yang ingin Anda hapus.

### Izin IAM yang diperlukan

`AutomationAssumeRole`Parameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

### Langkah Dokumen

- `aws:executeAwsApi`- Menghapus ENI yang Anda tentukan dalam `NetworkInterfaceId` parameter.
- `aws:executeScript`- Memverifikasi ENI telah dihapus.

## AWSConfigRemediation-DeleteUnusedSecurityGroup

### Deskripsi

AWSConfigRemediation-DeleteUnusedSecurityGroupRunbook menghapus grup keamanan yang Anda tentukan dalam parameter. `GroupId` Jika Anda mencoba menghapus grup keamanan yang terkait dengan instans Amazon Elastic Compute Cloud (Amazon EC2), atau direferensikan oleh grup keamanan lain, otomatisasi akan gagal. Otomatisasi ini tidak menghapus grup keamanan default.

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

### Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- GroupId

Jenis: String

Deskripsi: (Wajib) ID grup keamanan yang ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2>DeleteSecurityGroup

Langkah Dokumen

- aws:executeAwsApi- Mengembalikan nama grup keamanan menggunakan nilai yang Anda berikan dalam GroupId parameter.
- aws:branch- Mengonfirmasi bahwa nama grup tidak "default".
- aws:executeAwsApi- Menghapus grup keamanan yang ditentukan dalam GroupId parameter.
- aws:executeScript- Mengonfirmasi grup keamanan telah dihapus.

## **AWSConfigRemediation-DeleteUnusedVPCNetworkACL**

Deskripsi

AWSConfigRemediation-DeleteUnusedVPCNetworkACLRunbook menghapus daftar kontrol akses jaringan (ACL) yang tidak terkait dengan subnet.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen



## Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `NetworkAcId`

Jenis: String

Deskripsi: (Wajib) ID ACL jaringan yang ingin Anda hapus.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2>DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

### Langkah Dokumen

- `aws:executeAwsApi`- Menghapus ACL jaringan yang ditentukan dalam parameter. `NetworkAcId`

- `aws:executeScript`- Mengonfirmasi ACL jaringan yang ditentukan dalam `NetworkACLId` parameter telah dihapus.

## AWSConfigRemediation-DeleteVPCFlowLog

### Deskripsi

AWSConfigRemediation-DeleteVPCFlowLogRunbook menghapus log aliran virtual private cloud (VPC) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `FlowLogId`

Jenis: String

Deskripsi: (Wajib) ID log aliran yang ingin Anda hapus.

### Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2>DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

#### Langkah Dokumen

- `aws:executeAwsApi`- Menghapus log aliran yang Anda tentukan dalam `FlowLogId` parameter.
- `aws:executeScript`- Memverifikasi log aliran telah dihapus.

## **AWSConfigRemediation-DetachAndDeleteInternetGateway**

### Deskripsi

AWSConfigRemediation-DetachAndDeleteInternetGatewayRunbook melepaskan dan menghapus gateway internet yang Anda tentukan. Jika instans Amazon EC2 di cloud pribadi virtual (VPC) Anda memiliki alamat IP elastis atau alamat IPv4 publik yang terkait dengannya, runbook gagal.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- InternetGatewayId

Jenis: String

Deskripsi: (Wajib) ID gateway internet yang ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2>DeleteInternetGateway
- ec2:DescribeInternetGateways
- ec2:DetachInternetGateway

Langkah Dokumen

- aws:waitForAwsResourceProperty- Menerima ID gateway pribadi virtual dan menunggu sampai properti negara gateway pribadi virtual berubah available atau habis waktu.
- aws:executeAwsApi- Mengambil konfigurasi gateway pribadi virtual yang ditentukan.
- aws:branch- Cabang berdasarkan nilai VpcAttachments parameter.state.
- aws:waitForAwsResourceProperty- Menerima ID gateway pribadi virtual dan menunggu hingga VpcAttachments properti.state gateway pribadi virtual berubah attached atau habis waktu.
- aws:executeAwsApi- Menerima ID gateway pribadi virtual dan ID VPC Amazon sebagai input, dan melepaskan gateway pribadi virtual dari VPC Amazon.
- aws:waitForAwsResourceProperty- Menerima ID gateway pribadi virtual dan menunggu hingga VpcAttachments properti.state gateway pribadi virtual berubah detached atau habis waktu.

- `aws:executeAwsApi`- Menerima ID gateway pribadi virtual sebagai input dan menghapusnya.
- `aws:waitForAwsResourceProperty`- Menerima ID gateway pribadi virtual sebagai input dan memverifikasi penghapusannya.
  - `aws:executeAwsApi`- Mengumpulkan ID VPC dari ID gateway internet.
- `aws:executeAwsApi`- Melepaskan ID gateway internet dari VPC.
- `aws:executeAwsApi`- Menghapus gateway internet.

## **AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway**

### Deskripsi

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGatewayRunbook melepaskan dan menghapus gateway pribadi virtual Amazon Elastic Compute Cloud (Amazon EC2) yang terpasang pada virtual private cloud (VPC) yang dibuat dengan Amazon Virtual Private Cloud (Amazon VPC).

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `VpnGatewayId`

Jenis: String

Deskripsi: (Wajib) ID gateway pribadi virtual yang akan dihapus.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2>DeleteVpnGateway`
- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

### Langkah Dokumen

- `aws:waitForAwsResourceProperty`- Menerima ID gateway pribadi virtual dan menunggu sampai properti negara gateway pribadi virtual berubah `available` atau habis waktu.
- `aws:executeAwsApi`- Mengambil konfigurasi gateway pribadi virtual yang ditentukan.
- `aws:branch`- Cabang berdasarkan nilai `VpcAttachments parameter.state`.
- `aws:waitForAwsResourceProperty`- Menerima ID gateway pribadi virtual dan menunggu hingga `VpcAttachments properti.state` gateway pribadi virtual berubah `attached` atau habis waktu.
- `aws:executeAwsApi`- Menerima ID gateway pribadi virtual dan ID VPC Amazon sebagai input, dan melepaskan gateway pribadi virtual dari VPC Amazon.
- `aws:waitForAwsResourceProperty`- Menerima ID gateway pribadi virtual dan menunggu hingga `VpcAttachments properti.state` gateway pribadi virtual berubah `detached` atau habis waktu.

- `aws:executeAwsApi`- Menerima ID gateway pribadi virtual sebagai input dan menghapusnya.
- `aws:waitForAwsResourceProperty`- Menerima ID gateway pribadi virtual sebagai input dan memverifikasi penghapusannya.

## AWS-DisableIncomingSSHOnPort22

### Deskripsi

AWS-DisableIncomingSSHOnPort22Runbook menghapus aturan yang memungkinkan lalu lintas SSH masuk yang tidak dibatasi pada port TCP 22 untuk grup keamanan.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux,macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `SecurityGroupIds`

Jenis: String

Deskripsi: (Wajib) Daftar ID grup keamanan yang dipisahkan koma yang ingin Anda batasi lalu lintas SSH.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Langkah Dokumen

- `aws:executeAwsApi`- Menghapus semua aturan yang memungkinkan lalu lintas SSH masuk pada port TCP 22 dari grup keamanan yang Anda tentukan dalam parameter. `SecurityGroupIds`

Keluaran

`DisableIncomingSSTemplate.RestrictedSecurityGroupIds` - Daftar ID grup keamanan yang memiliki aturan SSH masuk dihapus.

## AWS-DisablePublicAccessForSecurityGroup

Deskripsi

Runbook ini menonaktifkan port SSH dan RDP default yang dibuka ke semua alamat IP.


### Important

Runbook ini gagal dengan "InvalidPermission.NotFound"kesalahan untuk grup keamanan yang memenuhi kedua kriteria berikut: 1) Grup keamanan terletak di VPC non-default; dan 2) Aturan masuk untuk grup keamanan tidak menentukan port terbuka menggunakan keempat pola berikut:

- `0.0.0.0/0`
- `::/0`



- SSH or RDP port + `0.0.0.0/0`
- SSH or RDP port + `::/0`

 Note

Runbook ini tidak tersedia di Wilayah AWS wilayah China.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- GroupId

Jenis: String

Deskripsi: (Wajib) ID grup keamanan tempat port harus dinonaktifkan.

- IpAddressToBlock

Jenis: String

Deskripsi: (Opsional) Alamat IPv4 tambahan dari mana akses harus diblokir, dalam format.

1.2.3.4/32

## **AWSConfigRemediation-DisableSubnetAutoAssignPublicIP**

### Deskripsi

AWSConfigRemediation-DisableSubnetAutoAssignPublicIPRunbook menonaktifkan atribut pengalamanan publik IPv4 untuk subnet yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- SubnetId

Jenis: String

Deskripsi: (Wajib) ID subnet tempat Anda ingin menonaktifkan atribut alamat IPv4 publik yang ditetapkan secara otomatis.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

### Langkah Dokumen

- `aws:executeAwsApi`- Menonaktifkan atribut alamat IPv4 publik yang ditetapkan secara otomatis untuk subnet yang Anda tentukan dalam parameter. SubnetId
- `aws:assertAwsResourceProperty`- Memverifikasi atribut telah dinonaktifkan.

## AWSSupport - EnableVPCFlowLogs

### Deskripsi

AWSSupport - EnableVPCFlowLogs Runbook membuat Log Aliran Amazon Virtual Private Cloud (Amazon VPC) untuk subnet, antarmuka jaringan, dan VPC di file Anda. Akun AWS Jika Anda membuat flow log untuk subnet atau VPC, setiap elastic network interface di subnet atau Amazon VPC akan dipantau. Data log aliran dipublikasikan ke grup CloudWatch log Amazon Logs atau bucket Amazon Simple Storage Service (Amazon S3) S3 yang Anda tentukan. Untuk informasi selengkapnya tentang log aliran, lihat [Log Aliran VPC](#) di Panduan Pengguna Amazon VPC.

#### Important

Biaya konsumsi data dan arsip untuk log vended berlaku saat Anda memublikasikan log aliran ke Log atau ke Amazon CloudWatch S3. Untuk informasi selengkapnya, lihat [harga Flow Logs](#)

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

## Pemilik

Amazon

## Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- DeliverLogsPermissionArn

Jenis: String

Deskripsi: (Opsional) ARN untuk peran IAM yang mengizinkan Amazon Elastic Compute Cloud (Amazon EC2) memublikasikan log alur ke grup log Log di akun Anda. CloudWatch Jika Anda menentukan s3 LogDestinationType parameter, jangan berikan nilai untuk parameter ini. Untuk informasi selengkapnya, lihat [Menerbitkan log alur ke CloudWatch Log](#) di Panduan Pengguna Amazon VPC.

- LogDestinationARN

Jenis: String

Deskripsi: (Opsional) ARN sumber daya tempat data log aliran diterbitkan. Jika cloud-watch-logs ditentukan untuk LogDestinationType parameter, berikan ARN dari grup CloudWatch log Log yang ingin Anda publikasikan data log aliran. Alternatif lainnya, gunakan LogGroupName sebagai gantinya. Jika s3 ditentukan untuk LogDestinationType parameter, Anda harus menentukan ARN bucket Amazon S3 yang ingin Anda publikasikan data log aliran untuk parameter ini. Anda juga dapat menentukan folder di ember.

- LogDestinationType

Jenis: String

Nilai yang valid: cloud-watch-logs | s3

Deskripsi: (Wajib) Menentukan di mana data log aliran diterbitkan. Jika Anda menentukan `LogDestinationType` sebagai `s3`, jangan tentukan `DeliverLogsPermissionArn` atau `LogGroupName`.

- `LogFormat`

Jenis: String

Deskripsi: (Opsional) Bidang yang akan disertakan dalam log aliran, dan urutan tampilannya dalam catatan. Untuk daftar bidang yang tersedia, lihat [Catatan log aliran](#) di Panduan Pengguna Amazon VPC. Jika Anda tidak memberikan nilai untuk parameter ini, log aliran dibuat menggunakan format default. Jika Anda menentukan parameter ini, Anda harus menentukan setidaknya satu bidang.

- `LogGroupName`

Jenis: String

Deskripsi: (Opsional) Nama grup CloudWatch log tempat data log aliran diterbitkan. Jika Anda menentukan `s3` `LogDestinationType` parameter, jangan berikan nilai untuk parameter ini.

- `ResourceIds`

Jenis: StringList

Deskripsi: (Wajib) Daftar ID yang dipisahkan koma untuk subnet, antarmuka jaringan elastis, atau VPC yang ingin Anda buat log alirannya.

- `TrafficType`

Jenis: String

Nilai yang valid: TERIMA | TOLAK | SEMUA

Deskripsi: (Wajib) Jenis lalu lintas untuk log. Anda dapat mencatat lalu lintas yang diterima atau ditolak sumber daya, atau semua lalu lintas.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2>DeleteFlowLogs`
- `ec2:DescribeFlowLogs`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:CreatePolicy`
- `iam>DeletePolicy`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:GetPolicy`
- `iam:GetRole`
- `iam:TagRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `iam:UpdateRole`
- `logs:CreateLogDelivery`
- `logs:CreateLogGroup`
- `logs>DeleteLogDelivery`
- `logs>DeleteLogGroup`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `s3:GetBucketAcl`

## Langkah Dokumen

- `aws:branch-` Cabang berdasarkan nilai yang ditentukan untuk `LogDestinationType` parameter.

- `aws:executeScript`- Membuat grup log jika tidak ada nilai yang ditentukan untuk `LogDestinationARN` parameter, dan `cloud-watch-logs` ditentukan untuk `LogDestinationType` parameter.
- `aws:executeScript`- Membuat log aliran berdasarkan nilai yang ditentukan dalam parameter runbook.

## AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

### Deskripsi

`AWSConfigRemediation-EnableVPCFlowLogsToCloudWatchRunbook` menggantikan log aliran Amazon VPC yang sudah ada yang menerbitkan data log aliran ke Amazon Simple Storage Service (Amazon S3) dengan log alur yang menerbitkan data log aliran ke grup log Amazon CloudWatch Logs (Log) yang Anda tentukan. CloudWatch

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `DestinationLogGroup`

Jenis: String

Deskripsi: (Wajib) Nama grup CloudWatch log Log yang ingin Anda publikasikan data log aliran.

- `DeliverLogsPermissionArn`

Jenis: String

Deskripsi: (Diperlukan) ARN dari peran AWS Identity and Access Management (IAM) yang ingin Anda gunakan yang menyediakan Amazon Elastic Compute Cloud (Amazon EC2) izin yang diperlukan untuk mempublikasikan data log aliran ke Log. CloudWatch

- `FlowLogId`

Jenis: String

Deskripsi: (Wajib) ID log alur yang diterbitkan ke Amazon S3 yang ingin Anda ganti.

- `MaxAggregationInterval`

Jenis: Integer

Nilai yang valid: 60 | 600

Deskripsi: (Opsional) Interval waktu maksimum, dalam detik, di mana aliran paket ditangkap dan dikumpulkan ke dalam catatan log aliran.

- `TrafficType`

Jenis: String

Nilai yang valid: TERIMA | TOLAK | SEMUA

Deskripsi: (Wajib) Jenis data log aliran yang ingin Anda rekam dan publikasikan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2>DeleteFlowLogs`



- `ec2:DescribeFlowLogs`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan detail tentang VPC Anda dari nilai yang Anda tentukan dalam `FlowLogId` parameter.
- `aws:executeAwsApi`- Membuat log aliran berdasarkan nilai yang Anda tentukan untuk parameter runbook.
- `aws:assertAwsResourceProperty`- Memverifikasi log alur yang baru dibuat diterbitkan ke CloudWatch Log.
- `aws:executeAwsApi`- Menghapus log aliran yang diterbitkan ke Amazon S3.
- `aws:executeScript`- Mengonfirmasi log aliran yang diterbitkan ke Amazon S3 telah dihapus.

## **AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket**

### Deskripsi

AWSConfigRemediation-EnableVPCFlowLogsToS3BucketRunbook menggantikan log aliran VPC Amazon yang sudah ada yang menerbitkan data log aliran ke Amazon CloudWatch Logs (CloudWatch Log) dengan log alur yang menerbitkan data log aliran ke bucket Amazon Simple Storage Service (Amazon S3) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- Destinas3 BucketArn

Jenis: String

Deskripsi: (Wajib) ARN bucket Amazon S3 yang ingin Anda publikasikan data log alur.

- FlowLogId

Jenis: String

Deskripsi: (Wajib) ID log alur yang diterbitkan ke CloudWatch Log yang ingin Anda ganti.

- MaxAggregationInterval

Jenis: Integer

Nilai yang valid: 60 | 600

Deskripsi: (Opsional) Interval waktu maksimum, dalam detik, di mana aliran paket ditangkap dan dikumpulkan ke dalam catatan log aliran.

- TrafficType

Jenis: String

Nilai yang valid: TERIMA | TOLAK | SEMUA

Deskripsi: (Wajib) Jenis data log aliran yang ingin Anda rekam dan publikasikan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`

- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

### Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan detail tentang VPC Anda dari nilai yang Anda tentukan dalam `FlowLogId` parameter.
- `aws:executeAwsApi`- Membuat log aliran berdasarkan nilai yang Anda tentukan untuk parameter runbook.
- `aws:assertAwsResourceProperty`- Memverifikasi log alur yang baru dibuat diterbitkan ke Amazon S3.
- `aws:executeAwsApi`- Menghapus log aliran yang diterbitkan ke CloudWatch Log.
- `aws:executeScript`- Mengonfirmasi alur log yang dipublikasikan ke CloudWatch Log telah dihapus.

## AWS-ReleaseElasticIP

### Deskripsi

Lepaskan alamat IP elastis yang ditentukan menggunakan ID alokasi.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- AllocationId

Jenis: String

Deskripsi: (Wajib) ID Alokasi alamat IP Elastis.

## **AWS-RemoveNetworkACLUnrestrictedSSHRDP**

Deskripsi

AWS-RemoveNetworkACLUnrestrictedSSHRDPRunbook menghapus semua aturan daftar kontrol akses jaringan (ACL) dari ACL jaringan tertentu yang memungkinkan lalu lintas masuk dari semua alamat sumber ke port SSH dan RDP default. Aturan yang menyertakan rentang port yang tumpang tindih dengan port SSH dan RDP default tidak dihapus.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan

tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- NetworkAcId

Jenis: String

Deskripsi: (Wajib) ID ACL jaringan yang ingin Anda hapus aturan tidak terbatas yang memungkinkan lalu lintas masuk dari semua alamat sumber ke port SSH dan RDP default.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkACLEntry`
- `ec2:DescribeNetworkACLs`

Langkah Dokumen

- `aws:executeScript`- Menghapus semua aturan masuk yang memungkinkan lalu lintas dari semua alamat sumber dari grup keamanan yang Anda tentukan dalam `SecurityGroupId` parameter.

Keluaran

`RemoveNACLEntriesAndVerify.VerificationMessage` - Pesan verifikasi dari aturan ACL jaringan yang berhasil dihapus.

`RemoveNACLEntriesAndVerify.RulesDeletedAndApiResponse` - Aturan ACL jaringan yang dihapus, dan tanggapan operasi `DeleteNetworkACLEntry` API.

## **AWSConfigRemediation- RemoveUnrestrictedSourceIngressRules**

Deskripsi

`AWSConfigRemediation-RemoveUnrestrictedSourceIngressRulesRunbook` menghapus semua aturan masuk dari grup keamanan yang Anda tentukan yang mengizinkan lalu lintas dari semua alamat sumber.

### [Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `SecurityGroupId`

Jenis: String

Deskripsi: (Wajib) ID grup keamanan tempat Anda ingin menghapus aturan masuknya yang mengizinkan lalu lintas dari semua alamat sumber.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

### Langkah Dokumen

- `aws:executeScript`- Menghapus semua aturan masuk yang memungkinkan lalu lintas dari semua alamat sumber dari grup keamanan yang Anda tentukan dalam `SecurityGroupId` parameter.

## **AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules**

### Deskripsi

`AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRulesRunbook` menghapus semua aturan dari grup keamanan default virtual private cloud (VPC) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `GroupId`

Jenis: String

Deskripsi: (Wajib) ID grup keamanan tempat Anda ingin menghapus semua aturan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Langkah Dokumen

- `aws:assertAwsResourceProperty`- Mengonfirmasi grup keamanan yang Anda tentukan dalam `GroupId` parameter bernama `default`.
- `aws:executeScript`- Menghapus semua aturan dari grup keamanan yang Anda tentukan dalam `GroupId` parameter.

## **AWSSupport-SetupIPMonitoringFromVPC**

Deskripsi

`AWSSupport-SetupIPMonitoringFromVPC` membuat instance Amazon Elastic Compute Cloud (Amazon EC2) di subnet yang ditentukan dan memantau IP target yang dipilih (IPv4 atau IPv6) dengan terus menjalankan pengujian ping, MTR, traceroute, dan tracetcp. Hasilnya disimpan di CloudWatch log Amazon Logs, dan filter metrik diterapkan untuk memvisualisasikan statistik latensi dan kehilangan paket dengan cepat di dasbor. CloudWatch

Informasi Tambahan

Data CloudWatch Log dapat digunakan untuk pemecahan masalah jaringan dan analisis pola/tren. Selain itu, Anda dapat mengonfigurasi CloudWatch alarm dengan notifikasi Amazon SNS



saat kehilangan paket dan/atau latensi mencapai ambang batas. Data juga dapat digunakan saat membuka kasus dengan AWS Support, untuk membantu mengisolasi masalah dengan cepat dan mengurangi waktu penyelesaian saat menyelidiki masalah jaringan.

#### Note

Untuk membersihkan sumber daya yang dibuat oleh `AWSSupport-SetupIPMonitoringFromVPC`, Anda dapat menggunakan runbook `AWSSupport-TerminateIPMonitoringFromVPC`. Untuk informasi selengkapnya, lihat [AWSSupport-TerminateIPMonitoringFromVPC](#).

### Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- `CloudWatchLogGroupNamePrefix`

Jenis: String

Default: `/AWSSupport-SetupIPMonitoringFromVPC`

Deskripsi: (Opsional) Awalan yang digunakan untuk setiap grup CloudWatch log yang dibuat untuk hasil pengujian.

- CloudWatchLogGroupRetentionInDays

Jenis: String

Nilai yang valid: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

Default: 7

Deskripsi: (Opsional) Jumlah hari Anda ingin menyimpan hasil pemantauan jaringan untuk.

- InstanceType

Jenis: String

Nilai yang valid: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

Default: t2.micro

Deskripsi: (Opsional) Jenis instans EC2 untuk instans EC2Rescue. Ukuran yang disarankan: t2.micro.

- SubnetId

Jenis: String

Deskripsi: (Wajib) ID subnet untuk contoh monitor. Ketahuilah bahwa jika Anda menentukan subnet pribadi, maka Anda harus memastikan ada akses Internet untuk memungkinkan instance monitor untuk mengatur pengujian (artinya, instal agen CloudWatch Log, berinteraksi dengan Systems Manager dan CloudWatch).

- TargetIPs

Jenis: String

Deskripsi: (Wajib) Daftar IPv4 dan/atau IPv6 yang dipisahkan koma untuk dipantau. Tidak boleh ada spasi. Ukuran maksimum adalah 255 karakter. Ketahuilah bahwa jika Anda memberikan IP yang tidak valid, maka otomatisasi akan gagal dan mengembalikan pengaturan pengujian.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan bahwa pengguna yang menjalankan otomatisasi memiliki kebijakan terkelola AmazonSSM AutomationRole IAM yang dilampirkan. Selain itu, pengguna harus memiliki kebijakan berikut yang dilampirkan ke akun pengguna, grup, atau peran mereka:

```

    {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteInstanceProfile",
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::
        AWS_account_ID
        :role/AWSSupport/SetupIPMonitoringFromVPC_*",
        "arn:aws:iam::
        AWS_account_ID
        :instance-profile/AWSSupport/SetupIPMonitoringFromVPC_*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource": [

```

```
        "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "cloudwatch:DeleteDashboards"
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypes",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:AssignIpv6Addresses",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "ssm:GetParameter",
        "ssm:SendCommand",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
    ],
    "Resource": [
        "*"
    ],
}
```

```

    "Effect": "Allow"
  }
]
}

```

## Langkah Dokumen

1. **aws:executeAwsApi**- jelaskan subnet yang disediakan.
2. **aws:branch**- mengevaluasi input TargetTips.

(IPv6) Jika TargetTips berisi IPv6:

**aws:assertAwsResourceProperty**- periksa subnet yang disediakan memiliki kolom IPv6 terkait

3. **aws:executeScript**- dapatkan arsitektur tipe instans dan jalur parameter publik untuk Amazon Linux 2 terbaru AMI.
4. **aws:executeAwsApi**- dapatkan Amazon Linux 2 terbaru AMI dari Parameter Store.
5. **aws:executeAwsApi**- buat grup keamanan untuk pengujian di VPC subnet.

(Pembersihan) Jika pembuatan grup keamanan gagal:

**aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

6. **aws:executeAwsApi**- memungkinkan semua lalu lintas keluar dalam kelompok keamanan uji.

(Pembersihan) Jika pembuatan aturan keluar grup keamanan gagal:

**aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

7. **aws:executeAwsApi**- buat peran IAM untuk instance EC2 pengujian

(Pembersihan) Jika pembuatan peran gagal:

a. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi, jika ada.

b. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

8. **aws:executeAwsApi**- lampirkan kebijakan terkelola ManagedInstanceCore AmazonSSM

(Pembersihan) Jika lampiran kebijakan gagal:

a. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi, jika dilampirkan.

- b. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
  - c. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.
9. **aws:executeAwsApi**- lampirkan kebijakan inline untuk memungkinkan pengaturan retensi grup CloudWatch log dan membuat dasbor CloudWatch

(Pembersihan) Jika lampiran kebijakan inline gagal:

- a. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi, jika dibuat.
  - b. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
  - c. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
  - d. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.
- 10 **aws:executeAwsApi**- membuat profil instans IAM.

(Pembersihan) Jika pembuatan profil instance gagal:

- a. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi, jika ada.
  - b. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
  - c. **aws:executeAwsApi**- hapus kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
  - d. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
  - e. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.
- 11 **aws:executeAwsApi**- mengaitkan profil instans IAM ke peran IAM.

(Pembersihan) Jika profil instance dan asosiasi peran gagal:

- a. **aws:executeAwsApi**- menghapus profil instans IAM dari peran, jika terkait.
  - b. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
  - c. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
  - d. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
  - e. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
- aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

12 **aws:sleep**- tunggu profil instance tersedia.

13 **aws:runInstances**- buat contoh pengujian di subnet yang ditentukan, dan dengan profil instance yang dibuat sebelumnya terlampir.

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
- b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
- c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
- d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
- e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
- f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
- g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

14 **aws:branch**- mengevaluasi input TargeTips.

(IPv6) Jika TargeTips berisi IPv6:

**aws:executeAwsApi**- menetapkan IPv6 untuk contoh pengujian.

15 **aws:waitForAwsResourceProperty**- tunggu instance pengujian menjadi instance terkelola.

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
- b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
- c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
- d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
- e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
- f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
- g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

16 **aws:runCommand**- instal prasyarat uji:

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
  - b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
  - c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
  - d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
  - e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
  - f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
  - g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.
- 17 **aws:runCommand**- memvalidasi IP yang disediakan adalah alamat IPv4 dan/atau IPv6 yang benar secara sintaksis:

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
  - b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
  - c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
  - d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
  - e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
  - f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
  - g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.
- 18 **aws:runCommand**- tentukan tes MTR untuk masing-masing IP yang disediakan.

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
- b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
- c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
- d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
- e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
- f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.



g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

19 **aws:runCommand**- tentukan tes ping pertama untuk masing-masing IP yang disediakan.

(Pembersihan) Jika langkah gagal:

a. **aws:changeInstanceState**- menghentikan contoh pengujian.

b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.

c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.

d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.

e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.

f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.

g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

20 **aws:runCommand**- tentukan tes ping kedua untuk masing-masing IP yang disediakan.

(Pembersihan) Jika langkah gagal:

a. **aws:changeInstanceState**- menghentikan contoh pengujian.

b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.

c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.

d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.

e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.

f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.

g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

21 **aws:runCommand**- tentukan tes tracepath untuk masing-masing IP yang disediakan.

(Pembersihan) Jika langkah gagal:

a. **aws:changeInstanceState**- menghentikan contoh pengujian.

b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.

c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.

d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.

- e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
- f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
- g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

22**aws:runCommand**- tentukan tes traceroute untuk masing-masing IP yang disediakan.

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
- b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
- c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
- d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
- e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
- f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
- g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

23**aws:runCommand**- mengkonfigurasi CloudWatch log.

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
- b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
- c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
- d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
- e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
- f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
- g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

24**aws:runCommand**- jadwalkan cronjobs untuk menjalankan setiap tes setiap menit.

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
- b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.

- c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
  - d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
  - e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
  - f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
  - g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.
- 25 **aws:sleep**- tunggu tes untuk menghasilkan beberapa data.
- 26 **aws:runCommand**- mengatur retensi grup CloudWatch log yang diinginkan.

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
  - b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
  - c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
  - d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
  - e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
  - f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
  - g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.
- 27 **aws:runCommand**- mengatur filter metrik grup CloudWatch log.

(Pembersihan) Jika langkah gagal:

- a. **aws:changeInstanceState**- menghentikan contoh pengujian.
- b. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
- c. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
- d. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
- e. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
- f. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
- g. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

**28aws:runCommand**- buat CloudWatch dasbor.

(Pembersihan) Jika langkah gagal:

- a. **aws:executeAwsApi**- hapus CloudWatch dasbor, jika ada.
- b. **aws:changeInstanceState**- menghentikan contoh pengujian.
- c. **aws:executeAwsApi**- menghapus profil instans IAM dari peran.
- d. **aws:executeAwsApi**- hapus profil instans IAM yang dibuat oleh otomatisasi.
- e. **aws:executeAwsApi**- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
- f. **aws:executeAwsApi**- lepaskan kebijakan ManagedInstanceCore terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
- g. **aws:executeAwsApi**- hapus peran IAM yang dibuat oleh otomatisasi.
- h. **aws:executeAwsApi**- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

Keluaran

createCloudWatchDashboards.Output - URL dasbor. CloudWatch

createManagedInstance. InstanceIds - ID contoh uji.

## **AWSSupport-TerminateIPMonitoringFromVPC**

Deskripsi

AWSSupport-TerminateIPMonitoringFromVPCmengakhiri tes pemantauan IP yang sebelumnya dimulai olehAWSSupport-SetupIPMonitoringFromVPC. Data yang terkait dengan ID tes yang ditentukan akan dihapus.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- AutomationExecutionId

Jenis: String

Deskripsi: (Wajib) ID eksekusi otomatisasi dari saat Anda sebelumnya menjalankan `AWSSupport-SetupIPMonitoringFromVPC` runbook. Semua sumber daya yang terkait dengan ID eksekusi ini dihapus.

- InstanceId

Jenis: String

Deskripsi: (Wajib) ID instans untuk instance monitor.

- SubnetId

Jenis: String

Deskripsi: (Wajib) ID subnet untuk contoh monitor.

## Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan bahwa pengguna yang menjalankan otomatisasi memiliki kebijakan terkelola `AmazonSSM AutomationRole` IAM yang dilampirkan. Selain itu, pengguna harus memiliki kebijakan berikut yang melekat pada pengguna, grup, atau peran mereka:

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Action": [
      "iam:DetachRolePolicy",
      "iam:RemoveRoleFromInstanceProfile",
      "iam>DeleteRole",
      "iam>DeleteInstanceProfile",
      "iam>DeleteRolePolicy"
    ],
    "Resource": [
      "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport/
SetupIPMonitoringFromVPC_*",
      "arn:aws:iam::An-AWS-Account-ID:instance-profile/AWSSupport/
SetupIPMonitoringFromVPC_*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "iam:DetachRolePolicy"
    ],
    "Resource": [
      "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "cloudwatch>DeleteDashboards"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "ec2:DescribeTags",
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups",
      "ec2>DeleteSecurityGroup",
      "ec2:TerminateInstances",
      "ec2:DescribeInstanceStatus"
    ]
  }
]

```

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

## Langkah Dokumen

1. `aws:assertAwsResourceProperty`- periksa `AutomationExecutionId` dan `InstanceId` terkait dengan tes yang sama.
2. `aws:assertAwsResourceProperty`- periksa `SubnetId` dan `InstanceId` terkait dengan tes yang sama.
3. `aws:executeAwsApi`- mengambil kelompok keamanan uji.
4. `aws:executeAwsApi`- hapus CloudWatch dasbor.
5. `aws:changeInstanceState`- menghentikan contoh pengujian.
6. `aws:executeAwsApi`- menghapus profil instans IAM dari peran.
7. `aws:executeAwsApi`- hapus profil instans IAM yang dibuat oleh otomatisasi.
8. `aws:executeAwsApi`- hapus kebijakan CloudWatch inline dari peran yang dibuat oleh otomatisasi.
9. `aws:executeAwsApi`- lepaskan kebijakan `ManagedInstanceCore` terkelola AmazonSSM dari peran yang dibuat oleh otomatisasi.
10. `aws:executeAwsApi`- hapus peran IAM yang dibuat oleh otomatisasi.
11. `aws:executeAwsApi`- hapus grup keamanan yang dibuat oleh otomatisasi, jika ada.

## Keluaran

Tidak ada

## AWS WAF

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan sebelumnya untuk AWS WAF Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

## Topik

- [AWS-AddWAFRegionalRuleToRuleGroup](#)
- [AWS-AddWAFRegionalRuleToWebAcl](#)
- [AWSConfigRemediation-EnableWAFClassicLogging](#)
- [AWSConfigRemediation-EnableWAFClassicRegionalLogging](#)
- [AWSConfigRemediation-EnableWAFV2Logging](#)

## AWS-AddWAFRegionalRuleToRuleGroup

### Deskripsi

AWS-AddWAFRegionalRuleToRuleGroupRunbook menambahkan aturan AWS WAF regional yang ada ke grup aturan AWS WAF regional. Hanya grup aturan regional AWS WAF Klasik yang didukung. AWS WAF Kelompok aturan regional klasik dapat memiliki maksimal 10 aturan.

### [Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- RuleGroupId

Jenis: String



Deskripsi: (Wajib) ID grup aturan yang ingin Anda perbarui.

- RulePriority

Jenis: Integer

Deskripsi: (Wajib) Prioritas untuk aturan baru. Prioritas aturan menentukan urutan di mana aturan dalam kelompok regional dievaluasi. Aturan dengan nilai yang lebih rendah memiliki prioritas lebih tinggi daripada aturan dengan nilai yang lebih tinggi. Nilai harus berupa bilangan bulat unik. Jika Anda menambahkan beberapa aturan ke grup aturan regional, nilainya tidak harus berurutan.

- RuleId

Jenis: String

Deskripsi: (Wajib) ID untuk aturan yang ingin Anda tambahkan ke grup aturan regional Anda.

- RuleAction

Jenis: String

Deskripsi: (Wajib) Menentukan tindakan yang AWS WAF dilakukan saat permintaan web cocok dengan kondisi aturan.

Nilai yang valid: IZINKAN | BLOK | HITUNG

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

Langkah Dokumen

- `getWAF ChangeToken (aws:executeAwsApi)` - Mengambil token AWS WAF perubahan untuk memastikan runbook tidak mengirimkan permintaan yang bertentangan ke layanan.
- `addWAF RuleTo WAF RegionalRuleGroup (AWS:executeScript)` - Menambahkan aturan yang ditentukan ke grup aturan regional. AWS WAF
- `VerifyChangeTokenPropagating (aws: waitforAwsResourceProperty)` - Memverifikasi token perubahan memiliki status PENDING atauINSYNC.
- `VerifyRuleAddedToRuleGroup (AWS:ExecuteScript)` - Memverifikasi aturan yang ditentukan ditambahkan ke AWS WAF grup aturan regional target.

## Keluaran

- `VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse` - Keluaran dari langkah yang memverifikasi bahwa aturan baru diajukan ke kelompok aturan regional.
- `VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse` - Output dari operasi `ListActivatedRulesInRuleGroup` API.

# AWS-AddWAFRegionalRuleToWebACL

## Deskripsi

AWS-AddWAFRegionalRuleToWebACLRunbook menambahkan aturan AWS WAF regional, grup aturan, atau aturan berbasis tarif yang ada ke daftar kontrol akses web regional AWS WAF Klasik (ACL). Runbook ini tidak memperbarui ACL web regional AWS WAF Classic yang ada yang dikelola oleh. AWS Firewall Manager

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux,macOS, Windows

## Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- WebACLId

Jenis: String

Deskripsi: (Wajib) ID ACL web yang ingin Anda perbarui.

- ActivatedRulePriority

Jenis: Integer

Deskripsi: (Wajib) Prioritas untuk aturan baru. Prioritas aturan menentukan urutan di mana aturan dalam ACL web dievaluasi. Aturan dengan nilai yang lebih rendah memiliki prioritas lebih tinggi daripada aturan dengan nilai yang lebih tinggi. Nilai harus berupa bilangan bulat unik. Jika Anda menambahkan beberapa aturan ke ACL web regional, nilainya tidak harus berurutan.

- ActivatedRuleRuleId

Jenis: String

Deskripsi: (Wajib) ID untuk aturan reguler, aturan berbasis tarif, atau grup yang ingin Anda tambahkan ke ACL web.

- ActivatedRuleAction

Jenis: String

Nilai yang valid: IZINKAN | BLOK | HITUNG

Deskripsi: (Opsional) Menentukan tindakan yang AWS WAF diambil ketika permintaan web cocok dengan kondisi aturan.

- ActivatedRuleType

Jenis: String

Nilai yang valid: `REGULER` | `RATE_BASED` | `KELOMPOK`

Default: `REGULER`

Deskripsi: (Opsional) Jenis aturan yang Anda tambahkan ke ACL web. Meskipun bidang ini opsional, perhatikan bahwa jika Anda mencoba menambahkan `RATE_BASED` aturan ke ACL web tanpa menyetel jenisnya, permintaan gagal karena permintaan default ke aturan. `REGULAR`

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

Langkah Dokumen

- `DetermineWebACL NotIn FMS AndRulePriority` (AWS: `ExecuteScript`) - Memverifikasi apakah ACL web AWS WAF berada dalam kebijakan keamanan Firewall Manager dan memverifikasi ID prioritas tidak bertentangan dengan ACL yang ada.
- `AddRuleOrRuleGroupToWebACL` (AWS: `ExecuteScript`) - Menambahkan aturan yang ditentukan ke ACL web. AWS WAF
- `VerifyRuleOrRuleGroupAddedToWebAcl` (AWS: `ExecuteScript`) - Memverifikasi AWS WAF aturan yang ditentukan ditambahkan ke ACL web target.

Keluaran

- `DetermineWebACL NotIn AndRulePriority FMS`. `PrereqResponse`: Keluaran dari `DetermineWebACLNotInFMSAndRulePriority` langkah.
- `VerifyRuleOrRuleGroupAddedToWebAcl`. `VerifyRuleOrRuleGroupAddedToWebACLResponse`: Keluaran dari langkah. `AddRuleOrRuleGroupToWebACL`

- `VerifyRuleOrRuleGroupAddedToWebAcl`. `ListActivatedRulesOrRuleGroupsInWebACLResponse`: Output dari langkah. `VerifyRuleOrRuleGroupAddedToWebAcl`

## AWSConfigRemediation-EnableWAFClassicLogging

### Deskripsi

AWSConfigRemediation-EnableWAFClassicLoggingRunbook memungkinkan pencatatan ke Amazon Data Firehose (Firehose) untuk AWS WAF daftar kontrol akses web (web ACL) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `DeliveryStreamName`

Jenis: String

Deskripsi: (Wajib) Nama aliran pengiriman Firehose yang ingin Anda kirim log.

- `WebACLId`

Jenis: String

Deskripsi: (Wajib) ID ACL AWS WAF web yang ingin Anda aktifkan untuk masuk.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

Langkah Dokumen

- `aws:executeAwsApi`- Mengonfirmasi aliran pengiriman yang Anda tentukan di yang `DeliveryStreamName` ada.
- `aws:executeAwsApi`- Mengumpulkan ARN dari ACL web AWS WAF yang ditentukan dalam parameter. `WebACLId`
- `aws:executeAwsApi`- Memungkinkan logging untuk ACL web.
- `aws:assertAwsResourceProperty`- Verifikasi logging telah diaktifkan di AWS WAF web ACL.

## **AWSConfigRemediation-EnableWAFClassicRegionalLogging**

Deskripsi

AWSConfigRemediation-EnableWAFClassicRegionalLoggingRunbook memungkinkan pencatatan ke Amazon Data Firehose (Firehose) untuk daftar kontrol akses web ( AWS WAF ACL) yang Anda tentukan.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `LogDestinationConfigs`

Jenis: String

Deskripsi: (Wajib) Nama Sumber Daya Amazon (ARN) dari aliran pengiriman Firehose yang ingin Anda kirim log.

- `WebACLIId`

Jenis: String

Deskripsi: (Wajib) ID ACL AWS WAF web yang ingin Anda aktifkan untuk masuk.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

### Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan ARN dari ACL web AWS WAF yang ditentukan dalam parameter. `WebACLId`
- `aws:executeAwsApi`- Memungkinkan logging untuk ACL web.
- `aws:assertAwsResourceProperty`- Verifikasi logging telah diaktifkan di AWS WAF web ACL.

## **AWSConfigRemediation-EnableWAFV2Logging**

### Deskripsi

`AWSConfigRemediation-EnableWAFV2LoggingRunbook` memungkinkan pencatatan untuk daftar kontrol akses web AWS WAF (AWS WAF V2) (ACL web) dengan aliran pengiriman Amazon Data Firehose (Firehose) yang ditentukan.

[Jalankan Otomasi ini \(konsol\)](#)

### Jenis dokumen

### Otomatisasi

### Pemilik

Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`




Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- LogDestinationConfigs

Jenis: String

Deskripsi: (Wajib) Aliran pengiriman Firehose ARN yang ingin Anda kaitkan dengan ACL web.

 Note

Aliran pengiriman Firehose ARN harus dimulai dengan awalan. `aws-waf-logs-` Misalnya, `aws-waf-logs-us-east-2-analytics`. Untuk informasi selengkapnya, lihat [Amazon Data Firehose](#).

- WebAclArn

Jenis: String

Deskripsi: (Diperlukan) ARN dari ACL web yang logging akan diaktifkan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
  
- `wafv2:GetLoggingConfiguration`

Langkah Dokumen

- `aws:executeScript`- Mengaktifkan logging untuk ACL web AWS WAF V2 dan memverifikasi bahwa logging memiliki konfigurasi yang ditentukan.

## Amazon WorkSpaces

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon WorkSpaces Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWS-CreateWorkSpace](#)
- [AWSSupport-RecoverWorkSpace](#)

### AWS-CreateWorkSpace

Deskripsi

`AWS-CreateWorkSpaceRunbook` membuat desktop WorkSpaces virtual Amazon baru, yang dikenal sebagai WorkSpace, berdasarkan nilai yang Anda tentukan untuk parameter input. Untuk selengkapnya WorkSpaces, lihat [Apa itu Amazon WorkSpaces?](#) di Panduan WorkSpaces Administrasi Amazon.

[Jalankan Otomasi ini \(konsol\)](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- BundleId

Jenis: String

Deskripsi: (Wajib) ID bundel yang akan digunakan untuk file WorkSpace.

- ComputeTypeName

Jenis: String

Nilai yang valid: NILAI | STANDAR | KINERJA | DAYA | GRAFIK | POWERPRO | GRAPHICSPRO

Deskripsi: (Opsional) Jenis komputasi untuk Anda WorkSpace.

- DirectoryId

Jenis: String

Deskripsi: (Wajib) ID direktori untuk menambahkan Anda WorkSpace ke.

- RootVolumeEncryptionEnabled

Jenis: Boolean

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Menentukan apakah volume root WorkSpace dienkripsi.

- RootVolumeSizeGib

Jenis: Integer

Deskripsi: (Wajib) Ukuran volume root untuk file WorkSpace.

- RunningMode

Jenis: String

Nilai yang valid: ALWAYS\_ON | AUTO\_STOP

Deskripsi: (Diperlukan) Mode berjalan dari WorkSpace.

- `RunningModeAutoStopTimeoutInMinutes`

Jenis: Integer

Deskripsi: (Opsional) Waktu setelah pengguna log off ketika WorkSpaces berhenti. Tentukan nilai dalam interval 60 menit.

- `Tag`

Jenis: String

Deskripsi: (Opsional) Tag yang ingin Anda terapkan pada WorkSpace.

- `UserName`

Jenis: String

Deskripsi: (Wajib) Nama pengguna untuk dikaitkan dengan WorkSpace.

- `UserVolumeEncryptionEnabled`

Jenis: Boolean

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Menentukan apakah volume pengguna WorkSpace dienkripsi.

- `UserVolumeSizeGib`

Jenis: Integer

Deskripsi: (Wajib) Ukuran volume pengguna untuk file WorkSpace.

- `VolumeEncryptionKey`

Jenis: String

Deskripsi: (Opsional) AWS Key Management Service Kunci simetris yang ingin Anda gunakan untuk mengenkripsi data yang disimpan pada Anda. WorkSpace

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

#### Langkah Dokumen

- `aws:executeScript`- Membuat `WorkSpace` berdasarkan nilai yang Anda tentukan untuk parameter input.
- `aws:waitForAwsResourceProperty`- Memverifikasi keadaan `WorkSpace` adalah `AVAILABLE`.

#### Keluaran

`CreateWorkspace.WorkspaceId`

## **AWSSupport-RecoverWorkSpace**

#### Deskripsi

`AWSSupport-RecoverWorkSpaceRunbook` melakukan langkah-langkah pemulihan di desktop `WorkSpaces` virtual Amazon, yang dikenal sebagai `WorkSpace`, yang Anda tentukan. Runbook mereboot `WorkSpace`, dan jika statusnya `UNHEALTHY`, mengembalikan atau membangun kembali `WorkSpace` berdasarkan nilai yang Anda tentukan untuk parameter input. Sebelum menggunakan runbook ini, kami sarankan untuk meninjau [Masalah Pemecahan Masalah WorkSpaces di Panduan Administrasi](#) Amazon. `WorkSpaces`

#### Important

Memulihkan atau membangun kembali `WorkSpace` adalah tindakan yang berpotensi merusak yang dapat mengakibatkan hilangnya data. Ini karena `WorkSpace` dipulihkan dari snapshot terakhir yang tersedia dan data yang dipulihkan dari snapshot bisa setua 12 jam.

Opsi pemulihan membuat ulang volume root dan volume pengguna berdasarkan snapshot terbaru. Opsi rebuild membuat ulang volume pengguna dari snapshot terbaru dan membuat ulang `WorkSpace` dari gambar yang terkait dengan bundel tempat dibuat. `WorkSpace` Aplikasi yang diinstal atau pengaturan sistem yang diubah setelah `WorkSpace` dibuat hilang. Untuk informasi selengkapnya tentang memulihkan dan membangun kembali

WorkSpaces, lihat [Memulihkan WorkSpace](#) dan [Membangun Kembali a WorkSpace di Panduan](#) Administrasi Amazon WorkSpaces .

## Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Jenis: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.

- Akui

Jenis: String

Nilai yang valid: Ya

Deskripsi: (Wajib) Memasukkan ya berarti Anda memahami tindakan pemulihan dan pembangunan kembali akan mencoba memulihkan WorkSpace dari snapshot terbaru, dan bahwa data yang dipulihkan dari snapshot ini bisa setua 12 jam.

- Mulai ulang

Jenis: String

Nilai yang valid: Ya | Tidak

Default: Ya

Deskripsi: (Wajib) Menentukan WorkSpace apakah reboot.

- Membangun kembali

Jenis: String

Nilai yang valid: Ya | Tidak

Default: tidak

Deskripsi: (Wajib) Menentukan WorkSpace apakah dibangun kembali.

- Memulihkan

Jenis: String

Nilai yang valid: Ya | Tidak

Default: tidak

Deskripsi: (Wajib) Menentukan WorkSpace apakah dipulihkan.

- Workspaceld

Jenis: String

Deskripsi: (Wajib) ID yang ingin WorkSpace Anda pulihkan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`

- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

## Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan keadaan yang WorkSpace Anda tentukan dalam `WorkspaceId` parameter.
- `aws:assertAwsResourceProperty`- Memverifikasi keadaan WorkSpace adalah `AVAILABLE`, `ERROR`, `IMPAIREDSTOPPED`, atau `UNHEALTHY`.
- `aws:branch`- Cabang berdasarkan keadaan WorkSpace.
- `aws:executeAwsApi`- Mulai WorkSpace.
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan untuk `Action` parameter.
- `aws:waitForAwsResourceProperty`- Menunggu WorkSpace status setelah dimulai.
- `aws:waitForAwsResourceProperty`- Menunggu WorkSpace negara berubah menjadi `AVAILABLE`, `ERRORIMPAIRED`, atau `UNHEALTHY` setelah dimulai.
- `aws:executeAwsApi`- Mengumpulkan keadaan WorkSpace setelah dimulai.
- `aws:branch`- Cabang berdasarkan keadaan WorkSpace setelah dimulai.
- `aws:executeAwsApi`- Mengumpulkan snapshot yang tersedia untuk memulihkan atau membangun kembali. WorkSpace
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan untuk `Reboot` parameter.
- `aws:executeAwsApi`- Reboot. WorkSpace
- `aws:executeAwsApi`- Mengumpulkan keadaan WorkSpace setelah dimulai.
- `aws:waitForAwsResourceProperty`- Menunggu keadaan berubah WorkSpace menjadi `REBOOTING`.
- `aws:waitForAwsResourceProperty`- Menunggu WorkSpace status berubah menjadi `AVAILABLE`, `ERROR`, atau `UNHEALTHY` setelah di-boot ulang.
- `aws:executeAwsApi`- Mengumpulkan keadaan WorkSpace setelah di-boot ulang.
- `aws:branch`- Cabang berdasarkan keadaan WorkSpace setelah reboot.
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan untuk `Restore` parameter.
- `aws:executeAwsApi`- Mengembalikan. WorkSpace Jika pemulihan gagal, runbook mencoba membangun kembali file. WorkSpace



- `aws:waitForAwsResourceProperty`- Menunggu keadaan berubah `WorkSpace` menjadi `RESTORING`.
- `aws:waitForAwsResourceProperty`- Menunggu `WorkSpace` negara berubah menjadi `AVAILABLE`, `ERROR`, atau `UNHEALTHY` setelah dipulihkan.
- `aws:executeAwsApi`- Mengumpulkan keadaan `WorkSpace` setelah dipulihkan.
- `aws:branch`- Cabang berdasarkan keadaan `WorkSpace` setelah pemulihan.
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan untuk `Rebuild` parameter.
- `aws:executeAwsApi`- Membangun kembali. `WorkSpace`
- `aws:waitForAwsResourceProperty`- Menunggu keadaan berubah `WorkSpace` menjadi `REBUILDING`.
- `aws:waitForAwsResourceProperty`- Menunggu `WorkSpace` negara berubah menjadi `AVAILABLE`, `ERROR`, atau `UNHEALTHY` setelah dibangun kembali.
- `aws:executeAwsApi`- Mengumpulkan keadaan `WorkSpace` setelah dibangun kembali.
- `aws:assertAwsResourceProperty`- Mengonfirmasi keadaan `WorkSpace` adalah `AVAILABLE`.

## X-Ray

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk. AWS X-Ray Untuk informasi selengkapnya tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

### Topik

- [AWSConfigRemediation-UpdateXRayKMSKey](#)

## AWSConfigRemediation-UpdateXRayKMSKey

### Deskripsi

`AWSConfigRemediation-UpdateXRayKMSKeyRunbook` memungkinkan enkripsi pada AWS X-Ray data Anda menggunakan kunci AWS Key Management Service (AWS KMS). Runbook ini hanya boleh digunakan sebagai baseline untuk memastikan bahwa AWS X-Ray data Anda dienkrpsi sesuai dengan praktik terbaik keamanan minimum yang direkomendasikan. Kami merekomendasikan mengenkripsi beberapa set data dengan kunci KMS yang berbeda.

[Jalankan Otomasi ini \(konsol\)](#)

## Jenis dokumen

### Otomatisasi

### Pemilik

### Amazon

### Platform

Linux, macOS, Windows

### Parameter

- `AutomationAssumeRole`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.

- `KeyId`

Jenis: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN), ID kunci, atau alias kunci kunci KMS yang ingin Anda gunakan AWS X-Ray untuk mengenkripsi data.

### Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

### Langkah Dokumen

- `aws:executeAwsApi`- Mengaktifkan enkripsi pada data X-Ray Anda menggunakan kunci KMS yang Anda tentukan dalam `KeyId` parameter.
- `aws:waitForAwsResourceProperty`- Menunggu status konfigurasi enkripsi X-Ray ACTIVE Anda.
- `aws:executeAwsApi`- Mengumpulkan ARN dari kunci yang Anda tentukan dalam `KeyId` parameter.
- `aws:assertAwsResourceProperty`- Memverifikasi enkripsi telah diaktifkan pada X-Ray Anda.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.