



Panduan Pengguna

AWS Systems Manager Referensi Buku Runbook Otomasi



AWS Systems Manager Referensi Buku Runbook Otomasi: Panduan Pengguna

Copyright © 2026 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 pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Referensi Buku Runbook Otomasi	1
Lihat konten runbook	4
API Gateway	4
AWSConfigRemediation-DeleteAPIGatewayStage	4
AWSConfigRemediation-EnableAPIGatewayTracing	6
AWSConfigRemediation-UpdateAPIGatewayMethodCaching	7
AWSSupport-TroubleshootAPIGatewayHttpErrors	9
AWS Batch	14
AWSSupport-TroubleshootAWSBatchJob	14
CloudFormation	20
AWS-DeleteCloudFormationStack	21
AWS-EnableCloudFormationSNSNotification	22
AWS-RunCfnLint	24
AWSSupport-TroubleshootCFNCustomResource	26
AWS-UpdateCloudFormationStack	28
CloudFront	29
AWSConfigRemediation-EnableCloudFrontDefaultRootObject	29
AWSConfigRemediation-EnableCloudFrontAccessLogs	31
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity	33
AWSConfigRemediation-EnableCloudFrontOriginFailover	34
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS	36
CloudTrail	38
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail	38
AWS-EnableCloudTrail	40
AWS-EnableCloudTrailCloudWatchLogs	41
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS	43
AWS-EnableCloudTrailKmsEncryption	44
AWSConfigRemediation-EnableCloudTrailLogFileValidation	46
AWS-EnableCloudTrailLogFileValidation	47
AWS-QueryCloudTrailLogs	48
CloudWatch	51
AWS-ConfigureCloudWatchOnEC2Instance	51
AWS-EnableCWAlarm	52
AWSSupport-TroubleshootCloudWatchAgent	55

AWSSupport-TroubleshootCloudWatchAlarm	62
Amazon DocumentDB	69
AWS-EnableDocDbClusterBackupRetentionPeriod	69
CodeBuild	72
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMScmk	72
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject	74
AWS CodeDeploy	75
AWSSupport-TroubleshootCodeDeploy	75
AWS Config	77
AWSSupport-SetupConfig	78
Amazon Connect	80
AWSSupport-AssociatePhoneNumbersToConnectContactFlows	81
AWSSupport-CollectAmazonConnectContactFlowLog	89
AWS Directory Service	95
AWS-CreateDSManagementInstance	95
AWSSupport-TroubleshootADConnectorConnectivity	100
AWSSupport-TroubleshootDirectoryTrust	104
AWS AppSync	107
AWS-EnableAppSyncGraphQLApiLogging	107
Amazon Athena	110
AWS-EnableAthenaWorkGroupEncryptionAtRest	110
DynamoDB	112
AWS-ChangeDDBRWCapacityMode	113
AWS-CreateDynamoDBBackup	115
AWS-DeleteDynamoDbBackup	116
AWSConfigRemediation-DeleteDynamoDbTable	117
AWS-DeleteDynamoDbTableBackups	118
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable	120
AWSConfigRemediation-EnablePITRForDynamoDbTable	121
AWS-EnableDynamoDbAutoscaling	123
AWS-RestoreDynamoDBTable	126
AWS Database Migration Service	129
AWSSupport-TroubleshootDMSTableErrors	129
AWSSupport-TroubleshootDMSEndpointConnection	135
Amazon EBS	145
AWSSupport-AnalyzeEBSResourceUsage	145

AWS-ArchiveEBSSnapshots	152
AWS-AttachEBSVolume	154
AWSSupport-CalculateEBSPerformanceMetrics	155
AWS-CopySnapshot	162
AWS-CreateSnapshot	163
AWS-DeleteSnapshot	164
AWSConfigRemediation-DeleteUnusedEBSVolume	165
AWS-DeregisterAMIs	167
AWS-DetachEBSVolume	168
AWSConfigRemediation-EnableEbsEncryptionByDefault	169
AWS-ExtendEbsVolume	171
AWSSupport-ModifyEBSSnapshotPermission	173
AWSConfigRemediation-ModifyEBSVolumeType	175
Amazon EC2	177
AWS-ASGEnterStandby	179
AWS-ASGExitStandby	180
AWS-CreateImage	181
AWS-DeleteImage	183
AWS-PatchAsgInstance	184
AWS-PatchInstanceWithRollback	187
AWS-QuarantineEC2Instance	189
AWS-ResizeInstance	191
AWS-RestartEC2Instance	192
AWS-SetupJupyter	193
AWS-StartEC2Instance	197
AWS-StopEC2Instance	198
AWS-TerminateEC2Instance	198
AWS-UpdateLinuxAmi	199
AWS-UpdateWindowsAmi	203
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck	207
AWSConfigRemediation-EnforceEC2InstanceIMDSv2	209
AWSEC2-CloneInstanceAndUpgradeSQLServer	210
AWSEC2-CloneInstanceAndUpgradeWindows	214
AWSEC2-PatchLoadBalancerInstance	218
AWSEC2-SQLServerDBRestore	219
AWSSupport-ActivateWindowsWithAmazonLicense	225

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2	228
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD	233
AWSSupport-CheckXenToNitroMigrationRequirements	238
AWSSupport-CloneXenEC2InstanceAndMigrateToNitro	241
AWSSupport-ConfigureEC2Metadata	249
AWSSupport-ContainEC2Instance	252
AWSSupport-CopyEC2Instance	263
AWSPremiumSupport-DiagnoseDiskUsageOnLinux	269
AWSSupport-EnableWindowsEC2SerialConsole	273
AWSPremiumSupport-ExtendVolumesOnWindows	281
AWSSupport-ExecuteEC2Rescue	285
AWSSupport-ListEC2Resources	288
AWSSupport-ManageRDPSettings	290
AWSSupport-ManageWindowsService	293
AWSSupport-MigrateEC2ClassicToVPC	295
AWSSupport-MigrateXenToNitroLinux	301
AWSSupport-ResetAccess	313
AWSSupport-ResetLinuxUserPassword	316
AWSSupport-RunEC2RescueForWindowsTool	323
AWSPremiumSupport-ResizeNitroInstance	327
AWSSupport-ShareEncryptedAMIOrEBSSnapshot	334
AWSSupport-RestoreEC2InstanceFromSnapshot	339
AWSSupport-SendLogBundleToS3Bucket	343
AWSSupport-StartEC2RescueWorkflow	345
AWSSupport-TroubleshootActiveDirectoryReplication	356
AWSPremiumSupport-TroubleshootEC2DiskUsage	361
AWSSupport-TroubleshootEC2InstanceConnect	366
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs	372
AWSSupport-TroubleshootRDP	375
AWSSupport-TroubleshootSSH	381
AWSSupport-TroubleshootSUSERegistration	385
AWSSupport-TroubleshootWindowsPerformance	387
AWSSupport-TroubleshootWindowsUpdate	394
AWSSupport-UpgradeWindowsAWSDrivers	401
Amazon ECS	405
AWSSupport-CollectECSInstanceLogs	405

AWS-InstallAmazonECSAgent	408
AWS-ECSRunTask	410
AWSSupport-TroubleshootECSTaskFailedToStart	414
AWSSupport-TroubleshootECSTaskFailedToStart	416
AWS-UpdateAmazonECSAgent	420
Amazon EFS	422
AWSSupport-CheckAndMountEFS	423
Amazon EKS	426
AWS-CreateEKSClusterWithFargateProfile	426
AWS-CreateEKSClusterWithNodegroup	430
AWS-DeleteEKSCluster	433
AWS-MigrateToNewEKSSelfManagedNodeGroup	437
AWSPremiumSupport-TroubleshootEKSCluster	443
AWSSupport-TroubleshootEKSWorkerNode	447
AWS-UpdateEKSCluster	449
AWS-UpdateEKSSelfManagedLinuxNodeGroups	450
AWS-UpdateEKSSelfManagedLinuxNodeGroups	454
AWSSupport-CollectEKSLinuxNodeStatistics	458
AWSSupport-CollectEKSInstanceLogs	464
AWSSupport-SetupK8sApiProxyForEKS	468
AWSSupport-TroubleshootEbsCsiDriversForEks	479
AWSSupport-TroubleshootEKSSALBControllerIssues	488
Elastic Beanstalk	499
AWSSupport-CollectElasticBeanstalkLogs	500
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ..	503
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications	504
AWSSupport-TroubleshootElasticBeanstalk	506
Elastic Load Balancing	509
AWSConfigRemediation-DropInvalidHeadersForALB	509
AWS-EnableCLBAccessLogs	511
AWS-EnableCLBConnectionDraining	513
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing	514
AWSConfigRemediation-EnableELBDeletionProtection	516
AWSConfigRemediation-EnableLoggingForALBAndCLB	517
AWSSupport-TroubleshootCLBConnectivity	519
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing	522

AWS-UpdateALBDesyncMitigationMode	523
AWS-UpdateCLBDesyncMitigationMode	525
AWSSupport-TroubleshootELBHealthChecks	527
Amazon EMR	532
AWSSupport-AnalyzeEMRLogs	532
AWSSupport-DiagnoseEMRLogsWithAthena	538
OpenSearch Layanan Amazon	547
AWSConfigRemediation-DeleteOpenSearchDomain	548
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain	549
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups	550
AWSSupport-TroubleshootOpenSearchRedYellowCluster	552
AWSSupport-TroubleshootOpenSearchHighCPU	558
EventBridge	565
AWS-AddOpsItemDedupStringToEventBridgeRule	565
AWS-DisableEventBridgeRule	567
AWS Glue	568
AWSSupport-TroubleshootGlueConnection	568
Amazon FSx	579
AWSSupport-ValidateFSxWindowsADConfig	580
GuardDuty	594
AWSConfigRemediation-CreateGuardDutyDetector	594
IAM	595
AWSSupport-TroubleshootIAMAccessDeniedEvents	596
AWS-AttachIAMToInstance	603
AWS-DeleteIAMInlinePolicy	605
AWSConfigRemediation-DeleteIAMRole	606
AWSConfigRemediation-DeleteIAMUser	608
AWSConfigRemediation-DeleteUnusedIAMGroup	610
AWSConfigRemediation-DeleteUnusedIAMPolicy	612
AWSConfigRemediation-DetachIAMPolicy	613
AWSConfigRemediation-EnableAccountAccessAnalyzer	615
AWSSupport-GrantPermissionsToIAMUser	616
AWSConfigRemediation-RemoveUserPolicies	621
AWSConfigRemediation-ReplaceIAMInlinePolicy	623
AWSConfigRemediation-RevokeUnusedIAMUserCredentials	625
AWSConfigRemediation-SetIAMPasswordPolicy	627

AWSSupport-ContainIAMPrincipal	630
AWSSupport-TroubleshootSAMLIssues	644
Deteksi dan Respon Insiden	650
AWSPremiumSupport-OnboardWorkloadToIDR	650
Amazon Kinesis Data Streams	657
AWS-EnableKinesisStreamEncryption	658
AWS KMS	660
AWSConfigRemediation-CancelKeyDeletion	660
AWSConfigRemediation-EnableKeyRotation	661
Lambda	663
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing	663
AWSConfigRemediation-DeleteLambdaFunction	664
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK	666
AWSConfigRemediation-MoveLambdaToVPC	667
AWSSupport-RemediateLambdaS3Event	669
AWSSupport-TroubleshootLambdaInternetAccess	672
AWSSupport-TroubleshootLambdaS3Event	676
Amazon Managed Workflows for Apache Airflow	677
AWSSupport-TroubleshootMWAAEnvironmentCreation	678
Neptune	684
AWS-EnableNeptuneDbAuditLogsToCloudWatch	684
AWS-EnableNeptuneDbBackupRetentionPeriod	685
AWS-EnableNeptuneClusterDeletionProtection	687
Amazon RDS	689
AWS-CreateEncryptedRdsSnapshot	690
AWS-CreateRdsSnapshot	693
AWSConfigRemediation-DeleteRDSCluster	694
AWSConfigRemediation-DeleteRDSClusterSnapshot	695
AWSConfigRemediation-DeleteRDSInstance	697
AWSConfigRemediation-DeleteRDSInstanceSnapshot	699
AWSConfigRemediation-DisablePublicAccessToRDSInstance	700
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster	702
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance	703
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance	705
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance	707
AWSConfigRemediation-EnableMultiAZOnRDSInstance	709

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance	710
AWSConfigRemediation-EnableRDSClusterDeletionProtection	713
AWSConfigRemediation-EnableRDSInstanceBackup	714
AWSConfigRemediation-EnableRDSInstanceDeletionProtection	716
AWSConfigRemediation-ModifyRDSInstancePortNumber	718
AWSSupport-ModifyRDSSnapshotPermission	720
AWSPremiumSupport-PostgreSQLWorkloadReview	722
AWS-RebootRdsInstance	738
AWSSupport-ShareRDSSnapshot	739
AWS-StartRdsInstance	743
AWS-StartStopAuroraCluster	744
AWS-StopRdsInstance	746
AWSSupport-TroubleshootConnectivityToRDS	747
AWSSupport-TroubleshootRDSIAMAuthentication	749
AWSSupport-ValidateRdsNetworkConfiguration	757
Amazon Redshift	763
AWSConfigRemediation-DeleteRedshiftCluster	763
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster	765
AWSConfigRemediation-EnableRedshiftClusterAuditLogging	766
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot	768
AWSConfigRemediation-EnableRedshiftClusterEncryption	769
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting	771
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster	772
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings	774
AWSConfigRemediation-ModifyRedshiftClusterNodeType	776
Amazon S3	778
AWS-ArchiveS3BucketToIntelligentTiering	779
AWS-ConfigureS3BucketLogging	781
AWS-ConfigureS3BucketVersioning	783
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock	784
AWSConfigRemediation-ConfigureS3PublicAccessBlock	786
AWS-CreateS3PolicyToExpireMultipartUploads	789
AWS-DisableS3BucketPublicReadWrite	791
AWS-EnableS3BucketEncryption	792
AWS-EnableS3BucketKeys	793
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy	795

AWSConfigRemediation-RestrictBucketSSLRequestsOnly	796
AWSSupport-TroubleshootS3PublicRead	797
AWSSupport-ConfigureS3ReplicationSameAndCrossAccount	803
AWSSupport-EmptyS3Bucket	822
AWSSupport-TroubleshootS3EventNotifications	829
AWSSupport-ContainS3Resource	836
Amazon SES	845
AWSSupport-AnalyzeSESMessagesSendingStatus	846
AWSSupport-DeploySESSendingLogsToCloudWatchLogs	850
SageMaker AI	856
AWS-DisableSageMakerNotebookRootAccess	856
Secrets Manager	858
AWSConfigRemediation-DeleteSecret	859
AWSConfigRemediation-RotateSecret	860
Security Hub CSPM	862
AWSConfigRemediation-EnableSecurityHub	862
AWS Shield	863
AWSPremiumSupport-DDoSResiliencyAssessment	864
Amazon SNS	872
AWS-EnableSNSTopicDeliveryStatusLogging	873
AWSConfigRemediation-EncryptSNSTopic	875
AWS-PublishSNSNotification	877
Amazon SQS	878
AWS-EnableSQSEncryption	878
Step Functions	880
AWS-EnableStepFunctionsStateMachineLogging	881
Systems Manager	883
AWS-BulkDeleteAssociation	884
AWS-BulkEditOpsItems	885
AWS-BulkResolveOpsItems	888
AWS-ConfigureMaintenanceWindows	890
AWS-CreateManagedLinuxInstance	892
AWS-CreateManagedWindowsInstance	894
AWSConfigRemediation-EnableCWLoggingForSessionManager	897
AWS-ExportOpsDataToS3	898
AWS-ExportPatchReportToS3	900

AWS-SetupInventory	902
AWS-SetupManagedInstance	906
AWS-SetupManagedRoleOnEC2Instance	907
AWSSupport-TroubleshootManagedInstance	909
AWSSupport-TroubleshootPatchManagerLinux	911
AWSSupport-TroubleshootSessionManager	915
Pihak ketiga	921
AWS-CreateJiraIssue	921
AWS-CreateServiceNowIncident	923
AWS-RunPacker	925
Amazon VPC	927
AWS-CloseSecurityGroup	928
AWSSupport-ConfigureDNSQueryLogging	930
AWSSupport-ConfigureTrafficMirroring	933
AWSSupport-ConnectivityTroubleshooter	935
AWSSupport-TroubleshootVPN	939
AWSConfigRemediation-DeleteEgressOnlyInternetGateway	945
AWSConfigRemediation-DeleteUnusedENI	947
AWSConfigRemediation-DeleteUnusedSecurityGroup	948
AWSConfigRemediation-DeleteUnusedVPCNetworkACL	949
AWSConfigRemediation-DeleteVPCFlowLog	951
AWSConfigRemediation-DetachAndDeleteInternetGateway	952
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway	954
AWS-DisableIncomingSSHOnPort22	956
AWS-DisablePublicAccessForSecurityGroup	957
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP	959
AWSSupport-EnableVPCFlowLogs	960
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch	967
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket	969
AWS-ReleaseElasticIP	971
AWS-RemoveNetworkACLUnrestrictedSSHRDP	972
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules	973
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules	975
AWSSupport-SetupIPMonitoringFromVPC	976
AWSSupport-TerminateIPMonitoringFromVPC	984
AWS WAF	988

AWS-AddWAFRegionalRuleToRuleGroup	988
AWS-AddWAFRegionalRuleToWebAcl	990
AWSConfigRemediation-EnableWAFClassicLogging	993
AWSConfigRemediation-EnableWAFClassicRegionalLogging	995
AWSConfigRemediation-EnableWAFV2Logging	996
Amazon WorkSpaces	998
AWS-CreateWorkSpace	998
AWSSupport-RecoverWorkSpace	1001
X-Ray	1005
AWSConfigRemediation-UpdateXRayKMSKey	1006
.....	mviii

Referensi Runbook Otomasi 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 Dukungan, dan AWS Config. Referensi Runbook menjelaskan setiap runbook standar yang disediakan oleh Systems Manager,, Dukungan 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 Dukungan, 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. Setiap nama runbook 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](#)
- [CloudFormation](#)
- [CloudFront](#)
- [CloudTrail](#)
- [CloudWatch](#)
- [Amazon DocumentDB](#)
- [CodeBuild](#)
- [AWS CodeDeploy](#)
- [AWS Config](#)
- [Amazon Connect](#)
- [AWS Directory Service](#)
- [AWS AppSync](#)
- [Amazon Athena](#)
- [DynamoDB](#)
- [AWS Database Migration Service](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [Amazon ECS](#)
- [Amazon EFS](#)
- [Amazon EKS](#)
- [Elastic Beanstalk](#)
- [Elastic Load Balancing](#)
- [Amazon EMR](#)

- [OpenSearch Layanan Amazon](#)
- [EventBridge](#)
- [AWS Glue](#)
- [Amazon FSx](#)
- [GuardDuty](#)
- [IAM](#)
- [Deteksi dan Respon Insiden](#)
- [Amazon Kinesis Data Streams](#)
- [AWS KMS](#)
- [Lambda](#)
- [Amazon Managed Workflows for Apache Airflow](#)
- [Neptune](#)
- [Amazon RDS](#)
- [Amazon Redshift](#)
- [Amazon S3](#)
- [Amazon SES](#)
- [SageMaker AI](#)
- [Secrets Manager](#)
- [Security Hub CSPM](#)
- [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 lebih lanjut 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](#)
- [AWSSupport-TroubleshootAPIGatewayHttpErrors](#)

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

Tipe: 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.

- StageArn

Tipe: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari tahap API Gateway yang ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 yang 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`

Tipe: 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.

- StageArn

Tipe: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari tahap API Gateway yang ingin Anda aktifkan penelusuran.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

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

Langkah Dokumen

- aws:executeScript- Memungkinkan penelusuran 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

Tipe: 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.

- CachingAuthorizedMethods

Jenis: StringList

Deskripsi: (Wajib) 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

Tipe: String

Deskripsi: (Wajib) API Gateway menampilkan ARN untuk API. REST

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

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

Langkah Dokumen

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

AWSSupport-TroubleshootAPIGatewayHttpErrors

Deskripsi

AWSSupport-TroubleshootAPIGatewayHttpErrorsRunbook membantu memecahkan masalah kesalahan 5XX/4XX saat menjalankan API REST Amazon API Gateway API yang diterapkan dengan mengurai log eksekusi and/or akses dan menganalisis kesalahan untuk memberikan langkah-langkah perbaikan melalui artikel dan dokumentasi re:Post. AWS

Important

Runbook ini memiliki batasan sebagai berikut:

- Logging harus diaktifkan. Lihat [Mengatur pencatatan Amazon CloudWatch API menggunakan konsol API Gateway](#).
- Log harus diaktifkan sebelum kesalahan terjadi. Pengambilan dan analisis log tidak dapat dilakukan secara retrospektif.
- Kesalahan tercakup: 500, 502, 503, 504, 401, 403, 429.
- Hanya REST APIs yang didukung. WebSocket dan HTTP (v2) tidak tercakup oleh runbook ini.

Important

Menggunakan runbook ini mungkin dikenakan biaya tambahan terhadap AWS akun Anda untuk CloudWatch Log Amazon yang ditangkap oleh REST API Anda, dan Wawasan CloudWatch Log yang digunakan dalam analisis. Lihat [CloudWatch Harga Amazon](#) untuk detail selengkapnya tentang biaya yang mungkin timbul. Jika `aws:deletestack` langkahnya gagal, buka CloudFormation konsol untuk menghapus tumpukan secara manual. Nama tumpukan yang dibuat oleh runbook ini dimulai dengan `AWSSupport-TroubleshootAPIGatewayHttpErrors`. Untuk informasi tentang menghapus

CloudFormation tumpukan, lihat [Menghapus tumpukan di Panduan Pengguna. AWS CloudFormation](#)

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah validasi dan analisis berikut:

- Memvalidasi bahwa REST API yang ditentukan ada dan Anda memiliki izin yang diperlukan.
- Memvalidasi bahwa tahap yang ditentukan ada di API.
- Memvalidasi bahwa jalur sumber daya yang ditentukan ada di API.
- Memvalidasi bahwa metode HTTP yang ditentukan ada untuk sumber daya.
- Menganalisis CloudWatch Log untuk parameter dan rentang waktu yang ditentukan untuk mengidentifikasi kesalahan dan memberikan rekomendasi remediasi.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `apigateway:GET`
- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`

- logs:PutLogEvents
- logs:StartQuery
- logs:GetQueryResults

Contoh kebijakan IAM:

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

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - Troubleshoot API Gateway HTTP Errors](#) Systems Manager di bawah Dokumen.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan SSM Automation untuk melakukan tindakan

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

- Tipe: `AWS::IAM::Role::Arn`
- RestApId (Diperlukan):
 - Deskripsi: (Wajib) ID API untuk API yang memerlukan pemecahan masalah. Harus berupa string alfanumerik 10 karakter.
 - Tipe: `String`
 - Pola yang Diizinkan: `^[a-zA-Z0-9]{10}$`
- StageName (Diperlukan):
 - Deskripsi: (Wajib) Nama tahap yang dikerahkan. Harus 1-128 karakter yang berisi huruf, angka, garis bawah, atau tanda hubung.
 - Tipe: `String`
 - Pola yang Diizinkan: `^[a-zA-Z0-9_\\-]{1,128}$`
- ResourcePath (Opsional):
 - Deskripsi: (Opsional) Jalur sumber daya untuk metode yang dikonfigurasi. Contoh: `./store/items/{resource}`.
 - Tipe: `String`
 - Default: `/`
- HttpMethod (Opsional):
 - Deskripsi: (Opsional) Metode untuk jalur sumber daya yang dikonfigurasi.
 - Tipe: `String`
 - Nilai yang Diizinkan: `[ANY, DELETE, HEAD, OPTIONS, GET, POST, PUT, PATCH]`
 - Default: `GET`
- StartTime (Opsional):
 - Deskripsi: (Opsional) Tanggal dan waktu mulai untuk menanyakan CloudWatch Log. Format: `yyyy-MM-ddTHH:mm:ss` di zona waktu UTC. Jika tidak ditentukan, defaultnya 3 hari sebelum waktu saat ini.
 - Tipe: `String`
 - Pola yang Diizinkan: `^$|^([0-9]{4}-(0[1-9]|1[0-2])-(0[1-9]|[1-2][0-9]|3[0-1])T(2[0-3]|[01][0-9]):[0-5][0-9]:[0-5][0-9])$`

- EndTime (Opsional):

- Deskripsi: (Opsional) Tanggal dan waktu akhir untuk menanyakan CloudWatch Log. Format: yyyy-MM-ddTHH:mm:ss di zona waktu UTC. Jika tidak ditentukan, default ke waktu saat ini.
- Tipe: String
- Pola yang Diizinkan: `^$|^([0-9]{4}-([01-9]|1[0-2])-([01-9]|1[0-2])[0-9]|3[0-1])T([0-3]|([01])[0-9]):([0-5])[0-9]:([0-5])[0-9]$`
- Default: ""
- AccessLogs (Opsional):
 - Deskripsi: (Opsional) Apakah log akses harus dianalisis.
 - Tipe: Boolean
 - Nilai yang Diizinkan: `[true, false]`
 - Default: false
- RequestId (Opsional):
 - Deskripsi: (Opsional) ID permintaan untuk permintaan di mana kesalahan diamati. Harus format UUID yang valid.
 - Tipe: String
 - Pola yang Diizinkan: `^$|^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})$`
 - Default: ""

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- CheckApiExists:

Memvalidasi bahwa REST API yang disediakan ada dan Anda memiliki izin yang diperlukan untuk mengaksesnya.

- CheckStageExists:

Memvalidasi bahwa nama tahap yang disediakan ada di API yang diberikan dan mengambil informasi grup log akses.

- CheckResourceExists:

Memvalidasi bahwa jalur sumber daya yang disediakan ada di API dan mengambil ID sumber

- **CheckMethodExists:**

Memvalidasi bahwa metode HTTP yang disediakan ada untuk sumber daya yang ditentukan.

- **AnalyseLogs:**

Mencari log menggunakan parameter yang disediakan dan mengembalikan rekomendasi berdasarkan kesalahan yang ditemukan. Langkah ini menganalisis log eksekusi dan akses (jika diaktifkan) untuk mengidentifikasi kesalahan 4XX dan 5XX dan memberikan panduan remediasi khusus.

7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci, termasuk analisis kesalahan dan rekomendasi remediasi.

Referensi

Otomatisasi Systems Manager

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

AWS Batch

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk AWS Batch. Untuk informasi lebih lanjut 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 v CPUs atau sumber daya memori daripada yang dapat disediakan oleh tipe instance 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. [AWSSupport-TroubleshootECSContainerInstance](#)
- 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 alasannya. Untuk informasi lebih lanjut, rujuk [AWSSupport-TroubleshootECSContainerInstance](#)runbook.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: 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

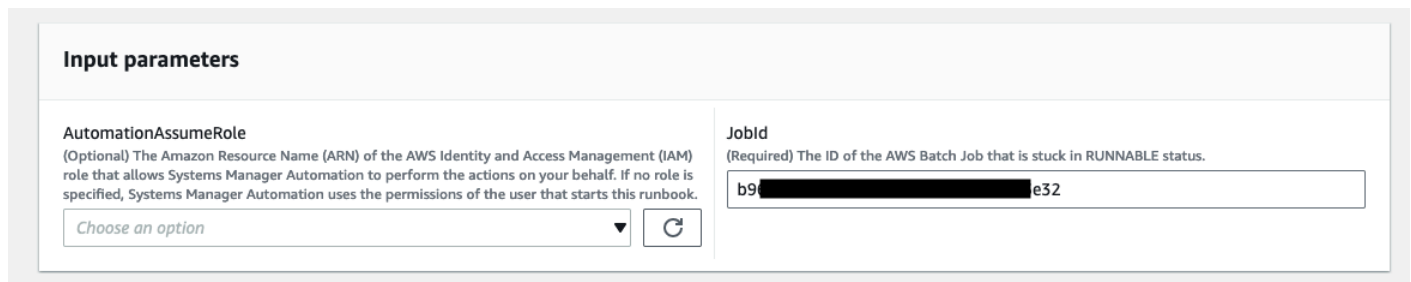
1. Arahkan ke [AWSSupport-TroubleshootAWSBatchJob](#) di AWS Systems Manager Konsol.
2. Pilih Jalankan Otomasi
3. Untuk parameter input, masukkan yang berikut ini:

- AutomationAssumeRole(Optional):

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

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. Choose an option ▼ 	JobId (Required) The ID of the AWS Batch Job that is stuck in RUNNABLE status. 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.

- ProceedOnlyIfBatchJobExistsAndIsInRunnableNegara:

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.

- `ProceedOnlyIfInstancesNotJoiningEcsCluster`:

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-egMKnNEEWmt8eY":
[ERROR]: Job "411-XXXXXXXXXXXXXXXXXXXX-606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnNEEWmt8eY" 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/creating-compute-environments.html
! [WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY".
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-XXXXXXXXXXXXXXXXXXXX-606" exists and is in RUNNABLE status, proceeding further for next steps in execution.

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

[INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY":
[ERROR]: Job "411-XXXXXXXXXXXXXXXXXXXX-606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnNEEWmt8eY" 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/creating-compute-environments.html
! [WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY".
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](#)

CloudFormation

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk AWS CloudFormation Untuk informasi lebih lanjut 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 CloudFormation tumpukan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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.

- StackNameOrId

Tipe: String

Deskripsi: (Wajib) 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 (CloudFormation) yang Anda tentukan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

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

- NotificationArn

Tipe: String

Deskripsi: (Wajib) ARN dari topik Amazon SNS yang ingin Anda kaitkan dengan tumpukan. 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 CloudFormation tentukan.
- EnableCfnSnsNotification (aws:executeAwsApi) - Mengaktifkan notifikasi Amazon SNS untuk tumpukan. CloudFormation
- VerificationCfnSnsNotification (aws:executeScript) - Memverifikasi bahwa notifikasi Amazon SNS telah diaktifkan untuk CloudFormation tumpukan.

Keluaran

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

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

AWS-RunCfnLint

Deskripsi

Runbook ini menggunakan [AWS CloudFormation Linter](#) (`cfn-python-lint`) untuk memvalidasi template YAMAL dan JSON terhadap spesifikasi sumber daya. 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

Tipe: 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.

- ConfigureRuleFlag

Tipe: String

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

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

- FormatFlag

Tipe: String

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

Nilai yang valid: Default | tenang | dapat diuraikan | json

Default: Default

- IgnoreChecksFlag

Tipe: String

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

Contoh: E1001, E1003, W7001

- IncludeChecksFlag

Tipe: String

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

Contoh: E1001, E1003, W7001

- InfoFlag

Tipe: String

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

Bawaan: salah

- TemplateFileName

Tipe: String

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

- **Template3 BucketName**

Tipe: String

Deskripsi: Nama bucket S3 yang berisi template packer.

- **RegionsFlag**

Tipe: String

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

Contoh: `us-east-1, us-west-1`

Langkah Dokumen

`RunCfnLintAgainstTemplate` — Menjalankan `cfn-python-lint` alat terhadap 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 khusus. Runbook memeriksa token layanan yang digunakan untuk sumber daya kustom dan pesan kesalahan yang dikembalikan. Setelah meninjau detail untuk sumber daya kustom, keluaran runbook memberikan penjelasan tentang perilaku tumpukan dan langkah pemecahan masalah untuk sumber daya kustom.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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.

- StackName

Tipe: String

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 CloudFormation tumpukan ada di tempat yang sama Akun AWS dan Wilayah AWS.
- `checkCustomResource`- Menganalisis 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 CloudFormation templat yang disimpan di bucket Amazon S3.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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.

- `LambdaAssumeRole`

Tipe: String

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

- StackNameOrId

Tipe: String

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

- TemplateUrl

Tipe: String

Deskripsi: (Diperlukan) Lokasi bucket S3 yang berisi CloudFormation template yang diperbarui (mis. `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`)

CloudFront

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon CloudFront Untuk informasi lebih lanjut 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

Tipe: 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.

- CloudFrontDistributionId

Tipe: String

Deskripsi: (Wajib) ID CloudFront distribusi yang ingin Anda konfigurasikan objek root default.

- DefaultRootObject

Tipe: String

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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`

Tipe: 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`

Tipe: String

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

Wilayah AWS

- CloudFrontId

Tipe: 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

Tipe: String

Deskripsi: (Opsional) String opsional yang CloudFront ingin Anda awali 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 mengaktifkan 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) tipe Asal tanpa identitas akses asal untuk distribusi yang Anda tentukan. CloudFront 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`

Tipe: 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.

- `CloudFrontDistributionId`

Tipe: String

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

- `OriginAccessIdentityId`

Tipe: String

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

Izin IAM yang diperlukan

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

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

Langkah Dokumen

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

AWSConfigRemediation-EnableCloudFrontOriginFailover

Deskripsi

`AWSConfigRemediation-EnableCloudFrontOriginFailover` Runbook mengaktifkan 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`

Tipe: 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.

- `CloudFrontDistributionId`

Tipe: String

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

- `OriginGroupId`

Tipe: String

Deskripsi: (Wajib) ID grup asal.

- `PrimaryOriginId`

Tipe: String

Deskripsi: (Wajib) ID asal utama di grup asal.

- `SecondaryOriginId`

Tipe: String

Deskripsi: (Wajib) ID asal sekunder di grup asal.

Izin IAM yang diperlukan

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

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

Langkah Dokumen

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

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

Deskripsi

`AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS` runbook mengaktifkan 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

Tipe: 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.

- CloudFrontDistributionId

Tipe: String

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

- ViewerProtocolPolicy

Tipe: String

Nilai yang valid: https-only, redirect-to-https

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 yang ditetapkan.

CloudTrail

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk AWS CloudTrail. Untuk informasi lebih lanjut 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-CreateCloudTrailMultiRegionTrailRunbook` 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

Tipe: 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

Tipe: String

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

- KeyPrefix

Tipe: String

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

- TrailName

Tipe: String

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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`- Mengaktifkan pencatatan 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`

Tipe: 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: String

Deskripsi: (Wajib) Nama bucket S3 yang ditujukan untuk menerbitkan file log.

 Note

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

- TrailName

Tipe: String

Deskripsi: (Wajib) 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

Tipe: 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

Tipe: String

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

- CloudWatchLogsRoleArn

Tipe: 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 terkelola pelanggan AWS Key Management Service (AWS KMS) yang Anda tentukan. Runbook ini hanya boleh digunakan sebagai baseline untuk memastikan bahwa CloudTrail jalur Anda dienkripsi sesuai dengan praktik terbaik keamanan minimum yang direkomendasikan. Kami merekomendasikan mengenkripsi beberapa jalur dengan kunci KMS yang berbeda. CloudTrail file 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 AWS CloudTrail Panduan Pengguna untuk informasi selengkapnya.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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.

- `KMSKeyId`

Tipe: String

Deskripsi: (Wajib) ARN, ID kunci, atau alias kunci dari kunci terkelola pelanggan yang ingin Anda gunakan untuk mengenkripsi jejak yang Anda tentukan dalam parameter. `TrailName`

- `TrailName`

Tipe: String

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

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

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

Tipe: 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.

- KMSKeyId

Tipe: String

Deskripsi: (Wajib) ID kunci 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`

Tipe: 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**

Tipe: 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`

Tipe: 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-QueryCloudTrailLogsRunbook membuat tabel Amazon Athena dari bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service () pilihan Anda yang berisi () log. AWS CloudTrail CloudTrail 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

Tipe: 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.

- Kueri

Tipe: String

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

- SourceBucketPath

Tipe: String

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

- TableName

Tipe: String

Deskripsi: (Opsional) Nama tabel Athena yang dibuat oleh otomatisasi.

Default: cloudtrail_logs

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 lebih lanjut tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWS-ConfigureCloudWatchOnEC2Instance](#)
- [AWS-EnableCWAAlarm](#)
- [AWSSupport-TroubleshootCloudWatchAgent](#)
- [AWSSupport-TroubleshootCloudWatchAlarm](#)

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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID EC2 instans Amazon tempat Anda ingin mengaktifkan CloudWatch pemantauan.

- properti

Tipe: String

Deskripsi: (Opsional) Parameter ini tidak didukung. 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 EC2 instance Amazon 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 Anda 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

Tipe: 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

Tipe: String

Nilai yang valid: GreaterThanOrEqualToThreshold GreaterThanThreshold | GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpperThreshold | LessThanLowerThreshold | LessThanOrEqualToThreshold | LessThanThreshold

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

- MetricName

Tipe: 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 ARNs

Jenis: StringList

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

- Statistik

Tipe: 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

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

AktifkanCWAAlarm. `SuccessfulResources`: Daftar sumber daya ARNs yang CloudWatch alarmnya berhasil dibuat.

AWSSupport-TroubleshootCloudWatchAgent

Deskripsi

AWSSupport-TroubleshootCloudWatchAgentRunbook mengotomatiskan pemecahan masalah Agen Amazon di CloudWatch instans Amazon Elastic Compute Cloud (Amazon EC2). Runbook melakukan pemecahan masalah ini melalui serangkaian pemeriksaan dasar, dan (opsional) yang diperluas.

Pemeriksaan dasar meliputi yang berikut:

- Periksa profil instans AWS Identity and Access Management (IAM)
- Verifikasi apakah izin IAM CloudWatch Agen Amazon yang diperlukan dilampirkan ke instans Amazon EC2

Pemeriksaan tambahan hanya dilakukan jika ID instans Amazon EC2 yang disediakan adalah instans yang dikelola Systems Manager. Pemeriksaan yang diperpanjang ini meliputi yang berikut:

- Periksa status CloudWatch Agen Amazon pada instans
- Menganalisis log CloudWatch Agen Amazon untuk masalah umum dan langkah-langkah pemecahan masalah yang relevan
- Zip log dan file konfigurasi yang relevan di instans Amazon EC2 dan unggah secara opsional ke bucket Amazon Simple Storage Service (Amazon S3) pilihan Anda
- Lakukan pemeriksaan konektivitas antara instance dan titik akhir yang diperlukan

⚠ Important

Ketika `RunVpcReachabilityAnalyzer` parameter diatur `true`, runbook ini akan menentukan apakah ada kebutuhan untuk memanggil runbook anak, `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook anak menggunakan VPC Reachability Analyzer yang memiliki biaya terkait. Untuk informasi lebih lanjut tentang harga, lihat dokumentasi [harga Amazon VPC](#).

⚠ Important

Runbook ini hanya memeriksa peran profil instans IAM Anda untuk izin yang diperlukan. Jika Anda mengandalkan kredensi yang ditentukan dalam `.aws/credentials` file, hasil `verifyIamPermissions` langkah mungkin tidak akurat.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- `getInstanceProfile`: Memverifikasi apakah instans Amazon EC2 yang disediakan memiliki profil instans IAM yang dilampirkan.
- `verifyIamPermissions`: Memeriksa profil instance yang terkait dengan instance untuk menentukan apakah izin IAM yang diperlukan diterapkan.
- `getInstanceInformation`: Memeriksa apakah instance memiliki agen Systems Manager yang aktif, dan mengambil jenis OS instance.
- `getAgentStatus`: Memeriksa status CloudWatch Agen Amazon pada instance (cek diperpanjang).
- `AnalyzeLogs/analyzeLogsWindows`: Menganalisis dan mengeluarkan temuan log CloudWatch Agen Amazon berdasarkan jenis OS.
- `CollectLogs/collectLogsWindows`: Bundel dan output file pemecahan masalah CloudWatch Agen Amazon yang relevan berdasarkan jenis OS.
- `checkEndpointReachability/checkEndpointReachabilityWindows`: Memeriksa apakah instance dapat mencapai titik akhir yang diperlukan berdasarkan jenis OS.
- `analyzeAwsEndpointReachabilityFromEC2`: Memanggil runbook otomatisasi anak untuk memeriksa jangkauan instance yang dipilih ke titik akhir yang diperlukan (jika diaktifkan).

Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- EC2: DescribeInstances
- saya: GetInstanceProfile
- saya: GetRole
- saya: ListAttachedRolePolicies
- saya: ListRolePolicies
- saya: GetRolePolicy
- saya: GetPolicy
- saya: GetPolicyVersion
- saya: SimulatePrincipalPolicy
- ssm: DescribeInstanceInformation
- ssm: SendCommand
- ssm: GetCommandInvocation
- ssm: DescribeInstanceAssociationsStatus
- ssm: StartAutomationExecution

Contoh Kebijakan:

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

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "iam:GetInstanceProfile",
      "iam:GetRole",
      "iam:ListAttachedRolePolicies",
      "iam:ListRolePolicies",
      "iam:GetRolePolicy",
      "iam:GetPolicy",
      "iam:GetPolicyVersion",
      "iam:SimulatePrincipalPolicy",
      "ssm:DescribeInstanceInformation",
      "ssm:SendCommand",
      "ssm:GetCommandInvocation",
      "ssm:DescribeInstanceAssociationsStatus",
      "ssm:StartAutomationExecution"
    ],
    "Resource": "*"
  }
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSsupport-TroubleshootCloudWatchAgent](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (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.
 - Tipe: `AWS::IAM::Role::Arn`
 - InstanceId (Diperlukan):
 - Deskripsi: (Wajib) ID instans Amazon EC2 yang ingin Anda gunakan untuk memecahkan masalah Agen Amazon CloudWatch .

- Tipe: `AWS::EC2::Instance::Id`
- Izinkan Pola: `^i-[0-9a-f]{8,17}$`
- S3 UploadBucket (Opsional):
 - Deskripsi: (Opsional) Nama bucket Amazon S3 untuk mengunggah log CloudWatch Agen Amazon yang dikumpulkan. Profil instans Amazon EC2 harus memiliki izin yang benar untuk mengunggah file ke bucket ini. Ini juga mengharuskan instans Amazon EC2 target menjadi instans yang dikelola Systems Manager.
 - Tipe: `AWS::S3::Bucket::Name`
 - Izinkan Pola: `^$|^[a-z0-9][a-z0-9.-]{1,61}[a-z0-9]$`
 - Default: `""`
- S3 BucketOwnerAccountId (Opsional):
 - Deskripsi: (Opsional) Nomor AWS Akun yang memiliki bucket Amazon S3 tempat Anda ingin mengunggah log Agen CloudWatch Amazon. Jika Anda tidak mengubah parameter ini, runbook menggunakan ID AWS akun pengguna atau peran di mana Otomasi berjalan.
 - Tipe: `String`
 - Izinkan Pola: `^\\{\{\{ global:ACCOUNT_ID \}\}\}$|^[0-9]{12}$`
 - Default: `{ { global:ACCOUNT_ID } }`
- Periksa EC2 Endpoint (Opsional):
 - Deskripsi: (Opsional) Tentukan `true` apakah konfigurasi agen Anda menggunakan opsi `append_dimensions` untuk menambahkan dimensi metrik Amazon EC2 ke metrik yang dikumpulkan oleh agen. Saat `append_dimensions` digunakan, CloudWatch Agen Amazon memerlukan konektivitas ke titik akhir API Amazon EC2, sehingga pengujian konektivitas tambahan akan dilakukan melalui pemeriksaan yang diperluas.
 - Tipe: `String`
 - Nilai yang Diizinkan: `[true, false]`
 - Default: `false`
- RunVpcReachabilityAnalyzer (Opsional):
 - Deskripsi: (Opsional) Tentukan `true` untuk menjalankan otomatisasi `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` anak jika masalah jaringan ditentukan oleh pemeriksaan yang diperluas, atau jika ID instans yang ditentukan bukan instance terkelola.
 - Tipe: `Boolean`
 - Default: `false`

- `RetainVpcReachabilityAnalysis` (Opsional):
 - Deskripsi: (Opsional) Hanya relevan jika `RunVpcReachabilityAnalyzer` adalah `true`. Tentukan `true` untuk mempertahankan jalur wawasan jaringan dan analisis terkait yang dibuat oleh VPC Reachability Analyzer. Secara default, sumber daya tersebut dihapus setelah analisis berhasil.
 - Tipe: `Boolean`
 - Default: `false`

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- `getInstanceProfile`:

Memverifikasi apakah instans Amazon EC2 yang disediakan memiliki profil instans IAM yang dilampirkan.

- `branchOnInstanceProfileStatus`:

Mem-cabang otomatisasi untuk memeriksa izin profil instans yang diperlukan jika profil instance dilampirkan ke instance.

- `verifyIamPermissions`:

Memeriksa profil instance yang terkait dengan instance untuk menentukan apakah izin IAM yang diperlukan diterapkan.

- `getInstanceInformation`:

Memeriksa apakah instans memiliki agen Systems Manager yang aktif, dan mengambil jenis OS instance.

- `branchOnManagedContoh`:

Cabang otomatisasi untuk melakukan pemeriksaan diperpanjang jika instance dikelola.

- `getAgentStatus`:

Memeriksa status CloudWatch Agen Amazon pada instance.

- `branchOnInstanceOsType`:

Cabang otomatisasi untuk menjalankan collection/analysis perintah log tertentu berdasarkan

- `analyzeLogsWindowsAnalyzeLogs/`:

Menganalisis dan mengeluarkan temuan log CloudWatch Agen Amazon berdasarkan jenis OS.

- `collectLogsWindowsCollectLogs/`:

Bundel dan output file pemecahan masalah CloudWatch Agen Amazon yang relevan berdasarkan jenis OS.

- `checkEndpointReachability/checkEndpointReachabilityJendela`:

Memeriksa apakah instance dapat mencapai titik akhir yang diperlukan berdasarkan jenis OS.

- `branchOnRunVpcReachabilityAnalyzer`:

Memcabangkan otomatisasi untuk menjalankan analisis jangkauan VPC jika diaktifkan dan masalah jaringan terdeteksi.

- `GenerateEndPoints`:

Menghasilkan titik akhir untuk memeriksa dari kegagalan pemeriksaan diperpanjang dan nilai `CheckEC2Endpoint`

- `analyzeAwsEndpointReachabilityFromEC2`:

Memanggil runbook otomatisasi, `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` untuk memeriksa jangkauan instance yang dipilih ke titik akhir yang diperlukan.

- `OutputTemuan`:

Menghasilkan hasil dari langkah-langkah eksekusi otomatisasi.

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

Referensi

Otomatisasi Systems Manager

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

AWSSupport-TroubleshootCloudWatchAlarm

Deskripsi

AWSSupport-TroubleshootCloudWatchAlarmRunbook membantu mengidentifikasi dan memecahkan masalah dengan Alarm Amazon CloudWatch () yang salah konfigurasi atau bermasalah. CloudWatch Ini memanfaatkan logika evaluasi alarm publik AWS APIs dan diketahui untuk mendeteksi titik data yang tertunda atau hilang dalam metrik yang dipantau, yang dapat menyebabkan tindakan alarm yang terlewat atau tertunda. Runbook ini menyediakan pendekatan terstruktur untuk menyelidiki dan menyelesaikan masalah terkait Amazon CloudWatch (CloudWatch) Alarm.

Bagaimana cara kerjanya?

Runbook AWSSupport-TroubleshootCloudWatchAlarm melakukan langkah-langkah berikut:

- Memverifikasi detail alarm Amazon CloudWatch (CloudWatch) dan nilai AlarmTriggerTimestamp parameter untuk memeriksa apakah itu dalam 2.592.000 detik (30 hari).
- Memeriksa apakah alarm didasarkan pada Matematika Metrik atau Metrik atau merupakan Alarm Detektor Anomali.
- Memeriksa apakah alarm dalam sate data tidak mencukupi.
- Memeriksa apakah metrik yang digunakan dalam alarm cocok dengan ListMetrics nilai.
- Memverifikasi apakah metrik tidak memiliki titik data pada stempel waktu tertentu.
- Mendapat sejarah terbaru untuk stempel waktu tertentu.
- Memeriksa apakah alarm tidak terpicu karena metrik yang tertunda atau tidak terjawab.
- Memeriksa apakah tindakan yang diaktifkan alarm was/were dikirimkan.
- Menghasilkan laporan pemecahan masalah yang menggabungkan semua hasil diagnostik.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmHistory`
- `cloudwatch:DescribeAnomalyDetectors`
- `cloudwatch:GetMetricData`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch:ListMetrics`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource": "*"
    }
  ]
}
```


}

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootCloudWatchAlarm](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Tipe: String
 - Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS 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.
 - CloudWatchMetricAlarmName(Diperlukan):
 - Tipe: String
 - Deskripsi: (Wajib) Nama Alarm metrik Amazon CloudWatch (CloudWatch) untuk memecahkan masalah.
 - Pola yang Diizinkan: `^[a-zA-Z0-9.:;,\_\&() ]{1,255}$`
 - AlarmTriggerTimestamp (Diperlukan):
 - Tipe: String
 - Deskripsi: (Wajib) Stempel waktu UTC saat masalah Alarm terjadi. Informasi ini sangat penting untuk memecahkan masalah dan memahami konteks di mana hal itu terjadi. Nilai stempel waktu harus berupa waktu dalam 30 hari terakhir dari hari ini dan dalam format. YYYY-MM-DDTHH:mm:ssZ Contoh: 2024-10-29T09:04:00Z
 - Pola yang Diizinkan: `^(\d{4})-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2})Z$`
4. Pilih Jalankan.
5. Otomatisasi dimulai.
6. Dokumen melakukan langkah-langkah berikut:

- **VerifyRunbookInputs**

Memverifikasi detail alarm Amazon CloudWatch (CloudWatch) dan nilai AlarmTriggerTimestamp parameter untuk memeriksa apakah itu dalam 2.592.000 detik (30 hari).

- **UpdateSSMDocumentInputChecksVariable**

Memperbarui variabel SSMDocumentInputChecks dengan nilai SSMDocumentInputChecks dari VerifyRunbookInputs langkah.

- **BranchOnAlarmIsVerified**

Cabang pada verifikasi AlarmTriggerTimestamp input Runbook dan. CloudWatchAlarmName

- **CheckMetricAlarmType**

Memeriksa apakah alarm didasarkan pada Matematika Metrik atau Metrik atau merupakan Alarm Detektor Anomali.

- **CheckAlarmInInsufficientDataState**

Memeriksa apakah alarm dalam sate data tidak mencukupi.

- **UpdateInsufficientDataChecksVariable**

Memperbarui variabel InsufficientDataChecks dengan nilai InsufficientDataChecks dari CheckAlarmInInsufficientDataState langkah.

- **BranchOnAlarmHasInsufficientData**

Cabang pada AlarmHasInsufficientData nilai dari CheckAlarmInInsufficientDataState langkah, langkah defaultnya adalahCheckMetricMismatch.

- **CheckMetricMismatch**

Memeriksa apakah metrik yang digunakan dalam alarm cocok dengan ListMetrics nilai.

- **UpdateMetricMismatchChecksVariable**

Memperbarui variabel MetricMismatchChecks dengan nilai MetricMismatchChecks dari CheckMetricMismatch langkah.

- **BranchOnMetricsMatched**

Cabang pada `MetricsMatched` nilai dari `CheckMetricMismatch` langkah, langkah defaultnya adalah `CheckMissingDatapoint`.

- **CheckMissingDatapoint**

Memverifikasi apakah metrik tidak memiliki titik data pada stempel waktu tertentu.

- **UpdateMetricMissingDatapointsChecksVariable**

Memperbarui variabel `MetricMissingDatapointsChecks` dengan nilai `MetricMissingDatapointsChecks` dari `CheckMissingDatapoint` langkah.

- **BranchOnMetricMissingDatapoint**

Cabang pada `MetricMissingDatapoint` nilai dari `CheckMissingDatapoint` langkah, langkah defaultnya adalah `GetAlarmHistoryDetails`.

- **GetAlarmHistoryDetails**

Mendapat sejarah terbaru untuk stempel waktu tertentu.

- **UpdateAlarmHistoryChecksVariable**

Memperbarui variabel `AlarmHistoryChecks` dengan nilai `AlarmHistoryChecks` dari `GetAlarmHistoryDetails` langkah.

- **BranchOnAlarmHistoryFound**

Cabang pada `AlarmHistoryFound` nilai dari `GetAlarmHistoryDetails` langkah, langkah defaultnya adalah `CheckDelayedMetric`.

- **CheckDelayedMetric**

Memeriksa apakah alarm tidak terpicu karena metrik yang tertunda atau tidak terjawab.

- **UpdateDelayedMetricChecksVariable**

Memperbarui variabel `DelayedMetricChecks` dengan nilai `DelayedMetricChecks` dari `CheckDelayedMetric` langkah.

- **BranchOnMetricDelayedAndDatapointsMeetThreshold**

Cabang pada `MetricDelayed` dan `DatapointsMeetThreshold` nilai dari `CheckDelayedMetric` langkah, langkah defaultnya adalah `GenerateReport`.

- **CheckActionDelivered**

Memeriksa apakah tindakan yang diaktifkan alarm was/were dikirimkan.

- **UpdateActionDeliveredChecksVariable**

Memperbarui variabel ActionDeliveredChecks dengan output ActionDeliveredChecks dari CheckActionDelivered langkah.

- **GenerateReport**

Mengkompilasi output dari langkah-langkah sebelumnya dan mengeluarkan laporan.

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

- GenerateReport.Laporkan

Laporan Alarm metrik Amazon CloudWatch (CloudWatch) yang disediakan.

```
-----
|                                     AWS CloudWatch Alarm Troubleshooting Results
|
-----
|      Alarm Name                      -      Demo-Alarm
|
|      Timestamp                      -
2025-03-04T06:31:00Z |
-----
|      # No Issue(s) Found
|
-----
```

```
=====
1. Validating SSM Document input parameters:
=====
```

```
# [PASSED]: Found a metric alarm with name Demo-Alarm
```

```
=====
2. Checking alarm's data state:
```

```
=====
# [PASSED]: The alarm is not in INSUFFICIENT_DATA state, alarm's
state is: ALARM
```

```
=====
3. Checking if the alarm experienced metric mismatches:
```

```
=====
# [PASSED]: Metric matches with the configured metric for Alarm.
```

```
=====
4. Checking if the alarm's metric(s) experienced missing
datapoint(s):
```

```
=====
# [PASSED]: Metric has datapoints
```

```
=====
5. Retrieving alarm's history for timestamp 2025-03-04T06:31:00Z:
```

```
=====
# [PASSED]: Found most recent alarm history item for the provided
timestamp: '2025-03-04T06:31:00Z'
```

```
=====
6. Checking if the alarm experienced metric delays or the alarm's
datapoint(s) did not meet the configured threshold:
```

```
=====
# [PASSED]: CloudWatch alarm did not experience any delayed metric
```

```
=====
7. Checking if the alarm has actions enabled and if action(s) were
delivered:
```

```
=====
# [PASSED]: Successfully executed action arn:aws:sns:us-
east-1:12345678910:Demo_Alarms_Topic
```

```
-----

# All the checks have passed for CloudWatch alarm, Demo-Alarm, the
alarm's configuration is correct.
```

Referensi

Otomatisasi Systems Manager

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

Amazon DocumentDB

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon DocumentDB (dengan kompatibilitas MongoDB). Untuk informasi lebih lanjut 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`

Tipe: 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`

Tipe: 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

Tipe: 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:assertAwsResourceProperty) - Memverifikasi jenis mesin Amazon DocumentDB adalah untuk mencegah perubahan yang tidak disengaja pada docdb jenis mesin Amazon RDS lainnya.
- VerifyDocDbStatus (aws:waitAwsResourceProperty) - Memverifikasi status cluster Amazon DocumentDB adalah. available
- ModifyDocDbRetentionPeriod (aws:executeAwsApi) - Menetapkan 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 untuk AWS CodeBuild. Untuk informasi lebih lanjut 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

Tipe: 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.

- KMSKeyId

Tipe: 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

Tipe: 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

Tipe: 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.

- ResourceId

Tipe: String

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 ResourceId parameter.

AWS CodeDeploy

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk. AWS CodeDeploy Untuk informasi lebih lanjut 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:

- CodeDeploy Agen tidak diinstal atau tidak berjalan di EC2 instans Amazon
- EC2 Instans Amazon tidak memiliki profil instance AWS Identity and Access Management (IAM) yang dilampirkan
- Profil instans IAM yang dilampirkan ke EC2 instans Amazon 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 berbeda Wilayah AWS dari instance Amazon EC2
- Masalah file spesifikasi aplikasi (AppSpec)
- Kesalahan “File sudah ada di lokasi”
- Kait peristiwa siklus hidup CodeDeploy terkelola yang gagal
- Kait peristiwa siklus hidup yang dikelola pelanggan yang gagal
- Peristiwa skala dalam selama penerapan

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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.

- `DeploymentId`

Tipe: String

Deskripsi: (Wajib) ID penerapan yang gagal.

- `InstanceId`

Tipe: String

Deskripsi: (Wajib) ID EC2 instans Amazon tempat penerapan gagal.

Izin IAM yang diperlukan

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

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

Langkah Dokumen

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

AWS Config

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk AWS Config. Untuk informasi lebih lanjut 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) AWS Config tempat mengirimkan snapshot konfigurasi dan file riwayat konfigurasi. Jika Anda menentukan nilai untuk `AggregatorAccountRegion` parameter `AggregatorAccountId` dan, buku runbook juga membuat otorisasi untuk agregasi data guna mengumpulkan data AWS Config konfigurasi dan kepatuhan dari beberapa dan beberapa Akun AWS . Wilayah AWSUntuk 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`

Tipe: 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.

- `AggregatorAccountId`

Tipe: String

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

- `AggregatorAccountRegion`

Tipe: String

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

- `IncludeGlobalResourcesRegion`

Tipe: String

Default: `us-east-1`

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

- `Partition`

Tipe: String

Default: `aws`

Deskripsi: (Wajib) Partisi yang ingin Anda kumpulkan AWS Config konfigurasi dan data kepatuhan.

- `S3 BucketName`

Tipe: 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` memerlukan 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 belum ada.
- `aws:executeScript`- Membuat perekam konfigurasi jika belum ada.
- `aws:executeScript`- Membuat bucket Amazon S3 untuk digunakan oleh saluran pengiriman jika belum ada.
- `aws:executeScript`- Membuat saluran pengiriman menggunakan sumber daya yang dibuat oleh runbook.
- `aws:executeAwsApi`- Memulai perekam konfigurasi.
- `aws:executeScript`- Jika Anda menentukan nilai untuk `AggregatorAccountId` dan `AggregatorAccountRegion` parameter, otorisasi untuk agregasi data multi-akun dan Multi-wilayah dikonfigurasi.

Amazon Connect

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

Topik

- [AWSSupport-AssociatePhoneNumbersToConnectContactFlows](#)
- [AWSSupport-CollectAmazonConnectContactFlowLog](#)

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"
    }
  ]
}

```

Jika memberikan `LambdaRoleArn` parameter, peran memerlukan tindakan berikut agar berhasil menggunakan runbook.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": "arn:aws:logs:us-east-1:111122223333:*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:us-east-1:111122223333:*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "connect:AssociatePhoneNumberContactFlow"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}

```

```
    },  
    {  
      "Action": [  
        "s3:PutObject",  
        "s3:GetObject"  
      ],  
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/DESTINATION_FILE_PATH*",  
      "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 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.

- 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, bucket, status kebijakan bucket ACLs, 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.

- **LambdaRoleArn (Opsional)**

ARN dari peran IAM yang memungkinkan AWS Lambda fungsi untuk mengakses AWS layanan dan sumber daya yang diperlukan. Jika tidak ada peran yang ditentukan, otomatisasi ini akan membuat satu peran IAM untuk Lambda di akun Anda.

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.Events**

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](#)

AWSSupport-CollectAmazonConnectContactFlowLog

Deskripsi

Runbook AWSSupport-CollectAmazonConnectContactFlowLog otomatisasi digunakan untuk mengumpulkan log alur kontak Amazon Connect untuk ID kontak tertentu. Dengan memberikan ID instans Amazon Connect dan ID kontak, runbook akan mencari log alur kontak untuk kontak dari grup CloudWatch log Amazon dan mengunggahnya ke bucket Amazon Simple Storage Service (Amazon S3) yang ditentukan dalam parameter permintaan. Runbook menghasilkan output yang menyediakan URL konsol Amazon S3 dan perintah AWS CLI bagi Anda untuk mengunduh log.

Bagaimana cara kerjanya?

Runbook AWSSupport-CollectAmazonConnectContactFlowLog otomatisasi membantu mengumpulkan log alur kontak Amazon Connect untuk ID kontak tertentu yang disimpan dalam grup CloudWatch log yang dikonfigurasi dan mengunggahnya ke bucket Amazon S3 yang ditentukan. Untuk membantu keamanan log yang dikumpulkan dari alur kontak Amazon Connect, otomatisasi mengevaluasi konfigurasi bucket Amazon S3 untuk menentukan apakah bucket memberikan izin

read publik write atau akses dan dimiliki oleh akun yang ditentukan AWS dalam parameter. `S3BucketOwnerAccountId` Jika bucket Amazon S3 Anda menggunakan enkripsi sisi server dengan AWS Key Management Service kunci (SSE-KMS), pastikan bahwa peran pengguna atau AWS Identity and Access Management (IAM) yang menjalankan otomatisasi ini memiliki izin pada kunci. `kms:GenerateDataKey` AWS KMS Untuk informasi selengkapnya tentang log yang dihasilkan oleh instans Amazon Connect, lihat [Log aliran yang disimpan dalam grup CloudWatch log Amazon](#).

 Important

Kueri Wawasan CloudWatch Log dikenakan biaya berdasarkan jumlah data yang ditanyakan. Pelanggan tingkat gratis hanya dikenakan biaya untuk penggunaan yang melebihi kuota layanan. Untuk informasi lebih lanjut, lihat [Amazon CloudWatch Harga](#).

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

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:::amzn-s3-demo-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-bucket"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "connect:DescribeInstance",
        "connect:DescribeContact",
        "ds:DescribeDirectories"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "logs:StartQuery",
        "logs:GetQueryResults"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - Collect Amazon Connect Contact Flow Log](#) 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.

- ContactId (Diperlukan):

ID kontak yang ingin Anda kumpulkan log alur kontak.

- S3 BucketName (Diperlukan):

Nama bucket Amazon S3 di akun tempat Anda ingin mengunggah log alur kontak. Pastikan kebijakan bucket tidak memberikan izin baca/tulis yang tidak perlu kepada pihak yang tidak memerlukan akses ke log yang dikumpulkan.

- S3 ObjectPrefix (Opsional):

Jalur objek Amazon S3 di bucket Amazon S3 untuk log alur kontak yang diunggah. Misalnya, jika Anda menentukan CollectedLogs, log akan diunggah sebagai `s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId][AWSAccountId].gz`. Jika Anda tidak menentukan parameter ini, ID eksekusi Systems Manager Automation digunakan, misalnya `s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz`. Catatan: jika Anda menentukan nilai untuk S3ObjectPrefix dan menjalankan otomatisasi ini menggunakan [ContactId] yang sama, log alur kontak akan ditimpa.

- S3 BucketOwnerAccount (Opsional):

Nomor AWS akun yang memiliki bucket Amazon S3 tempat Anda ingin mengunggah log alur kontak. Jika Anda tidak menentukan parameter ini, runbook menggunakan ID AWS akun pengguna atau peran di mana otomatisasi berjalan.

- S3 BucketOwnerRoleArn (Opsional):

ARN peran IAM dengan izin untuk mendapatkan bucket Amazon S3 dan pengaturan pemblokiran akun akses publik, konfigurasi enkripsi bucket, bucket, status kebijakan bucket ACLs, 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). Lihat bagian izin yang diperlukan di deskripsi buku runbook.

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. SSMAutomationRole C	ConnectInstanceId (Required) The ID of your Amazon Connect instance. fedcba98-7654-3210-fedc-ba9876543210
ContactId (Required) The ID of the contact that you want to collect Contact Flow Log for. 01234567-89ab-cdef-0123-456789abcdef	S3BucketName (Required) The Amazon S3 bucket name in your account where you want to upload Contact Flow Log. Make sure that bucket policy does not grant unnecessary read/write permissions to parties that do not need access to the collected logs. saw-example-bucket C
S3ObjectPrefix (Optional) The Amazon S3 object path in the Amazon S3 bucket for an uploaded the Contact Flow Log. For example, if you specify 'CollectedLogs', the log will be uploaded as 's3://your-s3-bucket/CollectedLogs/ContactFlowLog_{ContactId}_{AWSAccountId}.gr'. If you do not specify this parameter, the SSM Automation execution ID is used, example: 's3://your-s3-bucket/automation-EXECUTION_ID/ContactFlowLog_{ContactId}_{AWSAccountId}.gr'. Note: If you specify a value for 'S3ObjectPrefix' and you run this automation using the same [ContactId], the Contact Flow Log will be overwritten. String	S3BucketOwnerAccount (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. String
S3BucketOwnerRoleArn (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. C	

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- CheckConnectInstanceExistance

Memeriksa apakah instans Amazon Connect yang disediakan di `ConnectInstanceId` isACTIVE.

- Ceks3 BucketPublicStatus

Memeriksa apakah bucket Amazon S3 yang ditentukan dalam `S3BucketName` mengizinkan izin akses baca atau tulis anonim atau publik.

- GenerateLogSearchTimeRange

Menghasilkan `StartTime` dan `EndTime` untuk `StartQuery` langkah berdasarkan `InitiationTimestamp` dan `LastUpdateTimestamp` dikembalikan oleh `DescribeContact` API. `StartTime` akan menjadi satu jam sebelumnya `InitiationTimestamp` dan `EndTime` akan menjadi satu jam setelahnya `LastUpdateTimestamp`.

- StartQuery

Memulai log kueri untuk yang disediakan `ContactId` dalam grup CloudWatch log Log yang terkait dengan instans Amazon Connect yang disediakan `ConnectInstanceId`. Waktu kueri habis setelah 60 menit runtime. Jika waktu kueri Anda habis, kurangi rentang waktu yang dicari. Anda dapat melihat kueri yang sedang berlangsung serta riwayat kueri terbaru Anda di CloudWatch konsol. Untuk informasi selengkapnya, lihat [Melihat kueri atau riwayat kueri yang sedang berjalan](#).

- **WaitForQueryCompletion**

Menunggu CloudWatch log kueri Log ContactId untuk menyelesaikan yang disediakan. Perhatikan bahwa waktu kueri habis setelah 60 menit runtime. Jika waktu kueri Anda habis, kurangi rentang waktu yang dicari. Anda dapat melihat kueri yang sedang berlangsung serta riwayat kueri terbaru Anda di konsol Amazon Connect. Untuk informasi selengkapnya, lihat [Melihat kueri atau riwayat kueri yang sedang berjalan](#).

- **UploadContactFlowLog**

Mendapatkan hasil kueri dan mengunggah log alur kontak ke bucket Amazon S3 yang ditentukan. S3BucketName

- **GenerateReport**

Mengembalikan URL konsol Amazon S3 tempat log alur kontak diunggah dan contoh perintah AWS CLI yang dapat Anda gunakan untuk mengunduh file log.

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

- **GenerateReport.OutputPayload**

Output yang memberi tahu Anda bahwa runbook berhasil mengambil log alur kontak untuk kontak yang ditentukan. Laporan ini juga berisi URL konsol Amazon S3 dan contoh perintah AWS CLI sehingga Anda dapat mengunduh file log.

▼ Outputs

GenerateReport.OutputPayload

```
{ "Payload": "
```

```
=====
Amazon Connect Contact Flow Log Collector Result
=====
```

Successfully retrieved Contact Flow log for the contact '01234567-89ab-cdef-0123-456789abcdef'.

You can access the log file from the S3 Console URL below:

- S3 Console URL for the Contact Flow Log file
https://s3.console.aws.amazon.com/s3/object/saw-example-bucket?region=us-west-2&prefix=01234567-89ab-cdef-0123-456789abcdef/ContactFlowLog_01234567-89ab-cdef-0123-456789abcdef_123456789012.gz

Alternatively, you can download the log file by using the AWS CLI command below:

```
'''
aws s3 cp s3://saw-example-bucket/01234567-89ab-cdef-0123-456789abcdef/ContactFlowLog_01234567-89ab-cdef-0123-456789abcdef_123456789012.gz . --region us-west-2
'''
```

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 untuk AWS Directory Service. Untuk informasi lebih lanjut 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 instance Windows Amazon Elastic Compute Cloud (Amazon EC2) Windows 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

Tipe: 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.

- AmiID

Tipe: String

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

Deskripsi: (Opsional) Amazon Machine Image (AMI) id yang akan digunakan untuk meluncurkan instance. Secara Default, instans akan diluncurkan dengan Microsoft Windows Server 2019 Base AMI terbaru.

- DirectoryId

Tipe: String

Deskripsi: (Wajib) Id Direktori Directory Service direktori Anda.

- IamInstanceProfileName

Tipe: String

Deskripsi: (Opsional) nama profil instans IAM. Secara Default, jika tidak ada profil instance dengan nama Amazon SSMDirectoryServiceInstanceProfileRole, profil instance dengan nama Amazon SSMDirectory ServiceInstanceProfileRole akan dibuat.

Default: Amazon SSMDirectory ServiceInstanceProfileRole

- InstanceType

Tipe: String

Default: t3.medium

Nilai yang diizinkan:

- t2.nano
- t2.micro

- t2.small
- t2.medium
- t2.large
- t2.xlarge
- t2.2xlarge
- t3.nano
- t3.micro
- t3.small
- t3.medium
- t3.large
- t3.xlarge
- t3.2xlarge

Deskripsi: (Opsional) Jenis instance yang akan diluncurkan. Defaultnya adalah t3.medium.

- KeyPairName

Tipe: String

Deskripsi: (Opsional) Pasangan kunci yang akan digunakan saat meluncurkan instance. Windows tidak mendukung pasangan ED25519 kunci. Secara Default instance diluncurkan tanpa key pair (NoKeyPair).

Default: NoKeyPair

- RemoteAccessCidr

Tipe: String

Deskripsi: (Opsional) Membuat grup Keamanan dengan port untuk RDP (Rentang port 3389) terbuka untuk IPs ditentukan oleh CIDR (default adalah 0.0.0.0/0). Jika grup keamanan sudah ada, itu tidak akan diubah dan aturan tidak akan diubah.

Default 0.0.0.0/0

- SecurityGroupName

Tipe: String

Deskripsi: (Opsional) Nama grup keamanan. Secara Default, jika tidak ada grup keamanan dengan nama Amazon SSMDirectoryServiceSecurityGroup, grup keamanan dengan nama Amazon SSMDirectory ServiceSecurityGroup akan dibuat.

Default: Amazon SSMDirectory ServiceSecurityGroup

- Tanda

Jenis: MapList

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

Default: [{"Key":"Description","Value":"Created by AWS Systems Manager Automation"}, {"Key":"Created By","Value":"AWS Systems Manager Automation"}]

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 virtual private cloud (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 instance 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 instance baru ke direktori Anda.
- `aws:runCommand`- Menginstal alat administrasi server jarak jauh pada instance baru.

AWSSupport-TroubleshootADConnectorConnectivity

Deskripsi

AWSSupport-TroubleshootADConnectorConnectivityRunbook memverifikasi prasyarat berikut untuk AD Connector:

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

Ketika pemeriksaan prasyarat berhasil diselesaikan, runbook meluncurkan dua instans Amazon Elastic Compute Cloud (Amazon EC2) Linux t2.micro dalam subnet yang sama dengan AD Connector 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 EC2 instans Amazon, Akun AWS volume Amazon Elastic Block Store, dan Amazon Machine Image (AMI) dibuat selama otomatisasi. Untuk informasi selengkapnya, lihat [Amazon Elastic Compute Cloud Pricing](#) dan [Amazon Elastic Block Store Pricing](#).

Jika `aws:deletestack` langkahnya 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 CloudFormation tumpukan, lihat [Menghapus tumpukan di Panduan Pengguna AWS CloudFormation](#)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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.

- DirectoryId

Tipe: String

Deskripsi: (Wajib) ID direktori AD Connector yang ingin Anda pecahkan masalah konektivitas.

- `Ec2 InstanceProfile`

Tipe: String

Karakter maksimal: 128

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

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan 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`- Mengonfirmasi direktori yang ditentukan dalam `DirectoryId` parameter adalah AD Connector.
- `aws:executeAwsApi`- Mengumpulkan informasi tentang AD Connector.
- `aws:executeAwsApi`- Mengumpulkan informasi tentang grup keamanan yang terkait dengan AD Connector.
- `aws:executeAwsApi`- Mengumpulkan informasi tentang aturan ACL jaringan yang terkait dengan subnet untuk AD Connector.
- `aws:executeScript`- Mengubah aturan grup keamanan AD Connector untuk memverifikasi bahwa lalu lintas keluar yang diperlukan diizinkan.
- `aws:executeScript`- Mengubah aturan ACL jaringan AD Connector untuk memverifikasi bahwa lalu lintas jaringan keluar dan masuk yang diperlukan diperbolehkan.
- `aws:executeScript`- Memeriksa apakah titik akhir CloudWatch antarmuka AWS Systems Manager, AWS Security Token Service dan Amazon ada di VPC yang sama dengan AD Connector.
- `aws:executeScript`- Mengkompilasi output dari pemeriksaan yang dilakukan pada langkah sebelumnya.
- `aws:branch`- Cabang otomatisasi tergantung pada output dari langkah sebelumnya. Otomatisasi berhenti di sini jika aturan keluar dan masuk yang diperlukan tidak ada untuk grup keamanan dan jaringan. ACLs
- `aws:createStack`- Membuat CloudFormation tumpukan untuk meluncurkan EC2 instans Amazon untuk melakukan tes konektivitas.
- `aws:executeAwsApi`- Mengumpulkan EC2 contoh Amazon yang baru diluncurkan. IDs
- `aws:waitForAwsResourceProperty`- Menunggu EC2 instans Amazon pertama yang baru diluncurkan untuk melaporkan sebagaimana dikelola oleh AWS Systems Manager.
- `aws:waitForAwsResourceProperty`- Menunggu EC2 instans Amazon kedua yang baru diluncurkan untuk melaporkan 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 EC2 instans Amazon yang digunakan untuk tes konektivitas.
- `aws:deleteStack`- Menghapus CloudFormation tumpukan.
- `aws:executeScript`- Mengeluarkan instruksi tentang cara menghapus CloudFormation tumpukan secara manual jika otomatisasi gagal menghapus tumpukan.

AWSSupport-TroubleshootDirectoryTrust

Deskripsi

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

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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.

- DirectoryId

Tipe: String

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

Deskripsi: (Wajib) 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: (Wajib) CIDR (s) dari domain jarak jauh yang Anda coba untuk membangun hubungan kepercayaan dengan. Anda dapat menambahkan beberapa CIDRs menggunakan nilai yang dipisahkan koma. Misalnya, 172.31.48.0/20, 192.168.1.10/32.

- RemoteDomainName

Tipe: String

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

- RequiredTrafficACL

Tipe: String

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

Default: {"inbound": {"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]]}, "keluar": {"-1": [[0,65535]]}}

- RequiredTrafficSG

Tipe: String

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

Default: {"inbound": {"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]]}, "keluar": {"-1": [[0,65535]]}}

- TrustId

Tipe: String

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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- Mengonfirmasi jenis direktori adalah AWS Managed Microsoft AD.
- aws:executeAwsApi- Mendapat informasi tentang AWS Managed Microsoft AD.
- aws:branch- Otomatisasi cabang jika nilai disediakan untuk parameter TrustId input.
- aws:executeAwsApi- Mendapat informasi tentang hubungan kepercayaan.
- aws:executeAwsApi- Mendapat alamat IP DNS forwarder bersyarat untuk file. RemoteDomainName
- aws:executeAwsApi- Mendapat informasi tentang rute IP yang telah ditambahkan ke AWS Managed Microsoft AD.
- aws:executeAwsApi- CIDRs Mendapat AWS Managed Microsoft AD subnet.

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

Keluaran

`evalDirectorySecurityGroup.output` - Hasil dari evaluasi apakah aturan grup keamanan terkait dengan AWS Managed Microsoft AD mengizinkan lalu lintas yang diperlukan untuk pembuatan kepercayaan.

`evalAclEntries.output` - Hasil dari evaluasi apakah jaringan yang ACLs terkait dengan AWS Managed Microsoft AD memungkinkan lalu lintas yang diperlukan untuk pembuatan kepercayaan.

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

AWS AppSync

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk AWS AppSync. Untuk informasi lebih lanjut 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

Tipe: 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.

- ApId

Tipe: String

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

- FieldLogLevel

Tipe: String

Nilai Valid: ERROR | SEMUA

Deskripsi: (Wajib) Tingkat logging bidang.

- CloudWatchLogsRoleArn

Tipe: 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 yang telah ditentukan untuk Amazon Athena. Untuk informasi lebih lanjut 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`

Tipe: 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

Tipe: String

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

- EncryptionOption

Tipe: 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

Tipe: 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:assertAwsResource Properti` - Memverifikasi bahwa enkripsi untuk workgroup telah diaktifkan.

DynamoDB

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon DynamoDB. Untuk informasi lebih lanjut 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

Tipe: 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

Tipe: 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

Tipe: 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

Ubah DDBRWCapacity Mode. `SuccessesTables` - Daftar nama tabel DynamoDB di mana mode kapasitas berhasil diubah

Ubah DDBRWCapacity Mode. `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`

Tipe: 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.

- BackupName

Tipe: String

Deskripsi: (Wajib) Nama cadangan yang akan dibuat.

- LambdaAssumeRole

Tipe: 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.

- TableName

Tipe: String

Deskripsi: (Wajib) 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

Tipe: 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.

- BackupArn

Tipe: String

Deskripsi: (Diperlukan) ARN dari 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

Tipe: 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.

- TableName

Tipe: String

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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

Tipe: 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.

- LambdaAssumeRole

Tipe: 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.

- RetentionCount

Tipe: String

Default: 10

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

- RetentionDays

Tipe: String

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

- TableName

Tipe: String

Deskripsi: (Wajib) 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

Tipe: 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.

- KMSKeyId

Tipe: String

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

- `TableName`

Tipe: 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` mengaktifkan 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

Tipe: 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.

- TableName

Tipe: String

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

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

Langkah Dokumen

- aws:executeAwsApi- Mengaktifkan point-in-time pemulihan pada tabel DynamoDB yang Anda tentukan dalam parameter. TableName

- `aws:assertAwsResourceProperty`- Mengonfirmasi 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

Tipe: 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

Tipe: 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`) - Mengkonfigurasi 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)` - Memverifikasi 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 point-in-time menggunakan pemulihan (PITR).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AutomationAssumeRole

Tipe: 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.

- EnablePointInTimeRecoverAsNeeded

Jenis: Boolean

Default: betul

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

- GlobalSecondaryIndexOverride

Tipe: String

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

- LocalSecondaryIndexOverride

Tipe: String

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

- RestoreDateTime

Tipe: String

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

- SourceTableArn

Tipe: String

Deskripsi: (Wajib) ARN dari tabel yang ingin Anda pulihkan.

- SseSpecificationOverride

Tipe: String

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

- TargetTableName

Tipe: String

Deskripsi: (Wajib) Nama tabel untuk mengembalikan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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`

AWS Database Migration Service

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

Topik

- [AWSSupport-TroubleshootDMSTableErrors](#)
- [AWSSupport-TroubleshootDMSEndpointConnection](#)

AWSSupport-TroubleshootDMSTableErrors

Deskripsi

Runbook AWS Systems Manager `AWSSupport-TroubleshootDMSTableErrors` otomatisasi membantu Anda mengotomatiskan proses pemecahan masalah yang `Table errors` ditemukan dalam tugas migrasi Database atau replikasi Tanpa Server dari AWS Database Migration Service. Kesalahan ini terjadi ketika tabel gagal bermigrasi dari titik akhir sumber (database sumber) ke titik akhir target (database target) oleh tugas migrasi Database atau replikasi Tanpa Server yang dibuat dalam layanan. AWS DMS Runbook ini menganalisis pesan kesalahan tanda tangan dari CloudWatch log, khususnya berfokus pada log tugas untuk tugas migrasi Database tradisional dan log tanpa server untuk replikasi Tanpa Server. Ini juga memberikan saran yang ditargetkan dan langkah-langkah perbaikan untuk pesan kesalahan umum yang ditemui `Table error` selama AWS DMS migrasi.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Mengambil informasi tentang AWS DMS ARN yang disediakan, yang dapat berupa tugas migrasi Database atau replikasi Tanpa Server.
- Memverifikasi apakah AWS DMS sumber daya yang disediakan telah dimulai setidaknya sekali dengan memeriksa `FreshStartDate` nilai dalam `DescribeReplicationTasks` API (untuk tugas migrasi Database) dan `DescribeReplications` API (untuk replikasi Tanpa Server). Jika sumber daya belum dimulai, otomatisasi menimbulkan kesalahan.

- Jika sumber daya telah dimulai, otomatisasi memeriksa tabel di `TableError` negara bagian menggunakan `TableStatistics` informasi. Jika tidak ditemukan kesalahan, otomatisasi mengakhiri alur kerja setelah menampilkan pesan yang mengonfirmasi tidak ada kesalahan tabel yang ditemukan dalam tugas migrasi Database tertentu atau replikasi Tanpa Server.
- Jika tabel dengan `TableError` status ditemukan, otomatisasi memeriksa apakah CloudWatch logging diaktifkan untuk AWS DMS sumber daya yang ditentukan. Jika logging tidak diaktifkan, otomatisasi mengakhiri alur kerja setelah menampilkan pesan yang menunjukkan bahwa logging tidak diaktifkan.

Catatan: CloudWatch logging diharapkan diaktifkan, karena otomatisasi bergantung pada log ini untuk menganalisis dan mengidentifikasi masalah dengan tabel dalam `TableError` status.

- Jika logging diaktifkan, otomatisasi menganalisis CloudWatch log dan menghasilkan laporan untuk setiap tabel yang dalam `TableError` status. Laporan ini menyertakan saran untuk pesan kesalahan umum dan menyediakan log kesalahan yang relevan untuk membantu mengidentifikasi dan menyelesaikan masalah yang mencegah migrasi tabel berhasil dari titik akhir AWS DMS sumber ke titik akhir AWS DMS target.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Parameter

- `AutomationAssumeRole`

Tipe: 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.

- DMSArn

Tipe: String

Deskripsi: (Diperlukan) ARN dari tugas migrasi Database atau replikasi Tanpa Server

Pola yang Diizinkan: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+:\d{12}:(task|replication-config):[a-zA-Z0-9-]+$`

- StartTimeRange

Tipe: String

Deskripsi: (Opsional) Parameter ini mendefinisikan awal rentang waktu untuk analisis CloudWatch log dari tugas Migrasi Database yang diberikan atau replikasi Tanpa Server. Jika disediakan, hanya log yang dihasilkan dari waktu tertentu ini dan seterusnya yang akan dikumpulkan dan dianalisis. Harap dicatat, ada kemungkinan alur kerja bisa batas waktu jika rentang waktu antara `startDate` dan `endDate` terlalu lama. Nilai harus diberikan dalam format waktu tanggal ISO 6081.

Pola yang Diizinkan: `^$|^(\d{4})-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2})\.\d{3}Z$`

- EndTimeRange

Tipe: String

Deskripsi: (Opsional) Parameter ini menetapkan akhir rentang waktu untuk analisis CloudWatch log tugas migrasi Database yang diberikan atau replikasi Tanpa Server. Saat disediakan, hanya log yang dihasilkan hingga waktu tertentu ini yang akan dikumpulkan dan dianalisis. Harap dicatat, ada kemungkinan alur kerja bisa batas waktu jika rentang waktu antara `startDate` dan `endDate` terlalu lama. Nilai harus diberikan dalam format waktu tanggal ISO 6081.

Pola yang Diizinkan: `^$|^(\d{4})-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2})\.\d{3}Z$`

Izin IAM yang diperlukan

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

- `dms:DescribeReplicationTasks`
- `dms:DescribeReplications`
- `dms:DescribeEndpoints`
- `dms:DescribeReplicationConfigs`
- `dms:DescribeTableStatistics`
- `dms:DescribeReplicationTableStatistics`
- `logs:FilterLogEvents`

Contoh Kebijakan IAM untuk Otomasi Asumsikan Peran

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "dms:DescribeReplicationConfigs",
        "dms:DescribeEndpoints",
        "dms:DescribeReplicationTableStatistics",
        "dms:DescribeTableStatistics",
        "logs:FilterLogEvents",
        "dms:DescribeReplicationTasks",
        "dms:DescribeReplications"
      ],
      "Resource": "*"
    }
  ]
}
```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSsupport-TroubleshootDMSTableErrors](#) 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.

- DMSArn

ARN dari tugas migrasi Database atau replikasi Tanpa Server yang memiliki kesalahan Tabel.

- StartTimeRange

(Opsional) Format waktu tanggal ISO 6081 yang menentukan awal rentang waktu untuk menganalisis CloudWatch log tugas migrasi Database yang diberikan atau replikasi Tanpa Server.

- EndTimeRange

(Opsional) Format waktu tanggal ISO 6081 yang menentukan akhir rentang waktu untuk menganalisis CloudWatch log tugas migrasi Database yang diberikan atau replikasi Tanpa Server.

4. Pilih tombol Execute dari bawah halaman.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- memvalidasi DMSInput TypeAndGatherDetails

Memvalidasi input AWS DMS ARN yang diberikan dan mengumpulkan rincian dasar tugas migrasi Database atau replikasi tanpa server yang diperlukan dalam langkah berikutnya.

- branchOnTableKesalahan

Cabang alur kerja berdasarkan jumlah kesalahan Tabel yang ditemukan pada langkah di atas. Jika hitungan lebih besar dari 0, maka lanjutkan ke - branchOnCWLoggingStatus langkah. Lain, lanjutkan ke - outputNoTableErrors langkah.

- outputNoTableKesalahan

Keluarkan pesan yang menyatakan bahwa kesalahan tabel tidak ditemukan dalam tugas migrasi Database yang diberikan atau replikasi Tanpa Server.

- Status BranchOn CWLogging

Cabang alur kerja berdasarkan status CloudWatch pencatatan yang ditemukan pada langkah di atas. Jika diaktifkan, lanjutkan ke - `gatherTableDetails` langkah. Lain, lanjutkan ke - `outputNoCWLoggingEnabled` langkah.

- OutputTidak Diaktifkan CWLogging

Mengeluarkan pesan yang menyatakan bahwa CloudWatch logging tidak diaktifkan dalam tugas migrasi Database yang diberikan atau replikasi Tanpa Server.

- `gatherTableDetails`

Mengumpulkan `FullLoadEndTime` stempel waktu dari tabel yang gagal dan menghitung nilai `timerange` untuk menganalisis log. CloudWatch

- `analyzeCloudWatchLog`

Menganalisis log yang ditemukan di grup CloudWatch log berdasarkan pesan galat tanda tangan dan mengembalikan laporan ke Pengguna.

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

- Output dari kesalahan No Table ditemukan

Jika tidak ada kesalahan tabel yang ditemukan dalam tugas migrasi Database yang disediakan atau replikasi Tanpa Server, otomatisasi menunjukkan output yang menyatakan hal yang sama.

- Output dari Tidak ada CloudWatch login diaktifkan

Jika CloudWatch logging tidak diaktifkan dalam tugas migrasi Database yang disediakan atau replikasi Tanpa Server, otomatisasi menunjukkan output yang menyatakan hal yang sama dan menyediakan langkah-langkah untuk mengaktifkan logging.

- Laporan analisis log

Mengeluarkan laporan yang mengidentifikasi tabel dalam `Table error` keadaan baik dari tugas migrasi Database yang disediakan atau replikasi Tanpa Server, membedakan antara jenis kesalahan, mencantumkan pesan kesalahan yang ditemui, dan memberikan langkah-langkah perbaikan yang ditargetkan dan saran untuk setiap tabel yang diidentifikasi.

Referensi

Otomatisasi Systems Manager

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

AWSSupport-TroubleshootDMSEndpointConnection

Deskripsi

AWSSupport-TroubleshootDMSEndpointConnectionRunbook membantu mendiagnosis dan memecahkan masalah konektivitas antara instance AWS Database Migration Service replikasi dan titik akhir. AWS DMS Otomatisasi menggunakan pemeriksaan [Reachability](#) Analyzer untuk menguji konektivitas jaringan dan menganalisis konfigurasi jaringan untuk mengidentifikasi potensi masalah konektivitas yang dapat mencegah migrasi yang berhasil. AWS DMS

Important

Anda harus telah menguji konektivitas antara instance AWS DMS replikasi dan titik akhir menggunakan AWS DMS konsol atau API sebelum menjalankan runbook ini. Jika Anda belum menguji koneksi, lakukan terlebih dahulu, jika tidak, Anda mungkin perlu menjalankan kembali runbook ini. Baik contoh AWS DMS replikasi dan titik akhir harus dalam keadaan tersedia untuk pengujian konektivitas yang akurat.

Important

Runbook ini membuat dan memanggil AWS Lambda fungsi, yang akan dikenakan biaya Lambda. Setiap analisis Reachability Analyzer yang dijalankan juga menimbulkan biaya. [Untuk detail harga, lihat halaman Harga Amazon VPC di bawah tab Analisis Jaringan dan AWS Lambda Harga.](#)

Bagaimana cara kerjanya?

Runbook melakukan analisis sistematis AWS DMS konektivitas melalui fase-fase berikut:

Fase 1: Validasi Sumber Daya dan Prasyarat

- **Validasi Endpoint:** Memverifikasi AWS DMS titik akhir yang ada, mengambil konfigurasinya (nama server, port, jenis mesin), dan mengonfirmasi bahwa mesin database didukung untuk pemecahan masalah.
- **Status Uji Koneksi:** Mengambil status pengujian koneksi saat ini antara instance replikasi dan titik akhir menggunakan AWS DMS `DescribeConnections` API, termasuk pesan kegagalan apa pun dari upaya pengujian sebelumnya.
- **Analisis Instans Replikasi:** Mengumpulkan detail konfigurasi jaringan termasuk ID VPC Amazon, subnet, grup keamanan IDs IDs, dan mengidentifikasi Elastic Network Interface (ENI) terkait untuk instance replikasi.

Tahap 2: Resolusi DNS dan Penemuan Jalur Jaringan

- **Resolusi DNS berbasis Amazon VPC:** Membuat fungsi Lambda sementara dalam VPC Amazon yang sama dengan instance replikasi untuk menyelesaikan nama host titik akhir ke alamat IP-nya dari dalam konteks VPC Amazon, memastikan resolusi DNS pribadi yang akurat.
- **Identifikasi Target:** Menentukan target yang sesuai untuk Reachability Analyzer berdasarkan apakah titik akhir berada dalam VPC Amazon yang sama (menggunakan ENI) atau eksternal (menggunakan alamat IP yang diselesaikan).
- **IPv6 Pemeriksaan Kompatibilitas:** Memvalidasi alamat yang diselesaikan IPv4, karena Reachability Analyzer tidak mendukung alamat. IPv6

Fase 3: Analisis Jalur Jaringan Komprehensif

- **Eksekusi Reachability Analyzer:** Membuat Jalur Wawasan Jaringan dari instans replikasi ENI ke target (ENI titik akhir atau alamat IP) dan menjalankan analisis komprehensif untuk menguji konektivitas TCP pada port yang ditentukan.
- **Analisis Jaringan Multi-layer:** Memeriksa jalur jaringan lengkap termasuk tabel rute, grup keamanan, jaringan, gateway internet ACLs, gateway NAT, koneksi peering VPC Amazon, dan gateway transit untuk mengidentifikasi hambatan konektivitas.
- **Generasi Penjelasan Terperinci:** Untuk konektivitas yang gagal, berikan penjelasan spesifik untuk setiap komponen jaringan yang memblokir lalu lintas, termasuk nomor aturan yang tepat, blok CIDR, rentang port, dan pembatasan protokol.

Tahap 4: Pembuatan Laporan dan Pembersihan Sumber Daya

- **Pelaporan Komprehensif:** Menghasilkan laporan terperinci yang berisi ringkasan uji koneksi, hasil analisis jalur jaringan, dan penjelasan kegagalan spesifik dengan panduan remediasi.
- **Manajemen Sumber Daya:** Secara otomatis membersihkan sumber daya yang dibuat (fungsi Lambda, peran IAM, Jalur Wawasan Jaringan) kecuali `PersistReachabilityAnalyzerResults` parameter diatur untuk mempertahankan hasil analisis untuk penyelidikan lebih lanjut.
- **Penanganan Kesalahan:** Menyediakan laporan kesalahan spesifik untuk berbagai skenario kegagalan termasuk mesin basis data yang tidak didukung, sumber daya yang hilang, kegagalan resolusi DNS, dan masalah izin.

Runbook mendukung konektivitas pemecahan masalah untuk beberapa mesin database termasuk Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon Neptune, Amazon Redshift, Amazon S3, Azure SQL Database, MySQL, Oracle, PostgreSQL, SQL Server, dan banyak lainnya. DB2

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

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

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`

- `dms:DescribeEndpoints`
- `dms:DescribeReplicationInstances`
- `dms:DescribeConnections`
- `iam:GetRole`
- `iam:PassRole`
- `iam:SimulatePrincipalPolicy`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:GetFunction`
- `lambda:InvokeFunction`
- `lambda:ListTags`
- `lambda:TagResource`
- `lambda:UntagResource`
- `lambda:UpdateFunctionCode`

Izin IAM opsional

Izin berikut hanya diperlukan dalam `AutomationAssumeRole` jika Anda tidak memberikan `LambdaRoleArn` parameter dan ingin otomatisasi membuat peran eksekusi Lambda untuk Anda:

- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:AttachRolePolicy`
- `iam:DetachRolePolicy`
- `iam:TagRole`
- `iam:UntagRole`

 Important

Selain tindakan yang disebutkan di atas, [Amazon AutomationAssumeRole](#) harus memiliki [kebijakan VPCReachability AnalyzerFullAccessPolicy terkelola terlampir](#) sehingga pengujian [Reachability Analyzer](#) berhasil dilakukan.

Contoh Kebijakan:

```

{
  "Version": "2012-10-17"      ,
  "Statement": [
    {
      "Sid": "AllowDMSTroubleshootingActions",
      "Effect": "Allow",
      "Action": [
        "dms:DescribeEndpoints",
        "dms:DescribeReplicationInstances",
        "dms:DescribeConnections",
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowDMSLambdaInvocation",
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Resource": "arn*:lambda*:*:function:AWSSupport-
TroubleshootDMSEndpointConnection-*"
    },
    {
      "Sid": "AllowPassRoleToDMSLambda",

```

```

        "Effect": "Allow",
        "Action": [
            "iam:PassRole"
        ],
        "Resource": "arn:*:iam:*:role/AWSSupport-
TroubleshootDMSEndpointConnection-*",
        "Condition": {
            "StringLikeIfExists": {
                "iam:PassedToService": "lambda.amazonaws.com"
            }
        }
    },
    {
        "Sid": "AllowRolePolicyManagement",
        "Effect": "Allow",
        "Action": [
            "iam:AttachRolePolicy",
            "iam:DetachRolePolicy"
        ],
        "Resource": "*",
        "Condition": {
            "StringLikeIfExists": {
                "iam:ResourceTag/AWSSupport-
TroubleshootDMSEndpointConnection": "true"
            }
        }
    }
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootDMSEndpointConnection](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):

- Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan SSM Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, SSM Automation menggunakan izin pengguna yang memulai runbook ini.
- Tipe: `AWS::IAM::Role::Arn`
- DmsEndpointArn (Diperlukan)
 - Deskripsi: (Wajib) Nama Sumber Daya Amazon (ARN) dari Titik Akhir. AWS Database Migration Service
 - Tipe: `String`
 - Pola yang Diizinkan: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+:\d{12}:endpoint:[A-Z0-9]{1,48}$`
- DmsReplicationInstanceArn (Diperlukan)
 - Deskripsi: (Wajib) Nama Sumber Daya Amazon (ARN) dari instance AWS Database Migration Service Replikasi.
 - Tipe: `String`
 - Pola yang Diizinkan: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+:\d{12}:rep:[A-Z0-9]+$`
- PersistReachabilityAnalyzerResults (Opsional)
 - Deskripsi: (Opsional) Bendera yang menginformasikan apakah hasil eksekusi Analisis Wawasan Jaringan harus disimpan atau tidak.
 - Tipe: `Boolean`
 - Nilai yang Diizinkan: `[true, false]`
 - Default: `false`
- LambdaRoleArn (Opsional)
 - Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan AWS Lambda fungsi mengakses AWS layanan dan sumber daya yang diperlukan. Jika tidak ada peran yang ditentukan, Automasi Systems Manager ini akan membuat satu peran IAM untuk Lambda di akun Anda.
 - Tipe: `AWS::IAM::Role::Arn`
 - Default: `""`
- Akui (Diperlukan)

- Deskripsi: (Wajib) Masukkan yes untuk mengetahui bahwa runbook ini akan membuat fungsi Lambda di akun Anda dan akan membuat peran IAM jika tidak disediakan. `LambdaRoleArn`
- Tipe: `String`
- Pola yang Diizinkan: `^[Yy][Ee][Ss]$`

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- `DescribeEndpointAndCheckEngine`:

Mengambil konfigurasi AWS DMS endpoint dan memvalidasi jika tipe mesin database didukung untuk pemecahan masalah. Mengekstrak nama server, port, dan jenis mesin dari konfigurasi endpoint.

- `BranchOnEndpointAndCheckEngineErrors`:

Memcabangkan otomatisasi berdasarkan kesalahan apa pun dari validasi titik akhir. Jika kesalahan ditemukan, otomatisasi berlanjut untuk menghasilkan laporan kesalahan; jika tidak, itu berlanjut dengan pengujian konektivitas.

- `GetTestConnectionStatus`:

Mengambil status koneksi dan pesan kesalahan untuk AWS DMS titik akhir menggunakan API. `DescribeConnections` Langkah ini memeriksa apakah tes koneksi telah dilakukan dan menangkap pesan kegagalan apa pun.

- `BranchOnTestConnectionStatusErrors`:

Memcabangkan otomatisasi berdasarkan kesalahan status pengujian koneksi. Jika kesalahan terdeteksi, otomatisasi menghasilkan laporan kesalahan; jika tidak, itu dilanjutkan dengan analisis contoh replikasi.

- `DescribeReplicationInstance`:

Mengambil detail konfigurasi jaringan untuk instance AWS DMS replikasi termasuk ID VPC Amazon, subnet, grup keamanan IDs IDs, dan mengidentifikasi Antarmuka Jaringan Elastis (ENI) terkait.

- `ValidateResourcePermissions`:

Memvalidasi bahwa peran eksekusi memiliki izin yang diperlukan untuk membersihkan sumber daya yang akan dibuat selama proses otomatisasi.

- **Buat DNSResolver Lambda:**

Membuat AWS CloudFormation tumpukan yang berisi fungsi Lambda yang diterapkan dalam VPC Amazon yang sama dengan instance replikasi. Fungsi ini digunakan untuk menyelesaikan nama DNS ke alamat IP pribadi dari dalam konteks VPC Amazon.

- **DescribeCloudFormationErrorFromStackEvents:**

Jika pembuatan CloudFormation tumpukan gagal, langkah ini menjelaskan kesalahan dari peristiwa tumpukan untuk memberikan informasi kegagalan terperinci untuk pemecahan masalah.

- **Dapatkan DNSResolverLambdaName:**

Mengambil nama fungsi Lambda penyelesai DNS dari output tumpukan untuk digunakan CloudFormation pada langkah selanjutnya.

- **ResolveDmsEndpoint:**

Memanggil fungsi Lambda untuk menyelesaikan AWS DMS nama host endpoint ke alamat IP-nya dari dalam VPC Amazon. Ini memastikan resolusi DNS pribadi yang akurat dan memvalidasi kompatibilitas IPv4 .

- **BranchOnResolveDmsEndpointErrors:**

Cabang otomatisasi berdasarkan kesalahan resolusi DNS. Jika titik akhir tidak dapat diselesaikan atau diselesaikan ke IPv6 alamat, otomatisasi menghasilkan laporan kesalahan.

- **GetReachabilityAnalyzerTarget:**

Mengidentifikasi target yang sesuai untuk Reachability Analyzer berdasarkan konfigurasi Amazon VPC dan lokasi titik akhir. Menentukan apakah akan menggunakan ENI (untuk titik akhir VPC Amazon yang sama) atau alamat IP (untuk titik akhir eksternal) sebagai target.

- **GenerateErrors:**

Membuat laporan kesalahan komprehensif saat kegagalan terjadi pada langkah sebelumnya. Ini termasuk rincian tentang kesalahan validasi titik akhir, kegagalan pengujian koneksi, atau masalah resolusi DNS dengan panduan remediasi tertentu.

- **GenerateReport:**

Membuat laporan pemecahan masalah komprehensif yang berisi status koneksi, hasil analisis jalur jaringan menggunakan Reachability Analyzer, penjelasan rinci tentang hambatan konektivitas, dan tindakan yang direkomendasikan untuk resolusi.

- **CheckStackExists:**

Memeriksa apakah CloudFormation tumpukan berhasil dibuat dan perlu dihapus selama pembersihan. Langkah ini memastikan manajemen sumber daya yang tepat terlepas dari keberhasilan atau kegagalan otomatisasi.

- **Hapus DNSResolver Lambda:**

Menghapus CloudFormation tumpukan yang berisi fungsi Lambda penyelesai DNS dan sumber daya terkait (`PersistReachabilityAnalyzerResults` kecuali disetel `true` ke), memastikan tidak ada sumber daya sisa yang tersisa setelah otomatisasi selesai.

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

- **GetTestConnectionStatus.status**

Status pengujian koneksi saat ini antara instance AWS DMS replikasi dan titik akhir (misalnya, berhasil, gagal, pengujian).

- **DescribeCloudFormationErrorFromStackEvents.Acara**

Jika pembuatan CloudFormation tumpukan gagal, output ini berisi peristiwa kesalahan terperinci dari proses pembuatan tumpukan untuk membantu mendiagnosis masalah penerapan infrastruktur.

- **GenerateReport.laporan**

Laporan pemecahan masalah komprehensif yang berisi hasil analisis koneksi, temuan Reachability Analyzer, analisis jalur jaringan, hambatan konektivitas spesifik yang diidentifikasi, dan rekomendasi remediasi terperinci dengan tautan ke dokumentasi yang relevan. AWS

- **GenerateErrors.laporan**

Jika kesalahan terjadi selama proses otomatisasi, output ini memberikan laporan kesalahan terperinci termasuk alasan kegagalan spesifik, sumber daya yang terpengaruh, dan panduan untuk menyelesaikan masalah sebelum mencoba kembali otomatisasi.

Referensi

Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)

- [Support Automation Workflow landing page](#)

Amazon EBS

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Elastic Block Store. Untuk informasi lebih lanjut 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

Tipe: 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 read/write izin 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

Tipe: 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:

JSON

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

```

    "Statement": [{
      "Sid": "ReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ssm:DescribeAutomationExecutions"
      ],
      "Resource": "*"
    }, {
      "Sid": "KMSGeneratePermissions",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
      "Resource": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }, {
      "Sid": "S3ReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketAcl",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket2/"
      ]
    }, {
      "Sid": "S3CreatePermissions",
      "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 [AWS Support-AnalyzeEBSResourceUsage](#) dalam AWS Systems Manager konsol.

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.

- S3 BucketName (Diperlukan):

Bucket Amazon S3 di akun Anda untuk mengunggah laporan.

- CustomerManagedKmsKeyArn (Opsional):

AWS KMS Kunci 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

test-bucket-1

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

admin-my

arn:aws:iam:::role:

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

arn:aws:kms:eu-central-1::key/:-4216-a498-460a2132ca4c

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

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Deskripsi untuk snapshot Amazon EBS.

- DryRun

Tipe: 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

Tipe: String

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

- RetentionDays

Tipe: String

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

- SnapshotWithTag

Tipe: String

Nilai yang valid: Ya | Tidak

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

- TagKey

Tipe: String

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

- TagValue

Tipe: String

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

- VolumeId

Tipe: 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`

Tipe: 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

Tipe: String

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

- InstanceId

Tipe: String

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

- VolumeId

Tipe: 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 memberikan Amazon EC2 sebagai ResourceID, Amazon EC2 akan membuat dasbor dengan Total CloudWatch Aktual untuk instans IOPS/Throughput 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 Amazon akan membuat dasbor dengan grafik Estimasi Rata-Rata CloudWatch untuk volume tersebut. IOPS/Throughput
- 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), maksimum IOPS/throughput harus dipertimbangkan, sampai Anda memiliki keseimbangan burst. Setelah keseimbangan burst sepenuhnya digunakan yaitu menjadi nol, pertimbangkan metrik dasar IOPS/throughput .

Important

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

Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

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

Kebijakan Sampel

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "cloudwatch:PutDashboard",
      "Resource": "arn:aws:cloudwatch::111122223333: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 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.

- 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	
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. Choose an option	ResourceId (Required) The ID of the EC2 instance or EBS Volume.
StartTime (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.	EndTime (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.

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 CloudWatch 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.

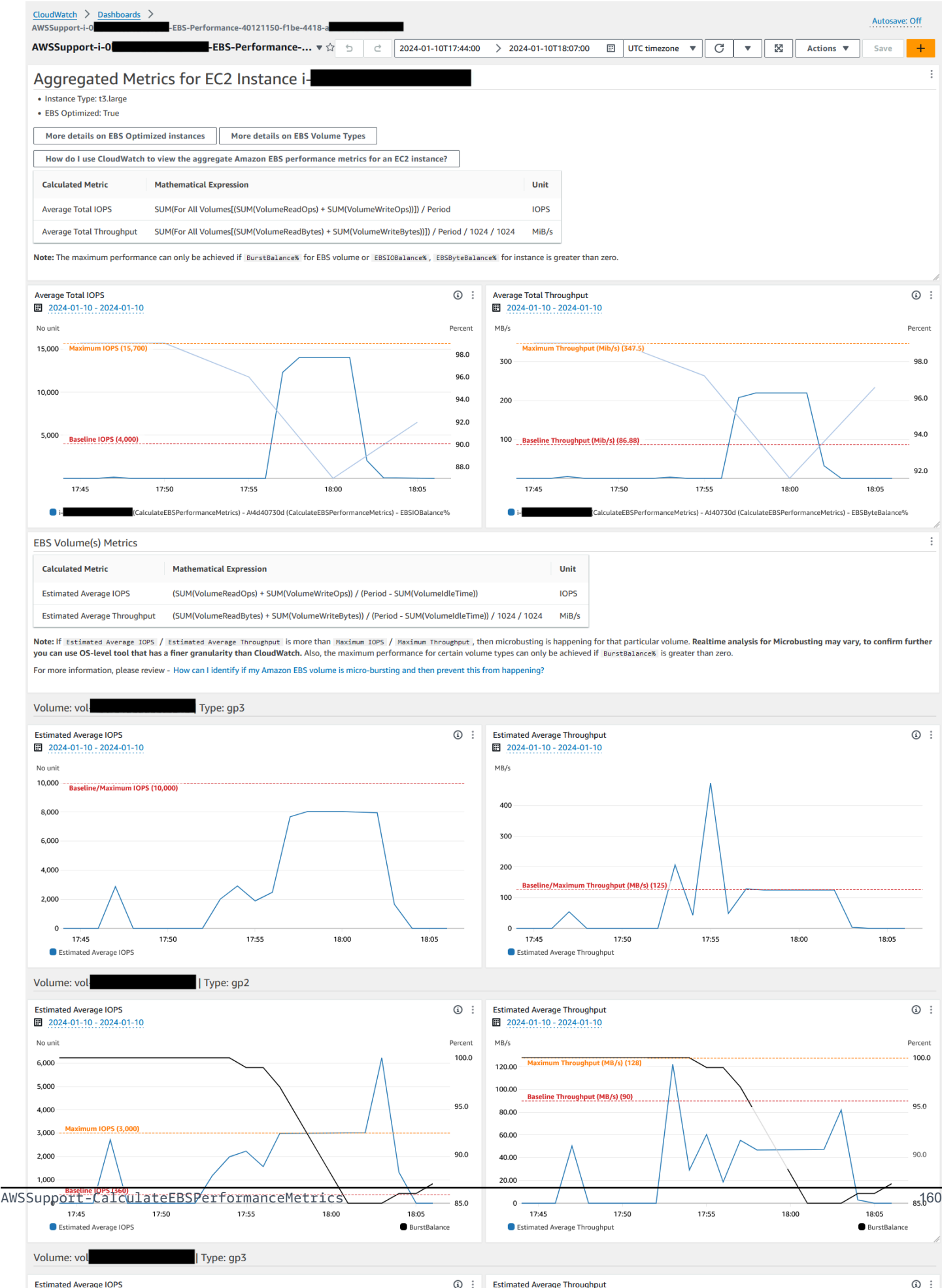
7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci:

```
▼ Outputs

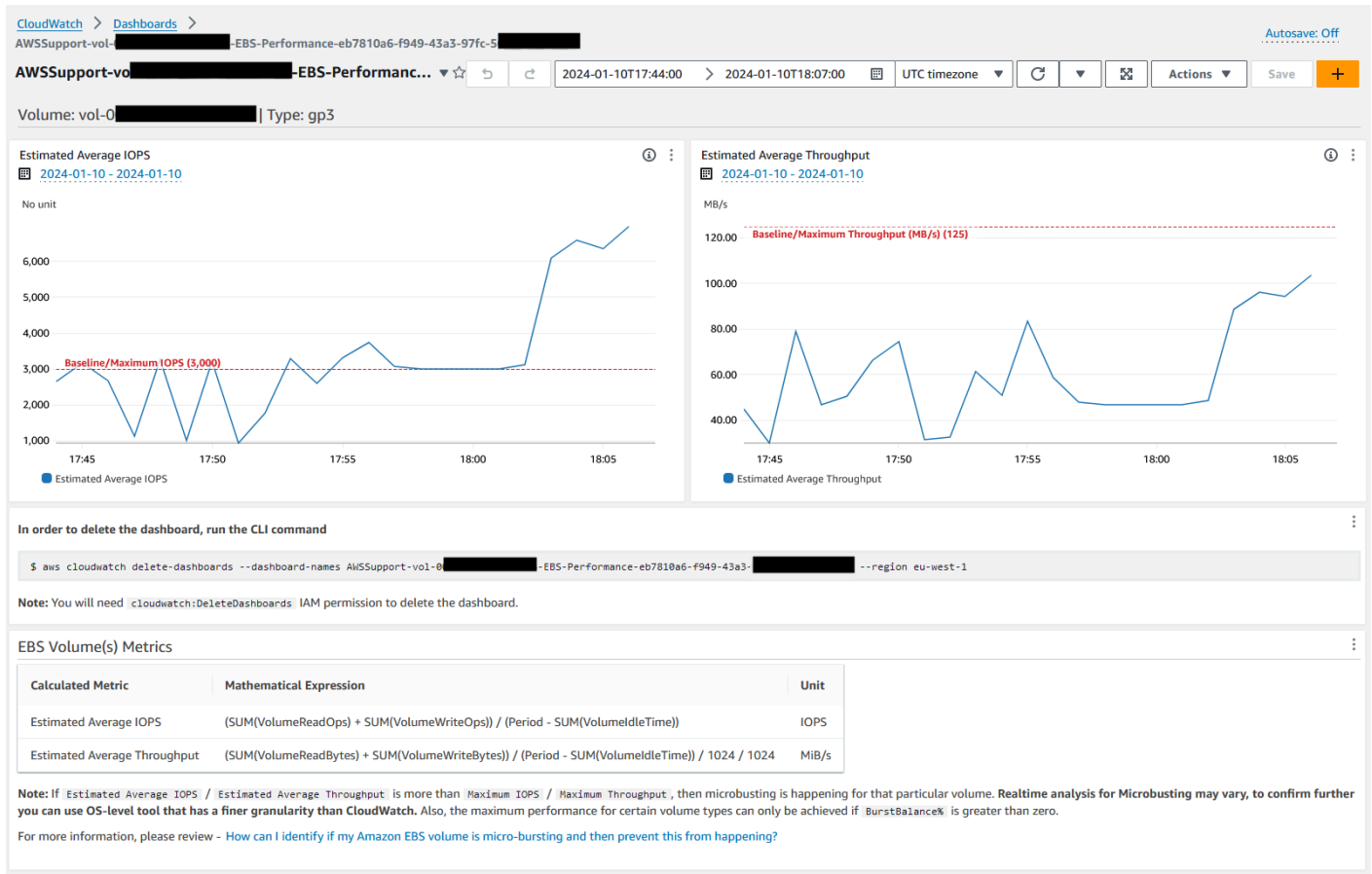
CreateCloudWatchDashboard.CloudWatchDashboardLink
https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#dashboards:name=AWSsupport-i-██████████:EBS-Performance-443096c1-df23-44ba-96dd-2d005b5ae971

CreateCloudWatchDashboard.CloudWatchDashboardMessage
Open the CloudWatch Dashboard URL in your browser to see the performance metrics for the target resource 'i-██████████'.
You can delete the CloudWatch Dashboard from the CloudWatch console.
```

Contoh CloudWatch Dasbor Untuk ID Sumber Daya sebagai instans Amazon EC2



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](#)

AWS dokumentasi 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

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Deskripsi untuk snapshot Amazon EBS.

- SnapshotId

Tipe: String

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

- SourceRegion

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Deskripsi untuk snapshot

- Volumeld

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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`

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: String

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

- `Umur`

Tipe: String

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

- `TagKey`

Tipe: String

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

- `TagValue`

Tipe: 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

Tipe: 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.

- LambdaAssumeRole

Tipe: String

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

- Volumeld

Tipe: 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`

Tipe: 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`

Tipe: 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.

- `DriveLetter`

Tipe: String

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

- **InstanceId**

Tipe: 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**

Tipe: String

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

- **SizeGib**

Tipe: String

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

- **VolumeId**

Tipe: 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`

Tipe: 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) Akun yang ingin Anda bagikan snapshot dengan. IDs Parameter ini diperlukan jika Anda memasukkan No nilai `Private` parameter.

- AccountPermissionOperation

Tipe: String

Nilai yang valid: tambahkan | hapus

Default: tidak ada

Deskripsi: (Opsional) Jenis operasi yang harus dilakukan.

- Privat

Tipe: String

Nilai yang valid: Ya | Tidak

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

- SnapshotIds

Jenis: StringList

Deskripsi: (Wajib) Snapshot Amazon EBS yang izinnnya ingin Anda ubah. IDs

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 snapshot yang disediakan dalam parameter. `IDs SnapshotIds` Setelah memverifikasi `IDs`, 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 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.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

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

- EbsVolumeType

Tipe: 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](#).

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 lebih lanjut tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWS-ASGEnterStandby](#)
- [AWS-ASGExitStandby](#)
- [AWS-CreatedImage](#)
- [AWS-DeleteImage](#)
- [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-PatchLoadBalancerInstance](#)
- [AWSEC2-SQLServerDBRestore](#)
- [AWSSupport-ActivateWindowsWithAmazonLicense](#)
- [AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2](#)
- [AWSPremiumSupport-ChangeInstanceTypeIntelToAMD](#)
- [AWSSupport-CheckXenToNitroMigrationRequirements](#)
- [AWSSupport-CloneXenEC2InstanceAndMigrateToNitro](#)
- [AWSSupport-ConfigureEC2Metadata](#)
- [AWSSupport-ContainEC2Instance](#)
- [AWSSupport-CopyEC2Instance](#)
- [AWSPremiumSupport-DiagnoseDiskUsageOnLinux](#)
- [AWSSupport-EnableWindowsEC2SerialConsole](#)
- [AWSPremiumSupport-ExtendVolumesOnWindows](#)
- [AWSSupport-ExecuteEC2Rescue](#)
- [AWSSupport-ListEC2Resources](#)
- [AWSSupport-ManageRDPSettings](#)
- [AWSSupport-ManageWindowsService](#)
- [AWSSupport-MigrateEC2ClassicToVPC](#)
- [AWSSupport-MigrateXenToNitroLinux](#)
- [AWSSupport-ResetAccess](#)
- [AWSSupport-ResetLinuxUserPassword](#)
- [AWSSupport-RunEC2RescueForWindowsTool](#)

- [AWSPremiumSupport-ResizeNitroInstance](#)
- [AWSSupport-ShareEncryptedAMIOrEBSSnapshot](#)
- [AWSSupport-RestoreEC2InstanceFromSnapshot](#)
- [AWSSupport-SendLogBundleToS3Bucket](#)
- [AWSSupport-StartEC2RescueWorkflow](#)
- [AWSSupport-TroubleshootActiveDirectoryReplication](#)
- [AWSPremiumSupport-TroubleshootEC2DiskUsage](#)
- [AWSSupport-TroubleshootEC2InstanceConnect](#)
- [AWSSupport-TroubleshootLinuxMGNDRSAgentLogs](#)
- [AWSSupport-TroubleshootRDP](#)
- [AWSSupport-TroubleshootSSH](#)
- [AWSSupport-TroubleshootSUSERegistration](#)
- [AWSSupport-TroubleshootWindowsPerformance](#)
- [AWSSupport-TroubleshootWindowsUpdate](#)
- [AWSSupport-UpgradeWindowsAWSDrivers](#)

AWS-ASGEnterStandby

Deskripsi

Ubah status siaga instans Amazon Elastic Compute Cloud EC2 (Amazon) dalam grup Auto Scaling.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID EC2 instans Amazon yang ingin Anda ubah status siaga dalam grup Auto Scaling.

- LambdaRoleArn

Tipe: 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.

AWS-ASGExitStandby

Deskripsi

Ubah status siaga instans Amazon Elastic Compute Cloud EC2 (Amazon) dalam grup Auto Scaling.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID EC2 instance yang ingin Anda ubah status siaga dalam grup Auto Scaling.

- LambdaRoleArn

Tipe: 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.

AWS-CreateImage

Deskripsi

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

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID dari instans EC2.

- NoReboot

Jenis: Boolean

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

JSON

```
{
  "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

Tipe: 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.

- ImageId

Tipe: String

Deskripsi: (Wajib) ID AMI.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DeleteSnapshot",
      "Resource": "arn:aws:ec2:*:*: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 Auto Scaling.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

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

- LambdaRoleArn

Tipe: 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.

- WaitForInstance

Tipe: String

Standar: PT2 M

Deskripsi: (Opsional) Durasi dimana Otomatisasi harus tidur untuk memungkinkan instans kembali ke layanan.

- WaitForReboot

Tipe: String

Standar: PT5 M

Deskripsi: (Opsional) Durasi dimana Otomatisasi harus tidur agar instance yang ditambah dapat di-reboot.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 EC2 instance sesuai dengan baseline patch yang berlaku. Mengembalikan volume root pada kegagalan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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`

Tipe: String

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

- `LambdaAssumeRole`

Tipe: 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.

- Laporan3Bucket

Tipe: String

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

Langkah Dokumen

Nomor langkah	Nama langkah	Tindakan otomasi
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

Nomor langkah	Nama langkah	Tindakan otomasi
10	DeleteSnapshot	aws:invokeLambdaFunction
11	deleteCloudFormationTemplate	aws:deleteStack

Keluaran

IdentifyRootVolume.Muatan

PrePatchSnapshot.Keluaran

SaveComplianceReportToS3.Payload

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`

Tipe: 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`

Tipe: String

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

- `IsolationSecurityGroup`

Tipe: String

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

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan 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 instans bukan bagian dari grup Auto Scaling.
- `aws:executeAwsApi`- Membuat snapshot dari volume root yang melekat pada instance.
- `aws:waitForAwsResourceProperty`- Menunggu status snapshot menjadi `completed`
- `aws:executeAwsApi`- Menetapkan grup keamanan yang ditentukan dalam `IsolationSecurityGroup` parameter untuk instance Anda.

Keluaran

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

AWS-ResizeInstance

Deskripsi

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

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instance.

- InstanceType

Tipe: String

Deskripsi: (Wajib) Jenis instance.

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

Tipe: 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: StringList

Deskripsi: (Wajib) EC2 Instans Amazon untuk memulai ulang. IDs

AWS-SetupJupyter

Deskripsi

AWS-SetupJupyterRunbook membantu Anda mengatur Notebook Jupyter di instans Amazon Elastic Compute Cloud (Amazon). EC2 Anda dapat menentukan instance yang ada, atau memberikan Amazon Machine Image (AMI) ID untuk otomatisasi untuk meluncurkan dan menyiapkan instance baru. Sebelum memulai, Anda harus membuat SecureString parameter di Parameter Store untuk digunakan sebagai kata sandi untuk Jupyter Notebook. Parameter Store adalah alat di 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

Tipe: 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.

- Amild

Tipe: String

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

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID instance tempat Anda ingin mengatur Notebook Jupyter.

- InstanceType

Tipe: String

Default: t3.medium

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

- JupyterPasswordSSMKey

Tipe: String

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

- **KeyPairName**

Tipe: String

Deskripsi: (Opsional) Key pair yang ingin Anda kaitkan dengan instance yang baru diluncurkan.

- **RemoteAccessCidr**

Tipe: String

Default 0.0.0.0/0

Deskripsi: (Opsional) Rentang CIDR yang ingin Anda izinkan lalu lintas SSH.

- **RoleName**

Tipe: String

Default: SSMManged InstanceProfileRole

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

- **StackName**

Tipe: String

Default: CreateManagedInstanceStack {{Automation:Execution_ID}}

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

- **SubnetId**

Tipe: String

Default: Default

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

- **VpcId**

Tipe: String

Default: Default

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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`- Menyiapkan Jupyter Notebook 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`

Tipe: 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: StringList

Deskripsi: (Wajib) EC2 instance 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

Tipe: 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.

- InstanceIds

Jenis: StringList

Deskripsi: (Wajib) EC2 instance untuk berhenti.

AWS-TerminateEC2Instance

Deskripsi

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

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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: StringList

Deskripsi: (Wajib) IDs dari satu atau beberapa EC2 contoh untuk dihentikan.

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

Tipe: 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.

Pola yang Diizinkan: `^$|^arn:aws[a-z0-9-]*:iam::(\d{12}|\{\{global:ACCOUNT_ID\}\}):role/[w/.@+,-]{1,1017}$`

- Harus berupa ARN peran IAM yang valid atau string kosong. Variabel sistem `{global:ACCOUNT_ID}` dapat digunakan sebagai pengganti ID AWS Akun di `arn`.
- ExcludePackages

Tipe: String

Default: tidak ada

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

Pola yang Diizinkan: `^(none|[a-zA-Z0-9\s,._+:=<>()\[\]/*-]+)$`

- Harus “tidak ada” ATAU daftar item yang dipisahkan koma yang terdiri dari huruf, angka, spasi, dan karakter berikut: `, . _ + : = < > ( ) [ ] / * -`
- IamInstanceProfileName

Tipe: String

Default: ManagedInstanceProfile

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

Pola yang Diizinkan: `^[\w+=, .@-]{1,128}$`

- Harus antara 1 dan 128 karakter dan hanya berisi huruf, angka, dan karakter ini: + = , . @ -

- IncludePackages

Tipe: String

Default: semua

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

Pola yang Diizinkan: `^(a11|[a-zA-Z0-9\s, ._:=<>()\[\]/*-]+)$`

- Harus "semua" ATAU daftar item yang dipisahkan koma yang terdiri dari huruf, angka, spasi, dan karakter berikut: , . _ + : = < > () [] / * -

- InstanceType

Tipe: String

Default: t2.micro

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

Pola yang Diizinkan: `^[a-z0-9]+(-[a-z0-9]+)*\.[a-z0-9]+$`

- Harus dalam format prefix.suffix di mana kedua bagian berisi huruf kecil dan angka, dan awalan mungkin termasuk tanda hubung

- MetadataOptions

Jenis: StringMap

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

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

Pola yang Diizinkan: `^{\[^<>\$;|&\\]*}$`

- Harus dibungkus dengan kurawal kurawal {} dan tidak dapat berisi karakter ini: < > \$; | & \
- PostUpdateScript

Tipe: String

Default: tidak ada

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

Pola yang Diizinkan: `^(none|https?:\/\/[\w\-. _~:\/?#\[\]\@!$&'()*+ , ; =% ]+)$`

- Harus “tidak ada” ATAU HTTP/HTTPS URL yang valid
- PreUpdateScript

Tipe: String

Default: tidak ada

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

Pola yang Diizinkan: `^(none|https?:\/\/[\w\-. _~:\/?#\[\]\@!$&'()*+ , ; =% ]+)$`

- Harus “tidak ada” ATAU HTTP/HTTPS URL yang valid
- SecurityGroupIds

Tipe: String

Deskripsi: (Wajib) Daftar terpisah koma IDs dari grup keamanan yang ingin Anda terapkan. AMI

Pola yang Diizinkan: `^sg-[a-z0-9]{8,17}$`

- Harus dimulai dengan “sg-” diikuti dengan 8-17 huruf kecil atau angka
- SourceAmiId

Tipe: String

Deskripsi: (Wajib) Sumber Amazon Machine Image ID.

Pola yang Diizinkan: `^ami-[a-z0-9]{8,17}$`

- Harus dimulai dengan “ami-” diikuti dengan 8-17 huruf kecil atau angka

- SubnetId

Tipe: String

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

Pola yang Diizinkan: `^$|^subnet-[a-z0-9]{8,17}$`

- Harus kosong ATAU mulai dengan “subnet-” diikuti dengan 8-17 huruf kecil atau angka

- TargetAmiName

Tipe: String

Default: `UpdateLinuxAmi _dari_ {{SourceAmiId}} _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.

Pola yang Diizinkan: `^[a-zA-Z0-9() \[\] \{ \} . / ' @ _ : -]{3,128}$`

- Harus antara 3 dan 128 karakter dan hanya berisi huruf, angka, spasi, dan karakter ini: () [] { } . / ' @ _ : -

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 melalui Windows Server 2022.

Important

Runbook ini tidak mendukung Windows Server 2025 dan versi yang lebih baru, karena driver AWS Paravirtual tidak kompatibel dengan versi ini. Untuk informasi selengkapnya, lihat [Driver paravirtual untuk instance Windows](#).

⚠ 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

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Tentukan satu atau beberapa artikel Pangkalan Pengetahuan Microsoft (KB) IDs untuk dikecualikan. Anda dapat mengecualikan beberapa IDs menggunakan nilai yang dipisahkan koma. Format yang valid: KB9876543 atau 9876543.

- IamInstanceProfileName

Tipe: String

Default: ManagedInstanceProfile

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

- IncludeKbs

Tipe: String

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

- InstanceType

Tipe: 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 selengkapnya, lihat [InstanceMetadataOptionsRequest](#).

- PostUpdateScript

Tipe: String

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

- PreUpdateScript

Tipe: String

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

- PublishedDateAfter

Tipe: 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

Tipe: 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

Tipe: 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.

- SecurityGroupIds

Tipe: String

Deskripsi: (Wajib) Daftar terpisah koma IDs dari grup keamanan yang ingin Anda terapkan. AMI

- SeverityLevels

Tipe: 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

Tipe: String

Deskripsi: (Wajib) AMI ID sumber.

- SubnetId

Tipe: String

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

- TargetAmiName

Tipe: 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`

Tipe: 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.

- `AutoScalingGroupARN`

Tipe: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari grup penskalaan otomatis tempat Anda ingin mengaktifkan pemeriksaan kesehatan.

- `HealthCheckGracePeriod`

Jenis: Integer

Default: 300

Deskripsi: (Opsional) Jumlah waktu, dalam hitungan detik, Auto Scaling menunggu sebelum memeriksa status kesehatan instans Amazon Elastic Compute Cloud (Amazon EC2) yang telah mulai beroperasi.

Izin IAM yang diperlukan

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

- `ssm:StartAutomationExecution`

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

Langkah Dokumen

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

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

Deskripsi

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

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `InstanceId`

Tipe: String

Deskripsi: (Wajib) ID EC2 instans Amazon yang ingin Anda gunakan IMDSv2.

- `AutomationAssumeRole`

Tipe: 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 EC2 contoh hosting container. 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` EC2 instans Amazon yang Anda tentukan dalam `InstanceId` parameter.
- `aws:assertAwsResourceProperty`- Memverifikasi `IMDSv2` diperlukan pada EC2 instans Amazon.

AWSEC2-CloneInstanceAndUpgradeSQLServer

Deskripsi

Buat sebuah AMI dari sebuah EC2 contoh untuk Windows Server menjalankan SQL Server 2008 atau yang lebih baru, dan kemudian meng-upgrade AMI ke versi SQL Server yang lebih baru. Hanya versi bahasa Inggris dari SQL Server yang didukung.

Jalur pemutakhiran berikut didukung:

- SQL Server 2008 ke SQL Server 2017, 2016, atau 2014
- SQL Server 2008 R2 ke SQL Server 2017, 2016, atau 2014
- SQL Server 2012 ke SQL Server 2019, 2017, 2016, atau 2014
- SQL Server 2014 ke SQL Server 2019, 2017, atau 2016
- SQL Server 2016 ke SQL Server 2019 atau 2017

Jika Anda menggunakan versi Windows Server sebelumnya yang tidak kompatibel dengan SQL Server 2019, dokumen otomatisasi harus memutakhirkan 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 peningkatan di tempat ke TargetSQLVersion pada instance sementara. Setelah upgrade, otomatisasi menciptakan yang 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 instance yang ditingkatkan.

Note

Jika Anda ingin memodifikasi nama komputer dari EC2 instance yang diluncurkan dari yang baru AMI, lihat [Mengganti nama Komputer yang Menghosting Instance SQL Server yang Berdiri Sendiri](#).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter

Prasyarat

- TLS versi 1.2.
- Hanya versi bahasa Inggris dari SQL Server yang didukung.
- EC2 Instance harus menggunakan versi Windows Server itu adalah Windows Server 2008 R2 (atau yang lebih baru) dan SQL Server 2008 (atau yang lebih baru).
- Pastikan bahwa SSM Agent diinstal pada instans Anda. Untuk informasi selengkapnya, lihat [Menginstal dan mengonfigurasi Agen SSM pada EC2 instans untuk Windows Server](#).
- Konfigurasi instance untuk menggunakan peran profil instans AWS Identity and Access Management (IAM). Untuk informasi selengkapnya, lihat [Buat profil instans IAM untuk Systems Manager](#).
- Verifikasi bahwa instans memiliki 20 GB ruang disk kosong di disk boot instans.
- Untuk instans yang menggunakan versi SQL Server Bawa Lisensi Sendiri (BYOL), prasyarat tambahan berikut ini berlaku:
 - Berikan ID snapshot EBS yang menyertakan media instalasi SQL Server target. Untuk melakukannya:
 1. Verifikasi bahwa EC2 instance menjalankan Windows Server 2008 R2 atau yang lebih baru.
 2. Buat volume EBS 6 GB di Availability Zone yang sama di mana instans berjalan. Lampirkan volume ke instans. Pasang, misalnya, sebagai drive D.
 3. Klik kanan ISO dan pasang ke instans sebagai, misalnya, drive E.
 4. Salin konten ISO dari drive E:\ ke drive D:\
 5. Buat snapshot EBS dari volume 6 GB yang dibuat pada langkah 2.

Batasan

- Pemutakhiran dapat dilakukan hanya pada SQL Server menggunakan autentikasi Windows.

- Verifikasi bahwa tidak ada pembaruan patch keamanan yang tertunda pada instans. Buka Panel Kontrol, lalu pilih Periksa pembaruan.
- Penerapan SQL Server dalam mode HA dan mirroring tidak didukung.

Parameter

- `IamInstanceProfile`

Tipe: String

Deskripsi: (Wajib) Profil instans IAM.

- `InstanceId`

Tipe: String

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

- `KeepPreUpgradeImageBackUp`

Tipe: String

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

- `SubnetId`

Tipe: String

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

- `SQLServerSnapshotId`

Tipe: String

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

- `RebootInstanceBeforeTakingImage`

Tipe: String

Deskripsi: (Opsional) Jika disetel ke `true`, otomatisasi akan me-reboot instance sebelum membuat AMI pra-upgrade. Secara default, otomatisasi tidak reboot sebelum memutakhirkan.

- Target SQLVersion

Tipe: 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 dibuat dari instance yang ditingkatkan ke versi SQL Server yang lebih baru.

AWSEC2-CloneInstanceAndUpgradeWindows

Deskripsi

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

- Windows Server 2008 R2 ke Windows Server 2016.
- Windows Server 2012 R2 ke Windows Server 2016.
- Windows Server 2012 R2 ke Windows Server 2019.
- Windows Server 2012 R2 ke Windows Server 2022.
- Windows Server 2016 ke Windows Server 2019.
- Windows Server 2016 ke Windows Server 2022.
- Windows Server 2019 ke Windows Server 2022.

Operasi upgrade adalah proses multi-langkah yang dapat memakan waktu 2 jam untuk menyelesaikannya. Kami merekomendasikan untuk melakukan upgrade sistem operasi pada instans dengan setidaknya 2 v CPUs dan 4GB RAM. 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 instance sementara. Otomatisasi kemudian melakukan peningkatan di tempat ke TargetWindowsVersion pada instance sementara. Untuk meng-upgrade Windows Server 2008 R2 misalnya untuk Windows Server 2016, 2019, atau 2022, peningkatan di tempat dilakukan dua kali karena peningkatan langsung 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 EC2 instance 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.
- Otomatisasi 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 Windows Server Media instalasi 2012 R2. Untuk melakukannya:
 - Verifikasi bahwa EC2 instance sedang berjalan Windows Server 2012 atau yang lebih baru.
 - Buat volume EBS 6 GB di Availability Zone yang sama tempat instance 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 EC2 instance untuk 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`

Tipe: 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.

- BYOLWindowsMediaSnapshotId

Tipe: String

Deskripsi: (Opsional) ID snapshot Amazon EBS untuk disalin yang menyertakan media instalasi Windows Server 2012R2. Diperlukan hanya jika Anda memutakhirkan instance BYOL.

- IamInstanceProfile

Tipe: String

Deskripsi: (Wajib) Nama profil instans IAM yang memungkinkan Systems Manager mengelola instance.

- InstanceId

Tipe: String

Deskripsi: (Wajib) EC2 Instance berjalan Windows Server 2008 R2, 2012 R2, 2016, atau 2019.

- KeepPreUpgradeImageBackUp

Tipe: String

Deskripsi: (Opsional) Jika disetel Benar, Otomasi tidak akan menghapus AMI yang dibuat dari EC2 instance sebelum upgrade. Jika disetel ke True, maka Anda harus menghapus AMI. Secara default, AMI dihapus.

- SubnetId

Tipe: String

Deskripsi: (Wajib) Ini adalah subnet untuk proses pemutakhiran dan tempat EC2 instance sumber Anda berada. Verifikasi bahwa subnet memiliki konektivitas keluar ke AWS layanan, Amazon S3, dan Microsoft (untuk mengunduh tambalan).

- TargetWindowsVersion

Tipe: String

Deskripsi: (Diperlukan) Pilih versi Windows target.

Bawaan: 2022

- RebootInstanceBeforeTakingImage

Tipe: String

Deskripsi: (Opsional) Jika disetel True, Automation akan me-reboot instance sebelum membuat AMI pra-upgrade. Secara default, Automation tidak reboot sebelum upgrade.

AWSEC2-PatchLoadBalancerInstance

Deskripsi

Tingkatkan dan tambal versi minor dari EC2 instans Amazon (Windows atau Linux) yang dilampirkan ke penyeimbang beban apa pun (klasik, ALB, atau NLB). Waktu pengeringan koneksi default diterapkan sebelum instance ditambal. Anda dapat mengganti waktu tunggu dengan memasukkan waktu pengeringan kustom Anda dalam menit (1-59) untuk parameter. ConnectionDrainTime

Alur kerja otomatisasi adalah sebagai berikut:

1. Penyeimbang beban atau kelompok target tempat instance dilampirkan ditentukan, dan instance diverifikasi sebagai sehat.
2. Instance dihapus dari penyeimbang beban atau kelompok target.
3. Otomatisasi menunggu periode waktu yang ditentukan untuk waktu pengeringan koneksi.
4. [RunPatchBaselineOtomatisasi AWS](#) dipanggil untuk menambal instance.
5. Instance disambungkan kembali ke penyeimbang beban atau kelompok target.

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

Jenis Dokumen

Otomatisasi

Pemilik

Amazon

Prasyarat

- Pastikan bahwa SSM Agent diinstal pada instans Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan Agen SSM pada EC2 instans untuk Windows Server](#).

Parameter

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID instance untuk ditambah yang terkait dengan penyeimbang beban (klasik, ALB, atau NLB).

- ConnectionDrainTime

Tipe: String

Deskripsi: (Opsional) Waktu pengeringan koneksi penyeimbang beban, dalam hitungan menit (1-59).

- S3 BucketLog

Tipe: String

Deskripsi: (Opsional) Nama bucket Amazon S3 yang akan digunakan untuk menyimpan respons keluaran perintah. Anda dapat menentukan ember yang Anda miliki atau ember yang dibagikan dengan Anda. Jika Anda memberikan parameter ini, Anda juga harus menyediakan runCommandAssumePeran.

- runCommandAssumePeran

Tipe: String

Deskripsi: (Opsional) ARN dari peran IAM yang akan digunakan untuk menjalankan perintah pada instance. Peran harus memiliki hubungan kepercayaan dengan prinsipal **ssm.amazonaws.com** layanan, harus memiliki SSMManged InstanceCore kebijakan Amazon yang dilampirkan, dan harus memiliki izin tulis untuk bucket Amazon S3 yang ditentukan untuk S3. BucketLog

AWSEC2-SQLServerDBRestore

Deskripsi

AWSEC2-SQLServerDBRestoreRunbook mengembalikan backup database Microsoft SQL Server yang disimpan di Amazon S3 ke SQL Server 2017 yang berjalan di instans Linux Amazon Elastic Compute Cloud (EC2). Anda dapat menyediakan instans EC2 Anda sendiri yang menjalankan SQL Server 2017 Linux. Jika instans EC2 tidak disediakan, otomatisasi akan meluncurkan dan mengonfigurasi instans Ubuntu 16.04 EC2 baru dengan SQL Server 2017. Otomatisasi mendukung pemulihan cadangan log penuh, diferensial, dan transaksional. Otomatisasi ini menerima beberapa file cadangan basis data 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 yang ditandatangani. 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 kata sandi pengguna SA Anda sendiri lagi sebelum Anda terhubung ke instance SQL Server.

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

Jenis Dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Prasyarat

Untuk menjalankan otomatisasi ini, Anda harus memenuhi prasyarat berikut:

- Pengguna atau peran IAM yang menjalankan otomatisasi ini harus memiliki kebijakan sebaris yang dilampirkan dengan izin yang diuraikan. [Izin IAM yang diperlukan](#)
- Jika Anda menyediakan 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 yang dilampirkan. 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.

Batasan

Otomatisasi ini tidak mendukung pemulihan ke SQL Server yang berjalan pada instans 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

Tipe: String

Deskripsi: (Opsional) Daftar nama database yang dipisahkan koma untuk dipulihkan.

- DataDirectorySize

Tipe: String

Deskripsi: (Opsional) Ukuran volume yang diinginkan (GiB) dari direktori Data SQL Server untuk instans EC2 baru.

Nilai default: 100

- KeyPair

Tipe: String

Deskripsi: (Opsional) Pasangan kunci yang akan digunakan saat membuat instans EC2 baru.

- `IamInstanceProfileName`

Tipe: String

Deskripsi: (Opsional) Profil instans IAM untuk dilampirkan ke instans EC2 baru. Profil instans IAM harus memiliki kebijakan `AmazonSSMManagedInstanceCore` terkelola yang dilampirkan.

- `Instanceld`

Tipe: String

Deskripsi: (Opsional) Instance yang menjalankan SQL Server 2017 di Linux. Jika tidak `Instanceld` disediakan, otomatisasi meluncurkan instans EC2 baru menggunakan `SQLServer` Edisi `InstanceType` dan yang disediakan.

- `InstanceType`

Tipe: String

Deskripsi: (Opsional) Jenis instans EC2 yang akan diluncurkan.

- `ISS3 PresignedUrl`

Tipe: String

Deskripsi: (Opsional) Jika `S3Input` adalah URL S3 yang telah ditandatangani sebelumnya, tunjukkan. `yes`

Nilai default: tidak

Nilai yang valid: `ya` | `tidak`

- `LogDirectorySize`

Tipe: String

Deskripsi: (Opsional) Ukuran volume yang diinginkan (GiB) dari direktori SQL Server Log untuk instans EC2 baru.

Nilai default: 100

- Masukan S3

Tipe: String

Deskripsi: (Diperlukan) Nama bucket S3, daftar kunci objek S3 yang dipisahkan koma, atau daftar S3 yang telah ditandatangani sebelumnya yang dipisahkan koma yang URLs berisi file cadangan SQL yang akan dipulihkan.

- SQLServerEdisi

Tipe: String

Deskripsi: (Opsional) Edisi SQL Server 2017 yang akan diinstal pada instans EC2 yang baru dibuat.

Nilai yang valid: Standar | Perusahaan | Web | Ekspres

- SubnetId

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Ukuran volume yang diinginkan (GiB) dari direktori TempDB SQL Server untuk instans EC2 baru.

Nilai default: 100

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut agar berhasil menggunakan runbook.

JSON

```
{  
  "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::111122223333: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 instans EC2 baru untuk Linux.
3. `aws:waitForAwsResourceProperty`- Tunggu instans EC2 yang baru dibuat siap.
4. `aws:executeAwsApi`- Reboot instance jika instance tidak siap.
5. `aws:assertAwsResourceProperty`- Verifikasi bahwa Agen SSM diinstal.
6. `aws:runCommand`- Jalankan skrip pemulihan SQL Server di PowerShell.

Untuk instans EC2 yang ada:

1. `aws:waitForAwsResourceProperty`- Verifikasi bahwa instans EC2 sudah siap.
2. `aws:executeAwsApi`- Reboot instance jika instance tidak siap.
3. `aws:assertAwsResourceProperty`- Verifikasi bahwa Agen SSM diinstal.
4. `aws:runCommand`- Jalankan skrip pemulihan SQL Server di PowerShell.

Keluaran

`getInstance.InstanceId`

`restoreToNewInstance.Output`

`restoreToExistingInstance.Output`

AWSSupport-ActivateWindowsWithAmazonLicense

Deskripsi

AWSSupport-ActivateWindowsWithAmazonLicenseRunbook mengaktifkan instans Amazon Elastic Compute Cloud (Amazon EC2) untuk Windows Server dengan lisensi yang disediakan oleh Amazon. Otomatisasi memverifikasi dan mengonfigurasi pengaturan sistem operasi layanan manajemen kunci yang diperlukan dan mencoba aktivasi. Ini termasuk rute sistem operasi ke server manajemen kunci Amazon dan pengaturan sistem operasi layanan manajemen kunci. Menyetel `AllowOffline` parameter untuk `true` memungkinkan otomatisasi berhasil menargetkan instance yang tidak dikelola oleh AWS Systems Manager, tetapi membutuhkan penghentian dan awal instance.

Note

Runbook ini tidak dapat digunakan pada model Bring Your Own License (BYOL) Windows Server contoh. Untuk informasi tentang menggunakan lisensi Anda sendiri, lihat [Microsoft Licensing on AWS](#).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Windows

Parameter

- AllowOffline

Tipe: String

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Setel ke `true` jika Anda mengizinkan remediasi aktivasi Windows offline jika pemecahan masalah online gagal, atau jika instance yang disediakan bukan instance terkelola.

Important

Metode offline mengharuskan EC2 instance 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

Tipe: 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.

- ForceActivation

Tipe: String

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Atur ke `true` jika Anda ingin melanjutkan bahkan jika Windows sudah diaktifkan.

- `InstanceId`

Tipe: String

Deskripsi: (Wajib) ID EC2 instans terkelola Anda untuk Windows Server.

- `SubnetId`

Tipe: String

Default: `CreateNew VPC`

Deskripsi: (Opsional) Hanya offline - ID subnet untuk instance EC2 Rescue yang digunakan untuk melakukan pemecahan masalah offline. Gunakan `SelectedInstanceSubnet` untuk menggunakan subnet yang sama dengan instance Anda, atau gunakan `CreateNewVPC` untuk membuat VPC baru. PENTING: Subnet harus berada di Availability Zone yang sama `InstanceId`, dan harus mengizinkan akses ke endpoint SSM.

Izin IAM yang diperlukan

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

Sebaiknya EC2 instans yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon `SSMManaged InstanceCore` Amazon yang dilampirkan. 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 diperlukan oleh `AWSsupport-StartEC2RescueWorkflow`

Langkah Dokumen

1. `aws:assertAwsResourceProperty`- Periksa platform instans yang disediakan adalah Windows.
2. `aws:assertAwsResourceProperty`- Konfirmasikan instance yang disediakan adalah instance terkelola:

- a. (Perbaiki aktivasi online) Jika instance input adalah instance terkelola, jalankan `aws:runCommand` untuk menjalankan PowerShell skrip untuk mencoba memperbaiki aktivasi Windows.
- b. (Perbaiki aktivasi offline) Jika instance input bukan instance terkelola:
 - i. `aws:assertAwsResourceProperty`- Memverifikasi `AllowOffline` bendera diatur `true`. Jika demikian, perbaikan offline dimulai; jika tidak, otomatisasi berakhir.
 - ii. `aws:executeAutomation`- Memanggil `AWSSupport-StartEC2RescueWorkflow` dengan skrip perbaikan offline aktivasi Windows. Skrip menggunakan `EC2 Config` atau `EC2 Launch`, 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instans Amazon EC2 atau antarmuka jaringan tempat Anda ingin menganalisis keterjangkauan.

- ServiceEndpoint

Tipe: String

Deskripsi: (Wajib) Nama host dari titik akhir layanan yang ingin Anda analisis jangkauan.

- RetainVpcReachabilityAnalysis

Tipe: 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 ini mengotomatiskan migrasi dari instans Elastic Compute Cloud (Amazon EC2) yang didukung Intel ke jenis instans bertenaga AMD yang setara. Runbook ini mendukung instans 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 data dan waktu henti, runbook memeriksa perilaku berhenti instans, apakah instans tersebut 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 dilampirkan, atau jika instance merupakan bagian dari AWS CloudFormation tumpukan. Jika Anda ingin mengubah perilaku ini, tentukan `yes` salah satu parameter `AllowInstanceStoreInstances` dan `AllowCloudFormationInstances` parameter.

Important

Akses ke `AWSPremiumSupport-*` runbook memerlukan Business + Support, Enterprise Support, atau Unified Operations Subscription. Untuk informasi selengkapnya, lihat [Bandingkan AWS Dukungan Paket](#).

Pertimbangan-pertimbangan

- Kami merekomendasikan untuk membuat cadangan instance Anda sebelum menggunakan runbook ini.
- Mengubah jenis instance membutuhkan runbook untuk menghentikan instance Anda. Ketika sebuah instance dihentikan, data apa pun yang disimpan dalam RAM atau volume penyimpanan instans hilang, dan IPv4 alamat publik otomatis dirilis. Untuk informasi selengkapnya, lihat [Menghentikan dan memulai instans Anda](#).
- Jika Anda tidak menentukan nilai untuk `TargetInstanceType` parameter, runbook mencoba mengidentifikasi instance AMD yang setara dalam hal virtual CPUs dan memori dalam keluarga

instance 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Enter yes untuk mengetahui bahwa instance target Anda akan dihentikan jika sedang berjalan.

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID instans Amazon EC2 yang tipenya ingin Anda ubah.

- TargetInstanceType

Tipe: String

Default: otomatis

Deskripsi: (Opsional) Jenis instans AMD yang ingin Anda ubah instans Anda. `automatic` Nilai default menggunakan jenis instance yang setara dalam hal virtual CPUs dan memori. Misalnya, `m5.large` akan diubah menjadi `m5a.large`.

- `AllowInstanceStoreInstances`

Tipe: String

Nilai yang valid: tidak | ya

Default: no

Deskripsi: (Opsional) Jika Anda menentukan `yes`, runbook berjalan pada instance yang memiliki volume penyimpanan instance yang dilampirkan.

- `AllowCloudFormationInstances`

Tipe: String

Nilai yang valid: tidak | ya

Default: no

Deskripsi: (Opsional) Jika disetel `yes`, runbook berjalan pada instance yang merupakan bagian dari tumpukan. `CloudFormation`

- `AllowCrossGeneration`

Tipe: String

Nilai yang valid: tidak | ya

Default: no

Deskripsi: (Opsional) Jika disetel `yes`, runbook mencoba menemukan jenis instans AMD setara terbaru dalam keluarga instance yang sama.

- `DryRun`

Tipe: String

Nilai yang valid: tidak | ya

Default: no

Deskripsi: (Opsional) Jika disetel `keyes`, runbook mengembalikan jenis instans AMD yang setara dan memvalidasi persyaratan migrasi tanpa membuat perubahan pada jenis instans.

- SleepWait

Tipe: String

Bawaan: PT3 S

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 Systems Manager](#).

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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`, `pending`, `stopped`, atau `stopping`. Jika tidak, otomatisasi berakhir.
2. `aws:executeAwsApi`: Mengumpulkan properti dari instans Amazon EC2 target.
3. `aws:branch`: Memcabangkan 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 instans Amazon EC2 bukan bagian dari grup Auto Scaling dengan memeriksa apakah tag diterapkan `aws:autoscaling:groupName`.
5. `aws:executeAwsApi`: Mengumpulkan properti tipe instance saat ini untuk menemukan tipe instans AMD yang setara.
6. `aws:assertAwsResourceProperty`: Mengonfirmasi bahwa kode AWS Marketplace produk tidak terkait dengan instans Amazon EC2. Beberapa produk tidak tersedia pada semua jenis instans.
7. `aws:branch`: Memcabangkan otomatisasi tergantung pada apakah Anda ingin otomatisasi memeriksa apakah instans Amazon EC2 adalah bagian dari tumpukan CloudFormation
 - a. Jika `aws:cloudformation:stack-name` tag diterapkan ke instance, otomatisasi berjalan `aws:assertAwsResourceProperty` untuk mengonfirmasi bahwa instance bukan bagian dari CloudFormation tumpukan.
8. `aws:branch`: Memcabangkan otomatisasi berdasarkan apakah jenis volume root instance 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 dalam proses menargetkan instance yang sama, ia mengembalikan kesalahan dan berakhir.
11. `aws:executeAwsApi`: Mengembalikan daftar jenis instance AMD dengan jumlah memori yang sama dan vCPUs.
12. `aws:executeScript`: Memeriksa apakah jenis instans saat ini didukung dan mengembalikan jenis instans AMD yang setara. Jika tidak ada yang setara, otomatisasi berakhir.

- 13 `aws:executeScript`: Mengonfirmasi bahwa jenis instans AMD tersedia di Availability Zone yang sama, dan memverifikasi izin IAM yang disediakan.
- 14 `aws:branch`: Memcabangkan otomatisasi berdasarkan apakah nilai `DryRun` parameter nyayes.
- 15 `aws:branch`: Memeriksa apakah jenis instans asli dan target sama. Jika mereka sama, otomatisasi berakhir.
- 16 `aws:executeAwsApi`: Mendapat status instance saat ini.
- 17 `aws:changeInstanceState`: Menghentikan instans Amazon EC2.
- 18 `aws:changeInstanceState`: Memaksa instance untuk berhenti jika macet dalam keadaan berhenti.
- 19 `aws:executeAwsApi`: Mengubah jenis instance ke tipe instans AMD target.
- 20 `aws:sleep`: Menunggu 3 detik setelah mengubah jenis instance untuk konsistensi akhirnya.
- 21 `aws:branch`: Memcabangkan otomatisasi berdasarkan status instance sebelumnya. Jika `yarunning`, instance dimulai.
- `aws:changeInstanceState`: Memulai instans Amazon EC2 jika dijalankan sebelum mengubah jenis instans.
 - `aws:waitForAwsResourceProperty`: Menunggu instans Amazon EC2 untuk lulus pemeriksaan status. Jika instance tidak lulus pemeriksaan status, instance diubah kembali ke tipe instans 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 macet dalam status berhenti.
 - `aws:executeAwsApi`: Mengubah instans Amazon EC2 ke tipe aslinya.
 - `aws:sleep`: Menunggu 3 detik setelah mengubah jenis instance untuk konsistensi akhirnya.
 - `aws:changeInstanceState`: Memulai instans Amazon EC2 jika dijalankan sebelum mengubah jenis instans.
 - `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 persyaratan untuk berhasil mengubah jenis instance dari instance tipe Xen ke tipe instans berbasis Nitro. Otomatisasi ini memeriksa hal-hal berikut:

- Perangkat root adalah volume Amazon Elastic Block Store (Amazon EBS).
- `enaSupportAtribut` diaktifkan.
- Modul ENA diinstal pada instance.
- NVMe Modul 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 Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Bawaan: salah

Deskripsi: (Wajib) ID EC2 instance Amazon yang ingin Anda periksa prasyaratnya sebelum bermigrasi ke jenis instans berbasis Nitro.

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`
- `ssm:SendCommand`
- `iam:ListRoles`
- `ec2:DescribeInstances`
- `ec2:DescribeInstancesTypes`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan rincian tentang contoh.
- `aws:executeAwsApi`- Mengumpulkan informasi tentang hypervisor misalnya.
- `aws:branch`- Cabang berdasarkan apakah instance target sudah menjalankan tipe instance berbasis Nitro.
- `aws:branch`- Memeriksa apakah OS instans didukung oleh instance berbasis Nitro.
- `aws:assertAwsResourceProperty`- Memverifikasi instance yang Anda tentukan dikelola oleh Systems Manager, dan statusnyaOnline.
- `aws:branch`- Cabang berdasarkan apakah perangkat root instance adalah volume Amazon EBS.
- `aws:branch`- Cabang berdasarkan apakah atribut ENA diaktifkan untuk instance.
- `aws:runCommand`- Memeriksa driver ENA pada instance.
- `aws:runCommand`- Memeriksa NVMe driver 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 sebelumnya.

Keluaran

`FinalOutput.Output` - Hasil pemeriksaan yang dilakukan oleh otomatisasi.

AWSSupport-CloneXenEC2InstanceAndMigrateToNitro

Deskripsi

AWSSupport-CloneXenEC2 InstanceAndMigrateToNitro [runbook mengkloning, menyiapkan, dan memigrasikan instans Linux Amazon Elastic Compute Cloud \(Amazon EC2\) yang dikloning,](#)

yang saat ini berjalan di platform Amazon EC2 Xen, untuk berjalan di platform Amazon EC2 Nitro.

Otomatisasi ini dibagi menjadi tiga cabang berbeda:

- **Pemeriksaan Awal:** Mengevaluasi semua prasyarat untuk melanjutkan migrasi termasuk memeriksa apakah instans Amazon EC2 target sudah berjalan di platform Nitro, menentukan status siklus hidup, memvalidasi sistem operasi, dan memverifikasi konektivitas Systems Manager.
- **Pengujian:** Membuat pengujian AMI dari instans Amazon EC2 target dan meluncurkan instance Amazon EC2 pengujian untuk memvalidasi proses migrasi sebelum melanjutkan.
- **CloneAndMigrate:** Membuat tiruan dari instans Amazon EC2 target, menginstal driver yang diperlukan, mengonfigurasi sistem untuk platform Nitro, dan mengubah jenis instans ke tipe Nitro yang diinginkan.

Important

Sebelum memberikan persetujuan untuk menghentikan instans Amazon EC2 target, pastikan semua aplikasi yang berjalan pada instance ditutup dengan baik. Jika instans Amazon EC2 tidak memiliki alamat IP Elastis yang terkait, IPv4 alamat publik otomatis akan berubah setelah instans dihentikan dan dimulai.

Important

Penafian: Menjalankan runbook ini dapat dikenakan biaya tambahan ke akun Anda untuk instans Amazon EC2, Amazon EBS Volume & s. AMI Silakan lihat Harga [Amazon EC2 & harga Amazon EBS untuk lebih jelasnya](#).

Important

Prasyarat

Instans Amazon EC2 target memerlukan akses keluar ke repositori untuk menginstal driver dan dependensi seperti `kernel-devel`, `gcc patch rpm-build` `wget` `dracut` `makelinux-headers`, dan menggunakan manajer paket jika diperlukan. `unzip`

Sistem Operasi yang Didukung

- Red Hat Enterprise Linux (RHEL) 8 dan 9
- Amazon Linux 2 dan AL2023
- Server Ubuntu 18.04 LTS, 20.04 dan 22.04
- Debian 11 dan 12 (hanya AWS partisi)
- SUSE12SP5 dan SUSE15 SP (5,6)

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah tingkat tinggi berikut:

- Memvalidasi prasyarat dan memeriksa apakah instance cocok untuk migrasi.
- Membuat dan menguji AMI untuk memastikan migrasi akan berhasil.
- Mengaktifkan atribut Enhanced networking (ENA) dan menginstal driver ENA terbaru.
- Memverifikasi dan mengonfigurasi NVMe modul di initramfs.
- Menganalisis dan memodifikasi /etc/fstab untuk mengganti nama perangkat dengan UUIDs
- Menonaktifkan penamaan antarmuka yang dapat diprediksi dan menghapus aturan jaringan yang persisten.
- Mengubah jenis instance kloning ke tipe Nitro yang diinginkan.
- Membuat final AMI yang dapat digunakan sebagai Golden Image untuk meluncurkan instance Nitro.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- autoscaling:DescribeAutoScalingInstances
- ec2:CreateImage
- ec2:CreateTags
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceState
- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DeregisterImage
- ec2:ModifyInstanceAttribute
- ec2:RunInstances
- ec2:StartInstances
- ec2:StopInstances
- ec2:TerminateInstances
- iam:PassRole
- sns:Publish
- ssm:DescribeAutomationExecutions
- ssm:DescribeInstanceInformation
- ssm:SendCommand

Contoh kebijakan IAM:

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

```

        "autoscaling:DescribeAutoScalingInstances",
        "ec2:CreateImage",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute:",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DeregisterImage",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "iam:PassRole",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:SendCommand"
    ],
    "Resource": "*"
}
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - Clone Xen EC2 Instance And Migrate To Nitro](#) Systems Manager di bawah Documents.
2. Pilih **Execute automation**.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (Opsional) 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.
 - Tipe: `AWS::IAM::Role::Arn`
 - TargetInstanceIds (Diperlukan):

- Deskripsi: (Wajib) ID Instance instans Amazon EC2 target yang ingin Anda migrasikan ke platform Nitro.
- Tipe: `AWS::EC2::Instance::Id`
- NitroInstanceType (Opsional):
 - Deskripsi: (Opsional) Masukkan jenis instans Nitro tujuan. Hanya instans Nitro M5, M6, C5, C6, R5, R6 dan T3 yang didukung (misalnya t3.small). Default: m5.xlarge.
 - Tipe: `String`
 - Pola yang Diizinkan: `^(m5a?z?d?n?|c5a?d?n?|r5a?d?n?b?|(c|m|r)6(a|i)?d?)\\.(2|4|8|12|16|24|32)?xlarge$|^t3a?\\.(x|2x)?large|nano|micro|small|medium)$`
 - Default: `m5.xlarge`
- SNSTopicArn (Diperlukan):
 - Deskripsi: (Wajib) Berikan ARN Topik Amazon SNS untuk pemberitahuan persetujuan. Topik Amazon SNS ini digunakan untuk mengirim pemberitahuan persetujuan selama eksekusi otomatisasi.
 - Tipe: `String`
 - Pola yang Diizinkan: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):sns:(us(-gov|-isob)?|ap|ca|af|me|cn|eu|sa)-(central|(north|south)?(east|west)?)-\\d:\\d{12}:[a-zA-Z0-9_-.]{1,256}$`
- ApproverIam (Diperlukan):
 - Deskripsi: (Wajib) Berikan daftar kepala sekolah AWS yang diautentikasi yang dapat menyetujui atau menolak tindakan tersebut. Jumlah maksimum pemberi persetujuan adalah 10.
 - Tipe: `StringList`
 - Pola yang Diizinkan: `^[a-zA-Z0-9_+=, .@\\-\\/] {1,128}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):(sts|iam)::[0-9]{12}:[a-zA-Z0-9_+=, .@\\-\\/] {1,256}$`
- MinimumRequiredApprovals (Opsional):
 - Deskripsi: (Opsional) Jumlah minimum persetujuan yang diperlukan untuk melanjutkan otomatisasi. Default: 1.
 - Jenis: `Integer`
 - Default: 1

- **DeleteResourcesOnFailure** (Opsional):
 - Deskripsi: (Opsional) Apakah akan menghentikan instans Amazon EC2 yang dikloning AMI dan jika otomatisasi gagal.
 - Tipe: Boolean
 - Nilai yang Diizinkan: [true, false]
 - Default: true
- Pengakuan (Diperlukan):
 - Deskripsi: (Wajib) Harap baca detail lengkap tindakan yang dilakukan oleh runbook otomatisasi ini dan tulis 'Ya, saya mengerti dan mengakui' jika Anda mengakui langkah-langkahnya.
 - Tipe: String
 - Pola yang Diizinkan: ^Yes, I understand and acknowledge\$
- **AllowInstanceStoreInstances** (Opsional):
 - Deskripsi: (Opsional) Jika Anda menentukannya, runbook berjalan pada instance yang memiliki volume penyimpanan instance yang dilampirkan. Peringatan: data dalam volume penyimpanan instance hilang saat instance dihentikan. Parameter ini membantu menghindari kehilangan data yang tidak disengaja.
 - Tipe: Boolean
 - Nilai yang Diizinkan: [yes, no]
 - Default: no

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **checkConcurrency:**

Memastikan hanya ada satu eksekusi runbook ini yang menargetkan instans Amazon EC2 saat ini.

- **getTargetInstanceProperties:**

Mengambil detail instans Amazon EC2 target.

- **checkIfNitroInstanceTypeIsSupportedInAZ:**

Menentukan apakah jenis instans Nitro target didukung di Availability Zone yang sama dengan instans Amazon EC2 target.

- **createTestImage:**

Membuat tes AMI dari contoh yang disediakan.

- **launchTestInstanceInSameSubnet:**

Meluncurkan instans Amazon EC2 pengujian dari AMI pengujian menggunakan konfigurasi yang sama dengan instans Amazon EC2 target.

- **approvalToStopTargetInstance:**

Menunggu persetujuan kepala sekolah yang ditunjuk untuk menghentikan instance target.

- **createBackupImage:**

Membuat AMI dari contoh yang disediakan untuk cadangan.

- **launchInstanceInSameSubnet:**

Meluncurkan instans Amazon EC2 baru dari AMI cadangan menggunakan konfigurasi yang sama dengan instans Amazon EC2 sumber.

- **checkAndInstallENADrivers:**

Menentukan ketersediaan driver Enhanced Networking Adapter (ENA) pada instans Amazon EC2 dan penginstalan, jika tidak ada.

- **checkAndAddNVMEDrivers:**

Menentukan ketersediaan driver NVMe pada instans Amazon EC2 yang dikloning dan menginstal, jika tidak ada.

- **checkAndModifyFSTABEntries:**

Menentukan apakah nama perangkat digunakan /etc/fstab dan menggantinya dengan mereka UUIDs, jika ditemukan.

- **setNitroInstanceTypeForClonedInstance:**

Menetapkan jenis instans Amazon EC2 target yang disediakan untuk instans Amazon EC2 yang dikloning.

- **approvalForCreatingImageAfterDriversInstallation:**

Menunggu persetujuan pengguna jika instans Amazon EC2 yang dikloning berhasil melakukan boot di platform Nitro.

- **createImageAfterDriversInstallation:**

Membuat Gambar dari instans Amazon EC2 baru hanya jika instans Amazon EC2 baru berhasil melakukan boot di Platform Nitro.

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

Referensi

AWS Systems Manager Otomasi

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

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 metadata misalnya.
- Konfigurasi `HttpPutResponseHopLimit` nilainya.
- Izinkan atau tolak akses metadata instance.

Untuk informasi selengkapnya tentang metadata instance, lihat [Mengonfigurasi Layanan Metadata Instans di Panduan Pengguna Amazon](#). EC2

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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.

- Menegakkan IMDSv2

Tipe: String

Nilai yang valid: wajib | opsional

Default: opsional

Deskripsi: (Opsional) Menegakkan IMDSv2. Jika Anda memilih `required`, EC2 instans Amazon hanya akan digunakan 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 menerapkan 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 di Panduan Pengguna Amazon](#). EC2

- HttpPutResponseHopLimit

Jenis: Integer

Nilai yang valid: 0-64

Default: 0

Deskripsi: (Opsional) Nilai batas hop respons HTTP PUT yang diinginkan (1-64) misalnya permintaan metadata. Nilai ini mengontrol jumlah hop yang dapat dilalui oleh respons PUT. Untuk mencegah respons berjalan di luar instance, 1 tentukan nilai parameter.

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID EC2 instans Amazon yang setelah metadatanya ingin Anda konfigurasi.

- MetadataAccess

Tipe: String

Nilai yang valid: diaktifkan | dinonaktifkan

Default: diaktifkan

Deskripsi: (Opsional) Izinkan atau tolak akses metadata instans di instans Amazon EC2 . Jika Anda menentukandisabled, semua parameter lain akan diabaikan dan akses metadata akan ditolak untuk contoh tersebut.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

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

Langkah Dokumen

1. branchOnMetadataAkses - Otomatisasi cabang berdasarkan nilai MetadataAccess parameter.

2. `disableMetadataAccess` - Memanggil tindakan `ModifyInstanceMetadataOptions` API untuk menonaktifkan akses titik akhir metadata.
3. `branchOnHttpPutResponseHopLimit` - Otomatisasi cabang berdasarkan nilai `HttpPutResponseHopLimit` parameter.
4. `maintainHopLimitAndConfigureImdsVersion` - Jika `HttpPutResponseHopLimit` 0, mempertahankan batas hop saat ini dan mengubah opsi metadata lainnya.
5. `waitBeforeAssertingIMDSv2Negara` - Menunggu 30 detik sebelum menegaskan IMDSv2 status.
6. `setHopLimitAndConfigureImdsVersion` - Jika `HttpPutResponseHopLimit` lebih besar dari 0, mengkonfigurasi opsi metadata menggunakan parameter input yang diberikan.
7. `waitBeforeAssertingHopLimit` - Menunggu 30 detik sebelum menegaskan opsi metadata.
8. `assertHopLimit` - Menegaskan `HttpPutResponseHopLimit` properti diatur ke nilai yang Anda tentukan.
9. `branchVerificationOnIMDSv2Ops` - Verifikasi cabang berdasarkan nilai `EnforceIMDSv2` parameter.
10. `assert IMDSv2 IsOptional` - Menegaskan `HttpTokens` nilai yang disetel ke. `optional`
11. `assert IMDSv2 IsEnforced` - Menegaskan `HttpTokens` nilai yang disetel 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`

AWS Support - ContainEC2Instance

Deskripsi

AWSSupport-ContainEC2InstanceRunbook menyediakan solusi otomatis untuk prosedur yang diuraikan dalam artikel [Bagaimana cara mengisolasi Instans Amazon EC2 saat dihadapkan dengan kemungkinan disusupi atau mencurigakan](#)? Cabang otomatisasi tergantung pada nilai yang Anda tentukan.

Bagaimana cara kerjanya?

Runbook Otomasi ini AWSSupport-ContainEC2Instance melakukan penahanan jaringan Instans Amazon EC2 melalui serangkaian langkah terkoordinasi. Ketika dieksekusi dalam Contain mode, pertama-tama memvalidasi parameter input dan memeriksa apakah instance tidak dihentikan. Kemudian mencadangkan konfigurasi grup keamanan saat ini ke bucket Amazon S3 untuk pemulihan nanti. Runbook membuat dua grup keamanan: grup keamanan “semua akses” sementara dan grup keamanan “penahanan” terakhir. Secara bertahap transisi antarmuka jaringan instance dari grup keamanan asli mereka ke grup keamanan semua akses, dan akhirnya ke grup keamanan penahanan. Jika ditentukan, itu membuat cadangan instance yang tidak terenkripsi dan terenkripsi. AMI Untuk instance dalam grup Auto Scaling, ini menangani modifikasi grup Auto Scaling yang diperlukan dan membawa instance ke status siaga. Ketika dijalankan dalam Release mode, ia mengembalikan instance ke konfigurasi jaringan aslinya menggunakan pengaturan cadangan dari Amazon S3. Runbook mendukung DryRun parameter untuk melihat pratinjau tindakan tanpa membuat perubahan aktual, dan menyertakan mekanisme penanganan dan pelaporan kesalahan yang komprehensif di seluruh alur kerja penahanan dan rilis.

Important

- Runbook ini melakukan berbagai operasi yang memerlukan hak istimewa yang lebih tinggi, seperti memodifikasi grup keamanan, membuat AMI s, dan berinteraksi dengan grup Auto Scaling. Tindakan ini berpotensi menyebabkan eskalasi hak istimewa atau memengaruhi beban kerja lain di akun Anda. Anda harus meninjau izin yang diberikan untuk peran yang ditentukan oleh AutomationAssumeRole parameter dan memastikannya sesuai untuk kasus penggunaan yang dimaksudkan. Anda dapat merujuk ke AWS dokumentasi berikut untuk informasi lebih lanjut tentang izin IAM: [AWS Identity and Access Management \(IAM\) PermissionsAWS Systems Manager Automation Permissions](#)
- Runbook ini melakukan tindakan mutatif yang berpotensi menyebabkan tidak tersedianya atau gangguan pada beban kerja Anda. Secara khusus, ini memodifikasi grup keamanan yang terkait dengan Instans Amazon EC2 target, yang dapat memengaruhi konektivitas

jaringan. Selain itu, jika instance merupakan bagian dari grup Auto Scaling, runbook dapat mengubah konfigurasi grup, yang berpotensi memengaruhi perilaku penskalaannya.

- Selama proses penahanan, buku runbook ini menciptakan sumber daya tambahan, seperti grup keamanan dan AMI s. Meskipun sumber daya ini ditandai untuk identifikasi, Anda harus menyadari pembuatannya dan memastikan pembersihan atau pengelolaan yang tepat setelah proses penahanan selesai.
- Jika Action parameter disetel keRelease, runbook ini mencoba mengembalikan konfigurasi Instans Amazon EC2 ke status semula. Namun, ada risiko bahwa proses restorasi mungkin gagal, meninggalkan instance dalam keadaan tidak konsisten. Runbook memberikan instruksi untuk restorasi manual jika terjadi kegagalan tersebut, tetapi Anda harus siap untuk menangani masalah potensial selama proses restorasi.

Disarankan untuk meninjau runbook secara menyeluruh, memahami potensi dampaknya, dan mengujinya di lingkungan non-produksi sebelum menjalankannya di lingkungan produksi Anda.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- penskalaan otomatis: CreateOrUpdateTags
- penskalaan otomatis: DeleteTags
- penskalaan otomatis: DescribeAutoScalingGroups

- penskalaan otomatis: DescribeAutoScalingInstances
- penskalaan otomatis: DescribeTags
- penskalaan otomatis: EnterStandby
- penskalaan otomatis: ExitStandby
- penskalaan otomatis: UpdateAutoScalingGroup
- EC2: AuthorizeSecurityGroupEgress
- EC2: AuthorizeSecurityGroupIngress
- EC2: CopyImage
- EC2: CreateImage
- EC2: CreateSecurityGroup
- EC2: CreateSnapshot
- EC2: CreateTags
- EC2: DeleteSecurityGroup
- EC2: DeleteTags
- EC2: DescribeImages
- EC2: DescribeInstances
- EC2: DescribeSecurityGroups
- EC2: DescribeSnapshots
- EC2: DescribeTags
- EC2: ModifyNetworkInterfaceAttribute
- EC2: RevokeSecurityGroupEgress
- km: CreateGrant
- km: DescribeKey
- km: GenerateDataKeyWithoutPlaintext
- km: ReEncryptFrom
- km: ReEncryptTo
- s3: CreateBucket
- s3: DeleteObjectTagging
- s3: GetAccountPublicAccessBlock
- s3: GetBucketAcl

- s3: GetBucketLocation
- s3: GetBucketOwnershipControls
- s3: GetBucketPolicy
- s3: GetBucketPolicyStatus
- s3: GetBucketPublicAccessBlock
- s3: GetObject
- s3: ListBucket
- s3: PutAccountPublicAccessBlock
- s3: PutBucketPolicy
- s3: PutBucketVersioning
- s3: PutObject
- s3: PutObjectTagging

Contoh Kebijakan:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOperations",
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "kms:DescribeKey",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
```

```

        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "*"
},
{
    "Sid": "WriteOperations",
    "Effect": "Allow",
    "Action": [
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteTags",
        "autoscaling:EnterStandby",
        "autoscaling:ExitStandby",
        "autoscaling:UpdateAutoScalingGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteTags",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupEgress",
        "kms:CreateGrant",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "s3:CreateBucket",
        "s3>DeleteObjectTagging",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutObject",
        "s3:PutObjectTagging"
    ],
    "Resource": "*"
}
]

```

}

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-ContainEC2Instance](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) peran AWS 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.
 - Tipe: `AWS::IAM::Role::Arn`
 - Tindakan (Diperlukan):
 - Deskripsi: (Diperlukan) Pilih `Contain` untuk mengisolasi instans Amazon EC2 `Restore` atau mencoba memulihkan konfigurasi asli konfigurasi instans Amazon EC2 dari cadangan sebelumnya.
 - Tipe: `String`
 - Pola yang Diizinkan: `Contain|Restore`
 - DryRun (Opsional):
 - Deskripsi: (Opsional) Saat diatur ke `true`, otomatisasi tidak akan menjalankan perintah apa pun, melainkan akan melaporkan apa yang akan dicoba dilakukannya, merinci setiap langkah. Nilai default: `true`.
 - Jenis: `Boolean`
 - Nilai yang Diizinkan: `true|false`
 - Buat AMIBackup (Opsional):
 - Deskripsi: (Opsional) Jika disetel ke `true`, Instans Amazon EC2 akan dibuat sebelum melakukan tindakan penahanan. AMI
 - Jenis: `Boolean`
 - Nilai yang Diizinkan: `true|false`

- KmsKey (Opsional):
 - Deskripsi: (Opsional) ID AWS KMS kunci yang akan digunakan untuk membuat instans Amazon EC2 target AMI terenkripsi. Default diatur ke alias/aws/ebs.
 - Tipe: String
 - Pola yang Diizinkan: `^(((arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}: [0-9]{12}:key/)?([a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}|mrk-[a-f0-9]{32})))|(arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}: [0-9]{12}:)?alias/.{1,})$`
- Backups3 BucketName (Bersyarat):
 - Deskripsi: Bucket Amazon S3 (Bersyarat) Amazon S3 untuk mengunggah konfigurasi Action kapan Contain ada atau untuk memulihkan konfigurasi Action kapan ada. Release Catatan: Jika bucket yang disediakan tidak ada di akun, otomatisasi akan membuat bucket Amazon S3 atas nama Anda.
 - Tipe: AWS::S3::Bucket::Name
- TagIdentifier (Opsional):
 - Deskripsi: (Opsional) Tag dalam format Key=BatchId, Value=78925 yang akan ditambahkan ke AWS sumber daya yang dibuat atau dimodifikasi oleh buku runbook ini selama alur kerja penahanan. Tag ini dapat digunakan untuk mengidentifikasi dan mengelola sumber daya yang terkait selama proses penahanan. Selama alur kerja pemulihan, tag yang ditentukan oleh parameter ini akan dihapus dari sumber daya. Catatan: Kunci dan nilai tag peka huruf besar/kecil.
 - Tipe: String
 - Pola yang Diizinkan: `^$|^([Kk])([Ee])([Yy])=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{1,128},([Vv])([Aa])([Ll])([Uu])([Ee])=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{0,128}$`
- Backups3 BucketAccess (Bersyarat):
 - Deskripsi: (Bersyarat) ARN pengguna IAM atau peran yang akan diizinkan mengakses bucket Amazon S3 cadangan setelah menjalankan tindakan penahanan. Parameter ini Action diperlukan kapanContain. AutomationAssumeRole, atau jika tidak ada pengguna yang konteksnya otomatisasi berjalan secara otomatis ditambahkan ke daftar.
 - Tipe: String

- Pola yang Diizinkan: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.-]+$`
- IngressTrafficRules (Opsional):
 - Deskripsi: (Opsional) Peta aturan masuknya grup keamanan yang dipisahkan koma dengan Cidr IpProtocol, FromPort dan ToPort dalam format yang akan diterapkan `[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}]` ke instans Amazon EC2. Jika tidak ada aturan yang disediakan, grup keamanan tanpa aturan masuk akan dilampirkan ke instans Amazon EC2, yang secara efektif mengisolasinya dari lalu lintas yang masuk.
 - Jenis: MapList
 - Pola yang Diizinkan: `^\\{\\}$|^\\{\\\"Cidr\\\":\\\"[\\x00-\\x7F+]{1,128}\\\", \\\"IpProtocol\\\":\\\"[\\x00-\\x7F+]{1,128}\\\", \\\"FromPort\\\":\\\"[\\x00-\\x7F+]{1,128}\\\", \\\"ToPort\\\":\\\"[\\x00-\\x7F+]{0,255}\\\"}\\\"\\\"}`
- EgressTrafficRules (Opsional):
 - Deskripsi: (Opsional) Peta aturan keluar grup keamanan yang dipisahkan koma dengan Cidr IpProtocol, FromPort dan ToPort dalam format yang akan diterapkan `[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}]` ke instans Amazon EC2 Amazon. Jika tidak ada aturan yang disediakan, grup keamanan tanpa aturan jalan keluar akan dilampirkan ke instans Amazon EC2, yang secara efektif mencegah semua lalu lintas keluar.
 - Jenis: MapList
 - Pola yang Diizinkan: `^\\{\\}$|^\\{\\\"Cidr\\\":\\\"[\\x00-\\x7F+]{1,128}\\\", \\\"IpProtocol\\\":\\\"[\\x00-\\x7F+]{1,128}\\\", \\\"FromPort\\\":\\\"[\\x00-\\x7F+]{1,128}\\\", \\\"ToPort\\\":\\\"[\\x00-\\x7F+]{0,255}\\\"}\\\"\\\"}`
- Backups3 KeyName (Opsional):
 - Deskripsi: (Opsional) Jika Action disetel keRestore, ini menentukan kunci Amazon S3 yang akan digunakan otomatisasi untuk mencoba memulihkan konfigurasi instans Amazon EC2 target. Kunci Amazon S3 biasanya mengikuti format ini: `{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json` Kuncinya dapat diperoleh dari output eksekusi otomatisasi penahanan sebelumnya.
 - Tipe: String
 - Pola yang Diizinkan: `^[a-zA-Z0-9\\.\\-\\_\\\\!*'()]/]{0,1024}$`

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- `ValidateRequiredInputs`

Memvalidasi bahwa semua input yang diperlukan disediakan.

- `AssertInstancelIsNotTerminated`

Memeriksa apakah Instans Amazon EC2 target tidak dihentikan (dihapus).

- `GetAutoScalingInstanceInfo`

Mendapatkan siklus hidup instans Amazon EC2 dan nama grup jika instans Amazon EC2 target adalah bagian dari grup Auto Scaling.

- `CheckBackupS3 BucketName`

Memeriksa apakah bucket Amazon S3 target berpotensi memberikan `read` atau akses `write` publik ke objeknya. Bucket Amazon S3 baru dibuat jika `BackupS3BucketName` bucket tidak ada.

- `BranchOnActionAndMode`

Cabang otomatisasi berdasarkan parameter input `Action` dan `DryRun`.

- `BranchOnAutoScalingGroupMembership`

Mem-cabang otomatisasi berdasarkan apakah Instance Amazon EC2 target adalah bagian dari grup Auto Scaling dan status siklus hidupnya.

- `DescribeAutoScalingGroups`

Mendapatkan dan menyimpan konfigurasi grup Amazon EC2 Auto Scaling terkait.

- `ModifyAutoScalingGroup`

Memodifikasi konfigurasi grup Amazon EC2 Auto Scaling terkait untuk tindakan penahanan, menyetel instans Amazon EC2 ke status, `Standby` dan menyesuaikan kapasitas grup Auto Scaling. `MinSize`

- `BackupInstanceSecurityGroups`

Mendapatkan dan menyimpan konfigurasi grup keamanan Instans Amazon EC2 target.

- `CreateAllAccessSecurityGroup`

Membuat grup keamanan sementara yang memungkinkan semua lalu lintas masuk yang menggantikan grup keamanan Instans Amazon EC2 target.

- `CreateContainmentSecurityGroup`

Membuat grup keamanan penahanan restriktif dengan aturan masuk dan keluar yang ditentukan, dan menggantikan grup semua akses sementara dengannya.

- `BranchOnCreateAMIBackup`

Cabang otomatisasi berdasarkan parameter `CreateAMIBackup` input.

- `AssertSourceInstanceRootVolumeIsEbs`

Memeriksa apakah target volume root Instans Amazon EC2 adalah Amazon EBS.

- `CreateImage`

Membuat AMI Instans Amazon EC2 target.

- `RestoreInstanceConfiguration`

Memulihkan konfigurasi Instans Amazon EC2 target dari cadangan.

- `ReportContain`

Menghasilkan detail dry run untuk tindakan penahanan.

- `ReportRestore`

Menghasilkan detail dry run untuk tindakan pemulihan.

- `ReportRestoreFailure`

Memberikan instruksi untuk memulihkan konfigurasi asli Instans Amazon EC2 target selama skenario kegagalan alur kerja pemulihan.

- `ReportContainmentFailure`

Memberikan instruksi untuk memulihkan konfigurasi asli Instans Amazon EC2 target selama skenario kegagalan alur kerja penahanan.

- `FinalOutput`

Menghasilkan detail tindakan penahanan.

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

Mengeluarkan detail tindakan penahanan yang dilakukan oleh runbook ini saat DryRun disetel ke False.

- `RestoreInstanceConfiguration.Keluaran`

Mengeluarkan tindakan pemulihan yang dilakukan oleh runbook ini saat DryRun disetel ke False.

- `ReportContain.Keluaran`

Mengeluarkan detail tindakan penahanan yang dilakukan oleh runbook ini saat DryRun disetel ke True.

- `ReportRestore.Keluaran`

Mengeluarkan detail tindakan pemulihan yang dilakukan oleh runbook ini saat DryRun disetel ke True.

- `ReportContainmentFailure.Keluaran`

Memberikan instruksi untuk memulihkan konfigurasi asli Instans Amazon EC2 target selama skenario kegagalan alur kerja penahanan.

- `ReportRestoreFailure.Keluaran`

Memberikan instruksi untuk memulihkan konfigurasi asli Instans Amazon EC2 target selama skenario kegagalan alur kerja pemulihan.

Referensi

Otomatisasi Systems Manager

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

AWSSupport-CopyEC2Instance

Deskripsi

AWSSupport-CopyEC2InstanceRunbook menyediakan solusi otomatis untuk prosedur yang diuraikan dalam artikel Pusat Pengetahuan [Bagaimana cara memindahkan EC2 instance saya ke subnet lain, Availability Zone, atau VPC?](#) Cabang otomatisasi tergantung pada nilai yang Anda tentukan untuk SubnetId parameter Region dan.

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 AMI di subnet yang Anda tentukan.

Jika Anda menentukan nilai untuk SubnetId parameter dan Region parameter, otomatisasi membuat AMI dari contoh target, menyalin AMI ke yang Wilayah AWS Anda tentukan, dan meluncurkan instance baru dari AMI di subnet yang Anda tentukan.

Jika Anda menentukan nilai untuk Region parameter tetapi bukan nilai untuk SubnetId parameter, otomatisasi membuat AMI dari contoh target, menyalin AMI ke Wilayah yang Anda tentukan, dan meluncurkan instance baru dari AMI di subnet default virtual private cloud (VPC) Anda di Wilayah tujuan.

Jika tidak ada nilai yang ditentukan untuk SubnetId parameter Region atau, otomatisasi membuat AMI dari instance target, dan meluncurkan instance baru dari AMI di subnet default VPC Anda.

Untuk menyalin AMI ke Wilayah yang berbeda, Anda harus memberikan nilai untuk AutomationAssumeRole parameter. Jika waktu otomatisasi habis 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) EBS). Untuk sistem file besar tanpa snapshot sebelumnya, AMI penciptaan bisa memakan waktu beberapa jam. Untuk mengurangi AMI waktu pembuatan, buat snapshot Amazon EBS sebelum Anda membuat 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 di instans Amazon saya ke Amazon EC2 EBS?](#)
- EC2 Instans Amazon baru memiliki alamat IPv6 IP pribadi IPv4 atau publik yang berbeda. Anda harus memperbarui semua referensi ke alamat IP lama (misalnya, dalam entri DNS) dengan alamat IP baru yang ditetapkan ke instance baru. Jika Anda menggunakan alamat IP Elastis pada instance sumber Anda, pastikan untuk melampirkannya ke instance baru.

- Masalah konflik pengenalan keamanan domain (SID) dapat terjadi ketika salinan diluncurkan dan mencoba 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 cara menggunakan Sysprep untuk membuat dan menginstal Windows yang dapat digunakan kembali khusus? AMIs](#)

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

Important

Kami tidak menyarankan menggunakan runbook ini untuk menyalin instance Microsoft Active Directory Domain Controller.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID dari instance yang ingin Anda salin.

- KeyPair

Tipe: String

Deskripsi: (Opsional) Key pair yang ingin Anda kaitkan dengan instance baru yang disalin. Jika Anda menyalin instance ke Region yang berbeda, pastikan key pair ada di Region yang ditentukan.

- Wilayah

Tipe: String

Deskripsi: (Opsional) Wilayah yang ingin Anda salin instance. Jika Anda menentukan nilai untuk parameter ini, tetapi tidak menentukan nilai untuk SecurityGroupIds parameter SubnetId dan, otomatisasi mencoba meluncurkan instance di VPC default dengan grup keamanan default. Jika EC2 -Classic diaktifkan di Wilayah tujuan, peluncuran akan gagal.

- SubnetId

Tipe: String

Deskripsi: (Opsional) ID subnet yang ingin Anda salin instance. Jika EC2 -Classic diaktifkan di Wilayah tujuan, Anda harus memberikan nilai untuk parameter ini.

- InstanceType

Tipe: String

Deskripsi: (Opsional) Jenis instance yang disalin harus diluncurkan sebagai. Jika Anda tidak menentukan nilai untuk parameter ini, jenis contoh sumber digunakan. Jika jenis instance sumber tidak didukung di Wilayah tempat instance disalin, otomatisasi gagal.

- SecurityGroupIds

Tipe: String

Deskripsi: (Opsional) Daftar grup keamanan yang dipisahkan koma yang ingin IDs Anda kaitkan dengan instance yang disalin. Jika Anda tidak menentukan nilai untuk parameter ini, dan instance tidak disalin ke Wilayah lain, grup keamanan yang terkait dengan instance sumber akan digunakan. Jika Anda menyalin instance ke Wilayah lain, 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` untuk parameter ini, otomatisasi tidak menghapus AMI dari contoh sumber. 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` untuk 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

Bawaan: salah

Deskripsi: (Opsional) Jika Anda menentukan `true` parameter ini, instance sumber tidak akan dimulai ulang sebelum membuat AMI. Ketika opsi ini digunakan, integritas sistem file pada gambar yang dibuat tidak dapat dijamin.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan 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 lain, 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 dari contoh sumber.
- `tagLocalAmi` - Tag 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 disediakan untuk `KeyPair` parameter untuk instance yang sedang disalin dalam Wilayah yang sama.
- `sameRegionLaunchInstanceWithKeyPair` - Meluncurkan EC2 instance Amazon dari AMI contoh sumber di subnet yang sama atau subnet yang Anda tentukan menggunakan key pair yang Anda tentukan.
- `sameRegionLaunchInstanceWithoutKeyPair` - Meluncurkan EC2 instance Amazon dari AMI contoh sumber di subnet yang sama atau subnet yang Anda tentukan tanpa key pair.
- `copyAmiToWilayah` - Menyalin AMI ke daerah tujuan.
- `waitForAvailableDestinationAmi` - Menunggu untuk disalin AMI negara untuk menjadi `available`.
- `destinationRegionLaunchInstance` - Meluncurkan EC2 Instans Amazon menggunakan yang disalin AMI.
- `branchAssertDestinationAmiToDelete` - Cabang berdasarkan nilai yang Anda berikan untuk `KeepImageDestinationRegion` parameter.
- `deregisterDestinationAmiAndDeleteSnapshots` - Deregister yang disalin AMI dan menghapus snapshot terkait.

- `branchAssertSourceAmiTodelete` - Cabang berdasarkan nilai yang Anda berikan untuk `KeepImageSourceRegion` parameter.
- `deregisterSourceAmiAndDeleteSnapshots` - Deregister AMI dibuat dari instance sumber dan menghapus snapshot terkait.
- `tidur` - Tidur otomatisasi selama 2 detik. Ini adalah langkah terminal.

Keluaran

`sameRegionLaunchInstanceWithKeyPair.InstanceIds`

`sameRegionLaunchInstanceWithoutKeyPair.InstanceIds`

`destinationRegionLaunchInstansDestinationInstanceId.`

AWSPremiumSupport-DiagnoseDiskUsageOnLinux

Deskripsi

AWSPremiumSupport-DiagnoseDiskUsageOnLinuxRunbook menganalisis target volume Amazon Elastic Compute Cloud (Amazon EC2) instans Amazon Elastic Block Store (Amazon EBS) instans Amazon Elastic Compute Cloud (Amazon EC2) untuk menentukan apakah volume tersebut memerlukan ekspansi. Ini memeriksa penggunaan setiap volume, jenis sistem file, dan riwayat ekspansi terhadap ambang batas yang ditentukan dalam parameter input runbook. Skrip mempertimbangkan faktor-faktor seperti modifikasi terbaru, sistem file yang didukung, dan batas AWS volume. Kemudian menghasilkan volume, jika ada, yang merupakan kandidat untuk ekspansi, bersama dengan detail yang relevan untuk setiap volume.

Bagaimana cara kerjanya?

Runbook ini melakukan operasi berikut:

- Memverifikasi bahwa instance target dikelola oleh Systems Manager dan tidak menjalankan Windows
- Mengambil detail instance termasuk platform dan jenis perangkat root
- Mengambil volume yang digunakan oleh instans Amazon EC2
- Menjalankan prechecks di Linux untuk menganalisis penggunaan disk dan menentukan kandidat ekspansi
- Volume keluaran yang merupakan kandidat untuk ekspansi dengan detail yang relevan

⚠ Important

Akses ke `AWSPremiumSupport` - * runbook memerlukan Business + Support, Enterprise Support, atau Unified Operations Subscription. Untuk informasi selengkapnya, lihat [Bandingkan AWS Dukungan Paket](#).

Jalankan Otomasi ini (konsol)

Izin IAM yang diperlukan

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

- `ssm: DescribeInstanceInformation`
- `EC2: DescribeInstances`
- `EC2: DescribeVolumes`
- `ssm: SendCommand`
- `ssm: ListCommandInvocations`

Contoh Kebijakan:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeInstanceInformation",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ssm:SendCommand",
        "ssm:ListCommandInvocations"
      ],
      "Resource": "*"
    }
  ]
}
```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSPremiumSupport-DiagnoseDiskUsageOnLinux](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (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.
 - Tipe: `AWS::IAM::Role::Arn`
 - InstanceId (Diperlukan):
 - Deskripsi: (Wajib) ID instans Amazon EC2 Anda.
 - Tipe: `String`
 - Izinkan Pola: `^i-[0-9a-f]{8,17}$`
 - VolumeExpansionUsageTrigger (Diperlukan):
 - Deskripsi: (Wajib) Penggunaan minimum ruang partisi yang diperlukan untuk memicu ekstensi (dalam persentase).
 - Tipe: `String`
 - Izinkan Pola: `^[0-9]{1,2}$`
 - VolumeExpansionCapSize (Diperlukan):
 - Deskripsi: (Wajib) Ukuran maksimum Volume Amazon EBS akan ditingkatkan menjadi (dalam GiB).
 - Tipe: `String`
 - Izinkan Pola: `^[0-9]{1,4}$`
 - VolumeExpansionGibIncrease (Diperlukan):
 - Deskripsi: (Wajib) Peningkatan GiB volume. Peningkatan bersih terbesar antara `VolumeExpansionGibIncrease` dan `VolumeExpansionPercentageIncrease` akan digunakan.

- Tipe: String
 - Izinkan Pola: `^[0-9]{1,4}$`
 - VolumeExpansionPercentageIncrease (Diperlukan):
 - Deskripsi: (Wajib) Peningkatan persentase volume. Peningkatan bersih terbesar antara VolumeExpansionGibIncrease dan VolumeExpansionPercentageIncrease akan digunakan.
 - Tipe: String
 - Izinkan Pola: `^[0-9]{1,2}$`
4. Pilih Jalankan.
 5. Otomatisasi dimulai.
 6. Dokumen melakukan langkah-langkah berikut:
 - AssertInstancelManagedInstance:

Memeriksa apakah instance target dikelola oleh Systems Manager.
 - DescribeInstance:

Menjelaskan instans Amazon EC2 target dan mengambil detail instans termasuk Platform, dan RootDeviceType
 - BranchOnPlatform:

Cabang pada jenis platform dan melanjutkan eksekusi jika berbeda dari Windows.
 - DescribeVolumes:

Mengambil volume yang digunakan oleh Instans Amazon EC2.
 - RunPreChecksOnLinux:

Jalankan pemeriksaan terhadap volume yang dikumpulkan pada langkah sebelumnya.
 7. Setelah selesai, tinjau bagian Output untuk hasil eksekusi yang terperinci.

Referensi

Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)

- [Support Automation Workflow](#)

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 instans 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.

JSON

```
{
  "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:aws:ec2:us-east-1:111122223333:instance/i-02573cafcfEXAMPLE",
        "arn:aws:ec2:us-east-1:111122223333:volume/vol-049df61146EXAMPLE",
        "arn:aws:iam:111122223333:instance-profile/instance-profile-name",
        "arn:aws:ssm:us-east-1:111122223333:parameter/aws/service/*",
        "arn:aws:ssm:us-east-1:*:document/AWSSupport-StartEC2RescueWorkflow",
        "arn:aws:ssm:us-east-1:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:us-east-1:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:us-east-1:111122223333:automation-execution/*"
    ]
},
{
    "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": {
    "StringEquals": {
      "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 keTrue.

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.

- `CheckIfInstanceTypelsNitro`:

Memeriksa apakah hypervisor tipe instance berbasis Nitro. Akses Konsol Serial hanya didukung pada instans virtual yang dibangun di Sistem Nitro.

- `CheckIfInstanceIsInAutoScalingGroup`:

Memeriksa apakah instans Amazon EC2 merupakan bagian dari grup Penskalaan Otomatis Amazon EC2 dengan memanggil API. `DescribeAutoScalingInstances` Jika instans merupakan bagian dari grup Amazon EC2 Auto Scaling, instans ini memastikan bahwa Porting Assistant 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 InstanceIsManagedBy SSM`:

Memeriksa apakah instance dikelola oleh AWS Systems Manager. Jika dikelola, runbook mengaktifkan SAC dan menu boot menggunakan PowerShell Run Command.

- `BranchOnPreEC2RescueBackup`:

Cabang berdasarkan parameter `CreateInstanceBackupBeforeScriptExecution` input.

- `CreateAmazonMachineImageBackup`:

Membuat cadangan AMI dari instance.

- `Aktifkan SACAndBootMenu`:

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.

- `CheckIfHelperInstanceProfilesProvided`:

Memeriksa apakah `HelperInstanceProfileName` yang ditentukan ada sebelum mengaktifkan SAC dan menu boot offline menggunakan instans Amazon EC2 sementara.

- `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu`:

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:

- Aktifkan `SACAndBootMenu` .Output:

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.

Referensi

Otomatisasi Systems Manager

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

AWSPremiumSupport-ExtendVolumesOnWindows

Deskripsi

AWSPremiumSupport-ExtendVolumesOnWindowsRunbook memperluas volume Amazon Elastic Block Store (Amazon EBS), partisinya, dan sistem file pada instans Amazon Elastic Compute Cloud (Amazon EC2) target.

Pertimbangan penting

- **Dampak Operasi dan Status Volume:** Modifikasi volume Amazon EBS terjadi dalam tiga fase: `modifying`, `optimizing`, dan `completed`. Otomatisasi ini berlanjut dengan ekstensi sistem file ketika volume mencapai status `optimizing`. Selama `optimizing` status, Anda mungkin mengalami dampak kinerja sementara dan potensi gangguan tingkat sistem file selama pengubahan ukuran partisi. Anda dapat [Memantau kemajuan modifikasi volume Amazon EBS](#).
- **Biaya dan Batasan:** Meningkatkan ukuran volume Amazon EBS akan menghasilkan biaya penyimpanan bulanan yang lebih tinggi. Untuk informasi selengkapnya, lihat [Harga Amazon EBS](#). AMI cadangan dan snapshot terkait yang dibuat oleh runbook ini akan dikenakan biaya tambahan berdasarkan ukuran dan lamanya waktu Anda menyimpannya. Untuk beberapa jenis volume, jika Anda perlu mempertahankan rasio IOPS per GB yang sama setelah ekspansi, Anda mungkin perlu memodifikasi IOPS yang disediakan.
- **Backup and Recovery:** Runbook membuat AMI cadangan sebelum membuat perubahan apa pun pada volume. AMI dan snapshot terkait tidak secara otomatis dihapus dari akun Anda. Anda harus menghapus cadangan ini secara manual jika tidak lagi diperlukan. Jika terjadi kegagalan, volume dapat dipulihkan dari snapshot AMI terkait seperti yang dijelaskan dalam [Ganti volume Amazon EBS menggunakan snapshot](#).

Bagaimana cara kerjanya?

Runbook ini melakukan operasi berikut:

- Memverifikasi bahwa instance target dikelola oleh Systems Manager dan menjalankan Windows Server
- Memastikan hanya ada satu eksekusi runbook ini yang menargetkan instans Amazon EC2 saat ini
- Membuat cadangan Amazon Machine Image (AMI) dari instance target

- Memperluas volume Amazon EBS yang ditentukan untuk ekspansi
- Memperluas sistem file pada instance target menggunakan perintah PowerShell

 Important

Akses ke `AWSPremiumSupport` - * runbook memerlukan Business + Support, Enterprise Support, atau Unified Operations Subscription. Untuk informasi selengkapnya, lihat [Bandingkan AWS Dukungan Paket](#).

Jalankan Otomasi ini (konsol)

Izin IAM yang diperlukan

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

- `ec2:DescribeInstances`
- `ec2:CreateImage`
- `ec2:DescribeImages`
- `ec2:DescribeVolumes`
- `ec2:ModifyVolume`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:DescribeInstanceInformation`

Contoh kebijakan IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
```

```

        "ec2:CreateImage",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolume",
        "ssm:SendCommand",
        "ssm:DescribeInstanceInformation",
        "ssm:ListCommandInvocations"
    ],
    "Resource": "*"
}
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSPremiumSupport-ExtendVolumesOnWindows](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (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.
 - Tipe: `AWS::IAM::Role::Arn`
 - InstanceId (Diperlukan):
 - Deskripsi: (Wajib) ID instans Amazon EC2.
 - Tipe: `String`
 - Izinkan Pola: `^i-[0-9a-f]{8,17}$`
 - VolumeExpansionCapSize (Diperlukan):
 - Deskripsi: (Wajib) Ukuran maksimum (dalam GiB) bahwa volume Amazon EBS akan ditingkatkan.
 - Tipe: `String`
 - Izinkan Pola: `^[0-9]{1,4}$`

- **DiagnosticResults (Diperlukan):**
 - Deskripsi: (Wajib) Hasil skrip prechecks dari DiagnoseDiskUsage dokumen, diformat sebagai CSV satu baris. String dimulai dengan EXTEND; diikuti oleh informasi volume yang dipisahkan koma untuk setiap volume, dengan volume dipisahkan oleh titik koma. Informasi setiap volume meliputi: ID Volume, huruf Drive, Perpanjang bendera (1 untuk memperpanjang, 0 untuk dilewati), Ukuran baru dalam GB, AWS wilayah, dan Alasan/Tindakan.
 - Tipe: String
 - Izinkan Pola: `^EXTEND;[0-9a-zA-Z\\.;_%:\\-\\/\\s]{7,5400}$`

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **AssertInstancelManagedInstance:**

Memverifikasi bahwa instance target dikelola oleh Systems Manager.

- **DescribeInstance:**

Mengambil informasi Platform dari instans Amazon EC2 target.

- **BranchOnPlatform:**

Mengonfirmasi bahwa platform instans Amazon EC2 target adalah Windows Server.

- **CheckConcurrency:**

Memastikan hanya ada satu eksekusi runbook ini yang menargetkan instans Amazon EC2 saat ini.

- **CreateImage:**

Membuat cadangan Amazon Machine Image (AMI) dari instance target.

- **WaitUntillImageReady:**

Menunggu Amazon Machine Image (AMI) untuk menyelesaikan pembuatan dan mencapai available status.

- **Memperpanjang EBSVolume:**

Memperluas volume Amazon EBS dari instans target yang ditentukan untuk ekspansi.

- **DescribeVolumes:**

Menjelaskan volume Amazon EBS dari instans target yang ditentukan untuk ekspansi.

- ExtendFilesystem:

Memperluas filesystem dari instance target menggunakan perintah. PowerShell

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

Referensi

Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow](#)
- [Minta modifikasi volume Amazon EBS](#)

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

Tipe: 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.

- EC2RescueInstanceType

Tipe: String

Nilai yang valid: t2.small | t2.medium | t2.large

Default: t2.small

Deskripsi: (Wajib) Jenis EC2 instans untuk EC2Rescue contoh. Ukuran yang disarankan: t2.small

- LogDestination

Tipe: String

Deskripsi: (Opsional) Nama bucket Amazon 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

Tipe: String

Default: CreateNew VPC

Deskripsi: (Opsional) ID subnet untuk EC2Rescue contoh. Secara default, AWS Systems Manager Automation membuat VPC baru. Atau, gunakan SelectedInstanceSubnet untuk menggunakan subnet yang sama dengan instance Anda, atau tentukan ID subnet kustom.

 Important

Subnet harus berada di Availability Zone yang sama denganUnreachableInstanceId, dan harus memungkinkan akses ke endpoint SSM.

- `UnreachableInstanceId`

Tipe: String

Deskripsi: (Wajib) ID dari instans Anda yang tidak dapat dijangkau EC2 .

 Important

Systems Manager Automation menghentikan instans ini, dan membuat AMI sebelum mencoba operasi apa pun. Data yang disimpan dalam volume penyimpanan instance akan hilang. Alamat IP publik akan berubah jika Anda tidak menggunakan alamat IP Elastis.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan 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 instance yang disediakan adalah Windows Server:
 - a. (EC2Rescue untuk Windows Server) Jika contoh yang diberikan adalah Windows Server contoh:
 - i. `aws:executeAutomation`- Memanggil `AWSSupport-StartEC2RescueWorkflow` dengan EC2 Penyelamatan untuk Windows Server skrip offline.
 - ii. `aws:executeAwsApi`- Mengambil ID AMI cadangan dari otomatisasi bersarang.
 - iii. `aws:executeAwsApi`- Mengambil ringkasan EC2 Penyelamatan dari otomatisasi bersarang.
 - b. (EC2Rescue untuk Linux) Jika instance yang disediakan adalah instance Linux:
 - i. `aws:executeAutomation`- Memanggil `AWSSupport-StartEC2RescueWorkflow` dengan EC2 Rescue untuk skrip offline Linux
 - ii. `aws:executeAwsApi`- Mengambil ID AMI cadangan dari otomatisasi bersarang.

- iii. `aws:executeAwsApi`- Mengambil ringkasan EC2 Penyelamatan dari otomatisasi bersarang.

Keluaran

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

Deskripsi

AWSSupport-ListEC2ResourcesRunbook menampilkan informasi tentang EC2 instans Amazon dan sumber daya terkait seperti volume Amazon Elastic Block Store (Amazon EBS), alamat IP Elastis, dan grup Amazon Auto EC2 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 value yang dipisahkan koma (.csv).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Nama bucket S3 tempat informasi dikumpulkan diunggah.

- DisplayResourceDeletionDocumentation

Tipe: String

Default: betul

Deskripsi: (Opsional) Jika disetel ke `true`, otomatisasi akan membuat tautan dalam output ke dokumentasi yang terkait dengan penghapusan sumber daya Anda.

- RegionsToQuery

Tipe: String

Default: Semua

Deskripsi: (Opsional) Wilayah tempat Anda ingin mengumpulkan informasi EC2 terkait Amazon.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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, `AutomationAssumeRole` diperlukan tindakan berikut:

- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:PutObject`

Langkah Dokumen

- `aws:executeAwsApi`- Mengumpulkan Wilayah yang diaktifkan untuk akun.
- `aws:executeScript`- Mengonfirmasi Wilayah yang diaktifkan untuk mendukung akun Wilayah yang ditentukan dalam `RegionsToQuery` parameter.
- `aws:branch`- Jika tidak ada Wilayah yang diaktifkan untuk akun, otomatisasi berakhir.
- `aws:executeScript`- Daftar semua EC2 instance untuk akun dan Wilayah yang Anda tentukan.
- `aws:executeScript`- Daftar semua Gambar Mesin Amazon (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 penyeimbang beban untuk akun dan Wilayah yang Anda tentukan.
- `aws:executeScript`- Mengunggah informasi yang dikumpulkan ke bucket S3 yang ditentukan jika Anda memberikan nilai untuk parameter. `Bucket`

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

Tipe: 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

Tipe: String

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

- NLASettingAksi

Tipe: String

Nilai yang valid: Periksa | Aktifkan | Nonaktifkan

Default: Periksa

Deskripsi: (Wajib) Tindakan yang harus dilakukan pada pengaturan NLA: Periksa, Aktifkan, Nonaktifkan.

- RDPPort

Tipe: String

Standar: 3389

Deskripsi: (Opsional) Tentukan port RDP baru. Digunakan hanya ketika tindakan diatur ke Modify. Nomor port harus antara 1025-65535. Catatan: Setelah port diubah, layanan RDP dimulai ulang.

- RDPPortAksi

Tipe: String

Nilai yang valid: Periksa | Ubah

Default: Periksa

Deskripsi: (Wajib) Tindakan untuk diterapkan ke port RDP.

- RemoteConnections

Tipe: String

Nilai yang valid: Periksa | Aktifkan | Nonaktifkan

Default: Periksa

Deskripsi: (Wajib) Tindakan yang harus dilakukan pada TSConnections pengaturan fDeny.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

EC2 Instance yang menerima perintah harus memiliki peran IAM dengan kebijakan terkelola Amazon SSMManaged InstanceCore Amazon yang dilampirkan. 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 skrip untuk mengubah atau memeriksa pengaturan RDP pada instance target.

Keluaran

kelola RDPSettings .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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID dari instans terkelola untuk mengelola layanan.

- ServiceAction

Tipe: String

Nilai yang valid: Periksa | Mulai Ulang | Mulai Ulang Paksa | Mulai | Berhenti | Berhenti Paksa | Jeda

Default: Periksa

Deskripsi: (Diperlukan) Tindakan untuk diterapkan ke layanan Windows. Perhatikan bahwa Force-Restart dan Force-Stop dapat digunakan untuk memulai ulang dan menghentikan layanan yang memiliki layanan dependen.

- StartupType

Tipe: String

Nilai yang valid: Periksa | Otomatis | Permintaan | Dinonaktifkan | DelayedAutoStart

Default: Periksa

Deskripsi: (Diperlukan) Jenis startup untuk diterapkan ke layanan Windows.

- WindowsServiceName

Tipe: String

Deskripsi: (Diperlukan) Nama layanan Windows yang valid.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan bahwa EC2 instance yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon SSMManaged InstanceCore Amazon yang dilampirkan. 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 virtual private cloud (VPC). Runbook ini mendukung migrasi EC2 instance Amazon dari jenis virtualisasi hardware virtual machine (HVM) dengan volume root Amazon Elastic Block Store (Amazon EBS).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Tipe: 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.

- ApproverIAM

Jenis: StringList

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARNs) 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 EC2 instans Amazon 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

Tipe: String

Deskripsi: (Opsional) ID subnet tempat Anda ingin memigrasikan EC2 instans Amazon Anda. Jika Anda tidak menentukan nilai untuk parameter ini, otomatisasi secara acak memilih subnet dari VPC Anda.

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID EC2 instance Amazon yang ingin Anda migrasikan.

- MigrationType

Tipe: String

Nilai yang valid: `CutOver` | `Uji`

Deskripsi: (Wajib) Jenis migrasi yang ingin Anda lakukan.

`CutOver`Opsi ini memerlukan persetujuan untuk menghentikan EC2 instans Amazon Anda yang berjalan di EC2 -Classic. Setelah tindakan ini disetujui, EC2 instans Amazon dihentikan dan otomatisasi membuat Amazon Machine Image (AMI). Ketika AMI statusnya adalah `available`, EC2 instance Amazon baru diluncurkan dari ini AMI di yang `DestinationSubnetId` Anda

tentukan di VPC Anda. Jika EC2 instans Amazon Anda yang berjalan di EC2 -Classic memiliki alamat IP Elastis yang dilampirkan, instance akan dipindahkan ke instans Amazon yang baru dibuat di EC2 VPC Anda. Jika peluncuran EC2 instans Amazon di VPC Anda gagal dibuat karena alasan apa pun, instans Amazon akan dihentikan dan persetujuan diminta untuk memulai EC2 instans Amazon Anda di -Classic. EC2

TestOpsi ini menciptakan sebuah AMI EC2 instance Amazon Anda yang berjalan di EC2 -Classic tanpa me-reboot. Karena EC2 instans Amazon tidak reboot, kami tidak dapat menjamin integritas sistem file dari gambar yang dibuat. Saat AMI statusnya adalah `available`, EC2 instance Amazon baru diluncurkan dari ini AMI dalam `DestinationSubnetId` yang Anda tentukan di VPC Anda. Jika EC2 instans Amazon Anda yang berjalan di EC2 -Classic memiliki alamat IP Elastis yang terpasang, otomatisasi akan memverifikasi bahwa yang `DestinationSubnetId` Anda tentukan bersifat publik. Jika peluncuran EC2 instans Amazon di VPC Anda gagal dibuat karena alasan apa pun, itu dihentikan dan otomatisasi berakhir.

- `SNSNotificationARNforPersetujuan`

Tipe: String

Deskripsi: (Opsional) ARN dari Amazon Simple Notification Service (Amazon SNS) topik yang ingin Anda kirim permintaan persetujuan. Parameter ini hanya berlaku jika Anda menentukan `CutOver` nilai untuk `MigrationType` parameter.

- `TargetInstanceType`

Tipe: String

Default: `t2.2xlarge`

Deskripsi: (Opsional) Jenis EC2 instans Amazon yang ingin Anda luncurkan di VPC Anda. Hanya tipe instans berbasis Xen, seperti T2, M4, atau C4, yang didukung.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan 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 EC2 instance Amazon yang Anda tentukan dalam `InstanceId` parameter.

- `aws:assertAwsResourceProperty`- Mengonfirmasi jenis instance yang Anda tentukan dalam `TargetInstanceType` parameter berbasis Xen.
- `aws:assertAwsResourceProperty`- Mengonfirmasi EC2 instans Amazon yang Anda tentukan dalam `InstanceId` parameter adalah tipe virtualisasi HVM.
- `aws:assertAwsResourceProperty`- Mengonfirmasi EC2 instans Amazon 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 tempat Anda menjalankan Wilayah AWS otomatisasi ini.
- `aws:executeAwsApi`- Secara acak memilih ID subnet yang terletak di VPC default.
- `aws:createImage`- Menciptakan sebuah AMI tanpa me-reboot instance Amazon EC2.
- `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 instance baru dari AMI dibuat tanpa me-reboot EC2 instance Amazon di EC2 -Classic.
- `aws:changeInstanceState`- Mengakhiri EC2 instans Amazon yang baru diluncurkan jika langkah sebelumnya gagal karena alasan apa pun.
- `aws:runInstances`- Meluncurkan instance baru dari AMI dibuat tanpa me-reboot EC2 instance Amazon di EC2 -Classic jika disediakan. `DestinationSubnetId`
- `aws:changeInstanceState`- Mengakhiri EC2 instans Amazon yang baru diluncurkan jika langkah sebelumnya gagal karena alasan apa pun.
- `aws:assertAwsResourceProperty`- Mengonfirmasi perilaku berhenti untuk EC2 instance Amazon yang berjalan di EC2 -Classic.
- `aws:approve`- Menunggu persetujuan untuk menghentikan EC2 instans Amazon.
- `aws:changeInstanceState`- Menghentikan EC2 instans Amazon yang berjalan di EC2 -Classic.
- `aws:changeInstanceState`- Force menghentikan EC2 instans Amazon yang berjalan di EC2 -Classic jika diperlukan.
- `aws:createImage`- Menciptakan sebuah AMI dari EC2 contoh Amazon setelah berhenti.

- `aws:branch`- Cabang berdasarkan nilai yang ditentukan untuk `DestinationSubnetId` parameter.
- `aws:runInstances`- Meluncurkan instance baru dari AMI dibuat dari EC2 instance Amazon yang dihentikan di EC2 -Classic.
- `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 EC2 instans Amazon yang baru diluncurkan.
- `aws:runInstances`- Meluncurkan instance baru dari AMI dibuat dari EC2 instance Amazon yang dihentikan di EC2 -Classic dari `DestinationSubnetId` parameter.
- `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 EC2 instans Amazon yang baru diluncurkan.
- `aws:changeInstanceState`- Memulai EC2 instance Amazon yang dihentikan di EC2 -Classic.
- `aws:branch`- Cabang berdasarkan apakah EC2 instans Amazon 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 Elastis yang dipindahkan ke VPC Anda.
- `aws:branch`- Cabang berdasarkan subnet mana EC2 instans Amazon yang berjalan di VPC Anda diluncurkan.
- `aws:executeAwsApi`- Melampirkan alamat IP Elastis ke instans yang baru diluncurkan di VPC Anda.
- `aws:executeScript`- Mengonfirmasi subnet EC2 instans Amazon Anda yang baru diluncurkan yang berjalan di VPC Anda bersifat publik.

Keluaran

`getInstanceProperties.virtualizationType` - Jenis virtualisasi EC2 instance Amazon yang berjalan di EC2 -Classic.

`getInstanceProperties.rootDeviceType`- Jenis perangkat root dari EC2 instance Amazon yang berjalan di EC2 -Classic.

`createAMIWithoutReboot.ImageId`- ID dari AMI dibuat tanpa me-reboot EC2 instance Amazon yang berjalan di EC2 -Classic.

`getDefaultVPC.VpcId`- ID VPC default tempat EC2 instans Amazon baru diluncurkan jika nilai untuk `DestinationSubnetId` parameter tidak disediakan.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`- ID subnet di VPC default tempat instance EC2 Amazon baru diluncurkan jika nilai untuk `DestinationSubnetId` parameter tidak disediakan.

`launchTestInstanceDefaultVPC.InstanceIds`- ID EC2 instans Amazon yang baru diluncurkan di VPC default Anda selama jenis Test migrasi.

`launchTestInstanceProvidedSubnet.InstanceIds`- ID EC2 instans Amazon yang baru diluncurkan dalam `DestinationSubnetId` yang Anda tentukan selama jenis Test migrasi.

`createAMIAfterStoppingInstance.ImageId`- ID dari AMI dibuat setelah menghentikan EC2 instance Amazon yang berjalan di EC2 -Classic.

`launchCutOverInstanceProvidedSubnet.InstanceIds`- ID EC2 instans Amazon yang baru diluncurkan dalam `DestinationSubnetId` yang Anda tentukan selama jenis CutOver migrasi.

`launchCutOverInstanceDefaultVPC.InstanceIds`- ID EC2 instans Amazon 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 `DestinationSubnetId` adalah publik.

AWSSupport-MigrateXenToNitroLinux

Deskripsi

AWSSupport-MigrateXenToNitroLinuxRunbook mengkloning, menyiapkan, dan memigrasikan instans Linux Xen Amazon Elastic Compute Cloud (EC2Amazon) ke [Nitro jenis contoh](#). Runbook ini menyediakan dua opsi untuk jenis operasi:

- **Clone&Migrate**— Alur kerja opsi ini terdiri dari Pemeriksaan Awal, Pengujian, dan Clone&Migrate fase. Alur kerja dijalankan menggunakan `AWSSupport-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 EC2 instans Amazon, pembuatan volume Amazon Elastic Block Store (Amazon EBS), dan AMIs. Untuk detail selengkapnya, lihat [EC2 Harga Amazon dan Harga Amazon EBS](#).

Pemeriksaan awal

Otomatisasi melakukan pemeriksaan pendahuluan 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 Nitro jenis contoh.
- Memeriksa apakah opsi pembelian Instans Spot digunakan untuk instance target.
- Memeriksa apakah volume penyimpanan instance dilampirkan ke instance target.
- Memverifikasi sistem operasi instance target (OS) adalah Linux.
- Memeriksa apakah instance target adalah bagian dari grup EC2 Auto Scaling Amazon. Jika itu adalah bagian dari grup Auto Scaling, otomatisasi memverifikasi bahwa instance dalam status `standby`.
- Memverifikasi bahwa instance dikelola oleh AWS Systems Manager.

Pengujian

Otomatisasi menciptakan Amazon Machine Image (AMI) dari instance target dan meluncurkan instance pengujian dari yang baru dibuat AMI. Fase ini hanya bagian dari Clone&Migrate alur kerja.

Jika instans pengujian melewati semua pemeriksaan status, otomatisasi dijeda dan persetujuan dari prinsipal yang ditunjuk akan diminta melalui notifikasi Amazon Simple Notification Service (Amazon

SNS). Jika persetujuan diberikan, otomatisasi menghentikan instance pengujian, menghentikan instance target, dan melanjutkan migrasi, sementara yang baru dibuat AMI dideregistrasi di akhir alur kerja. Clone&Migrate

Note

Sebelum memberikan persetujuan, sebaiknya verifikasi bahwa semua aplikasi yang berjalan pada instans target telah ditutup dengan baik.

Kloning dan Migrasi

Otomatisasi menciptakan yang lain AMI dari instance target, dan meluncurkan instance baru untuk diubah menjadi Nitro jenis contoh. Otomatisasi melengkapi prasyarat berikut sebelum melanjutkan migrasi. Jika salah satu pemeriksaan gagal, otomatisasi berakhir. Fase ini juga hanya bagian dari Clone&Migrate alur kerja.

- Mengaktifkan atribut jaringan yang disempurnakan (ENA).
- Menginstal versi terbaru driver ENA jika belum diinstal, atau memperbarui versi driver ENA ke versi terbaru. Untuk memastikan kinerja jaringan maksimum, pembaruan ke versi driver ENA terbaru diperlukan jika Nitro tipe instance adalah generasi ke-6.
- Memverifikasi bahwa NVMe modul 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 masing-masing UUIDs. 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 instance diubah menjadi Nitro jenis contoh yang Anda tentukan. Otomatisasi menunggu instance yang baru dibuat untuk lulus semua pemeriksaan status setelah memulai sebagai Nitro jenis contoh. Otomatisasi kemudian menunggu persetujuan dari kepala sekolah yang ditunjuk untuk membuat AMI dari yang berhasil diluncurkan Nitro contoh.

Jika persetujuan ditolak, otomatisasi berakhir, membiarkan instance yang baru dibuat berjalan, dan instance target tetap dihentikan.

Ganti root Amazon EBS Volume

Jika Anda memilih `FullMigration` sebagai `OperationType`, otomatisasi memigrasikan EC2 instans Amazon target ke Nitro jenis contoh yang Anda tentukan. Otomatisasi meminta persetujuan dari prinsipal yang ditunjuk untuk mengganti volume root Amazon EBS dari instans Amazon target dengan volume root EC2 instans Amazon yang dikloning. EC2 Setelah migrasi berhasil, EC2 instance Amazon yang dikloning dihentikan. Jika otomatisasi gagal, volume root Amazon EBS asli dilampirkan ke EC2 instans Amazon target. Jika volume Amazon EBS root yang dilampirkan ke EC2 instans Amazon target memiliki tag dengan `aws:awslauncher` yang diterapkan, `FullMigration` operasi tidak didukung.

Sebelum Anda memulai

Instance target harus memiliki akses internet keluar. Ini untuk mengakses repositori untuk driver dan dependensi seperti `kernel-devel`, `gcc`, `patch`, `rpm-build`, `wget`, `dracut`, `make`, `linux-headers`, dan `unzip`. Package manager 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:

- RHEL 7.x - 8.5
- Amazon Linux (2018.03), Amazon Linux 2
- Debian Server
- Server Ubuntu 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

Tipe: 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.

- Pengakuan

Tipe: String

Deskripsi: (Wajib) Baca detail lengkap tindakan yang dilakukan oleh runbook otomatisasi ini, dan masukkan **Yes, I understand and acknowledge** untuk melanjutkan menggunakan runbook.

- ApproverIAM

Tipe: String

Deskripsi: (Wajib) ARNs 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 instance yang baru dibuat dan AMI untuk migrasi dihapus jika otomatisasi gagal.

Nilai yang valid: Benar | Salah

Bawaan: BETUL

- MinimumRequiredApprovals

Tipe: String

Deskripsi: (Opsional) Jumlah minimum persetujuan yang diperlukan untuk terus menjalankan otomatisasi saat persetujuan diminta.

Nilai yang valid: 1-10

Default: 1

- NitroInstanceType

Tipe: String

Deskripsi: (Diperlukan) Nitro jenis instance yang ingin Anda ubah instance. Jenis instans yang didukung termasuk M5, M6, C5, C6, R5, R6, dan T3.

Default: m5.xlarge

- OperationType

Tipe: String

Deskripsi: (Wajib) Operasi yang ingin Anda lakukan. FullMigrationOps ini melakukan tugas yang sama Clone&Migrate dan juga menggantikan volume root dari 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: Klon&Migrasi | FullMigration

- SNSTopicArn

Tipe: String

Deskripsi: (Wajib) ARN topik Amazon SNS untuk pemberitahuan persetujuan. Topik Amazon SNS digunakan untuk mengirim pemberitahuan persetujuan yang diperlukan selama otomatisasi.

- TargetInstanceid

Tipe: String

Deskripsi: (Wajib) ID EC2 instans Amazon untuk bermigrasi.

Clone&Migrate alur kerja

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 EC2 instans Amazon target didukung di Availability Zone yang sama dengan instance target.
- `getXenInstanceTypeDetails`- Mengumpulkan rincian tentang jenis instance sumber.
- `checkIfInstanceHypervisorIsNitroAlready`- Memeriksa apakah instance target sudah berjalan sebagai Nitro jenis contoh.
- `checkIfTargetInstanceLifecycleIsSpot`- Memeriksa apakah opsi pembelian dari instans target adalah Spot.
- `checkIfOperatingSystemIsLinux`- Memeriksa apakah OS instance target adalah Linux.
- `verifySSMConnectivityForTargetInstance`- Memverifikasi bahwa instance target dikelola oleh Systems Manager.
- `checkIfEphemeralVolumeAreSupported`- Memeriksa apakah jenis instance saat ini dari instance target mendukung volume penyimpanan instance.
- `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 contoh pengujian dari pengujian AMI menggunakan konfigurasi yang sama dengan instance target.
- `cleanupTestInstance`- Mengakhiri contoh pengujian.
- `endOfTestBranch`- Akhir cabang Pengujian.
- `checkIfTestingBranchSucceeded`- Memeriksa status cabang Pengujian.

- `approvalToStopTargetInstance`- Menunggu persetujuan dari kepala sekolah yang ditunjuk untuk menghentikan instance target.
- `stopTargetEC2Instance`- Menghentikan instance target.
- `forceStopTargetEC2Instance`- Paksa menghentikan instance target hanya jika langkah sebelumnya gagal menghentikan instance.
- `startOfCloneAndMigrateBranch`- Cabang ke Clone&Migrate alur kerja.
- `createBackupImage`- Menciptakan AMI dari instance 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 NVMe driver diinstal pada instance yang baru dibuat, dan menginstal driver jika diperlukan.
- `checkAndModifyFSTABEntries`- Memeriksa apakah nama perangkat digunakan `/etc/fstab` dan menggantinya dengan UUIDs jika diperlukan.
- `stopClonedInstance`- Menghentikan instance yang baru dibuat.
- `forceStopClonedInstance`- Paksa menghentikan instance yang baru dibuat hanya jika langkah sebelumnya gagal menghentikan instance.
- `checkENAAtributeForClonedInstance`- Memeriksa apakah atribut jaringan yang disempurnakan diaktifkan untuk instance yang baru dibuat.
- `setNitroInstanceTypeForClonedInstance`- Mengubah jenis instance untuk instance yang baru dibuat ke Nitro jenis contoh yang Anda tentukan.
- `startClonedInstance`- Memulai instance yang baru dibuat yang jenis instancenya Anda ubah.
- `approvalForCreatingImageAfterDriversInstallation`- Jika instance berhasil dimulai sebagai Nitro tipe instance, otomatisasi menunggu persetujuan dari kepala sekolah yang diperlukan. Jika persetujuan diberikan, AMI diciptakan untuk digunakan sebagai emas AMI.
- `createImageAfterDriversInstallation`- Menciptakan AMI untuk digunakan sebagai emas AMI.
- `endOfCloneAndMigrateBranch`- Akhir dari Clone&Migrate cabang.

- `cleanupTestImage`- Deregister 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`- Deregister AMI dibuat untuk pengujian.
- `onFailureApprovalToStartTargetInstance`- Jika otomatisasi gagal, tunggu persetujuan dari kepala sekolah yang ditunjuk untuk memulai instance target.
- `onFailureStartTargetInstance`- Jika otomatisasi gagal, mulai instance target.

FullMigration alur kerja

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 EC2 instans Amazon yang Anda tentukan. Jika runbook menemukan otomatisasi lain dalam proses yang menargetkan instance yang sama, otomatisasi berakhir.
- `getTargetInstanceProperties`- Mengumpulkan rincian dari contoh target.
- `checkRootVolumeTags`- Menentukan apakah volume root EC2 instance Amazon 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 kepala sekolah, otomatisasi dilanjutkan 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`- Memulai alur kerja cabang Replace Root EBS Volume.
- `checkIfTargetInstanceIsManagedByCFN`- Menentukan apakah instance target dikelola oleh AWS CloudFormation tumpukan.
- `branchOnCFNStackStatus`- Cabang berdasarkan status CloudFormation tumpukan.
- `approvalForRootVolumesReplacement(WithCFN)`- Jika instance target diluncurkan oleh CloudFormation, otomatisasi menunggu persetujuan setelah instance yang baru diluncurkan berhasil dimulai sebagai Nitro jenis contoh. Saat 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 Nitro jenis contoh. Saat 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 sedang berjalan, otomatisasi menghentikan instance sebelum mengganti volume root.
- `forceStopTargetInstanceForRootVolumeReplacement`- Paksa menghentikan instance target jika langkah sebelumnya gagal.
- `stopClonedInstanceForRootVolumeReplacement`- Menghentikan instans yang baru dibuat sebelum mengganti volume Amazon EBS.
- `forceStopClonedInstanceForRootVolumeReplacement`- Paksa menghentikan instance yang baru dibuat jika langkah sebelumnya gagal.
- `getBlockDeviceMappings`- Mengambil pemetaan perangkat blok untuk target dan instance yang baru dibuat.
- `replaceRootEbsVolumes`- Mengganti volume root dari instance target dengan volume root dari instance yang baru dibuat.
- `EndOfReplaceRootEBSVolumeBranch`- Akhir alur kerja cabang Replace Root EBS Volume.
- `checkENAAtributeForTargetInstance`- Memeriksa apakah atribut jaringan yang disempurnakan (ENA) diaktifkan untuk EC2 instans Amazon target.

- `enableENAAttributeForTargetInstance`- Mengaktifkan atribut ENA untuk EC2 instance Amazon target jika diperlukan.
- `setNitroInstanceTypeForTargetInstance`- Mengubah instance target ke Nitro jenis contoh yang Anda tentukan.
- `replicateRootVolumeTags`- Mereplikasi tag pada volume Amazon EBS root dari instans Amazon EC2 target.
- `startTargetInstance`- Memulai EC2 instance Amazon target setelah mengubah jenis instance.
- `onFailureStopTargetEC2Instance`- Menghentikan EC2 instance Amazon target jika gagal memulai sebagai Nitro jenis contoh.
- `onFailureForceStopTargetEC2Instance`- Paksa menghentikan EC2 instans Amazon target jika langkah sebelumnya gagal.
- `OnFailureRevertOriginalInstanceType`- Mengembalikan EC2 instance Amazon target ke tipe instans asli jika instance target gagal dimulai sebagai Nitro jenis contoh.
- `onFailureRollbackRootVolumeReplacement`- Mengembalikan semua perubahan yang dilakukan oleh `replaceRootEbsVolumes` langkah jika diperlukan.
- `onFailureApprovalToStartTargetInstance`- Menunggu persetujuan kepala sekolah yang ditunjuk untuk memulai EC2 instans Amazon target setelah memutar kembali perubahan sebelumnya.
- `onFailureStartTargetInstance`- Memulai EC2 instans target Amazon.
- `terminateClonedEC2Instance`- Mengakhiri EC2 instance Amazon yang dikloning setelah mengganti volume root Amazon EBS.

AWSSupport-ResetAccess

Deskripsi

Runbook ini akan menggunakan alat EC2 Rescue pada EC2 instance yang ditentukan untuk mengaktifkan kembali dekripsi kata sandi menggunakan EC2 Console (Windows) atau untuk menghasilkan dan menambahkan key pair SSH baru (Linux). Jika Anda kehilangan key pair, otomatisasi ini akan membuat AMI berkemampuan sandi yang dapat Anda gunakan untuk meluncurkan instance EC2 baru dengan key pair yang Anda miliki (Windows).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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.

- EC2RescueInstanceType

Tipe: String

Nilai yang valid: t2.small | t2.medium | t2.large

Default: t2.small

Deskripsi: (Wajib) Jenis EC2 instans untuk instance EC2 Rescue. Ukuran yang disarankan: t2.small.

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID dari EC2 instance yang ingin Anda atur ulang aksesnya.

Important

Systems Manager Automation menghentikan instance ini, dan membuat AMI sebelum mencoba operasi apa pun. Data yang disimpan dalam volume penyimpanan instance akan hilang. Alamat IP publik akan berubah jika Anda tidak menggunakan IP Elastis.

- SubnetId

Tipe: String

Default: CreateNew VPC

Deskripsi: (Opsional) ID subnet untuk contoh EC2 Penyelamatan. Secara default, Systems Manager Automation membuat VPC baru. Atau, Gunakan SelectedInstanceSubnet untuk menggunakan subnet yang sama dengan instance 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 memerlukan 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- Tegaskan jika instance yang disediakan adalah Windows.
 - a. (EC2Rescue untuk Windows) Jika instance yang disediakan adalah Windows:
 - i. aws:executeAutomation- Panggil AWSSupport-StartEC2RescueWorkflow dengan EC2 Rescue untuk skrip reset kata sandi offline Windows
 - 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 EC2 Penyelamatan dari otomatisasi bersarang
 - b. (EC2Rescue for Linux) Jika instance yang disediakan adalah Linux:
 - i. aws:executeAutomation- Memanggil AWSSupport-StartEC2RescueWorkflow dengan EC2 Rescue untuk skrip injeksi kunci SSH offline Linux

- 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 EC2 Penyelamatan dari otomatisasi bersarang

Keluaran

dapatkan `EC2 RescueForWindowsResult .Output`

`getWindowsBackupAmi. ImageId`

`getWindowsPasswordEnabledAmi.ImageId`

dapatkan `EC2 RescueForLinuxResult .Output`

`getLinuxBackupAmi. ImageId`

Parameter `GetLinuxSSHKey. 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 di Akun AWS Anda dengan peran yang AWS Identity and Access Management dibuat secara otomatis (IAM) atau profil instans IAM kustom yang Anda tentukan. Profil instans kustom (IAM) harus memiliki izin untuk mengambil nilai AWS Secrets Manager rahasia yang berisi kata sandi.

Runbook menghentikan instans Amazon EC2 target Anda, melepaskan volume root Amazon Elastic Block Store (Amazon EBS) 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 root Amazon EBS disambungkan kembali ke instans target Anda. Runbook juga menyediakan opsi untuk membuat snapshot volume root di awal otomatisasi.

Sebelum Anda memulai

Buat rahasia Secrets Manager dengan nilai kata sandi yang ingin Anda tetapkan ke pengguna OS Anda. Nilai harus dalam plaintext. Untuk informasi selengkapnya, lihat [Membuat AWS Secrets Manager rahasia](#) di Panduan AWS Secrets Manager Pengguna.

Pertimbangan-pertimbangan

- Kami merekomendasikan untuk membuat cadangan instance 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 instance hilang. Juga, setiap IPv4 alamat publik yang ditetapkan secara otomatis akan dirilis. Untuk informasi selengkapnya tentang apa yang terjadi saat Anda menghentikan instans, lihat [Menghentikan dan memulai instans Anda](#) di Panduan Pengguna Amazon EC2.
- Jika volume Amazon EBS yang dilampirkan ke instans Amazon EC2 target Anda dienkripsi dengan kunci AWS Key Management Service terkelola pelanggan AWS KMS(), pastikan AWS KMS kuncinya `deleted` tidak `disabled` atau instans Anda akan gagal untuk memulai.
- Menggunakan profil instans IAM kustom memerlukan `GetInstanceProfile` izin IAM `AutomationAssumeRole` untuk validasi, dan profil instans kustom itu sendiri harus menyertakan izin akses Systems Manager dan Secrets Manager. Runbook memvalidasi keberadaan profil instance di muka tetapi akan gagal selama operasi instance helper jika profil instance tidak memiliki akses yang diperlukan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- `AutomationAssumeRole`

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instans Amazon EC2 Linux yang berisi kata sandi pengguna OS yang ingin Anda atur ulang.

- LinuxUserName

Tipe: String

Default: ec2-pengguna

Deskripsi: (Opsional) Akun pengguna OS yang kata sandinya ingin Anda atur ulang.

- SecretArn

Tipe: String

Deskripsi: (Wajib) ARN rahasia Secrets Manager Anda yang berisi kata sandi baru.

- SecurityGroupId

Tipe: String

Deskripsi: (Opsional) ID grup keamanan untuk dilampirkan ke instans Amazon EC2 sementara. Jika Anda tidak memberikan nilai untuk parameter ini, grup keamanan Amazon Virtual Private Cloud (Amazon VPC) default akan digunakan.

- SubnetId

Tipe: String

Deskripsi: (Opsional) ID subnet tempat Anda ingin meluncurkan instans sementara Amazon EC2. Secara default, otomatisasi memilih subnet yang sama dengan instance target Anda. Jika Anda memilih untuk menyediakan subnet yang berbeda, subnet tersebut harus berada di Availability Zone yang sama dengan instance target dan memiliki akses ke endpoint Systems Manager.

- `CreateSnapshot`

Tipe: 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`

Tipe: String

Nilai yang valid: Ya | Tidak

Default: tidak

Deskripsi: Enter **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 IPv4 alamat publik otomatis dirilis. Untuk informasi selengkapnya, lihat [Menghentikan dan memulai instans Anda](#) di Panduan Pengguna Amazon EC2.

- `InstanceProfileName`

Tipe: String

Deskripsi: (Opsional) Nama profil instans IAM untuk dilampirkan ke instans Amazon EC2 helper. Jika tidak disediakan, profil instance sementara dengan izin yang diperlukan akan dibuat secara otomatis. Profil instans kustom harus memiliki izin untuk mengakses rahasia Secrets Manager dan Systems Manager yang ditentukan.

Izin IAM yang diperlukan

`AutomationAssumeRoleParameter` memerlukan 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`
- `iam:GetInstanceProfile`

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 status `running` atau `stopped`. Jika tidak, otomatisasi berakhir.
3. `aws:executeAwsApi`— Mendapatkan properti instans Amazon EC2.
4. `aws:executeAwsApi`— Mendapat properti volume root.
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 target volume root instans Amazon EC2 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 berada dalam status siklus hidup `Standby`.
12. `aws:branch`— Memcabangkan otomatisasi tergantung pada apakah nama profil instans IAM khusus diberikan atau tidak.
13. `aws:assertAwsResourceProperty`— Memastikan profil instans IAM kustom ada dan memvalidasi namanya cocok dengan parameter input.
14. `aws:createStack`— Membuat instans Amazon EC2 sementara yang digunakan untuk mengatur ulang kata sandi untuk pengguna OS yang Anda tentukan.

- 15 `aws:waitForAwsResourceProperty`— Menunggu hingga instans Amazon EC2 sementara yang baru diluncurkan berjalan.
- 16 `aws:executeAwsApi`— Mendapat ID instans Amazon EC2 sementara.
- 17 `aws:waitForAwsResourceProperty`— Menunggu instans Amazon EC2 sementara untuk melaporkan sebagaimana dikelola oleh Systems Manager.
- 18 `aws:changeInstanceState`— Menghentikan instans Amazon EC2 target.
- 19 `aws:changeInstanceState`— Memaksa instans Amazon EC2 target untuk berhenti jika macet dalam keadaan berhenti.
- 20 `aws:branch`— Memcabangkan otomatisasi tergantung pada apakah snapshot volume root instans Amazon EC2 target diminta.
- 21 `aws:executeAwsApi`— Membuat snapshot dari volume root instans Amazon EC2 target Amazon EBS.
- 22 `aws:waitForAwsResourceProperty`— Menunggu snapshot berada dalam keadaan `completed`.
- 23 `aws:executeAwsApi`— Melepaskan volume root Amazon EBS dari instans Amazon EC2 target.
- 24 `aws:waitForAwsResourceProperty`— Menunggu volume root Amazon EBS terlepas dari instans Amazon EC2 target.
- 25 `aws:executeAwsApi`— Melampirkan volume Amazon EBS root ke instans Amazon EC2 sementara.
- 26 `aws:waitForAwsResourceProperty`— Menunggu volume root Amazon EBS dilampirkan ke instans Amazon EC2 sementara.
- 27 `aws:runCommand`— Mengatur ulang kata sandi pengguna target dengan menjalankan skrip shell menggunakan Run Command pada instance Amazon EC2 sementara.
- 28 `aws:executeAwsApi`— Melepaskan volume root Amazon EBS dari instans Amazon EC2 sementara.
- 29 `aws:waitForAwsResourceProperty`— Menunggu volume root Amazon EBS terlepas dari instans Amazon EC2 sementara.
- 30 `aws:executeAwsApi`— Melepaskan volume root Amazon EBS dari instans Amazon EC2 sementara setelah terjadi kesalahan.
- 31 `aws:waitForAwsResourceProperty`— Menunggu volume root Amazon EBS terlepas dari instans Amazon EC2 sementara setelah kesalahan.
- 32 `aws:branch`— Memcabangkan otomatisasi tergantung pada apakah snapshot volume root diminta untuk menentukan jalur pemulihan jika terjadi kesalahan.

- 33 `aws:executeAwsApi`— Memasang kembali volume Amazon EBS root ke instans Amazon EC2 target.
- 34 `aws:waitForAwsResourceProperty`— Menunggu volume root Amazon EBS dilampirkan ke instans Amazon EC2.
- 35 `aws:executeAwsApi`— Membuat volume Amazon EBS baru dari snapshot volume root instans Amazon EC2 target.
- 36 `aws:waitForAwsResourceProperty`— Menunggu hingga volume Amazon EBS baru dalam keadaan. `available`
- 37 `aws:executeAwsApi`— Melampirkan volume Amazon EBS baru ke instans target sebagai volume root.
- 38 `aws:waitForAwsResourceProperty`— Menunggu volume Amazon EBS berada dalam keadaan. `attached`
- 39 `aws:executeAwsApi`— Menjelaskan peristiwa CloudFormation tumpukan jika runbook gagal membuat atau memperbarui CloudFormation tumpukan.
- 40 `aws:branch`— Memcabangkan otomatisasi tergantung pada status instans Amazon EC2 sebelumnya. Jika negara itu `running`, instance dimulai. Jika dalam `stopped` keadaan, otomatisasi berlanjut.
- 41 `aws:changeInstanceState`— Memulai instans Amazon EC2 jika diperlukan.
- 42 `aws:waitForAwsResourceProperty`— Menunggu sampai CloudFormation tumpukan berada dalam status terminal sebelum menghapus.
- 43 `aws:executeAwsApi`— Menghapus CloudFormation tumpukan termasuk instans Amazon EC2 sementara.

AWSSupport-RunEC2RescueForWindowsTool

Deskripsi

RescueForWindowsToolRunbook AWSSupport-RunEC2 menjalankan alat pemecahan masalah Amazon EC2 Rescue untuk Windows Server pada instans terkelola Windows Amazon Elastic Compute Cloud (Amazon EC2) target untuk membantu memecahkan masalah umum. Runbook ini mendukung tiga tindakan utama:

- **ResetAccess:** Mengatur ulang kata sandi Administrator lokal. Kata sandi dibuat secara acak dan disimpan dengan aman di AWS Systems Manager Parameter Store sebagai `/EC2Rescue/Password/<instance_id>` Jika Anda tidak memberikan parameter, kata sandi dienkripsi

dengan kunci default AWS Key Management Service (AWS KMS). `alias/aws/ssm` Secara opsional, Anda dapat menentukan ID AWS KMS kunci untuk mengenkripsi kata sandi dengan kunci Anda sendiri.

- **CollectLogs:** Mengumpulkan log dan file konfigurasi dari sistem operasi dan mengunggahnya ke bucket Amazon Simple Storage Service (Amazon S3) di akun Anda dengan menjalankan Amazon EC2 Rescue dengan opsi tersebut. `/collect:all`
- **FixAll:** Mencoba mendeteksi dan mengatasi masalah pada volume root Windows offline yang dilampirkan ke instans saat ini dengan menjalankan Amazon EC2 Rescue dengan opsi. `/rescue:all`

Important

Runbook ini mensyaratkan bahwa instance target adalah instance yang dikelola Windows dengan AWS Alat untuk Windows PowerShell diinstal. Runbook menginstal alat Amazon EC2 Rescue untuk Windows Server menggunakan paket Systems Manager Distributor. `AWSSupport-EC2Rescue`

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Menginstal alat pemecahan masalah Amazon EC2 Rescue untuk Windows Server menggunakan paket Systems Manager Distributor.
- Mengeksekusi tindakan yang ditentukan (`ResetAccess`, `CollectLogs`, atau `FixAll`) dengan parameter yang disediakan.
- `UntukResetAccess:` Menghasilkan kata sandi yang aman dan menyimpannya di Parameter Store.
- `UntukCollectLogs:` Mengumpulkan log sistem dan mengunggahnya ke bucket Amazon S3 yang ditentukan.
- `UntukFixAll:` Mencoba memperbaiki masalah pada volume offline yang ditentukan.

[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:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:DescribeInstanceInformation`
- `ssm:GetCommandInvocation`
- `ssm:PutParameter`(untuk ResetAccess tindakan)
- `kms:Encrypt`(untuk ResetAccess tindakan dengan AWS KMS kunci khusus)
- `s3:PutObject`(untuk CollectLogs tindakan)
- `s3:GetBucketAcl`(untuk CollectLogs tindakan)
- `s3:GetBucketPolicy`(untuk CollectLogs tindakan)
- `s3:GetBucketPolicyStatus`(untuk CollectLogs tindakan)

Contoh Kebijakan:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
```

```

        "ssm:PutParameter",
        "kms:Encrypt",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus"
    ],
    "Resource": "*"
}
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - RunEC2RescueForWindowsTool](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - Perintah (Diperlukan):
 - Deskripsi: (Wajib) Tindakan yang harus dilakukan.
 - Tipe: String
 - Izinkan Nilai: [ResetAccess, CollectLogs, FixAll]
 - Default: ResetAccess
 - Parameter (Diperlukan):
 - Deskripsi: (Diperlukan) Parameter untuk perintah:
 - UntukResetAccess: ID AWS KMS kunci atau alias (default:alias/aws/ssm)
 - UntukCollectLogs: Nama bucket Amazon S3 untuk mengunggah log
 - UntukFixAll: Nama perangkat untuk remediasi offline (misalnya,xvdf)
 - Tipe: String
 - Izinkan Pola: `^[0-9a-z][a-z0-9-.]{3,63}$|^(dev\/[a-z0-9]{2,10}|xv[a-z0-9]{1,10})$|^(alias\\aws\\ssm|[a-zA-Z0-9-/_]{1,32})$`
4. Pilih Jalankan.
5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- instal EC2 Rescue:

Menginstal alat pemecahan masalah Amazon EC2 Rescue untuk Windows Server menggunakan paket Systems Manager Distributor. `AWSSupport-EC2Rescue`

- jalankan EC2 RescueForWindows:

Menjalankan PowerShell skrip dengan tindakan yang ditentukan dalam parameter Command untuk melakukan operasi yang diminta.

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

Referensi

Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow](#)
- [Gunakan Amazon EC2 Rescue untuk Windows Server dengan Systems Manager Run Command](#)

AWSPremiumSupport-ResizeNitroInstance

Deskripsi

AWSPremiumSupport-ResizeNitroInstanceRunbook ini 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-hal berikut:

- Perilaku berhenti contoh.
- Jika instans merupakan bagian dari grup Amazon EC2 Auto Scaling, standby dan dalam mode.
- Status instans dan sewa.
- Jenis instans yang ingin Anda ubah untuk mendukung jumlah antarmuka jaringan yang saat ini dilampirkan ke instance Anda.

- Arsitektur prosesor dan jenis virtualisasi untuk tipe instans saat ini dan target adalah sama.
- Jika instance sedang berjalan, 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 memutar kembali ke jenis instance sebelumnya.

Secara default, runbook ini tidak akan mengubah jenis instance jika sedang berjalan dan volume penyimpanan instance dilampirkan. Runbook juga tidak akan mengubah jenis instance jika instance adalah bagian dari AWS CloudFormation tumpukan. Jika Anda ingin mengubah salah satu perilaku ini, yes tentukan `AllowCloudFormationInstances` parameter `AllowInstanceStoreInstances` dan.

Runbook menyediakan dua cara berbeda untuk menentukan jenis instance yang ingin Anda ubah:

- Untuk otomatisasi sederhana yang menargetkan satu instance, tentukan jenis instance yang ingin Anda ubah menggunakan parameter. `TargetInstanceTypeFromParameter`
- Untuk menjalankan otomatisasi pada skala untuk mengubah jenis instance dari beberapa instance, tentukan jenis instance menggunakan parameter. `TargetInstanceTypeFromTagValue` Untuk informasi tentang menjalankan otomatisasi dalam skala besar, lihat [Menjalankan otomatisasi dalam skala besar](#).

Jika Anda tidak menentukan nilai untuk salah satu parameter, otomatisasi gagal.

Important

Akses ke `AWSPremiumSupport` - * runbook memerlukan Business + Support, Enterprise Support, atau Unified Operations Subscription. Untuk informasi selengkapnya, lihat [Bandingkan AWS Dukungan Paket](#).

Pertimbangan-pertimbangan

- Kami merekomendasikan untuk membuat cadangan instance Anda sebelum menggunakan runbook ini.
- Untuk informasi tentang kompatibilitas untuk mengubah jenis instance, lihat [Kompatibilitas untuk mengubah jenis instance](#).

- Jika otomatisasi gagal dan kembali ke jenis instans asli, lihat [Memecahkan masalah mengubah jenis instance](#).
- Mengubah jenis instance membutuhkan runbook untuk menghentikan instance Anda. Ketika sebuah instance dihentikan, data apa pun yang disimpan dalam memori atau pada volume penyimpanan instance hilang. Juga, setiap IPv4 alamat publik yang ditetapkan secara otomatis akan dirilis. Untuk informasi selengkapnya tentang apa yang terjadi ketika Anda menghentikan sebuah instans, lihat [Berhenti dan mulai instance Anda](#).
- Dengan menggunakan `SkipInstancesWithTagKey` parameter, Anda dapat melewati instance yang memiliki kunci tag Amazon EC2 tertentu yang diterapkan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Enter **yes** untuk mengetahui bahwa instans Anda akan dihentikan jika sedang berjalan.

- AllowInstanceStoreInstances

Tipe: String

Nilai yang valid: tidak | ya

Default: no

Deskripsi: (Opsional) Jika Anda menentukannya, Anda mengizinkan runbook berjalan pada instance yang memiliki volume penyimpanan instans yang dilampirkan.

- AllowCloudFormationInstances

Tipe: String

Nilai yang valid: tidak | ya

Default: no

Deskripsi: (Opsional) Jika Anda menentukannya, runbook berjalan pada instance yang merupakan bagian dari tumpukan. CloudFormation

- DryRun

Tipe: String

Nilai yang valid: tidak | ya

Default: no

Deskripsi: (Opsional) Jika Anda menentukannya, buku runbook memvalidasi persyaratan pengubahan ukuran tanpa membuat perubahan pada jenis instance.

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID instans Amazon EC2 yang jenisnya ingin Anda ubah.

- SkipInstancesWithTagKey

Tipe: String

Deskripsi: (Opsional) Otomatisasi melewati instance target jika kunci tag yang Anda tentukan diterapkan ke instance.

- SleepTime

Tipe: String

Default: 3

Deskripsi: (Opsional) Jumlah detik runbook ini harus tidur setelah selesai.

- TagInstance

Tipe: String

Deskripsi: (Opsional) Tandai 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 sensitif huruf besar dan kecil.

- TargetInstanceTypeFromParameter

Tipe: String

Deskripsi: (Opsional) Jenis instans yang ingin Anda ubah instans Anda. Biarkan parameter ini kosong jika Anda ingin menggunakan nilai kunci tag yang disediakan dalam TargetInstanceTypeFromTagValue parameter.

- TargetInstanceTypeFromTagValue

Tipe: String

Deskripsi: (Opsional) Kunci tag diterapkan ke instance target Anda yang nilainya berisi jenis instance 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 memerlukan 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 parameter. `SkipInstancesWithTagKey` 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 stop dan tidak `terminate`.
9. `aws:branch`: Memastikan instans Amazon EC2 bukan instance 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 sedang berlangsung dengan menargetkan instance yang sama, otomatisasi mengembalikan kesalahan dan berakhir.

12 `aws:branch`: Memcabangkan 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 Auto Scaling dengan memanggil `DescribeAutoScalingInstances` operasi API. Jika instans merupakan bagian dari grup Auto Scaling, pastikan instans Amazon EC2 dalam mode `standby`.

14 `aws:branch`: Memcabangkan otomatisasi tergantung pada apakah Anda ingin otomatisasi memeriksa apakah instans Amazon EC2 adalah bagian dari tumpukan: CloudFormation

- a. `aws:executeScript` Memastikan instans Amazon EC2 bukan bagian dari CloudFormation tumpukan dengan memanggil operasi `DescribeStackResources` API.

15 `aws:executeAwsApi`: Mengembalikan daftar jenis instance dengan tipe arsitektur prosesor yang sama, tipe virtualization, dan yang mendukung jumlah antarmuka jaringan yang saat ini dilampirkan ke instance target.

16 `aws:executeAwsApi`: Mendapat nilai tipe instance 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`: Memcabangkan otomatisasi berdasarkan apakah nilai `DryRun` parameter disetel `keyes`. Jika `yes`, otomatisasi berakhir.

19 `aws:branch`: Memeriksa apakah jenis instans asli dan target sama. Jika mereka sama, otomatisasi berakhir.

20 `aws:executeAwsApi`: Mendapat status instance saat ini.

21 `aws:changeInstanceState`: Menghentikan instans Amazon EC2.

22 `aws:changeInstanceState`: Memaksa instance untuk berhenti jika macet di `stopping` negara bagian.

23 `aws:executeAwsApi`: Mengubah jenis instance ke tipe instance target.

24 `aws:sleep`: Menunggu 3 detik setelah mengubah jenis instance untuk konsistensi akhirnya.

25. `aws:branch`: Memcabangkan otomatisasi berdasarkan status instance sebelumnya. Jika `yarunning`, instance dimulai.

- a. `aws:changeInstanceState`: Memulai instans Amazon EC2 jika dijalankan 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 tipe instans 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 macet dalam status berhenti.
 - iii. `aws:executeAwsApi`: Mengubah instans Amazon EC2 ke tipe aslinya.
 - iv. `aws:sleep`: Menunggu 3 detik setelah mengubah jenis instance untuk konsistensi akhirnya.
 - v. `aws:changeInstanceState`: Memulai instans Amazon EC2 jika dijalankan sebelum mengubah jenis instans.
 - vi. `aws:waitForAwsResourceProperty`: Menunggu instans Amazon EC2 untuk lulus pemeriksaan status.

26. `aws:sleep`: Menunggu sebelum mengakhiri runbook.

AWSSupport-ShareEncryptedAMIorEBSSnapshot

Deskripsi

Runbook ini mengotomatiskan proses berbagi snapshot terenkripsi s Amazon Machine Image atau Amazon Elastic Block Store dengan akun Amazon Web Services lainnya. Runbook ini menangani persyaratan kompleks untuk berbagi sumber daya terenkripsi lintas akun, termasuk modifikasi kebijakan AWS Key Management Service utama dan pembaruan izin sumber daya.

Otomatisasi ini melakukan langkah-langkah yang diuraikan dalam artikel Blog AWS Keamanan [Cara berbagi AML s terenkripsi di seluruh akun untuk meluncurkan instans Amazon Elastic Compute Cloud terenkripsi](#).

Pertimbangan Penting

- Runbook ini akan mengubah sumber daya Anda: Runbook akan menambahkan izin lintas akun ke kebijakan Kunci Terkelola AWS KMS Pelanggan (CMK) Anda dan memberikan AMI izin peluncuran atau snapshot Amazon EBS membuat izin volume ke akun tujuan.
- Biaya tambahan mungkin berlaku: Saat menyalin sumber daya (wilayah berbeda atau enkripsi kunci AWS terkelola), biaya tambahan akan dikeluarkan untuk snapshot EBS baru atau AMI Amazon dan transfer data lintas wilayah apa pun.
- Harap verifikasi ID akun tujuan: Periksa kembali ID akun tujuan karena runbook ini tidak dapat memvalidasi keberadaan akun.
- Rollback otomatis dengan verifikasi manual: Runbook ini mencoba untuk secara otomatis memutar kembali perubahan jika gagal. Namun, jika rollback itu sendiri gagal, harap verifikasi bahwa tidak ada salinan AMI /Snapshot tambahan yang tersisa di akun Anda, LaunchPermission/CreateVolumePermission atribut sumber daya tidak menyertakan akun yang tidak diinginkan, dan kebijakan AWS KMS kunci dalam keadaan semula.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah tingkat tinggi berikut:

- Memvalidasi keberadaan sumber daya input, status, dan konfigurasi enkripsi
- Memeriksa izin berbagi sumber daya saat ini dengan akun tujuan
- Menganalisis kebijakan AWS KMS utama dan membuat pratinjau komprehensif dari semua perubahan yang diperlukan
- Meminta persetujuan dari kepala sekolah yang ditunjuk sebelum melakukan perubahan
- Menjalankan perubahan yang disetujui termasuk penyalinan sumber daya (jika diperlukan), pembaruan izin, dan modifikasi kebijakan AWS KMS utama
- Menyediakan laporan eksekusi komprehensif dengan informasi rollback jika diperlukan

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

AutomationAssumeRole Parameter membutuhkan tindakan berikut:

- EC2: DescribeImages
- EC2: DescribeSnapshots
- EC2: DescribeImageAttribute
- EC2: DescribeSnapshotAttribute
- EC2: ModifyImageAttribute
- EC2: ModifySnapshotAttribute
- EC2: CopyImage
- EC2: CopySnapshot
- EC2: DeregisterImage
- EC2: DeleteSnapshot
- km: DescribeKey
- km: GetKeyPolicy
- km: PutKeyPolicy
- km: CreateGrant
- km: * GenerateDataKey
- km: * ReEncrypt
- kms:Decrypt
- accessanalyzer: CheckAccessNotGranted

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSsupport-ShareEncryptedAMIorEBSSnapshot](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):

Nama Sumber Daya Amazon dari AWS AWS Identity and Access Management peran 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.

- **Penyetuju (Diperlukan):**

Daftar kepala sekolah yang AWS diautentikasi yang dapat menyetujui atau menolak tindakan tersebut. Jumlah maksimum pemberi persetujuan adalah 10. Anda dapat menentukan prinsipal dengan menggunakan salah satu format berikut: nama pengguna, ARN pengguna, ARN peran IAM, atau IAM berperan ARN.

- **ResourceId (Diperlukan):**

AMI atau ID Snapshot Amazon EBS untuk dibagikan (misalnya, ami-123456789012 atau snap-123456789012).

- **DestinationAccountId (Diperlukan):**

ID AWS akun 12 digit tempat sumber daya akan dibagikan.

- **CustomerManagedKeyId (Opsional):**

AWS KMS ID CMK untuk mengenkripsi ulang sumber daya. Diperlukan jika sumber daya dienkripsi dengan kunci AWS terkelola atau ketika DestinationRegion ditentukan untuk penyalinan lintas wilayah. Untuk penyalinan lintas wilayah, kunci ini harus ada di wilayah tujuan.

- **DestinationRegion (Opsional):**

AWS Wilayah tempat sumber daya akan disalin. Nilai default adalah wilayah saat ini. Jika wilayah yang berbeda ditentukan, sumber daya akan disalin ke wilayah tujuan menggunakan AWS KMS CMK yang ditentukan dalam parameter. CustomerManagedKeyId

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **ValidateResources:**

Memvalidasi keberadaan sumber daya input, status, konfigurasi enkripsi, dan menentukan perubahan yang diperlukan untuk berbagi.

- **BranchOnResourcePermission:**

Cabang alur kerja berdasarkan apakah izin berbagi sumber daya perlu diperiksa.

- **CheckResourcePermission:**

Memeriksa apakah akun target telah memerlukan izin berbagi untuk sumber daya.

- **AnalyzeChanges:**

Menganalisis kebijakan AWS KMS utama dan membuat pratinjau komprehensif dari semua perubahan yang diperlukan.

- **BranchOnChanges:**

Cabang alur kerja berdasarkan apakah perubahan memerlukan persetujuan.

- **GetApproval:**

Menunggu persetujuan kepala sekolah AWS IAM yang ditunjuk untuk melanjutkan perubahan yang diperlukan.

- **ExecuteChanges:**

Mengeksekusi perubahan yang disetujui dengan rollback pada kegagalan.

- **Results:**

Menghasilkan laporan eksekusi komprehensif yang merangkum semua tindakan yang diambil selama proses berbagi terenkripsi AMI atau snapshot.

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

AWS AWS Identity and Access Management Kebijakan yang Diperlukan untuk Akun Tujuan

Peran IAM atau pengguna di akun tujuan harus mengonfigurasi izin IAM berikut untuk meluncurkan instans Amazon EC2 terenkripsi dari terenkripsi bersama atau untuk membuat volume dari snapshot Amazon EBS terenkripsi AMI bersama:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "kms:Decrypt"
      ]
    }
  ]
}
```

```
    ],
    "Resource": [
        "arn:aws:kms:<region>:<account-id>:key/<key-id>"
    ]
}
}
```

Referensi

Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow](#)
- [Bagikan AWS KMS kunci](#)

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

Tipe: 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.

- EndDate

Tipe: String

Deskripsi: (Opsional) Tanggal terakhir Anda ingin otomatisasi untuk 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 menggantikan volume root yang ada yang dilampirkan ke instance Anda.

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID instance 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

Tipe: String

Deskripsi: (Opsional) Interval di mana snapshot dilewati saat mencari snapshot untuk memulihkan instance Anda. Misalnya, jika ada 100 snapshot yang tersedia, dan Anda menentukan nilai 2 untuk parameter ini, maka setiap snapshot ketiga ditinjau.

Default: 0

- SnapshotId

Tipe: String

Deskripsi: (Opsional) ID snapshot yang ingin Anda pulihkan instance.

- StartDate

Tipe: String

Deskripsi: (Opsional) Kencan pertama Anda ingin otomatisasi untuk mencari snapshot.

- TotalSnapshotsToLook

Tipe: String

Deskripsi: (Opsional) Jumlah snapshot ulasan otomatisasi.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 instance target yang 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 dari contoh.
7. `aws:executeAwsApi`- Mengumpulkan detail tentang AMI dibuat pada langkah sebelumnya.
8. `aws:waitForAwsResourceProperty`- Menunggu untuk AMI negara menjadi available sebelum melanjutkan.
9. `aws:executeScript`- Meluncurkan instance baru dari yang baru dibuat AMI.
10. `aws:assertAwsResourceProperty`- Memverifikasi status instance adalah available.
11. `aws:executeAwsApi`- Mengumpulkan rincian tentang instance yang baru diluncurkan.
12. `aws:branch`- Cabang berdasarkan apakah Anda memberikan nilai untuk `SnapshotId` parameter.
13. `aws:executeScript`- Mengembalikan daftar snapshot dalam periode waktu yang ditentukan.
14. `aws:executeAwsApi`- Menghentikan instance.
15. `aws:waitForAwsResourceProperty`- Menunggu status volume menjadi available.

- 16aws:waitForAwsResourceProperty- Menunggu status instance menjadistopped.
- 17aws:executeAwsApi- Melepaskan volume root.
- 18aws:waitForAwsResourceProperty- Menunggu volume root terlepas.
- 19aws:executeAwsApi- Melampirkan volume root baru.
- 20aws:waitForAwsResourceProperty- Menunggu volume baru dilampirkan.
- 21aws:executeAwsApi- Mulai contoh.
- 22aws:waitForAwsResourceProperty- Menunggu status instance menjadiavailable.
- 23aws:waitForAwsResourceProperty- Menunggu pemeriksaan status sistem dan instance untuk lulus untuk instance.
- 24aws:executeScript- Menjalankan skrip untuk menemukan snapshot yang dapat digunakan untuk berhasil membuat volume.
- 25aws: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
- 26aws:executeScript- Menghapus sumber daya yang dibuat oleh otomatisasi.

Keluaran

launchCloneInstance.InstanceIds

ListSnapshotByDate.FinalSnapshots

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.WorkingSnapshot

InstanceRecovery.hasil

AWSSupport - SendLogBundleToS3Bucket

Deskripsi

AWSSupport-SendLogBundleToS3BucketRunbook mengunggah bundel log yang dihasilkan oleh alat EC2 Rescue dari instance target ke bucket S3 yang ditentukan. Runbook menginstal versi khusus platform EC2 Rescue 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instance terkelola Windows atau Linux yang ingin Anda kumpulkan log.

- S3BucketName

Tipe: String

Deskripsi: (Diperlukan) bucket S3 untuk mengunggah log ke.

- S3Path

Tipe: String

Default:AWSSupport-SendLogBundleToS3Bucket/

Deskripsi: (Opsional) jalur S3 untuk log yang dikumpulkan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan bahwa EC2 instance yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon SSMManaged InstanceCore Amazon yang dilampirkan. 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 EC2 Rescue melalui `AWS-ConfigureAWSPackage`.
2. `aws:runCommand`- Jalankan PowerShell skrip untuk mengumpulkan log pemecahan masalah Windows dengan EC2 Rescue.
3. `aws:runCommand`- Jalankan skrip bash untuk mengumpulkan log pemecahan masalah Linux dengan Rescue. EC2

Keluaran

`collectAndUploadWindowsLogBundle`.Keluaran

`collectAndUploadLinuxLogBundle`.Keluaran

AWSSupport-StartEC2RescueWorkflow

Deskripsi

AWSSupport-StartEC2RescueWorkflowRunbook menjalankan skrip berenkode base64 yang disediakan (Bash atau Powershell) pada instance helper yang dibuat untuk menyelamatkan instance Anda. Volume root instance Anda dilampirkan dan dipasang ke instance helper, juga dikenal sebagai instance EC2 Rescue. Jika instance 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 (AMIs) tidak didukung oleh otomatisasi ini.

Informasi Tambahan

Untuk base64 menyandikan skrip, Anda dapat menggunakan Powershell atau Bash. PowerShell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

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: RESCUE_AC COUNT_ID EC2	{{global:Account_ID}}	123456789012
\$ env: RESCUE_DATE EC2	{{global:tanggal}}	2018-09-07
\$ env: RESCUE_DATE_TIME EC2	{{global:tanggal_waktu}}	2018-09-07_18.09.59
\$ env: EC2 MENYELAMA TKAN_ RW_DIR EC2	EC2Rescue untuk jalur instalasi Windows	C:\Program Files\ Amazon\ EC2 Penyelamatan
\$ env: EC2 MENYELAMA TKAN_ RW_DIR EC2	EC2Rescue untuk jalur instalasi Windows	C:\Program Files\ Amazon\ EC2 Penyelamatan
\$env: RESCUE_EX ECUTION_ID EC2	{{Automation:Execution_ID}}	7ef8008e-219b-4aca -8bb5-65e2e898e20b

Variabel	Deskripsi	Nilai contoh
\$env: RESCUE_OF FLINE_CURRENT_CONTROL_SET EC2	Offline Windows Kontrol Saat Ini Set jalur	HKLM:\AWSTempSystem \ControlSet001
\$env: RESCUE_OF FLINE_DRIVE EC2	Huruf drive Windows offline	D:\
\$env: RESCUE_OF FLINE_EBS_DEVICE EC2	Perangkat EBS volume root offline	xvdf
\$env: RESCUE_OF FLINE_KERNEL_VER EC2	Versi Kernel Windows Offline	6.1.7601.24214
\$env: RESCUE_OF FLINE_OS_ARCHITECTURE EC2	Arsitektur Windows Offline	AMD64
\$env: RESCUE_OF FLINE_OS_CAPTION EC2	Keterangan Windows Offline	Pusat Data Windows Server 2008 R2
\$env: RESCUE_OF FLINE_OS_TYPE EC2	Jenis OS Windows Offline	Server
\$env: RESCUE_OF FLINE_PROGRAM_FILE S_DIR EC2	Jalur direktori file Program Windows Offline	D:\Program Berkas
\$env: RESCUE_OF FLINE_PROGRAM_FILE S_X86_DIR EC2	Offline Windows Program file jalur direktori x86	D:\Program Berkas (x86)
\$env: RESCUE_OF FLINE_REGISTRY_DIR EC2	Jalur direktori registri Windows offline	D:\Windows\System32\config
\$env: RESCUE_OF FLINE_SYSTEM_ROOT EC2	Jalur direktori root sistem Windows offline	D:\Windows

Variabel	Deskripsi	Nilai contoh
\$ env: RESCUE_REGION EC2	{{global:wilayah}}	us-west-1
\$env: RESCUE_S3_BUCKET EC2	{{S3BucketName }}	amzn-s3-demo-ember
\$env: RESCUE_S3_AWALAN EC2	{{S3Awalan}}	myprefix/
\$env: RESCUE_SO URCE_INSTANCE EC2	{{ InstanceId }}	abcdefgh123456789
\$ skrip: EC2 RESCUE_OF FLINE_WINDOWS_INSTALL	Metadata Instalasi Windows Offline	Objek Powershell Pelanggan

Linux:

Variabel	Deskripsi	Nilai contoh
EC2RESCUE_ACCOUNT_ID	{{global:Account_ID}}	123456789012
EC2RESCUE_DATE	{{global:tanggal}}	2018-09-07
EC2RESCUE_DATE_TIME	{{global:tanggal_waktu}}	2018-09-07_18.09.59
EC2MENYELAMATKAN_EC2 RL_DIR	EC2Penyelamatan untuk jalur instalasi Linux	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTIO N_ID	{{Automation:Execution_ID}}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_ DEVICE	Nama perangkat offline	/dev/xvdf1
EC2RESCUE_OFFLINE_ EBS_DEVICE	Perangkat EBS volume root offline	/dev/sdf

Variabel	Deskripsi	Nilai contoh
EC2RESCUE_OFFLINE_SYSTEM_ROOT	Titik pemasangan volume root offline	/mnt/mount
EC2RESCUE_PYTHON	Versi Python	python2.7
EC2RESCUE_REGION	{{global:wilayah}}	us-west-1
EC2RESCUE_S3_BUCKET	{{S3BucketName }}	amzn-s3-demo-ember
EC2RESCUE_S3_AWALAN	{{S3Awalan}}	myprefix/
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	abcdefgh123456789

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AMIPrefix

Tipe: String

Default: AWSsupport-EC2Rescue

Deskripsi: (Opsional) Awalan untuk nama AMI cadangan.

- AutomationAssumeRole

Tipe: 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.

- `CreatePostEC2RescueBackup`

Tipe: String

Nilai yang valid: benar/salah

Bawaan: 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.

- `CreatePreEC2RescueBackup`

Tipe: String

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Setel `true` untuk membuat AMI InstanceId sebelum menjalankan skrip. AMI akan bertahan setelah otomatisasi selesai. Anda bertanggung jawab untuk mengamankan akses ke AMI, atau menghapusnya.

- `EC2RescueInstanceType`

Tipe: String

Nilai yang valid: `t2.small` | `t2.medium` | `t2.large` | `t3.small` | `t3.medium` | `t3.large` | `i3.large`

Default: `t3.medium`

Deskripsi: (Opsional) Jenis instans EC2 untuk instans EC2 Rescue.

- `InstanceId`

Tipe: String

Deskripsi: (Wajib) ID instans EC2 Anda. PENTING: AWS Systems Manager Otomasi menghentikan instance ini. Data yang disimpan dalam volume penyimpanan instance akan hilang. Alamat IP publik akan berubah jika Anda tidak menggunakan IP Elastis.

- **OfflineScript**

Tipe: String

Deskripsi: (Wajib) Skrip yang dikodekan Base64 untuk dijalankan terhadap instance helper. Gunakan Bash jika instance sumber Anda adalah Linux, dan PowerShell jika itu adalah Windows.

- **S3 BucketName**

Tipe: String

Deskripsi: (Opsional) Nama bucket S3 di akun tempat Anda ingin mengunggah log pemecahan masalah. Pastikan kebijakan bucket tidak memberikan read/write izin yang tidak perlu kepada pihak yang tidak memerlukan akses ke log yang dikumpulkan.

- **S3Prefix**

Tipe: String

Default: `AWSSupport-EC2Rescue`

Deskripsi: (Opsional) Awalan untuk log S3.

- **SubnetId**

Tipe: String

Default: `SelectedInstanceSubnet`

Deskripsi: (Opsional) ID subnet untuk contoh EC2 Penyelamatan. Secara default, subnet yang sama di mana instance yang disediakan berada digunakan. PENTING: Jika Anda menyediakan subnet kustom, subnet tersebut harus berada di Availability Zone yang sama InstanceId, dan harus mengizinkan akses ke endpoint SSM.

- **UniqueId**

Tipe: String

Default: `{{Automation:Execution_ID}}`

Deskripsi: (Opsional) Pengidentifikasi unik untuk otomatisasi.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan bahwa pengguna yang menjalankan otomatisasi memiliki kebijakan terkelola IAM SSMAutomationPeran Amazon yang dilampirkan. Selain kebijakan itu, pengguna harus memiliki:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:*:111122223333: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::111122223333:role/AWSSupport-EC2Rescue-*",
        "arn:aws:iam::111122223333: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 diberikan
 - a. (Gunakan subnet instance saat ini) - Jika `* SubnetId = SelectedInstanceSubnet *` lalu jalankan `aws:createStack` untuk menyebarkan tumpukan Rescue EC2 CloudFormation
 - b. (Buat VPC baru) - Jika `* SubnetId = CreateNew VPC *` kemudian jalankan `aws:createStack` untuk menyebarkan tumpukan Rescue EC2 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 EC2 Penyelamatan CloudFormation
6. `aws:invokeLambdaFunction`- Lakukan validasi masukan tambahan
7. `aws:executeAwsApi`- Perbarui CloudFormation tumpukan EC2 Rescue untuk membuat instance pembantu EC2 Rescue
8. `aws:waitForAwsResourceProperty`- Tunggu pembaruan CloudFormation tumpukan EC2 Rescue selesai
9. `aws:executeAwsApi`- Jelaskan output CloudFormation stack EC2 Rescue untuk mendapatkan ID instans EC2 Rescue helper
10. `aws:waitForAwsResourceProperty`- Tunggu instance pembantu EC2 Rescue menjadi instance terkelola
11. `aws:changeInstanceState`- Hentikan contoh yang disediakan
12. `aws:changeInstanceState`- Hentikan contoh yang disediakan
13. `aws:changeInstanceState`- Paksa menghentikan contoh yang disediakan
14. `aws:assertAwsResourceProperty`- Periksa nilai `CreatePre EC2 RescueBackup` masukan

- a. (Buat cadangan pra- EC2 Penyelamatan) - Jika * CreatePre EC2 RescueBackup = benar*
- b. `aws:executeAwsApi`- Buat cadangan AMI dari instance yang disediakan
- c. `aws:createTags`- Tandai cadangan AMI

15 `aws:runCommand`- Instal EC2 Rescue pada contoh pembantu EC2 Rescue

16 `aws:executeAwsApi`- Lepaskan volume root dari instance yang disediakan

17 `aws:assertAwsResourceProperty`- Periksa platform instance yang disediakan

- a. (Instans adalah Windows):

`aws:executeAwsApi`- Lampirkan volume root ke instance EC2 Rescue helper sebagai `*xvdf*`

`aws:sleep`- Tidur 10 detik

`aws:runCommand`- Jalankan skrip offline yang disediakan di Powershell

- b. (Instance adalah Linux):

`aws:executeAwsApi`- Lampirkan volume root ke instance EC2 Rescue helper sebagai `*/dev/sdf*`

`aws:sleep`- Tidur 10 detik

`aws:runCommand`- Jalankan skrip offline yang disediakan di Bash

18 `aws:changeInstanceState`- Hentikan contoh pembantu EC2 Penyelamatan

19 `aws:changeInstanceState`- Paksa menghentikan contoh pembantu EC2 Penyelamatan

20 `aws:executeAwsApi`- Lepaskan volume root dari instance EC2 Rescue helper

21 `aws:executeAwsApi`- Pasang kembali volume root ke instance yang disediakan

22 `aws:assertAwsResourceProperty`- Periksa nilai CreatePost EC2 RescueBackup masukan

- a. (Buat cadangan pasca- EC2 Penyelamatan) - Jika * CreatePost EC2 RescueBackup = benar*
- b. `aws:executeAwsApi`- Buat cadangan AMI dari instance yang disediakan
- c. `aws:createTags`- Tandai cadangan AMI

23 `aws:executeAwsApi`- Kembalikan penghapusan awal pada status terminasi untuk volume root dari instance yang disediakan

24 `aws:changeInstanceState`- Kembalikan status awal dari instance yang disediakan (menjalankan/berhenti)

25 `aws:deleteStack`- Hapus CloudFormation tumpukan EC2 Rescue

Keluaran

runScriptForLinux.Keluaran

runScriptForWindows.Keluaran

preScriptBackup.Imageld

postScriptBackup.Imageld

AWSSupport-TroubleshootActiveDirectoryReplication

Deskripsi

AWSSupport-TroubleshootActiveDirectoryReplicationRunbook membantu memecahkan masalah kegagalan replikasi pengontrol domain Microsoft Active Directory (AD) dengan memeriksa pengaturan umum pada instance pengontrol domain target. Runbook ini menjalankan serangkaian PowerShell perintah terhadap instance pengontrol domain yang disediakan untuk memeriksa status replikasi saat ini dan melaporkan kesalahan yang berpotensi menyebabkan masalah replikasi domain. Runbook secara opsional dapat memulai replikasi layanan kritis (Netlogon, RPCSS, W32Time, dan KDC) jika dihentikan dan menyinkronkan waktu sistem dengan berjalan `w32tm /resync /force` pada instance target.

Important

AWS Microsoft AD yang dikelola tidak berada dalam lingkup runbook ini.

Important

Saat otomatisasi menjalankan perintah pada instance target, perubahan dilakukan pada sistem file instance target. Perubahan ini termasuk pembuatan direktori log (`$env:ProgramData\TroubleshootActiveDirectoryReplication`) dan file laporan.

Bagaimana cara kerjanya?

Runbook melakukan pemeriksaan dan tindakan berikut:

- Memverifikasi instans target menjalankan Windows dan dikelola oleh Systems Manager.

- Menjalankan PowerShell skrip untuk memeriksa konfigurasi dan status replikasi Direktori Aktif.
- Memeriksa grup keamanan dan pengaturan ACL jaringan untuk konektivitas mitra replikasi.
- Memecahkan masalah sinkronisasi waktu dan status layanan kritis.
- Mengunggah file log ke bucket Amazon S3 yang ditentukan untuk analisis.

[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`
- `secretsmanager:GetSecretValue`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicy`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutObject`

Contoh Kebijakan:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "secretsmanager:GetSecretValue",
        "ssm:DescribeInstanceInformation",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Secrets Manager penyiapan

PowerShell Skrip replikasi cek terhubung ke pengontrol domain Microsoft Active Directory target dengan mengambil nama pengguna dan kata sandi dengan panggilan runtime ke. AWS Secrets Manager Ikuti langkah-langkah di [Buat AWS Secrets Manager rahasia](#) untuk membuat AWS Secrets Manager rahasia baru. Pastikan nama pengguna dan kata sandi disimpan menggunakan key/value pasangan dalam format{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}. Setelah membuat AWS Secrets Manager rahasia, pastikan Anda memberikan secretsmanager:GetSecretValue izin pada ARN rahasia ke peran profil instans IAM pengontrol domain target Anda.

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSsupport-TroubleshootActiveDirectoryReplication](#) Systems Manager di bawah Documents.

3. Untuk parameter input, masukkan yang berikut ini:

- AutomationAssumeRole (Opsional):
 - 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.
 - Tipe: `AWS::IAM::Role::Arn`
- InstanceId (Diperlukan):
 - Deskripsi: (Wajib) ID instance pengontrol domain Amazon EC2 yang ingin Anda atasi masalah replikasi Direktori Aktif. Perhatikan bahwa instance yang disediakan harus menjadi pengontrol domain.
 - Tipe: `AWS::EC2::Instance::Id`
- SecretsManagerArn (Diperlukan):
 - Deskripsi: (Wajib) ARN AWS Secrets Manager rahasia Anda yang berisi nama pengguna dan kata sandi Direktori Aktif dengan Admin Perusahaan atau izin yang setara untuk mengakses domain Direktori Aktif dan konfigurasi hutan Anda. Pastikan nama pengguna dan kata sandi disimpan menggunakan key/value pasangan dalam format `{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}`. Pastikan untuk melampirkan `secretsmanager:GetSecretValue` izin pada ARN rahasia ke peran profil instans IAM pengontrol domain target Anda.
 - Tipe: `String`
 - Pola yang Diizinkan: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z0-9-]{2,20}:[0-9]{12}:secret:[a-zA-Z0-9]{1}[a-zA-Z0-9\\/_+=.@-]{1,256}$`
- TimeSync (Opsional):
 - Deskripsi: (Opsional) Pilih `Check` atau `Sync`. Jika Anda memilih `Check`, runbook mencetak status sinkronisasi waktu sistem saat ini. Jika `Sync` dipilih, runbook akan mencoba resync waktu paksa dengan menjalankan `w32tm /resync /force` instance target.
 - Tipe: `String`
 - Nilai yang Diizinkan: `[Check, Sync]`
 - Default: `Check`

- Deskripsi: (Opsional) Pilih Check atau Fix. Jika Anda memilih Check, runbook mencetak status saat ini dari Netlogon, Windows Time service (W32Time) Remote Procedure Call (RPC) Service, dan Key Distribution Center (KDC) layanan. Jika Fix dipilih, runbook akan mencoba memulai layanan ini jika ada yang dihentikan.
- Tipe: String
- Nilai yang Diizinkan: [Check, Fix]
- Default: Check
- LogDestination (Diperlukan):
 - Deskripsi: (Diperlukan) Bucket Amazon S3 Amazon di AWS akun Anda untuk mengunggah output perintah.
 - Tipe: String

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- assertIfOperatingSystemIsWindows:

Memeriksa apakah sistem operasi instans Amazon EC2 target yang disediakan adalah Windows.

- assertIfInstancesSsmManaged:

Memastikan instans Amazon EC2 dikelola oleh Systems Manager, jika tidak, otomatisasi akan berakhir.

- CheckReplication:

Menjalankan PowerShell skrip pada instance pengontrol domain tertentu untuk mendapatkan konfigurasi dan status replikasi domain Active Directory.

- checkInstanceSgAndNACL:

Memeriksa apakah lalu lintas ke mitra replikasi diizinkan oleh grup keamanan dan ACL jaringan yang terkait dengan instance pengontrol domain target.

- Pemecahan masalah Plikasi:

Menjalankan PowerShell skrip untuk memecahkan masalah sinkronisasi waktu dan status layanan penting.

Memeriksa apakah bucket Amazon S3 yang ditentukan dalam `LogDestination` mengizinkan izin akses baca atau tulis anonim, atau publik.

- **runUploadScript:**

Menjalankan PowerShell skrip untuk mengunggah arsip log ke bucket AAmazon S3 yang ditentukan dalam `LogDestination` parameter dan menghapus file log yang diarsipkan dari OS. File log dapat digunakan untuk pemecahan masalah atau untuk dibagikan dengan AWS Support saat memecahkan masalah replikasi.

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

Referensi

Otomatisasi Systems Manager

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

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 memulihkan 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 diubah, runbook memperluas partisi dan sistem file dari volume yang terpengaruh.

⚠ Important

Akses ke `AWSPremiumSupport` - * runbook memerlukan Business + Support, Enterprise Support, atau Unified Operations Subscription. Untuk informasi selengkapnya, lihat [Bandingkan AWS Dukungan 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, optimalisasi kapasitas, dan identifikasi penghematan biaya. Untuk informasi selengkapnya, lihat [AWS Managed Services](#).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, Windows

Parameter

- `InstanceId`

Tipe: String

Nilai yang diizinkan: `^i-[a-z0-9]{8,17}$`

Deskripsi: (Wajib) ID instans Amazon EC2 Anda.

- `VolumeExpansionEnabled`

Jenis: Boolean

Deskripsi: (Opsional) Tandai untuk mengontrol apakah dokumen akan memperpanjang volume dan partisi yang terpengaruh.

Default: betul

- VolumeExpansionUsageTrigger

Tipe: String

Deskripsi: (Opsional) Penggunaan minimum ruang partisi yang diperlukan untuk memicu ekstensi (dalam persentase).

Nilai yang diizinkan: ^ [0-9] {1,2} \$

Default: 85

- VolumeExpansionCapSize

Tipe: String

Deskripsi: (Opsional) Ukuran maksimum volume Amazon Elastic Block Store (Amazon EBS) akan ditingkatkan menjadi (dalam GiB).

Nilai yang diizinkan: ^ [0-9] {1,4} \$

Standar: 2048

- VolumeExpansionGibIncrease

Tipe: String

Deskripsi: (Opsional) Peningkatan GiB volume. Peningkatan bersih terbesar antara VolumeExpansionGibIncrease dan VolumeExpansionPercentageIncrease akan digunakan.

Nilai yang diizinkan: ^ [0-9] {1,4} \$

Default: 20

- VolumeExpansionPercentageIncrease

Tipe: String

Deskripsi: (Opsional) Peningkatan persentase volume. Peningkatan bersih terbesar antara VolumeExpansionGibIncrease dan VolumeExpansionPercentageIncrease akan digunakan.

Nilai yang diizinkan: ^ [0-9] {1,2} \$

Default: 20

- AutomationAssumeRole

Tipe: 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.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 Systems Manager
2. `aws:executeAwsApi`- Menjelaskan contoh untuk mendapatkan platform.
3. `aws:branch`- Otomatisasi cabang berdasarkan platform instans.

a. Jika instancenya 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 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 windows) 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 menjadi `available`

III. `aws:executeAutomation-` Jalankan `AWSPremiumSupport-ExtendVolumesOnLinux` runbook untuk melakukan modifikasi volume serta langkah-langkah yang diperlukan dalam OS untuk membuat ruang baru tersedia.

Keluaran

`diagnoseDiskUsageAlertOnWindows.Keluaran`

`extendVolumesOnWindows.Keluaran`

`diagnoseDiskUsageAlertOnLinux.Keluaran`

`extendVolumesOnLinux.Keluaran`

`CadanganAMILinux. ImageId`

`CadanganAMIWindows. ImageId`

AWSSupport-TroubleshootEC2InstanceConnect

Deskripsi

`AWSSupport-TroubleshootEC2InstanceConnect` otomatisasi 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 Instance Metadata Service (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.

- `EC2InstanceConnectRoleOrUser`(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

AWS::EC2::Instance::Id

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.

EC2InstanceConnectRoleOrUser

(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.

String

SourceNetworkType

(Optional) The network access method to the EC2 instance: "Browser": you are connecting to the EC2 instance using your browser by clicking the connect button from the console. "Public": you are accessing the EC2 instance located in a public subnet over the internet (example: from your local computer). "Private": you are connecting to your instance through its private IP address.

Browser

Username

(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.

String

SSHPort

(Optional) The SSH port configured on the EC2 instance. Default value is "22". The port number must be between "1-65535".

22

SourceIpCIDR

(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.

None

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.

- `CheckIfAWSRegionDidukung`:

Memeriksa apakah instans Amazon EC2 terletak di wilayah yang didukung Amazon EC2 Instance Connect AWS .

- `BranchOnIfAWSRegionDidukung`:

Melanjutkan eksekusi jika AWS Wilayah didukung oleh Amazon EC2 Instance Connect. Jika tidak, itu menciptakan output dan keluar dari otomatisasi.

- `CheckIfInstanceAMIsDidukung`:

Memeriksa apakah AMI yang terkait dengan instans didukung oleh Amazon EC2 Instance Connect.

- `BranchOnIfInstanceAMIsDidukung`:

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.

- `Periksa IMDSReachabilityFromOs`:

Menjalankan skrip Bash pada instans Linux Amazon EC2 target untuk memeriksa apakah skrip tersebut dapat mencapai file. `IMDSv2`

- `Periksa EICPackage Instalasi`:

Menjalankan skrip Bash pada instans Linux Amazon EC2 target untuk memeriksa apakah paket Amazon EC2 Instance Connect diinstal dan dikonfigurasi dengan benar.

- `Periksa SSHConfigFromOs`:

Menjalankan skrip Bash pada instans Linux Amazon EC2 target untuk memeriksa apakah port

- **CheckMetadataHTTPEndpointIsEnabled:**

Memeriksa apakah layanan metadata instance HTTP endpoint diaktifkan.

- **Periksa EICNetwork Akses:**

Memeriksa apakah konfigurasi jaringan (grup keamanan, ACL jaringan, dan aturan tabel rute) mengizinkan koneksi ke instans melalui Amazon EC2 Instance Connect.

- **Periksa IAMRoleOrUserPermissions:**

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](#)

AWS dokumentasi layanan

- [Bagaimana cara mengatasi masalah saat terhubung ke instans Amazon EC2 menggunakan Amazon EC2 Instance Connect?](#)

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

Deskripsi

AWSSupport-TroubleshootLinuxMGNDRSAgentLogsRunbook otomatisasi digunakan untuk mendeteksi kesalahan umum saat menginstal agen replikasi AWS Application Migration Service (AWS MGN) dan AWS Elastic Disaster Recovery (AWS DRS) di server Linux untuk memigrasikan server sumber ke cloud. AWS

Bagaimana cara kerjanya?

Runbook AWSSupport-TroubleshootLinuxMGNDRSAgentLogs mengambil jalur Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) di mana log instalasi AWS MGN atau AWS DRS diunggah sebagai parameter. `aws_replication_agent_installer.log` Kemudian, ia melakukan tugas-tugas berikut:

- Validasi: Memeriksa apakah file log yang disediakan valid dan berisi setidaknya satu instalasi agen.
- Parsing: Mem-parsing secara menyeluruh instalasi agen terbaru dalam file log untuk kesalahan AWS MGN atau AWS DRS yang diketahui.
- Deteksi dan resolusi Kesalahan: Berdasarkan penguraian, ia mendeteksi dan mencantumkan kesalahan atau masalah apa pun selama proses instalasi agen. Untuk setiap kesalahan yang terdeteksi, buku runbook menyediakan langkah-langkah terperinci untuk membantu menyelesaikan atau mengurangi masalah.

Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `s3:GetObject`
- `s3:ListBucket`

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSsupport-TroubleshootLinuxMGNDRSagentLogs](#) 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 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 (Diperlukan):

Nama bucket Amazon S3 tempat log agen replikasi disimpan.

- S3 ObjectKey (Diperlukan):

Kunci objek Amazon S3 tempat file log penginstal agen replikasi disimpan.

Contoh: Jika URI Amazon S3 adalah `s3://bucket_name/path/to/file/aws_replication_agent_installer.log`, maka Anda harus memasukkan `path/to/file/aws_replication_agent_installer.log`

- ServiceName (Diperlukan):

Nama layanan tempat agen replikasi diinstal. Nilai yang diizinkan: AWS MGN atau AWS DRS

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. 	BucketName (Required) The name of the Amazon S3 bucket where the replication agent log is stored. s3bucket-name
S3ObjectKey (Required) The key of S3 object where the replication agent installer log file is stored. Example: if S3 URI is <code>s3://bucket_name/path/to/file/aws_replication_agent_installer.log</code> then you should provide <code>path/to/file/aws_replication_agent_installer.log</code> as input. aws_replication_agent_installer.log	ServiceName (Required) The name of the service for which the Replication agent is done: AWS MGN : AWS Application Migration Service. AWS DRS : AWS Elastic Disaster Recovery. AWS MGN

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **ValidateInput**

Memastikan bahwa file log agen replikasi valid dan dapat diakses menggunakan nama bucket Amazon S3 yang disediakan dan jalur ke objek, lalu mengembalikan nomor byte instalasi agen terbaru.

- **CheckReplicationAgentLogErrors**

Membaca file log agen replikasi mulai dari byte instalasi terbaru dan mencari kesalahan AWS MGN atau AWS DRS yang diketahui.

- **MakeFinalOutput**

Membuat output dari pemeriksaan sebelumnya termasuk informasi tentang kesalahan yang ditemukan dan rekomendasi pemecahan masalah.

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

▼ Outputs

MakeFinalOutput.Output

Input Validation Step

✅ The replication agent log file is valid and accessible using the provided S3 path.

Log file error checking results

❌ Detected error: Kernel development package for [REDACTED] are missing from repositories

✅ Recommendations and troubleshooting steps:

During agent installation, the installer downloads a matching "kernel-devel/linux-headers" package from the repository configured in your Linux operating system. This error occurs when the agent installation workflow can't install the matching "kernel-devel/linux-headers" package to the Linux OS current running kernel.

1. Check the current kernel version on the source server:

```
$ sudo uname -r
```

2. Make sure to install the version that corresponds exactly to the current kernel version that you are running (displayed in the output of "sudo uname -r" command).

Use the following commands to install "kernel-devel/linux-headers" package for the running kernel:

+ For all Red Hat and CentOS source servers:

```
$ sudo yum install kernel-devel-`uname -r`
```

+ For all Ubuntu/Debian source servers:

```
$ sudo apt-get install linux-headers-`uname -r`
```

+ For all SUSE source servers:

```
$ sudo zypper install kernel-default-devel-`uname -r`
```

Note: When the "kernel-devel/linux-headers" packages are installed for both the running kernel and other installed kernels, you will find the following directories generated for each installed kernel. They are located under "/usr/src/kernels" for all Red Hat-based operating systems and under "/usr/src" for Ubuntu and Debian-based operating systems:

```
$ sudo ls -la /usr/src/kernels
```

```
$ sudo ls -la /usr/src
```

3. Sometimes, you will find that the "kernel-devel/linux-headers" package for the running kernel is not available in your server repositories. In that case, you have three options:

Referensi

Otomatisasi Systems Manager

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

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

- Tindakan

Tipe: String

Nilai yang valid: CheckAll | FixAll | Kustom

Default: Kustom

Deskripsi: (Opsional) [Kustom] Gunakan nilai dari Firewall RDPServiceStartupType,, RDPService RDP Port Tindakan, NLASetting Tindakan, dan RemoteConnections untuk mengelola pengaturan. [CheckAll] Baca nilai pengaturan tanpa mengubahnya. [FixAll] Kembalikan pengaturan default RDP, dan nonaktifkan Windows Firewall.

- AllowOffline

Tipe: String

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Perbaiki saja - Setel ke true jika Anda mengizinkan remediasi RDP offline jika pemecahan masalah online gagal, atau instance yang disediakan bukan instance terkelola. Catatan: Untuk remediasi offline, SSM Automation menghentikan instans, dan membuat AMI sebelum mencoba operasi apa pun.

- AutomationAssumeRole

Tipe: 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.

- firewall

Tipe: String

Nilai yang valid: Periksa | Nonaktifkan

Default: Periksa

Deskripsi: (Opsional) Periksa atau nonaktifkan firewall Windows (semua profil).

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID instance untuk memecahkan masalah pengaturan RDP.

- NLASettingAksi

Tipe: String

Nilai yang valid: Periksa | Nonaktifkan

Default: Periksa

Deskripsi: (Opsional) Periksa atau nonaktifkan Network Layer Authentication (NLA).

- RDPPortAksi

Tipe: String

Nilai yang valid: Periksa | Ubah

Default: Periksa

Deskripsi: (Opsional) Periksa port saat ini yang digunakan untuk koneksi RDP, atau ubah port RDP kembali ke 3389 dan restart layanan.

- RDPServiceAksi

Tipe: String

Nilai yang valid: Periksa | Mulai | Mulai Ulang | Mulai Ulang Paksa

Default: Periksa

Deskripsi: (Opsional) Periksa, mulai, mulai ulang, atau restart paksa layanan RDP (). TermService

- RDPServiceStartupType

Tipe: String

Nilai yang valid: Periksa | Otomatis

Default: Periksa

Deskripsi: (Opsional) Periksa atau atur layanan RDP untuk memulai secara otomatis saat Windows melakukan booting.

- RemoteConnections

Tipe: String

Nilai yang valid: Periksa | Aktifkan

Default: Periksa

Deskripsi: (Opsional) Tindakan yang harus dilakukan pada TSConnections pengaturan fDeny: Periksa, Aktifkan.

- S3 BucketName

Tipe: 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

Tipe: String

Default: SelectedInstanceSubnet

Deskripsi: (Opsional) Hanya offline - ID subnet untuk instance EC2 Rescue 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 InstanceId, dan harus mengizinkan akses ke endpoint SSM.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan bahwa EC2 instance yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon SSMManged InstanceCore Amazon yang dilampirkan. 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 instans
2. aws:assertAwsResourceProperty- Periksa apakah instance tersebut adalah instance terkelola
3. (Pemecahan masalah online) Jika instance adalah instance terkelola, maka:

a. `aws:assertAwsResourceProperty`- Periksa nilai Tindakan 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. (Perbaikan 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 skrip 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`- Tegaskan `AllowOffline` = benar

b. `aws:assertAwsResourceProperty`- Tegaskan Tindakan = `FixAll`

c. `aws:assertAwsResourceProperty`- Menegaskan nilai `SubnetId`

(Gunakan subnet instance yang disediakan) Jika `SubnetId` `SELECTED_INSTANCE_SUBNET`

`aws:executeAwsApi`- Ambil subnet instance saat ini.

`aws:executeAutomation`- Jalankan `AWSSupport-ExecuteEC2Rescue` dengan subnet instance 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

mengelola `RDPService` Pengaturan.Output

kelola `RDPSettings` .Output

`checkFirewallProfiles`.Keluaran

periksa `RDPService` Pengaturan.Output

periksa `RDPSettings` .Output

`disableFirewallProfiles`.Keluaran

Pulihkan Pengaturan `RDPService` Default.Output

Pulihkan.Output `RDPSettings` Default

memecahkan masalah.Output `RDPOffline`

memecahkan masalah.Output `RDPOffline WithSubnetId`

AWSSupport-TroubleshootSSH

Deskripsi

`AWSSupport-TroubleshootSSH`Runbook menginstal alat Amazon EC2 Rescue untuk Linux, dan kemudian menggunakan alat EC2 Rescue 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 hanya-baca.

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

Untuk informasi tentang bekerja dengan `AWSSupport-TroubleshootSSH` runbook, lihat [topik `AWSSupport-TroubleshootSSH` pemecahan masalah](#) ini dari Dukungan Premium AWS .

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- Tindakan

Tipe: String

Nilai yang valid: CheckAll | FixAll

Default: CheckAll

Deskripsi: (Wajib) Tentukan apakah akan memeriksa masalah tanpa memperbaikinya atau untuk memeriksa dan secara otomatis memperbaiki masalah yang ditemukan.

- AllowOffline

Tipe: String

Nilai yang valid: benar/salah

Bawaan: salah

Deskripsi: (Opsional) Perbaiki saja - Setel ke true jika Anda mengizinkan remediasi SSH offline jika pemecahan masalah online gagal, atau instance yang disediakan bukan instance terkelola.

Catatan: Untuk remediasi offline, SSM Automation menghentikan instans, dan membuat AMI sebelum mencoba operasi apa pun.

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID EC2 instans Anda untuk Linux.

- S3 BucketName

Tipe: 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

Tipe: String

Default: SelectedInstanceSubnet

Deskripsi: (Opsional) Hanya offline - ID subnet untuk instance EC2 Rescue 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 memungkinkan akses ke endpoint SSM.

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

Disarankan bahwa EC2 instance yang menerima perintah memiliki peran IAM dengan kebijakan terkelola Amazon `SSMManaged InstanceCore` Amazon yang dilampirkan. 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 terkelola
 - a. (Remediasi online) Jika instance adalah instance terkelola, maka:
 - i. `aws:configurePackage`- Instal EC2 Rescue untuk Linux melalui `AWS-ConfigureAWSPackage`.
 - ii. `aws:runCommand`- Jalankan skrip bash untuk menjalankan EC2 Rescue untuk Linux.
 - b. (Remediasi offline) Jika instance bukan instance terkelola maka:
 - i. `aws:assertAwsResourceProperty`- Tegaskan `AllowOffline` = benar
 - ii. `aws:assertAwsResourceProperty`- Tegaskan Tindakan = `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 disediakan.

Keluaran

Pemecahan masalahSH.Output

memecahkan masalah.Output SSHOffline

memecahkan masalah.Output SSHOffline WithSubnetId

AWSSupport-TroubleshootSUSERegistration

Deskripsi

AWSSupport-TroubleshootSUSERegistrationRunbook membantu Anda mengidentifikasi mengapa mendaftarkan Amazon Elastic Compute Cloud (Amazon) EC2 SUSE Linux Enterprise Server contoh dengan Infrastruktur Pembaruan SUSE gagal. Output otomatisasi menyediakan langkah-langkah untuk menyelesaikan, atau membantu Anda memecahkan masalah, masalah. Jika instans melewati semua pemeriksaan selama otomatisasi, instance terdaftar dengan SUSE Update Infrastructure.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Tipe: 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.

- InstancedId

Tipe: String

Deskripsi: (Wajib) ID EC2 instans Amazon yang ingin Anda pecahkan masalah.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan 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 EC2 instans Amazon dikelola oleh AWS Systems Manager.
- `aws:runCommand`- Memeriksa apakah platform EC2 instans Amazon SLES.
- `aws:runCommand`- Memeriksa apakah `cloud-regionsrv-client` versi paket lebih besar dari atau sama dengan versi yang diperlukan 9.0.10.
- `aws:runCommand`- Memeriksa apakah tautan simbolis untuk produk dasar rusak, dan memperbaiki tautan yang rusak.
- `aws:runCommand`- Memeriksa apakah file host (`/etc/hosts`) berisi catatan untuk `smt-ec2-suscloud.net`. Otomatisasi menghapus entri duplikat apa pun.
- `aws:runCommand`- Memeriksa apakah `curl` perintah diinstal.
- `aws:runCommand`- Memeriksa apakah EC2 instans Amazon dapat mengakses alamat Layanan Metadata Instans (IMDS) 169.254.169.254.
- `aws:runCommand`- Memeriksa apakah EC2 instans Amazon memiliki kode penagihan atau kode AWS Marketplace produk.
- `aws:runCommand`- Memeriksa apakah EC2 instans Amazon dapat mencapai setidaknya 1 server regional melalui HTTPS.

- `aws:runCommand`- Memeriksa apakah EC2 instans Amazon dapat mencapai server Alat Manajemen Berlangganan (SMT) melalui HTTP.
- `aws:runCommand`- Memeriksa apakah EC2 instans Amazon dapat mencapai server Alat Manajemen Berlangganan (SMT) melalui HTTPS.
- `aws:runCommand`- Memeriksa apakah EC2 instans Amazon dapat mencapai `smt-ec2.susecloud.net` alamat melalui HTTPS.
- `aws:runCommand`- Mendaftarkan EC2 instans Amazon dengan Infrastruktur Pembaruan SUSE.
- `aws:executeScript`- Mengumpulkan dan mengeluarkan 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 menghapus 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. Default-nya 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 read/write izin yang tidak perlu kepada pihak yang tidak memerlukan akses ke log yang diambil. Instans Windows Amazon EC2 harus memiliki akses ke bucket Amazon S3.

- **Instal EC2 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,,, UDPv4 dan menyimpannya ke analysis_output.log dalam folder output.

- **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. EC2Rescuemenangkap 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. CleanUpLogsOnFailureLangkah 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 dimana 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_... created successfully.

Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance_... started successfully.

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_... deleted successfully.

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 %
spsvc	Processor	0.00	106.00	9.00
WinPrvSE#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
❌ Failed

Failed
1

All executed steps
2

Cancelled
0

Succeeded
1

TimedOut
0

Executed steps (2)

Find Steps

< 1 >

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 langkahAssertInstanceIsWindows.

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
Verification

FailureStage
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-AnalyzeAWSEndpointReachabilityFromEC2Runbook 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

AWS::EC2::Instance::Id

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'.

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'.

false

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **getWindowsServerAndSSMAgentVersion:**

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 akan 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.

Runbook ini mendukung sistem operasi berikut:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

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

Windows

Parameter

- AllowOffline

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instans EC2 Anda untuk Windows Server.

- SubnetId

Tipe: String

Default: SelectedInstanceSubnet

Deskripsi: (Opsional) Offline saja - ID subnet untuk instance EC2 Rescue 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 AML.
 - ii. `aws:createTags`- Menandai cadangan AML.
 - iii. `aws:runCommand`- Menginstal driver jaringan ENA.
 - iv. `aws:runCommand`- Menginstal NVMe driver.
 - v. `aws:runCommand`- Menginstal driver AWS PV.
 - 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 AML dari instance sumber.
 - v. `aws:createTags`- Tandai cadangan AML dari instance sumber.
 - vi. `aws:executeAwsApi`- Aktifkan ENA untuk contoh
 - vii. `aws:assertAwsResourceProperty`- Tegaskan ForceUpgrade benderanya.
 - viii. (Paksa peningkatan 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.ImageId`

`preOfflineUpgradeCadangan. ImageId`

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

`upgradeDriversOffline.Keluaran`

`forceUpgradeDriversOffline.Output`

Amazon ECS

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon Elastic Container Service. Untuk informasi lebih lanjut 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, instance target harus memiliki AWS Command Line Interface (AWS CLI) untuk instance Linux atau AWS Tools untuk Windows PowerShell untuk instance Windows diinstal. Otomatisasi 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 kumpulan g yang telah ditentukan Amazon S3, 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`

Tipe: 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.

- `ECSInstanceId`

Tipe: String

Deskripsi: (Wajib) ID dari instance yang ingin Anda kumpulkan log. Instance yang Anda tentukan harus dikelola oleh Systems Manager.

- `LogDestination`

Tipe: 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

Tipe: 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.

- InstanceIds

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

InstallAmazonECSAgent. SuccessfullInstances - ID dari contoh di mana instalasi agen Amazon ECS berhasil.

`InstallAmazonECSAgent.FailedInstances` - ID instance di mana instalasi agen Amazon ECS gagal.

`InstallAmazonECSAgent.InProgressInstances` - ID contoh di mana instalasi 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`

Tipe: 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.

- `capacityProviderStrategy`

Tipe: String

Deskripsi: (Opsional) Strategi penyedia kapasitas yang digunakan untuk tugas tersebut.

- **klaster**

Tipe: String

Deskripsi: (Opsional) Nama pendek atau ARN cluster untuk menjalankan tugas Anda. Jika Anda tidak menentukan cluster, cluster default digunakan.

- **count**

Tipe: String

Deskripsi: (Opsional) Jumlah instantiasi tugas yang ditentukan untuk ditempatkan di klaster Anda. Anda dapat menentukan hingga 10 tugas untuk setiap permintaan.

- **aktifkan ECSManaged Tag**

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 wadah dalam tugas ini. Jika benar, ini mengaktifkan fungsionalitas perintah eksekusi pada semua kontainer dalam tugas.

- **grup**

Tipe: String

Deskripsi: (Opsional) Nama kelompok tugas untuk dikaitkan dengan tugas. Nilai default adalah nama keluarga dari definisi tugas. Misalnya, `family:my-family-name`.

- **LaunchType**

Tipe: String

Nilai yang valid: EC2 | FARGATE | EKSTERNAL

Deskripsi: (Opsional) Infrastruktur untuk menjalankan tugas mandiri Anda.

- **networkConfiguration**

Tipe: String

Deskripsi: (Opsional) Konfigurasi jaringan untuk tugas tersebut. Parameter ini diperlukan untuk definisi tugas yang menggunakan mode `aws_vpc` jaringan untuk menerima elastic network interface mereka sendiri, dan tidak didukung untuk mode jaringan lainnya.

- `mengesampingkan`

Tipe: 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`

Tipe: 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`

Tipe: String

Deskripsi: (Opsional) Objek strategi penempatan yang akan digunakan untuk tugas. Anda dapat menentukan maksimal 5 aturan strategi untuk setiap tugas.

- `platformVersion`

Tipe: 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`

Tipe: 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`

Tipe: String

Deskripsi: (Opsional) ID referensi yang akan digunakan untuk tugas. ID referensi dapat memiliki panjang maksimum 1024 karakter.

- `dimulaiOleh`

Tipe: 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`

Tipe: 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`

Tipe: 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-TroubleshootECSTaskInstance

Deskripsi

AWSSupport-TroubleshootECSTaskInstanceRunbook 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 kluster 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 kluster Amazon ECS harus `ACTIVE`

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama klaster Amazon ECS yang gagal didaftarkan instans.

- InstanceId

Tipe: 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 Pencatatan 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.

Ketika peran Lambda IAM disediakan, otomatisasi akan menggunakannya alih-alih membuat yang baru. Peran IAM Lambda yang disediakan harus mencakup kebijakan yang AWS dikelola `AWSLambdaVPCAccessExecutionRole` dan memiliki kebijakan kepercayaan yang memungkinkannya diasumsikan oleh kepala layanan Lambda. `lambda.amazonaws.com`

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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.

- LambdaRoleArn

Tipe: String

Deskripsi: (Opsional) ARN dari peran IAM yang memungkinkan AWS Lambda fungsi untuk mengakses AWS layanan dan sumber daya yang diperlukan. Jika tidak ada peran yang ditentukan, Otomasi Systems Manager ini akan membuat satu peran IAM untuk Lambda di akun Anda dengan `NetworkToolSSMRunbookExecution<ExecutionId>` nama yang menyertakan kebijakan terkelola: `AWSLambdaVPCLambdaAccessExecutionRole`

- ClusterName

Tipe: 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

Tipe: 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:DescribeDhcpOptions
- ec2:DescribeInstances
- ec2:DescribeInstanceAttribute
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribeVpcAttribute
- elasticfilesystem:DescribeFileSystems
- elasticfilesystem:DescribeMountTargets
- elasticfilesystem:DescribeMountTargetSecurityGroups
- elasticfilesystem:DescribeFileSystemPolicy

- `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:ListUsers`
- `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`

Ketika `LambdaRoleArn` disediakan, otomatisasi tidak perlu membuat peran dan izin berikut dapat dikecualikan:

- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:AttachRolePolicy`
- `iam:DetachRolePolicy`

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

Tipe: 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.

- 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

`UpdateAmazonECSAgent`. `UpdatedContainers` - ID instance tempat pembaruan agen Amazon ECS berhasil.

`UpdateAmazonECSAgent`. `FailedContainers` - ID instance di mana pembaruan agen Amazon ECS gagal.

`UpdateAmazonECSAgent`. `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 lebih lanjut 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-CheckAndMountEFSRunbook 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

Tipe: 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.

- Tindakan

Tipe: String

Nilai yang valid: Periksa | CheckAndMount

Deskripsi: (Wajib) Menentukan apakah runbook memverifikasi prasyarat, atau memverifikasi prasyarat dan memasang sistem file.

- EfsId

Tipe: String

Deskripsi: (Wajib) ID sistem file yang ingin Anda pasang.

- InstanceId

Tipe: String

Deskripsi: (Wajib) ID instans Amazon EC2 tempat Anda ingin memasang sistem file.

- MountOptions

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Direktori tempat Anda ingin memasang sistem file. Jika Anda menentukan `Check` nilai untuk `Action` parameter, parameter ini tidak boleh ditentukan.

- MountTargetIP

Tipe: String

Deskripsi: (Opsional) Alamat IP target mount. Pemasangan berdasarkan alamat IP berfungsi di lingkungan di mana DNS dinonaktifkan, seperti virtual private cloud (VPCs) dengan nama host DNS dinonaktifkan. Selain itu, Anda dapat menggunakan opsi ini jika lingkungan Anda menggunakan penyedia DNS selain Amazon Route 53 (Rute 53).

- Region

Tipe: 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 lebih lanjut tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWS-CreateEKSClusterWithFargateProfile](#)
- [AWS-CreateEKSClusterWithNodegroup](#)
- [AWS-DeleteEKSCluster](#)
- [AWS-MigrateToNewEKSSelfManagedNodeGroup](#)
- [AWSPremiumSupport-TroubleshootEKSCluster](#)
- [AWSSupport-TroubleshootEKSWorkerNode](#)
- [AWS-UpdateEKSCluster](#)
- [AWS-UpdateEKSMangedNodeGroup](#)
- [AWS-UpdateEKSSelfManagedLinuxNodeGroups](#)
- [AWSSupport-CollectEKSLinuxNodeStatistics](#)
- [AWSSupport-CollectEKSInstanceLogs](#)
- [AWSSupport-SetupK8sApiProxyForEKS](#)
- [AWSSupport-TroubleshootEbsCsiDriversForEks](#)
- [AWSSupport-TroubleshootEKSSALBControllerIssues](#)

AWS-CreateEKSClusterWithFargateProfile

Deskripsi

AWS-CreateEKSClusterWithFargateProfileRunbook ini membuat kluster Amazon Elastic Kubernetes Service (Amazon EKS) menggunakan 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama unik untuk cluster.

- ClusterRoleArn

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama profil Fargate.

- `FargateProfileRoleArn`

Tipe: String

Deskripsi: (Wajib) ARN dari peran IAM Eksekusi Amazon EKS Pod.

- `FargateProfileSelectors`

Tipe: String

Deskripsi: (Wajib) Penyeleksi untuk mencocokkan pod dengan profil Fargate.

- `SubnetIds`

Jenis: StringList

Deskripsi: (Wajib) Subnet yang ingin Anda gunakan untuk kluster Amazon EKS Anda. IDs Amazon EKS membuat antarmuka jaringan elastis di subnet ini untuk komunikasi antara node Anda dan bidang kontrol Kubernetes. Anda harus menentukan setidaknya dua subnet IDs.

- `EKSEndpointPrivateAccess`

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.

- `EKSEndpointPublicAccess`

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.

- `PublicAccessCIDRs`

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 titik akhir 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.
- `Verifikasi EKSCluster IsActive` (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`

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama unik untuk cluster.

- ClusterRoleArn

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama unik untuk grup node.

- NodegroupRoleArn

Tipe: String

Deskripsi: (Wajib) ARN dari peran IAM untuk dikaitkan dengan grup node Anda. Daemon kubelet node pekerja Amazon EKS melakukan panggilan atas nama Anda AWS APIs . 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) Subnet yang ingin Anda gunakan untuk klaster Amazon EKS Anda. IDs Amazon EKS membuat antarmuka jaringan elastis di subnet ini untuk komunikasi antara node Anda dan bidang kontrol Kubernetes. Anda harus menentukan setidaknya dua subnet IDs.

- `EKSEndpointPrivateAccess`

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.

- `EKSEndpointPublicAccess`

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.

- `PublicAccessCIDRs`

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 titik akhir 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.
- `Verifikasi EKSCluster IsActive` (`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, 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

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

Tipe: 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.

- EKSClusterNama

Tipe: String

Deskripsi: (Wajib) Nama Cluster Amazon EKS yang akan dihapus.

- VPCCloudFormationStack

Tipe: String

Deskripsi: (Opsional) nama CloudFormation tumpukan untuk VPC untuk kluster EKS yang dihapus. Ini menghapus CloudFormation tumpukan untuk VPC dan sumber daya apa pun yang dibuat oleh tumpukan.

- VPCCloudFormationStackRole

Tipe: String

Deskripsi: (Opsional) ARN dari peran IAM yang CloudFormation mengasumsikan untuk menghapus tumpukan VPC. CloudFormation CloudFormation menggunakan kredensi peran untuk melakukan panggilan atas nama Anda.

- SelfManagedNodeStacks

Tipe: String

Deskripsi: (Opsional) Daftar nama CloudFormation tumpukan yang dipisahkan koma untuk node yang dikelola sendiri, Ini akan menghapus CloudFormation tumpukan untuk node yang dikelola sendiri.

- SelfManagedNodeStacksRole

Tipe: String

Deskripsi: (Opsional) ARN dari peran IAM yang CloudFormation mengasumsikan untuk menghapus Tumpukan Node yang dikelola sendiri. 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- HapusEKSCluster: Hapus kluster EKS.

- `aws:executeScript`- Hapus VPCCloudFormationStack: 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

Tipe: 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.

- OldStackName

Tipe: String

Deskripsi: (Wajib) Nama atau ID tumpukan CloudFormation tumpukan Anda yang ada.

- NewStackName

Tipe: String

Deskripsi: (Opsional) Nama 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`

Tipe: 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 CloudFormation tumpukan yang ada akan digunakan.

- `NodeInstanceType`

Tipe: 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 CloudFormation tumpukan yang ada akan digunakan.

- `NodeGroupName`

Tipe: String

Deskripsi: (Opsional) Nama grup node baru Anda. Jika Anda tidak menentukan nilai untuk parameter ini, nama grup node yang ditentukan dalam CloudFormation tumpukan yang ada akan digunakan.

- `NodeAutoScalingGroupDesiredCapacity`

Tipe: 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 CloudFormation tumpukan yang ada akan digunakan.

- `NodeAutoScalingGroupMaxSize`

Tipe: 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 CloudFormation tumpukan yang ada akan digunakan.

- **NodeAutoScalingGroupMinSize**

Tipe: 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 CloudFormation tumpukan yang ada akan digunakan.

- **NodeImageId**

Tipe: String

Deskripsi: (Opsional) ID dari Amazon Machine Image (AMI) yang Anda inginkan grup node untuk digunakan.

- **NodeImageIdSSMParam**

Tipe: String

Deskripsi: (Opsional) Parameter Systems Manager publik untuk AMI yang Anda inginkan untuk digunakan oleh grup node.

- **NodeVolumeSize**

Tipe: 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 CloudFormation tumpukan yang ada akan digunakan.

- **NodeVolumeType**

Tipe: 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 CloudFormation tumpukan yang ada akan digunakan.

- **KeyName**

Tipe: 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 CloudFormation tumpukan yang ada akan digunakan.

- Subnet

Jenis: StringList

Deskripsi: (Opsional) Daftar subnet yang dipisahkan koma IDs yang ingin Anda gunakan untuk grup node baru Anda. Jika Anda tidak menentukan nilai untuk parameter ini, subnet yang ditentukan dalam CloudFormation tumpukan yang ada akan digunakan.

- Nonaktifkan IMDSv1

Jenis: Boolean

Deskripsi: (Opsional) Tentukan `true` untuk menonaktifkan Layanan Metadata Instans Versi 1 (IMDSv1). Secara default, node mendukung IMDSv1 dan IMDSv2.

- BootstrapArguments

Tipe: 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 CloudFormation tumpukan untuk grup node baru.
- `GetNewStackNodeInstanceRole` (`aws:executeAwsApi`) - Mendapat peran instance node.
- `GetNewStackSecurityGroup` (`aws:executeAwsApi`) - Langkahnya 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:assertAwsResource Properti`) - 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 CloudFormation tumpukan untuk grup node baru.

`CreateStack`. `StackId` - ID CloudFormation tumpukan untuk grup node baru.

AWSPremiumSupport-TroubleshootEKSCluster

Deskripsi

`AWSPremiumSupport-TroubleshootEKSClusterRunbook` mendiagnosis masalah umum dengan klaster Amazon Elastic Kubernetes Service (Amazon EKS), infrastruktur dasar, dan menyediakan langkah-langkah remediasi yang direkomendasikan.

Important

Akses ke `AWSPremiumSupport-*` runbook memerlukan Business + Support, Enterprise Support, atau Unified Operations Subscription. Untuk informasi selengkapnya, lihat [Bandingkan AWS Dukungan Paket](#).

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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama kluster Amazon EKS yang ingin Anda pecahkan masalah.

- S3 BucketName

Tipe: String

Deskripsi: (Wajib) 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 (ACLs) 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 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-TroubleshootEKSTaskWorkerNode

Deskripsi

AWSSupport-TroubleshootEKSTaskWorkerNodeRunbook 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 cluster. 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 kluster Amazon EKS harus `ACTIVE`

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- `AutomationAssumeRole`

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama cluster Amazon EKS.

- WorkerID

Tipe: 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 kluster 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama cluster Amazon EKS Anda.

- Versi

Tipe: 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 menjadiSuccessful.

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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Nama cluster yang grup simpulnya ingin Anda perbarui.

- `NodeGroupName`

Tipe: String

Deskripsi: (Wajib) Nama grup node yang akan diperbarui.

- `UpdateType`

Tipe: 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:

- `AMIReleaseVersi`

Tipe: 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`

Tipe: String

Deskripsi: (Opsional) Versi Kubernetes untuk memperbarui grup node ke.

- `LaunchTemplateId`

Tipe: String

Deskripsi: (Opsional) ID dari template peluncuran.

- `LaunchTemplateName`

Tipe: String

Deskripsi: (Opsional) Nama template peluncuran.

- `LaunchTemplateVersion`

Tipe: 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 kluster 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`

Tipe: 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**

Tipe: String

Deskripsi: (Wajib) Nama cluster Amazon EKS.

- **NodeGroupName**

Tipe: String

Deskripsi: (Wajib) Nama grup node terkelola.

- **ClusterControlPlaneSecurityGroup**

Tipe: String

Deskripsi: (Wajib) ID grup keamanan pesawat kontrol.

- **Nonaktifkan IMDSv1**

Jenis: Boolean

Deskripsi: (Opsional) Menentukan apakah Anda ingin mengizinkan Layanan Metadata Instans Versi 1 (IMDSv1) dan. IMDSv2

- **KeyName**

Tipe: String

Deskripsi: (Opsional) Nama kunci untuk instance.

- **NodeAutoScalingGroupDesiredCapacity**

Tipe: String

Deskripsi: (Opsional) Jumlah node yang harus dipertahankan oleh kelompok node.

- **NodeAutoScalingGroupMaxSize**

Tipe: String

Deskripsi: (Opsional) Jumlah maksimum node yang dapat diskalakan oleh kelompok node.

- **NodeAutoScalingGroupMinSize**

Tipe: String

Deskripsi: (Opsional) Jumlah minimum node yang dapat diskalakan oleh kelompok node.

- `NodeInstanceType`

Tipe: String

Default: `t3.large`

Deskripsi: (Opsional) Jenis instance yang ingin Anda gunakan untuk grup node.

- `NodeImageId`

Tipe: String

Deskripsi: (Opsional) ID dari Amazon Machine Image (AMI) yang Anda inginkan grup node untuk digunakan.

- `NodeImageIdSSMParam`

Tipe: String

Default: `/aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id`

Deskripsi: (Opsional) Parameter Systems Manager publik untuk AMI yang Anda inginkan untuk digunakan oleh grup node.

- `StackName`

Tipe: String

Deskripsi: (Wajib) Nama CloudFormation tumpukan yang digunakan untuk memperbarui grup node.

- `Subnet`

Tipe: String

Deskripsi: (Wajib) Daftar subnet yang IDs dipisahkan koma yang ingin digunakan kluster Anda.

- `VpcId`

Tipe: String

Default: `Default`

Deskripsi: (Wajib) Virtual Private Cloud (VPC) tempat kluster 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 kluster Amazon EKS sesuai dengan nilai yang Anda tentukan untuk parameter input runbook.
- aws:waitForAwsResourceProperty- Menunggu status pembaruan CloudFormation tumpukan dikembalikan.

AWSSupport-CollectEKSLinuxNodeStatistics

Deskripsi

AWSSupport-CollectEKSLinuxNodeStatisticsRunbook mengumpulkan statistik Linux dari instans Amazon EC2 yang merupakan bagian dari kluster Amazon EKS, dan dari wadah yang berjalan pada instance jika ID penampung containerd ditentukan. Instans Amazon EC2 harus dikelola oleh AWS Systems Manager

Statistik Linux tingkat host yang dikumpulkan meliputi:

- Informasi OS.

- Statistik antarmuka jaringan - dari `ethtool` dan `/sys/class/net/interface/statistics` direktori.
- Deskriptor file diperhitungkan.
- Port fana dihitung.
- Sebuah dump `iptables` aturan.
- Periksa tabel `conntrack` lengkap.

Statistik Linux tingkat kontainer meliputi:

- Informasi pengenalan - URI gambar dan label.
- Statistik antarmuka jaringan - dari `ethtool` dan `/sys/class/net/interface/statistics` direktori.
- Traceroute dan DNS menghasilkan jika parameter diisi. `NetworkTargets`
- Jumlah analisis pengambilan paket - Transmisi Ulang TCP, paket Out of Order, dll.

Runbook mengumpulkan data dari berbagai distribusi Linux termasuk Amazon Linux 2, Amazon Linux 2023 dan Debian/Ubuntu. Ini menggunakan versi terbaru dari gambar-gambar berikut dari galeri publik Amazon ECR:

- `amazon-ecs-network-sidecar` gambar untuk mendapatkan akses ke alat pemecahan masalah.
- `aws-cli` gambar untuk mengunggah laporan statistik file JSON dan file pengambilan paket ke bucket Amazon S3 yang ditentukan.

Important

Runbook ini tidak mendukung instance Fargate. Runbook ini mungkin gagal jika instance dimatikan atau terputus selama eksekusi.

Bagaimana cara kerjanya?

Runbook melakukan tindakan berikut:

- Memverifikasi bucket Amazon S3 target tidak memberikan akses baca atau tulis publik.

- Memastikan instans Amazon EC2 target dikelola oleh Systems Manager dan dalam keadaan berjalan.
- Memverifikasi instance menjalankan sistem operasi Linux.
- Mengumpulkan statistik Linux komprehensif dari instans Amazon EC2 dan secara opsional dari wadah tertentu.
- Mengunggah statistik yang dikumpulkan ke bucket Amazon S3 yang ditentukan.

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

AutomationAssumeRoleParameter membutuhkan tindakan berikut:

- s3:GetAccountPublicAccessBlock
- s3:GetBucketPublicAccessBlock
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetBucketLocation
- s3:GetEncryptionConfiguration
- s3:PutObject
- ssm:DescribeInstanceInformation
- ssm:SendCommand
- ssm:GetCommandInvocation
- ec2:DescribeInstances

Contoh kebijakan IAM:

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

```

    "Action": [
        "s3:GetAccountPublicAccessBlock"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::S3_BUCKET_NAME"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::S3_BUCKET_NAME/*"
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:DescribeInstanceInformation"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": [
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ec2:*:111122223333:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetCommandInvocation"
    ]
}

```

```

    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances"
    ],
    "Resource": "*"
  }
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-CollectEKSLinuxNodeStatistics](#) 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 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 Amazon EC2 untuk mengumpulkan statistik.

- S3 BucketName (Diperlukan):

Nama bucket Amazon S3 untuk mengeksport output JSON dari instans Amazon EC2 sebagai file.

- S3 KeyPrefix (Opsional):

Awalan kunci Amazon S3 (sub-folder) untuk mengeksport output JSON dari instans Amazon EC2 sebagai file. Default: `AWSSupport-CollectEKSLinuxNodeStatistics`.

- S3 BucketOwnerRoleArn (Opsional):

ARN peran IAM dengan izin untuk mendapatkan bucket Amazon S3 dan pengaturan pemblokiran akun akses publik, konfigurasi enkripsi bucket, bucket, status kebijakan bucket ACLs, 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).

- **S3 BucketOwnerAccount** (Opsional):

AWS Akun yang memiliki ember Amazon S3. Jika Anda tidak menentukan parameter ini, runbook mengasumsikan bahwa bucket ada di akun ini.

- **ContainerId** (Opsional):

ID penampung yang berjalan pada instans Amazon EC2 yang ditentukan.

- **NetworkTargets** (Opsional):

Daftar IPv4 alamat nama and/or DNS yang dipisahkan koma untuk menguji resolusi DNS, dan konektivitas menggunakan traceroute.

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **CheckBucketAccess:**

Memeriksa apakah bucket Amazon S3 target berpotensi memberikan akses publik baca and/or tulis ke objeknya.

- **AssertInstanceIsSSMManaged:**

Memastikan instans Amazon EC2 target dikelola oleh Systems Manager, jika tidak, otomatisasi akan berakhir.

- **VerifyInstanceState:**

Memverifikasi bahwa instans Amazon EC2 dalam status berjalan sebelum mencoba mengumpulkan statistik.

- **BranchOnVerifyLinuxInstance:**

Memverifikasi bahwa instance tersebut adalah instance Linux sebelum melanjutkan.

- **BranchOnVerifyInstanceRunning:**

Memverifikasi bahwa instance dalam keadaan berjalan sebelum melanjutkan.

- **CollectEKSLinuxNodeStatistics:**

Mengumpulkan statistik Linux komprehensif dari instans Amazon EC2 termasuk informasi OS, statistik antarmuka jaringan, deskriptor file, port sementara, aturan firewall, dan statistik tingkat kontainer opsional.

- **GenerateStatisticsOutputS3Uri:**

Menghasilkan URI Amazon S3 lengkap ke file statistik Linux untuk digunakan sebagai output dokumen otomatisasi.

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

Referensi

Otomatisasi Systems Manager

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

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 Amazon 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

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.

 Note

Otomatisasi ini memerlukan setidaknya 10 persen 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

Linux

Parameter

- AutomationAssumeRole

Tipe: 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.

- EKSIInstanceId

Tipe: String

Deskripsi: (Wajib) ID instans Amazon EC2 Amazon EKS Amazon EC2 tempat Anda ingin mengumpulkan log.

- LogDestination

Tipe: String

Deskripsi: (Opsional) Bucket Amazon Simple Storage Service (Amazon 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

Izin IAM yang diperlukan untuk profil instans Amazon EC2

Profil instans yang digunakan oleh EKSIInstanceId harus memiliki kebijakan terkelola SSMMManagedInstanceCoreAmazon Amazon yang dilampirkan padanya.

Itu juga harus dapat mengakses ember LogDestination Amazon S3 sehingga dapat mengunggah log yang dikumpulkan. Di bawah ini adalah contoh kebijakan IAM yang dapat dilampirkan ke profil instance tersebut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::LogDestination/*",
```

```

        "arn:aws:s3:::LogDestination"
    ]
}
]
}

```

Jika LogDestination menggunakan AWS KMS enkripsi, maka pernyataan tambahan harus ditambahkan ke kebijakan IAM, memberikan akses ke AWS KMS kunci yang digunakan dalam enkripsi:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::LogDestination/*",
        "arn:aws:s3:::LogDestination"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:REGION:ACCOUNT:key/KMS-KEY-ID"
    }
  ]
}

```

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 Amazon S3 yang Anda tentukan dalam `LogDestination` parameter.

AWSSupport-SetupK8sApiProxyForEKS

Deskripsi

Runbook otomatisasi `AWSSupport-SetupK8sApiProxyForEKS` menyediakan cara untuk membuat AWS Lambda fungsi yang bertindak sebagai proxy untuk membuat panggilan API bidang kontrol ke titik akhir kluster Amazon Elastic Kubernetes Service. Ini berfungsi sebagai blok bangunan untuk runbook yang memerlukan pembuatan panggilan API bidang kontrol untuk mengotomatisasi tugas dan memecahkan masalah dengan kluster Amazon EKS.

Important

Semua sumber daya yang dibuat oleh otomatisasi ini ditandai sehingga dapat dengan mudah ditemukan. Tag yang digunakan adalah:

- `AWSSupport-SetupK8sApiProxyForEKS`: benar

Note

- Otomatisasi adalah runbook pembantu dan tidak dapat dieksekusi sebagai runbook mandiri. Ini dipanggil sebagai otomatisasi anak untuk runbook yang memerlukan panggilan API bidang kontrol ke cluster Amazon EKS.
- Pastikan untuk menjalankan `Cleanup` operasi setelah penggunaan untuk menghindari biaya yang tidak diinginkan.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama kluster Amazon Elastic Kubernetes Service.

- Operasi

Tipe: String

Deskripsi: (Wajib) Operasi yang harus dilakukan: Setup ketentuan fungsi Lambda di akun, Cleanup akan membatalkan penyediaan sumber daya yang dibuat sebagai bagian dari fase penyiapan.

Nilai yang Diizinkan: Setup | Cleanup

Default: Pengaturan

- LambdaRoleArn

Tipe: String

Deskripsi: (Opsional) ARN dari peran IAM yang memungkinkan AWS Lambda fungsi untuk mengakses AWS layanan dan sumber daya yang diperlukan. Jika tidak ada peran yang ditentukan, Otomasi Systems Manager ini akan membuat satu peran IAM untuk Lambda di akun Anda dengan Automation-K8sProxy-Role-<ExecutionId> nama yang menyertakan kebijakan AWSLambdaBasicExecutionRole terkelola: dan. AWSLambdaVPCLambdaAccessExecutionRole

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Memvalidasi bahwa otomatisasi berjalan sebagai eksekusi anak. Runbook tidak akan berfungsi saat dipanggil sebagai runbook mandiri karena tidak melakukan pekerjaan yang berarti sendiri.
- Memeriksa CloudFormation tumpukan yang ada untuk fungsi Lambda proxy untuk cluster yang ditentukan.
 - Jika tumpukan ada, infrastruktur yang ada digunakan kembali alih-alih membuatnya kembali.
 - Penghitung referensi dipertahankan menggunakan tag untuk memastikan runbook tidak menghapus infrastruktur jika digunakan kembali oleh runbook lain untuk cluster yang sama.
- Lakukan jenis operasi (Setup/Cleanup) yang ditentukan untuk pemanggilan:
 - Pengaturan: Membuat atau menjelaskan sumber daya yang ada.

Pembersihan: Menghapus sumber daya yang disediakan, jika infrastruktur tidak digunakan oleh runbook lain.

Izin IAM yang Diperlukan

AutomationAssumeRoleParameter membutuhkan izin berikut yang diberikan tidak LambdaRoleArn diteruskan:

- `cloudformation:CreateStack`
- `cloudformation:DescribeStacks`
- `cloudformation>DeleteStack`
- `cloudformation:UpdateStack`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2>DeleteNetworkInterface`
- `eks:DescribeCluster`
- `lambda:CreateFunction`

- `lambda:DeleteFunction`
- `lambda:ListTags`
- `lambda:GetFunction`
- `lambda:ListTags`
- `lambda:TagResource`
- `lambda:UntagResource`
- `lambda:UpdateFunctionCode`
- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:TagResource`
- `logs:UntagResource`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:ListTagsForResource`
- `iam:CreateRole`
- `iam:AttachRolePolicy`
- `iam:DetachRolePolicy`
- `iam:PassRole`
- `iam:GetRole`
- `iam>DeleteRole`
- `iam:TagRole`
- `iam:UntagRole`
- `tag:GetResources`
- `tag:TagResources`

Ketika `LambdaRoleArn` disediakan, otomatisasi tidak perlu membuat peran dan izin berikut dapat dikecualikan:

- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:TagRole`

- iam:UntagRole
- iam:AttachRolePolicy
- iam:DetachRolePolicy

Di bawah ini adalah contoh kebijakan yang menunjukkan izin yang diperlukan untuk AutomationAssumeRole saat tidak LambdaRoleArn diteruskan:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "eks:DescribeCluster",
        "iam:GetRole",
        "cloudformation:DescribeStacks",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "lambda:GetFunction",
        "lambda:ListTags",
        "logs:ListTagsForResource"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowActionsWithoutConditions"
    },
    {
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
      }
    }
  ]
}
```

```

    },
    "Action": "iam:CreateRole",
    "Resource": [
        "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "AllowCreateRoleWithRequiredTag"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": [
        "iam>DeleteRole",
        "iam:TagRole",
        "iam:UntagRole"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "IAMActions"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        },
        "StringLike": {
            "iam:PolicyARN": [
                "arn:aws:iam::111122223333:policy/service-role/
AWSLambdaBasicExecutionRole",
                "arn:aws:iam::111122223333:policy/service-role/
AWSLambdaVPCLAccessExecutionRole"
            ]
        }
    },
    "Action": [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
    ],
    "Resource": [

```

```

        "arn:aws:iam:111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "AttachRolePolicy"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode"
    ],
    "Resource": "arn:aws:lambda:us-east-1:111122223333:function:Automation-K8sProxy*",
    "Effect": "Allow",
    "Sid": "LambdaActions"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
    ],
    "Resource": "arn:aws:cloudformation:us-east-1:111122223333:stack/AWSSupport-SetupK8sApiProxyForEKS*",
    "Effect": "Allow",
    "Sid": "CloudFormationActions"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    }
}

```

```

    },
    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource"
    ],
    "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/Automation-K8sProxy*",
        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/Automation-K8sProxy*:*"
    ],
    "Effect": "Allow",
    "Sid": "LogsActions"
},
{
    "Condition": {
        "StringLikeIfExists": {
            "iam:PassedToService": "lambda.amazonaws.com"
        }
    },
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam:111122223333:role/Automation-K8sProxy-Role*"
    ],
    "Effect": "Allow",
    "Sid": "PassRoleToLambda"
}
]
}

```

Jika diteruskan, pastikan bahwa ia memiliki [AWSLambdaBasicExecutionRole](#) kebijakan yang melekat padanya untuk kluster publik dan tambahan, [AWSLambdaVPCLambdaAccessExecutionRole](#) untuk kluster pribadi. LambdaRoleArn

Sumber Daya Dibuat

Sumber daya berikut dibuat selama Setup operasi:

1. AWS Lambda fungsi
2. Peran IAM: Peran eksekusi Lambda, jika tidak disediakan.
3. CloudWatch Grup Log (Lambda Log)

Fungsi Lambda dan peran eksekusi dipertahankan sampai *Cleanup* operasi dijalankan. Grup log Lambda akan disimpan selama 30 hari atau hingga dihapus secara manual.

Instruksi

Runbook adalah utilitas pembantu yang dirancang untuk dieksekusi dari dalam runbook lain sebagai otomatisasi anak. Ini memfasilitasi pembuatan infrastruktur yang memungkinkan runbook induk untuk membuat panggilan API bidang kontrol Amazon EKS K8s. Untuk menggunakan runbook, Anda dapat mengikuti langkah-langkah di bawah ini dari konteks otomatisasi induk.

1. Fase Pengaturan: Memanggil otomatisasi menggunakan operasi `aws:executeAutomation` tindakan dari runbook yang ingin membuat panggilan API bidang kontrol Amazon EKS K8s dengan operasi disetel ke. Setup

Contoh parameter input:

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Setup"
}
```

Output dari `aws:executeAutomation` langkah akan berisi ARN dari fungsi Lambda proxy.

2. Menggunakan Proxy Lambda: Panggil fungsi Lambda di dalam `aws:executeScript` tindakan menggunakan boto3's `Lambda.Client.invoke(...)` dengan daftar jalur panggilan API dan token pembawa. Fungsi Lambda akan melakukan GET panggilan HTTP ke jalur yang ditentukan dengan meneruskan token pembawa sebagai bagian dari header otorisasi.

Contoh acara pemanggilan Lambda:

```
{
  "ApiCalls": ["/api/v1/pods/", ...],
  "BearerToken": "..."
```

```
}
```

Note

Token pembawa harus dihasilkan sebagai bagian dari skrip otomatisasi induk. Anda perlu memastikan bahwa prinsipal yang menjalankan runbook induk memiliki izin hanya-baca ke kluster Amazon EKS yang ditentukan.

3. Fase Pembersihan: Memanggil otomatisasi menggunakan operasi `aws:executeAutomation` tindakan dari runbook yang ingin membuat panggilan API bidang kontrol Amazon EKS K8s dengan operasi disetel ke `Cleanup`

Contoh parameter input:

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Cleanup"
}
```

Langkah Otomasi

1. ValidateExecution

- Memverifikasi bahwa otomatisasi tidak berjalan sebagai eksekusi mandiri.

2. CheckForExistingStack

- Memeriksa apakah CloudFormation tumpukan sudah disediakan untuk nama cluster yang ditentukan.
- Mengembalikan status keberadaan tumpukan dan apakah aman untuk dihapus.

3. BranchOnIsStackExists

- Langkah keputusan yang bercabang berdasarkan keberadaan tumpukan.
- Rute untuk memperbarui nama tumpukan yang ada atau melanjutkan dengan percabangan operasi.

4. UpdateStackName

- Memperbarui `StackName` variabel dengan nama tumpukan yang ada.
- Hanya dieksekusi jika tumpukan sudah ada.

5. BranchOnOperation

- Rutekan otomatisasi berdasarkan Operation parameter (Setup/Cleanup).
- UntukSetup: Rute untuk membuat tumpukan baru atau menjelaskan sumber daya yang ada.
- UntukCleanup: Lanjutkan ke penghapusan tumpukan jika aman untuk dihapus.

6. GetClusterNetworkConfig

- Menjelaskan cluster Amazon EKS untuk mendapatkan konfigurasi VPC.
- Mengambil titik akhir, ID VPC, subnet, ID grup keamanan IDs, dan data CA.

7. ProvisionResources

- Membuat CloudFormation tumpukan dengan sumber daya yang dibutuhkan.
- Ketentuan fungsi Lambda dengan konfigurasi jaringan yang diperlukan.
- Menandai semua sumber daya untuk pelacakan dan manajemen.

8. DescribeStackResources

- Mengambil informasi tentang created/existing tumpukan.
- Mendapat ARN dari fungsi Lambda yang disediakan.

9. BranchOnIsLambdaDeploymentRequired

- Menentukan apakah penyebaran kode Lambda diperlukan.
- Hanya melanjutkan ke penerapan untuk tumpukan yang baru dibuat.

10DeployLambdaFunctionCode

- Menyebarkan kode fungsi Lambda menggunakan paket penerapan.
- Memperbarui fungsi dengan implementasi proxy.

11AssertLambdaAvailable

- Memverifikasi bahwa pembaruan kode fungsi Lambda berhasil.
- Menunggu fungsi berada dalam Successful keadaan.

12PerformStackCleanup

- Menghapus CloudFormation tumpukan dan sumber daya terkait.
- Dieksekusi selama Cleanup operasi atau pada kegagalan Setup operasi.

Keluaran

LambdaFunctionArn: ARN dari fungsi Lambda proxy

Referensi

Otomatisasi Systems Manager

- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow](#)

AWSSupport-TroubleshootEbsCsiDriversForEks

Deskripsi

AWSSupport-TroubleshootEbsCsiDriversForEksRunbook membantu memecahkan masalah dengan pemasangan volume Amazon Elastic Block Store di Amazon Elastic Kubernetes Service (Amazon EKS) dan masalah driver Amazon EBS Container Storage Interface (CSI)

Important

Saat ini Driver Amazon EBS CSI yang berjalan tidak AWS Fargate didukung.

Bagaimana cara kerjanya?

Runbook AWSSupport-TroubleshootEbsCsiDriversForEks melakukan langkah-langkah tingkat tinggi berikut:

- Memverifikasi apakah kluster Amazon EKS target ada dan dalam status aktif.
- Menerapkan sumber daya autentikasi yang diperlukan untuk membuat panggilan API Kubernetes berdasarkan apakah addon tersebut dikelola Amazon EKS atau dikelola sendiri.
- Melakukan pemeriksaan kesehatan dan diagnostik pengontrol Amazon EBS CSI.
- Menjalankan pemeriksaan izin IAM pada peran node dan peran akun layanan.
- Mendiagnosis masalah pembuatan volume persisten untuk pod aplikasi yang ditentukan.
- Memeriksa node-to-pod penjadwalan dan memeriksa peristiwa pod.
- Mengumpulkan Kubernetes dan log aplikasi yang relevan, mengunggahnya ke bucket Amazon S3 yang ditentukan.
- Melakukan pemeriksaan kesehatan node dan memverifikasi konektivitas dengan titik akhir Amazon EC2.
- Meninjau lampiran perangkat blok volume persisten dan status pemasangan.

- Membersihkan infrastruktur otentikasi yang dibuat selama pemecahan masalah.
- Menghasilkan laporan pemecahan masalah komprehensif yang menggabungkan semua hasil diagnostik.

Note

- Mode otentikasi kluster Amazon EKS harus disetel ke salah satu API atau `API_AND_CONFIG_MAP`. Kami merekomendasikan menggunakan entri Amazon EKS Access. Runbook memerlukan izin Kubernetes Role-based access control (RBAC) untuk melakukan panggilan API yang diperlukan.
- Jika Anda tidak menentukan peran IAM untuk fungsi Lambda `LambdaRoleArn` (parameter), otomatisasi akan membuat peran `Automation-K8sProxy-Role-<ExecutionId>` bernama di akun Anda. Peran ini mencakup kebijakan yang dikelola `AWSLambdaBasicExecutionRole` dan `AWSLambdaVPCLambdaAccessExecutionRole`.
- Beberapa langkah diagnostik mengharuskan node pekerja Amazon EKS menjadi instans yang dikelola Systems Manager. Jika node bukan instance terkelola Systems Manager, langkah-langkah yang memerlukan akses Systems Manager akan dilewati, tetapi pemeriksaan lain berlanjut.
- Otomatisasi mencakup langkah pembersihan yang menghapus sumber daya infrastruktur otentikasi. Langkah pembersihan ini berjalan bahkan ketika langkah sebelumnya gagal, yang membantu mencegah sumber daya yatim piatu di akun Anda. AWS

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeInstanceStatus`
- `ec2:GetEbsEncryptionByDefault`
- `eks:DescribeAddon`
- `eks:DescribeAddonVersions`
- `eks:DescribeCluster`
- `iam:GetInstanceProfile`
- `iam:GetOpenIDConnectProvider`
- `iam:GetRole`
- `iam:ListOpenIDConnectProviders`
- `iam:SimulatePrincipalPolicy`
- `s3:GetBucketLocation`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketVersioning`
- `s3:ListBucket`
- `s3:ListBucketVersions`
- `ssm:DescribeInstanceInformation`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Buat peran otomatisasi SSM `TroubleshootEbsCsiDriversForEks-SSM-Role` di akun Anda. Verifikasi bahwa hubungan kepercayaan berisi kebijakan berikut.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Lampirkan kebijakan di bawah ini ke peran IAM untuk memberikan izin yang diperlukan untuk melakukan tindakan yang ditentukan pada sumber daya yang ditentukan.
 - Jika Anda mengharapkan untuk mengunggah eksekusi dan log sumber daya ke bucket Amazon S3 di wilayah AWS yang sama, `arn:{partition}:s3::BUCKET_NAME/*` ganti seperti milik Anda. `OptionalRestrictPutObjects`
 - Bucket Amazon S3 harus mengarah ke bucket Amazon S3 yang benar jika Anda akan `S3BucketName` memilih dalam eksekusi SSM.
 - Izin ini opsional jika Anda tidak menentukan `S3BucketName`
 - Bucket Amazon S3 harus bersifat pribadi dan di AWS wilayah yang sama tempat Anda menjalankan otomatisasi SSM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OptionalRestrictPutObjects",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ]
    }
  ]
}
```

```

        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeIamInstanceProfileAssociations",
            "ec2:DescribeInstanceStatus",
            "ec2:GetEbsEncryptionByDefault",
            "eks:DescribeAddon",
            "eks:DescribeAddonVersions",
            "eks:DescribeCluster",
            "iam:GetInstanceProfile",
            "iam:GetOpenIDConnectProvider",
            "iam:GetRole",
            "iam:ListOpenIDConnectProviders",
            "iam:SimulatePrincipalPolicy",
            "s3:GetBucketLocation",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketVersioning",
            "s3:ListBucket",
            "s3:ListBucketVersions",
            "ssm:DescribeInstanceInformation",
            "ssm:GetAutomationExecution",
            "ssm:GetDocument",
            "ssm:ListCommandInvocations",
            "ssm:ListCommands",
            "ssm:SendCommand",
            "ssm:StartAutomationExecution"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SetupK8sApiProxyForEKSActions",
        "Effect": "Allow",
        "Action": [
            "cloudformation:CreateStack",
            "cloudformation>DeleteStack",
            "cloudformation:DescribeStacks",
            "cloudformation:UpdateStack",
            "ec2:CreateNetworkInterface",
            "ec2>DeleteNetworkInterface",

```

```

        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:GetRole",
        "iam:TagRole",
        "iam:UntagRole",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource",
        "ssm:DescribeAutomationExecutions",
        "tag:GetResources",
        "tag:TagResources"
    ],
    "Resource": "*"
},
{
    "Sid": "PassRoleToAutomation",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
        "arn:aws:iam::*:role/TroubleshootEbsCsiDriversForEks-SSM-Role",
        "arn:aws:iam::*:role/Automation-K8sProxy-Role-*"
    ],
    "Condition": {
        "StringLikeIfExists": {

```

```

        "iam:PassedToService": [
            "lambda.amazonaws.com",
            "ssm.amazonaws.com"
        ]
    },
    {
        "Sid": "AttachRolePolicy",
        "Effect": "Allow",
        "Action": [
            "iam:AttachRolePolicy",
            "iam:DetachRolePolicy"
        ],
        "Resource": "*",
        "Condition": {
            "StringLikeIfExists": {
                "iam:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
            }
        }
    }
]
}

```

3. Berikan izin yang diperlukan untuk Amazon EKS cluster RBAC (Role-Based Access Control). Pendekatan yang disarankan adalah membuat Entri Akses di kluster Amazon EKS Anda.

Di konsol Amazon EKS, navigasikan ke cluster Anda. Untuk entri akses Amazon EKS, verifikasi konfigurasi akses Anda disetel ke `API_AND_CONFIG_MAP` atau `API`. Untuk langkah-langkah mengonfigurasi mode autentikasi untuk entri akses, lihat [Menyiapkan entri akses](#).

Pilih Buat entri akses.

- Untuk ARN utama IAM, pilih peran IAM yang Anda buat untuk otomatisasi SSM pada langkah sebelumnya.
- Untuk Jenis, pilih `Standard`.

4. Tambahkan kebijakan akses:

- Untuk cakupan Akses, pilih `Cluster`.
- Untuk nama Kebijakan, pilih `AmazonEKSAAdminViewPolicy`.

Pilih Tambahkan kebijakan.

Jika Anda tidak menggunakan entri akses untuk mengelola izin API Kubernetes, Anda harus memperbarui `aws-auth ConfigMap` dan membuat ikatan peran antara pengguna atau peran IAM Anda. Pastikan entitas IAM Anda memiliki izin API Kubernetes hanya-baca berikut:

- DAPATKAN `/apis/apps/v1/namespaces/{namespace}/deployments/{name}`
- DAPATKAN `/apis/apps/v1/namespaces/{namespace}/replicasets/{name}`
- DAPATKAN `/apis/apps/v1/namespaces/{namespace}/daemonsets/{name}`
- DAPATKAN `/api/v1/nodes/{name}`
- DAPATKAN `/api/v1/namespaces/{namespace}/serviceaccounts/{name}`
- DAPATKAN `/api/v1/namespaces/{namespace}/persistentvolumeclaims/{name}`
- DAPATKAN `/api/v1/persistentvolumes/{name}`
- DAPATKAN `/apis/storage.k8s.io/v1/storageclasses/{name}`
- DAPATKAN `/api/v1/namespaces/{namespace}/pods/{name}`
- DAPATKAN `/api/v1/namespaces/{namespace}/pods`
- DAPATKAN `/api/v1/namespaces/{namespace}/pods/{name}/log`
- DAPATKAN `/api/v1/events`

5. Jalankan otomatisasi [AWSSupport-TroubleshootEbsCsiDriversForEks \(konsol\)](#)

6. Pilih Jalankan otomatisasi.

7. Untuk parameter input, masukkan yang berikut ini:

- `AutomationAssumeRole` (Opsional):
 - Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan SSM Automation untuk melakukan tindakan atas nama Anda. Peran tersebut perlu ditambahkan ke entri akses kluster Amazon EKS atau izin RBAC untuk mengizinkan panggilan API Kubernetes.
 - Tipe: `AWS::IAM::Role::Arn`
 - Contoh: `TroubleshootEbsCsiDriversForEks-SSM-Role`
- `EksClusterName`:
 - Deskripsi: Nama kluster target Amazon Elastic Kubernetes Service (Amazon EKS).
 - Tipe: `String`
- `ApplicationPodName`:
 - Deskripsi: Nama pod aplikasi Kubernetes mengalami masalah dengan driver Amazon EBS

- Tipe: String
- ApplicationNamespace:
 - Deskripsi: Namespace Kubernetes untuk pod aplikasi mengalami masalah dengan driver Amazon EBS CSI.
 - Tipe: String
- EbsCsiControllerDeploymentName(Optional):
 - Deskripsi: (Opsional) Nama penerapan untuk pod pengontrol Amazon EBS CSI.
 - Tipe: String
 - Default: ebs-csi-controller
- EbsCsiControllerNamespace(Optional):
 - Deskripsi: (Opsional) Namespace Kubernetes untuk pod pengontrol Amazon EBS CSI.
 - Tipe: String
 - Default: kube-system
- S3 BucketName (Optional):
 - Deskripsi: (Opsional) Nama bucket Amazon S3 target tempat log pemecahan masalah akan diunggah.
 - Tipe: AWS::S3::Bucket::Name
- LambdaRoleArn (Optional):
 - Deskripsi: (Opsional) ARN dari peran IAM yang memungkinkan AWS Lambda fungsi untuk mengakses AWS layanan dan sumber daya yang diperlukan.
 - Tipe: AWS::IAM::Role::Arn

Pilih Jalankan.

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

Referensi

Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)

Untuk informasi selengkapnya tentang Driver Amazon EBS CSI, lihat Driver [Amazon EBS CSI](#).

AWSSupport-TroubleshootEKSALBControllerIssues

Deskripsi

Runbook AWSSupport-TroubleshootEKSALBControllerIssues otomatisasi membantu mendiagnosis masalah umum yang mencegah AWS Load Balancer Controller menyediakan dan mengelola Application Load Balancer (ALB) dan Network Load Balancer (NLB) dengan benar untuk masuk dan layanan Kubernetes.

Runbook ini melakukan end-to-end validasi komponen penting termasuk pengaturan penyedia identitas OIDC, konfigurasi IRSA, prasyarat jaringan, konfigurasi, dan kuota sumber daya. ingress/service Ini juga menangkap log pengontrol dan konfigurasi sumber daya Kubernetes yang relevan untuk membantu mengidentifikasi kesalahan konfigurasi atau masalah operasional.

Important

Runbook otomatisasi ini dirancang untuk kluster Amazon EKS menggunakan grup node Amazon Elastic Compute Cloud (Amazon EC2) dan saat ini tidak mendukung cluster yang berjalan. AWS Fargate

Bagaimana cara kerjanya?

Runbook AWSSupport-TroubleshootEKSALBControllerIssues melakukan langkah-langkah tingkat tinggi berikut:

- Memvalidasi status kluster Amazon EKS, konfigurasi entri akses, dan penyiapan penyedia OIDC.
- Membuat proxy Lambda sementara untuk komunikasi API Kubernetes.
- Memeriksa penyebaran AWS Load Balancer Controller dan konfigurasi akun layanan.
- Memverifikasi webhook identitas pod dan injeksi peran IAM.
- Memvalidasi konfigurasi subnet dan penandaan untuk Application Load Balancer dan penyediaan Network Load Balancer.
- Memeriksa kuota akun Application Load Balancer dan Network Load Balancer terhadap penggunaan saat ini.
- Memvalidasi anotasi sumber daya masuk dan layanan.
- Memeriksa penandaan grup keamanan node pekerja untuk integrasi penyeimbang beban.

- Mengumpulkan log pod pengontrol untuk diagnostik.
- Membersihkan sumber daya otentikasi sementara.
- Menghasilkan laporan diagnostik dengan temuan dan langkah-langkah remediasi.

Note

- Cluster Amazon EKS harus memiliki entri akses yang dikonfigurasi untuk entitas IAM yang menjalankan otomatisasi ini. Mode otentikasi cluster harus diatur ke salah satu API atau API_AND_CONFIG_MAP. Tanpa konfigurasi entri akses yang tepat, otomatisasi akan berakhir selama validasi awal.
- LambdaRoleArnParameter diperlukan dan harus memiliki kebijakan AWS terkelola AWSLambdaBasicExecutionRole dan AWSLambdaVPCLambdaAccessExecutionRole dilampirkan untuk memungkinkan fungsi proxy berkomunikasi dengan Kubernetes API.
- AWS Load Balancer Controller harus versi v2.1.1 atau yang lebih baru.
- Otomatisasi mencakup langkah pembersihan yang menghapus sumber daya infrastruktur otentikasi sementara. Langkah pembersihan ini berjalan bahkan ketika langkah-langkah sebelumnya gagal, memastikan tidak ada sumber daya yatim piatu yang tersisa di akun Anda. AWS

Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateStack`
- `ec2:CreateNetworkInterface`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `eks:DescribeCluster`
- `eks:ListAssociatedAccessPolicies`
- `elasticloadbalancing:DescribeAccountLimits`
- `elasticloadbalancing:DescribeLoadBalancers`
- `iam:GetRole`
- `iam:ListOpenIDConnectProviders`
- `iam:PassRole`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:GetFunction`
- `lambda:InvokeFunction`
- `lambda:ListTags`
- `lambda:TagResource`
- `lambda:UntagResource`
- `lambda:UpdateFunctionCode`
- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:DescribeLogGroups`

- logs:DescribeLogStreams
- logs:ListTagsForResource
- logs:PutLogEvents
- logs:PutRetentionPolicy
- logs:TagResource
- logs:UntagResource
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- tag:GetResources
- tag:TagResources

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi dan menjalankan otomatisasi:

Note

Sebelum menjalankan otomatisasi, ikuti langkah-langkah berikut untuk mengonfigurasi peran IAM yang diperlukan: satu untuk Systems Manager Automation untuk menjalankan runbook, dan satu lagi untuk Lambda untuk berkomunikasi dengan Kubernetes API:

1. Buat peran otomatisasi SSM TroubleshootEKSALBController-SSM-Role di akun Anda. Verifikasi bahwa hubungan kepercayaan berisi kebijakan berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

}

2. Lampirkan kebijakan IAM berikut untuk memberikan izin yang diperlukan:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "TroubleshootEKSSALBControllerIssuesActions",
    "Effect": "Allow",
    "Action": [
      "eks:DescribeCluster",
      "eks:ListAssociatedAccessPolicies",
      "iam:GetRole",
      "iam:ListOpenIDConnectProviders",
      "ssm:StartAutomationExecution",
      "ssm:GetAutomationExecution",
      "ssm:DescribeAutomationExecutions",
      "ec2:DescribeSubnets",
      "ec2:DescribeRouteTables",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeAccountLimits",
      "ec2:DescribeInstances",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups"
    ],
    "Resource": "*"
  },
  {
    "Sid": "SetupK8sApiProxyForEKSActions",
    "Effect": "Allow",
    "Action": [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:UpdateStack",
      "ec2:CreateNetworkInterface",
      "ec2>DeleteNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "eks:DescribeCluster",
      "iam:GetRole",
```

```

        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource",
        "ssm:DescribeAutomationExecutions",
        "tag:GetResources",
        "tag:TagResources"
    ],
    "Resource": "*"
},
{
    "Sid": "PassRoleToAutomation",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringLikeIfExists": {
            "iam:PassedToService": [
                "lambda.amazonaws.com",
                "ssm.amazonaws.com"
            ]
        }
    }
}]
}

```

3. Konfigurasi entri akses untuk kluster Amazon EKS Anda. Ini adalah persyaratan wajib untuk otomatisasi. Untuk langkah-langkah mengonfigurasi mode autentikasi untuk entri akses, lihat [Menyiapkan entri akses](#).

Di konsol Amazon EKS, navigasikan ke cluster Anda dan ikuti langkah-langkah berikut:

- Di bagian Access, verifikasi konfigurasi autentikasi Anda diatur ke salah satu API atau `API_AND_CONFIG_MAP`.
 - Pilih Buat entri akses dan konfigurasi:
 - Untuk ARN utama IAM, pilih peran IAM yang Anda buat ().
`TroubleshootEKSALBController-SSM-Role`
 - Untuk Jenis, pilih `Standard`.
 - Tambahkan kebijakan akses:
 - Untuk nama Kebijakan, pilih `AmazonEKSAAdminViewPolicy`.
 - Untuk cakupan Akses, pilih `Cluster`.
 - Pilih Tambahkan kebijakan.
 - Verifikasi detailnya dan pilih Buat.
4. Buat peran IAM untuk fungsi Lambda (direferensikan `LambdaRoleArn` seperti pada parameter input):
- Buat peran IAM baru dengan kebijakan kepercayaan berikut:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- Lampirkan kebijakan AWS terkelola berikut ke peran ini:
 - `AWSLambdaBasicExecutionRole`
 - `AWSLambdaVPCLambdaAccessExecutionRole`
- Perhatikan ARN dari peran ini karena Anda akan membutuhkannya untuk parameter `LambdaRoleArn` input.

1. Arahkan ke [AWSSupport-TroubleshootEKSALBControllerIssues](#) konsol AWS Systems Manager.
2. Pilih Eksekusi otomatisasi.
3. Untuk parameter input masukkan yang berikut ini:

- AutomationAssumeRole (Opsional):

Jenis: AWS::IAM::Role: :Arn

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.

Pola yang Diizinkan: ^arn :(? :aws|aws-cn|aws-us-gov) :iam::\ d {12} :peran/? [A-Za-Z_0-9+=, .@ \ -_ /] +\$

- EksClusterName (Diperlukan):

Tipe: String

Deskripsi: (Wajib) Nama klaster Amazon Elastic Kubernetes Service (Amazon EKS).

Pola yang Diizinkan: ^ [0-9A-Za-Z] [A-Za-z0-9-_] {0,99} \$

- ALBControllerDeploymentName (Opsional):

Tipe: String

Deskripsi: (Opsional) Nama penerapan AWS Load Balancer Controller di klaster Amazon EKS Anda. Ini biasanya 'aws-load-balancer-controller' kecuali Anda telah menyesuaikannya selama instalasi.

Pola yang Diizinkan: ^ [a-z0-9] ([-a-z0-9] {0,251} [a-z0-9])? \$

Default: aws-load-balancer-controller

- ALBControllerNamespace (Opsional):

Tipe: String

Deskripsi: (Opsional) Namespace Kubernetes tempat Load Balancer AWS Controller di-deploy. Secara default, ini adalah 'kube-system', tetapi mungkin berbeda jika Anda telah menginstal controller di namespace khusus.

Pola yang Diizinkan: `^[a-z0-9]([-a-z0-9]{0,61}[a-z0-9])?$`

Default: kube-system

- ServiceAccountName (Opsional):

Tipe: String

Deskripsi: (Opsional) Nama Akun Layanan Kubernetes yang terkait dengan Load Balancer AWS Controller. Ini biasanya 'aws-load-balancer-controller' kecuali disesuaikan selama instalasi.

Pola yang Diizinkan: `^[a-z0-9]([a-z0-9]{0,251}[a-z0-9])?$`

Default: aws-load-balancer-controller

- ServiceAccountNamespace (Opsional):

Tipe: String

Deskripsi: (Opsional) Namespace Kubernetes tempat Account Service untuk Load Balancer AWS Controller berada. Ini biasanya 'kube-system', tetapi mungkin berbeda jika Anda telah menggunakan namespace khusus.

Pola yang Diizinkan: `^[a-z0-9]([-a-z0-9]{0,61}[a-z0-9])?$`

Default: kube-system

- IngressName (Opsional):

Tipe: String

Deskripsi: (Opsional) Nama sumber daya Ingress untuk divalidasi (Application Load Balancer). Jika tidak ditentukan, validasi Ingress akan dilewati.

Pola yang Diizinkan: `^[a-z0-9]([a-z0-9]{0,251}[a-z0-9])?$`

Default: "" (string kosong)

- IngressNamespace (Opsional):

Tipe: String

Deskripsi: (Opsional) Namespace dari sumber daya Ingress. Diperlukan IngressName jika ditentukan.

Pola yang Diizinkan: `^$|^ [a-z0-9] [a-z0-9-] {0,61} [a-z0-9] $`

Default: "" (string kosong)

- **ServiceName (Opsional):**

Tipe: String

Deskripsi: (Opsional) Nama sumber daya Layanan tertentu untuk memvalidasi anotasi Network Load Balancer (Network Load Balancer). Jika tidak ditentukan, validasi sumber daya layanan akan dilewati.

Pola yang Diizinkan: `^$|^ [a-z0-9] [a-z0-9-] {0,251} [a-z0-9] $`

Default: "" (string kosong)

- **ServiceNamespace (Opsional):**

Tipe: String

Deskripsi: (Opsional) Namespace sumber daya Layanan. Diperlukan **ServiceName** jika ditentukan.

Pola yang Diizinkan: `^$|^ [a-z0-9] [a-z0-9-] {0,61} [a-z0-9] $`

Default: "" (string kosong)

- **LambdaRoleArn (Diperlukan):**

Jenis: `AWS::IAM::Role` :Arn

Deskripsi: (Wajib) ARN dari peran IAM yang memungkinkan fungsi (AWS Lambda Lambda) untuk mengakses layanan dan sumber daya yang diperlukan. AWS Kaitkan kebijakan AWS terkelola: `AWSLambdaBasicExecutionRole` dan `AWSLambdaVPCAccessExecutionRole` ke peran IAM eksekusi fungsi lambda Anda.

Pola yang Diizinkan: `^arn :(? :aws|aws-cn|aws-us-gov) :iam::\ d {12} :peran/? [A-Za-Z_0-9+=, .@ \ -_/] +$`

4. Pilih Eksekusi.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

a. `ValidateAccessEntryAndOIDCProvider`:

Memvalidasi penyiapan IAM cluster Amazon EKS dengan memeriksa izin entri akses dan konfigurasi penyedia OIDC.

b. `SetupK8sAuthenticationClient`:

Jalankan SAW Document `AWSSupport-SetupK8sApiProxy FOREKS` untuk menyiapkan fungsi lambda untuk menjalankan panggilan Amazon EKS API di cluster.

c. Verifikasi `ALBController` Dan `IRSASetup`:

Memeriksa apakah pengontrol Service Account & Application Load Balancer yang diberikan ada di ruang nama masing-masing. Juga memeriksa kebijakan Anotasi Peran & Kepercayaan Akun Layanan Pengontrol Application Load Balancer.

d. `VerifyPodIdentityWebhookAndEnv`:

Memeriksa `pod-identity-webhook` apakah sedang berjalan. Juga memeriksa apakah IRSA disuntikkan ke variabel ENV pod.

e. `ValidateSubnetRequirements`:

Periksa setidaknya dua subnet dalam dua AZ dengan 8 IP yang tersedia, penandaan subnet yang tepat ada untuk public/private penyeimbang beban.

f. `CheckLoadBalancerLimitsAndUsage`:

Bandingkan limit akun dengan jumlah Application Load Balancer dan Network Load Balancer.

g. `CheckIngressOrServiceAnnotations`:

Memeriksa anotasi dan spesifikasi yang benar dalam sumber daya Ingress dan Service untuk memastikan mereka dikonfigurasi dengan benar untuk Application Load Balancer dan penggunaan Network Load Balancer.

h. `CheckWorkerNodeSecurityGroupTags`:

Verifikasi bahwa tepat satu grup keamanan yang dilampirkan ke node pekerja memiliki tag cluster yang diperlukan.

i. Tangkap `ALBController` Log:

Mengambil log diagnostik terbaru dari pod AWS Load Balancer Controller yang berjalan di cluster Amazon EKS.

j. `sAuthenticationClientBersihUPK8`:

Mengeksekusi Dokumen SAW 'AWSSupport-SetupK8 sApiProxy FOREKS' menggunakan operasi 'Pembersihan' untuk membersihkan sumber daya yang dibuat sebagai bagian dari otomatisasi.

k. `GenerateReport`:

Menghasilkan laporan otomatisasi.

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

a. Laporkan:

Memberikan ringkasan komprehensif dari semua pemeriksaan yang dilakukan, termasuk status kluster Amazon EKS, pengaturan Application Load Balancer Controller, konfigurasi IRSA, persyaratan subnet, batas penyeimbang beban, ingress/service anotasi, tag grup keamanan node pekerja, dan log Application Load Balancer Controller. Ini juga mencakup masalah yang diidentifikasi dan langkah-langkah perbaikan yang direkomendasikan.

Referensi

Otomatisasi Systems Manager

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

Dokumentasi yang berkaitan dengan AWS Load Balancer Controller

- [AWS Pengontrol Load Balancer](#)
- [Menyiapkan entri akses](#)

Elastic Beanstalk

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk AWS Elastic Beanstalk Untuk informasi lebih lanjut 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 mengakibatkan peningkatan CPU Utilization pada 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* . *accountID* Nilai *region* dan akan berbeda berdasarkan Wilayah dan Akun AWS Anda menjalankan otomatisasi di. Bundel log akan disimpan ke resources/environments/logs/bundle/ *environmentID* / *instanceID* direktori. Nilai *environmentID* dan *instanceID* nilai akan berbeda berdasarkan lingkungan Elastic Beanstalk Anda 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:GetBucketAcl`, `s3:GetBucketPolicy`, `s3: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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) ID lingkungan Elastic Beanstalk Anda yang ingin Anda kumpulkan bundel log.

- InstanceId

Tipe: String

(Wajib) ID instans Amazon EC2 di lingkungan Elastic Beanstalk tempat Anda ingin mengumpulkan bundel log.

- S3 BucketName

Tipe: String

(Opsional) Bucket Amazon S3 yang ingin Anda unggah log yang diarsipkan.

- S3 BucketPath

Tipe: 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`

Tipe: 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**

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID lingkungan Elastic Beanstalk yang ingin Anda aktifkan notifikasi.

- TopicArn

Tipe: 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 Amazon EC2 Auto Scaling, 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 (ACLs) 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. Dukungan

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama aplikasi Elastic Beanstalk Anda.

- EnvironmentName

Tipe: String

Deskripsi: (Wajib) Nama lingkungan Elastic Beanstalk Anda.

- AWSS3UploaderLink

Tipe: String

Deskripsi: (Opsional) URL yang diberikan kepada Anda oleh Dukungan untuk mengunggah bundel log dari lingkungan Elastic Beanstalk Anda ke. Opsi ini hanya tersedia untuk pelanggan yang telah membeli Dukungan 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 langkah sebelumnya.
- `aws:executeScript`- Mengumpulkan informasi tentang lingkungan Elastic Beanstalk termasuk load balancer CloudFormation , stack, grup Auto Scaling, instans Amazon EC2, dan konfigurasi VPC.
- `aws:executeScript`- Memeriksa masalah konektivitas jaringan dengan tabel rute dan ACLs 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 Dukungan.
- `aws:executeScript`- Mengeluarkan laporan item tindakan untuk membantu Anda memecahkan masalah yang mungkin memengaruhi status lingkungan Elastic Beanstalk Anda.

Elastic Load Balancing

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Elastic Load Balancing. Untuk informasi lebih lanjut 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-UpdateALBDesyncMitigationMode](#)
- [AWS-UpdateCLBDesyncMitigationMode](#)
- [AWSSupport-TroubleshootELBHealthChecks](#)

AWSConfigRemediation-DropInvalidHeadersForALB

Deskripsi

AWSConfigRemediation-DropInvalidHeadersForALBRunbook 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

Tipe: 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

Tipe: String

Deskripsi: (Diperlukan) 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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Daftar Classic Load Balancer yang dipisahkan koma yang ingin Anda aktifkan log akses.

- `S3 BucketName`

Tipe: String

Deskripsi: (Wajib) Nama bucket Amazon Simple Storage Service (Amazon S3) tempat log akses disimpan.

- `S3 BucketPrefix`

Tipe: 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

Aktifkan CLBAccess Log. `SuccessesLoadBalancers` - Daftar nama penyeimbang beban tempat log akses berhasil diaktifkan.

Aktifkan CLBAccess Log. 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 CLBs, 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

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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`

Tipe: 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`

Tipe: 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 pencatatan 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama Classic Load Balancer atau Application Load Balancer ARN.

- S3 BucketName

Tipe: String

Deskripsi: (Wajib) Nama bucket Amazon S3.

- S3 BucketPrefix

Tipe: 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

Tipe: 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

Tipe: String

Nilai yang valid: Praktik Terbaik | Masalah Konektivitas | Dasbor Pemecahan Masalah

Deskripsi: (Wajib) Operasi yang Anda inginkan untuk menjalankan runbook.

- LoadBalancerName

Tipe: String

Deskripsi: (Wajib) Nama CLB.

- S3Location

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Awalan kunci Amazon S3 (subfolder) yang ingin Anda unggah output otomatisasi. Output format disimpan dalam format berikut: `amzn-s3-demo-bucket/S3LocationPrefix/{{}} _ {{automation:InvestigationType}} .txt. EXECUTION_ID`

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-EnableNLBCrossZoneLoadBalancing`Runbook memungkinkan penyeimbangan beban lintas zona untuk penyeimbang beban jaringan (NLB) yang Anda tentukan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: 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-UpdateALBDesyncMitigationMode

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

Tipe: 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

Tipe: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari ALB yang ingin Anda ubah mode mitigasi desync.

- DesyncMitigationMode

Tipe: 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: assertAwsResource Property) - 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-UpdateCLBDesyncMitigationMode

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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Nama CLB yang ingin Anda ubah mode mitigasi desync.

- `DesyncMitigationMode`

Tipe: 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.

AWSSupport-TroubleshootELBHealthChecks

Deskripsi

`AWSSupport-TroubleshootELBHealthChecksRunbook` membantu memecahkan masalah pemeriksaan AWS kesehatan Elastic Load Balancing (Elastic Load Balancing) dengan menganalisis metrik CloudWatch Amazon CloudWatch () terkait, memverifikasi konektivitas jaringan, dan menjalankan perintah diagnostik pada instance targetnya.

Runbook ini membahas kasus penggunaan berikut:

- Ada contoh yang tidak sehat dalam contoh target penyeimbang beban atau kelompok sasaran.
- Meskipun tidak ada contoh yang tidak sehat, CloudWatch metrik menunjukkan titik data untuk `UnHealthyHostCounts`

Important

Pertimbangan penting:

- Otomatisasi berfokus pada pemecahan masalah target jenis instans.
- Jumlah maksimum instance yang diizinkan untuk pemecahan masalah adalah 50.

- Instance target harus dikelola oleh Systems Manager untuk mengaktifkan eksekusi perintah diagnostik pada tingkat instans.
- S3BucketNameParameternya opsional, tetapi hasil diagnostik tertentu diunggah langsung ke bucket Amazon S3 yang ditentukan dan tidak ditampilkan dalam output otomatisasi.
- IPv6 pemecahan masalah konektivitas jaringan tidak didukung.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeTargetGroups
- elasticloadbalancing:DescribeTargetHealth
- elasticloadbalancing:DescribeInstanceHealth
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- cloudwatch:GetMetricStatistics
- ssm:SendCommand
- ssm:GetCommandInvocation
- ssm:DescribeInstanceInformation

- s3:GetBucketLocation
- s3:GetBucketAcl
- s3:PutObject

Contoh Kebijakan:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeInstanceHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "cloudwatch:GetMetricStatistics",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - Troubleshoot ELB Health Checks](#) Systems Manager di bawah Dokumen.

2. Pilih Jalankan otomatisasi.

3. Untuk parameter input, masukkan yang berikut ini:

- AutomationAssumeRole (Opsional):
 - Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan SSM Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, SSM Automation menggunakan izin pengguna yang memulai runbook ini.
 - Tipe: `AWS::IAM::Role::Arn`
- LoadBalancerOrTargetGroupName (Diperlukan):
 - Deskripsi: (Wajib) Nama Classic Load Balancer, atau nama grup target yang terkait dengan Application Load Balancer atau Network Load Balancer.
 - Tipe: `String`
 - Pola yang Diizinkan: `^[a-zA-Z0-9-]+$`
- ExecutionMode (Diperlukan):
 - Deskripsi: (Diperlukan) Mengontrol mode eksekusi otomatisasi. `Complete` menjalankan semua langkah termasuk `RunCommands` di instans Amazon EC2. `SkipRunCommands` mengeksekusi semua langkah kecuali menjalankan perintah pada instance.
 - Tipe: `String`
 - Nilai yang Diizinkan: `[Complete, SkipRunCommands]`
- S3 BucketName (Opsional):
 - Deskripsi: (Opsional) Nama bucket Amazon S3 di akun tempat Anda ingin mengunggah log pemecahan masalah.
 - Tipe: `String`
 - Default: `""`

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- `getBucketPublicStatus`:

Memeriksa apakah bucket Amazon S3 target berpotensi memberikan akses publik baca atau tulis ke objeknya.

- `getLoadBalancerRincian`:

Mengidentifikasi jenis penyeimbang beban dan mengembalikan objek detail penyeimbang beban terpadu.

- `checkLoadBalancerJenis`:

Memeriksa apakah penyeimbang beban ada.

- `getTargets`:

Berdasarkan berbagai jenis penyeimbang beban, kueri menjelaskan APIs untuk mengembalikan peta detail target yang sehat dan tidak sehat.

- `checkCloudWatchMetrik`:

Memeriksa CloudWatch metrik `HealthyHostCounts` dan `UnHealthyHostCounts` dan menghasilkan CloudWatch tautan.

- `checkUnhealthyReasons`:

Memeriksa alasan yang tidak sehat dan menyaring target.

- `Periksa Konektivitas`:

Memeriksa konektivitas antara penyeimbang beban dan instance-nya.

- `RunCommands`:

Menjalankan perintah pemecahan masalah pada instance dan mengunggah output jika nama bucket disediakan.

- `GenerateReport`:

Buat laporan akhir berdasarkan output dari langkah sebelumnya dan unggah laporan ke bucket Amazon S3 jika ditentukan.

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

Perintah Diagnostik

Runbook mengeksekusi perintah diagnostik berikut pada instance:

- Linux Shell: `atas`, `gratis`, `ss`, `curl`, `iptables`, `tcpdump`
- Windows PowerShell: `Dapatkan-CimInstance`, `Dapatkan-`, `Dapatkan-NetFirewallProfile`, `Memanggil-NetFirewallRule`, `netstatWebRequest`, `netsh`, `pktmon`

Referensi

Otomatisasi Systems Manager

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

Amazon EMR

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

Topik

- [AWSsupport-AnalyzeEMRLogs](#)
- [AWSsupport-DiagnoseEMRLogsWithAthena](#)

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`

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID cluster yang node log Anda ingin menganalisis.

- Operasi

Tipe: String

Nilai yang valid: Jalankan Sekali | Jadwal | Hapus Jadwal

Deskripsi: (Wajib) Operasi untuk melakukan pada cluster.

- IntervalTime

Tipe: 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

Tipe: 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

Tipe: 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`

Tipe: 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`

Tipe: 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` atau `Schedule`:
 - `aws:assertAwsResourceProperty`- Memverifikasi cluster tersedia.
 - `aws:executeAwsApi`- Mengumpulkan IDs 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 adalah `no`:
 - `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`

`ListingClusterInstancesInstansIDs.`

`CreatingScheduleCloudFormationStack.StackStatus`

`RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus`

`CheckIfLogGroupExists.keluaran`

`FindLogPatternOnEMRNode.CommandId`

AWS Support - Diagnose EMR Logs With Athena

Deskripsi

`AWS Support - Diagnose EMR Logs With Athena` Runbook membantu mendiagnosis log EMR Amazon menggunakan Amazon Athena dalam integrasi dengan Katalog Data. AWS Glue Amazon Athena digunakan untuk menanyakan file log EMR Amazon untuk wadah, log node, atau keduanya, dengan parameter opsional untuk rentang tanggal tertentu atau pencarian berbasis kata kunci.

Runbook dapat secara otomatis mengambil lokasi log EMR Amazon untuk klaster yang ada, atau Anda dapat menentukan lokasi log Amazon S3. Untuk menganalisis log, runbook:

- Membuat AWS Glue database dan mengeksekusi kueri Amazon Athena Data Definition Language (DDL) di lokasi log Amazon EMR Amazon S3 Amazon untuk membuat tabel untuk log cluster dan daftar masalah yang diketahui.
- Menjalankan kueri Data Manipulation Language (DHTML) untuk mencari pola masalah yang diketahui di log EMR Amazon. Kueri menampilkan daftar masalah yang terdeteksi, jumlah kemunculannya, dan jumlah kata kunci yang cocok menurut jalur file Amazon S3.
- Hasilnya diunggah ke bucket Amazon S3 yang Anda tentukan di bawah awalan.
`saw_diagnose_EMR_known_issues`
- Runbook mengembalikan hasil kueri Amazon Athena, menyoroti temuan, rekomendasi, dan referensi ke artikel Pusat Pengetahuan Amazon (KC) yang bersumber dari subset yang telah ditentukan.
- Setelah selesai atau gagal, AWS Glue database dan file masalah yang diketahui yang diunggah ke bucket Amazon S3 akan dihapus.

Bagaimana cara kerjanya?

`AWSSupport-DiagnoseEMRLogsWithAthena` Melakukan analisis log EMR Amazon menggunakan Amazon Athena untuk mendeteksi kesalahan dan menyoroti temuan, rekomendasi, dan artikel Pusat Pengetahuan yang relevan.

Runbook melakukan langkah-langkah berikut:

- Dapatkan lokasi log klaster EMR Amazon menggunakan ID cluster atau masukan lokasi Amazon S3 untuk mengambil lokasi dan ukuran log.
- Berikan perkiraan biaya Athena berdasarkan ukuran lokasi log.
- Dapatkan persetujuan untuk melanjutkan dengan meminta persetujuan dari kepala sekolah IAM yang ditunjuk sebelum menjalankan pertanyaan Athena dan melanjutkan ke langkah berikutnya.
- Unggah masalah yang diketahui ke bucket Amazon S3 yang ditentukan, buat AWS Glue database dan tabel.
- Jalankan kueri Athena pada data log EMR Amazon. Kueri dapat mencari berdasarkan rentang tanggal, kata kunci, kedua kriteria, atau berjalan tanpa filter berdasarkan input yang disediakan.
- Menganalisis hasil untuk menyoroti temuan, rekomendasi, dan artikel KC yang relevan.
- Tautan keluaran untuk hasil kueri DMLAmazon Athena.
- Bersihkan lingkungan dengan menghapus database yang dibuat, tabel, dan masalah yang diketahui yang diunggah.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

AutomationAssumeRole Parameter memerlukan tindakan berikut agar berhasil menggunakan runbook:

- Athena: GetQueryExecution
- Athena: StartQueryExecution
- Athena: GetPreparedStatement
- Athena: CreatePreparedStatement
- iam: GetDatabase
- iam: CreateDatabase
- iam: DeleteDatabase
- iam: CreateTable
- iam: GetTable
- iam: DeleteTable
- elasticmapreduce: DescribeCluster
- s3: ListBucket
- s3: GetBucketVersioning
- s3: ListBucketVersions
- s3: GetBucketPublicAccessBlock
- s3: GetBucketPolicyStatus
- s3: GetObject
- s3: GetBucketLocation
- harga: GetProducts
- harga: GetAttributeValues
- harga: DescribeServices

- harga: ListPriceLists

Important

Untuk membatasi akses hanya ke sumber daya yang dibutuhkan oleh otomatisasi ini, lampirkan kebijakan berikut ke peran IAM yang mempercayai Layanan SSM. Ganti Partisi, Wilayah, dan Akun dengan nilai yang sesuai untuk partisi, wilayah, dan nomor akun tempat buku run dijalankan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticmapreduce:DescribeCluster",
        "glue:GetDatabase",
        "athena:GetQueryExecution",
        "athena:StartQueryExecution",
        "athena:GetPreparedStatement",
        "athena:CreatePreparedStatement",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:ListBucketVersions",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "pricing:GetProducts",
        "pricing:GetAttributeValues",
        "pricing:DescribeServices",
        "pricing:ListPriceLists"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RestrictPutObjects",
      "Effect": "Allow",
```

```

        "Action": [
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::*/results/*",
            "arn:aws:s3:::*/saw_diagnose_emr_known_issues/*"
        ]
    },
    {
        "Sid": "RestrictDeleteAccess",
        "Effect": "Allow",
        "Action": [
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
        ],
        "Resource": [
            "arn:aws:s3:::*/saw_diagnose_emr_known_issues/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "glue:GetDatabase",
            "glue:CreateDatabase",
            "glue:DeleteDatabase"
        ],
        "Resource": [
            "arn:aws:glue:us-east-1:111122223333:database/
saw_diagnose_emr_database_*",
            "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/*",
            "arn:aws:glue:us-east-1:111122223333:userDefinedFunction/
saw_diagnose_emr_database_*/*",
            "arn:aws:glue:us-east-1:111122223333:catalog"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "glue:CreateTable",
            "glue:GetTable",
            "glue:DeleteTable"
        ],
        "Resource": [

```

```

        "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/saw_diagnose_emr_known_issues",
        "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/saw_diagnose_emr_logs_table",
        "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/j_*",
        "arn:aws:glue:us-east-1:111122223333:database/
saw_diagnose_emr_database_*",
        "arn:aws:glue:us-east-1:111122223333:catalog"
    ]
}
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Navigasikan [AWS Support-DiagnoseEMRLogsWithAthena](#) di AWS Systems Manager 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.

- ClusterId (Diperlukan):

ID cluster EMR Amazon.

- S3 LogLocation (Opsional):

Lokasi log EMR Amazon S3 Amazon. Masukkan URL gaya Path-style lokasi Amazon S3, misalnya: s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/ Berikan parameter ini jika klaster EMR Amazon telah dihentikan selama lebih dari beberapa hari. 30

- S3 BucketName (Diperlukan):

Nama bucket Amazon S3 untuk mengunggah daftar masalah yang diketahui, dan keluaran kueri Amazon Athena. Bucket harus [mengaktifkan Blokir Akses Publik](#) dan berada di AWS wilayah dan akun yang sama dengan cluster EMR Amazon.

- **Penyetuju (Diperlukan):**

Daftar kepala sekolah yang AWS diautentikasi yang dapat menyetujui atau menolak tindakan tersebut. Anda dapat menentukan prinsipal dengan menggunakan salah satu format berikut: nama pengguna, ARN pengguna, ARN peran IAM, atau IAM berperan ARN. Jumlah maksimum pemberi persetujuan adalah 10.

- **FetchNodeLogsOnly (Opsional):**

Jika disetel ke `true`, otomatisasi mendiagnosis log wadah aplikasi Amazon EMR. Nilai default-nya adalah `false`.

- **FetchContainersLogsOnly (Opsional):**

Jika disetel ke `true`, otomatisasi mendiagnosis log kontainer EMR Amazon. Nilai default-nya adalah `false`.

- **EndSearchDate (Opsional):**

Tanggal akhir untuk pencarian log. Jika disediakan, otomatisasi akan secara eksklusif mencari log yang dihasilkan hingga tanggal yang ditentukan dalam format YYYY-MM-DD (misalnya: 2024-12-30).

- **DaysToCheck (Opsional):**

Ketika `EndSearchDate` disediakan, parameter ini diperlukan untuk menentukan jumlah hari untuk secara retrospektif mencari log dari yang ditentukan. `EndSearchDate` Nilai maksimumnya adalah 30 hari. Nilai default-nya adalah 1.

- **SearchKeywords (Opsional):**

Daftar kata kunci untuk mencari di log, dipisahkan dengan koma. Kata kunci tidak dapat berisi tanda kutip tunggal atau ganda.

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.	ClusterID (Required) The Amazon EMR cluster ID.
S3LogLocation (Optional) The Amazon S3 URL that contains the Amazon EMR logs. Provide this parameter if the Amazon EMR cluster has been terminated for more than 30 days. Provide the full Amazon S3 path prefix for the EMR logs. Example s3://mybucket/myfolder/j-1K48XXXXXXHCB/.	S3BucketName (Required) The Amazon S3 bucket name to upload a list of known issues, and the output of Amazon Athena queries. The bucket should have [Block Public Access Enabled](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html) and be in the same AWS region as the Amazon EMR cluster provided.
Approvers (Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats: 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN.	FetchNodeLogsOnly (Optional) If set to "true", the automation diagnoses the Amazon EMR node logs.
FetchContainersLogsOnly (Optional) If set to "true", the automation diagnoses the Amazon EMR containers logs related to applications on the cluster.	EndSearchDate (Optional) The end date for log searches. If provided, the automation will exclusively search for logs generated up to the specified date in the format YYYY-MM-DD (for example: "2024-12-30").
DaysToCheck (Optional) When "EndSearchDate" is provided, this parameter is required to determine the number of days to retrospectively search for logs from the specified "EndSearchDate". The maximum value is "30" days.	SearchKeywords (Optional) The list of keywords to search in the logs, separated by commas. The keywords cannot contain single or double quotes.

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **getLogLocation:**

Mengambil lokasi log Amazon S3 dengan menanyakan ID Cluster EMR Amazon yang ditentukan. Jika otomatisasi tidak dapat menanyakan lokasi log dari ID cluster EMR Amazon, runbook menggunakan parameter input. `S3LogLocation`

- **branchOnValidLog:**

Memverifikasi lokasi log EMR Amazon. Jika lokasinya valid, lanjutkan untuk memperkirakan biaya potensial Amazon Athena saat menjalankan kueri di log EMR Amazon.

- **estimateAthenaCosts:**

Menentukan ukuran log EMR Amazon dan memberikan perkiraan biaya untuk menjalankan pemindaian Athena pada kumpulan data log. Untuk wilayah non-komersial (AWS non-partisi), langkah ini hanya menyediakan ukuran log tanpa memperkirakan biaya. Biaya dapat dihitung menggunakan dokumentasi harga Athena di wilayah yang ditentukan.

- **Menyetujui Otomasi:**

Menunggu persetujuan kepala IAM yang ditunjuk untuk melanjutkan langkah otomatisasi selanjutnya. Pemberitahuan persetujuan berisi perkiraan biaya pemindaian Amazon Athena di log EMR Amazon, dan detail tentang sumber daya yang disediakan oleh otomatisasi.

- **uploadKnownIssuesExecuteAthenaQueries:**

Mengunggah masalah yang telah ditentukan sebelumnya ke bucket Amazon S3 yang ditentukan dalam parameter. `S3BucketName` Membuat AWS Glue database dan tabel. Menjalankan kueri Amazon Athena dalam AWS Glue database berdasarkan parameter input.

- `getQueryExecutionStatus`:

Menunggu hingga eksekusi kueri Amazon Athena dalam status. `SUCCEEDED` Kueri DML Amazon Athena mencari kesalahan dan pengecualian di log klaster Amazon EMR.

- `analyzeAthenaResults`:

Menganalisis hasil Amazon Athena untuk memberikan temuan, rekomendasi, dan artikel Pusat Pengetahuan (KC) yang bersumber dari serangkaian pemetaan yang telah ditentukan sebelumnya.

- `getAnalyzeResultsExecutionStatusKueri1`:

Menunggu sampai eksekusi kueri dalam `SUCCEEDED` status. Kueri DML Amazon Athena menganalisis hasil dari kueri DML sebelumnya. Kueri analisis ini akan mengembalikan pengecualian yang cocok dengan resolusi dan artikel KC

- `getAnalyzeResultsExecutionStatusKueri2`:

Menunggu sampai eksekusi kueri dalam `SUCCEEDED` status. Kueri DML Amazon Athena menganalisis hasil dari kueri DML sebelumnya. Kueri analisis ini akan mengembalikan daftar exceptions/errors terdeteksi di setiap jalur log Amazon S3.

- `printAthenaQueriesPesan`:

Mencetak tautan untuk hasil kueri DML Amazon Athena.

- `CleanUpresources`:

Membersihkan sumber daya dengan menghapus AWS Glue database yang dibuat dan menghapus file masalah yang diketahui yang dibuat di bucket log EMR Amazon.

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

Output menyediakan tiga tautan untuk hasil kueri Athena:

- Daftar semua kesalahan dan pengecualian yang sering terjadi ditemukan di log klaster EMR Amazon, bersama dengan lokasi log yang sesuai (awalan Amazon S3).
- Ringkasan pengecualian unik yang diketahui cocok di log EMR Amazon, bersama dengan resolusi yang direkomendasikan dan artikel KC untuk membantu dalam pemecahan masalah.

- Detail tentang di mana kesalahan dan pengecualian tertentu muncul di jalur log Amazon S3, untuk mendukung diagnosis lebih lanjut.

▼ Outputs

```
printAthenaQueryMessage.QueryLinksMessage
Log View Query Link: This link provides a comprehensive view of all the exceptions encountered within your EMR logs.
https://[redacted]
Analysis Query 1 Link: This link provides a summary of unique issues detected from your logs, along with insights. It shows the issue ID, matched keywords for each issue, number of times the issue occurred, a summary of what the issue is, a description providing more details, and relevant links to knowledge center articles.
https://[redacted]
Analysis Query 2 Link: This link provides visibility into issues that have occurred, specified by S3 file path. It gives a breakdown of the number of times each unique issue has happened along with the keyword matched for that issue. The output allows precise tracing of exceptions and errors in each file, guiding remediation efforts and debugging
https://[redacted]
```

Referensi

Otomatisasi Systems Manager

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

AWS dokumentasi layanan

- Lihat [Pemecahan Masalah Amazon EMR Cluster](#) untuk informasi lebih lanjut

OpenSearch Layanan Amazon

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon OpenSearch Service. Untuk informasi lebih lanjut 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

Tipe: 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

Tipe: 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`

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama domain OpenSearch Layanan Amazon yang ingin Anda gunakan untuk memperbarui grup keamanan.

- SecurityGroupList

Jenis: StringList

Deskripsi: (Wajib) Grup keamanan IDs yang ingin Anda tetapkan ke domain OpenSearch Layanan Amazon.

- AutomationAssumeRole

Tipe: 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 OpenSearch

Layanan APIs terhadap klaster untuk menentukan mengapa klaster dalam keadaan merah atau kuning.

- Menghapus fungsi Lambda.
- Menampilkan pemeriksaan yang dilakukan dan langkah-langkah yang disarankan berikutnya untuk menyelesaikan masalah klaster 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](#).

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "es:ESHttpGet",
        "Resource": [
          "arn:aws:es:us-east-1:111122223333:domain/domain-name/",
          "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cluster/health",
          "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cat/indices",
          "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cat/allocation",
          "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cluster/allocation/explain"
        ]
      },
      {
        "Condition": {
          "ArnLikeIfExists": {
            "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333: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](#) dalam 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.

- 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 JVMMemory Tekanan. 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

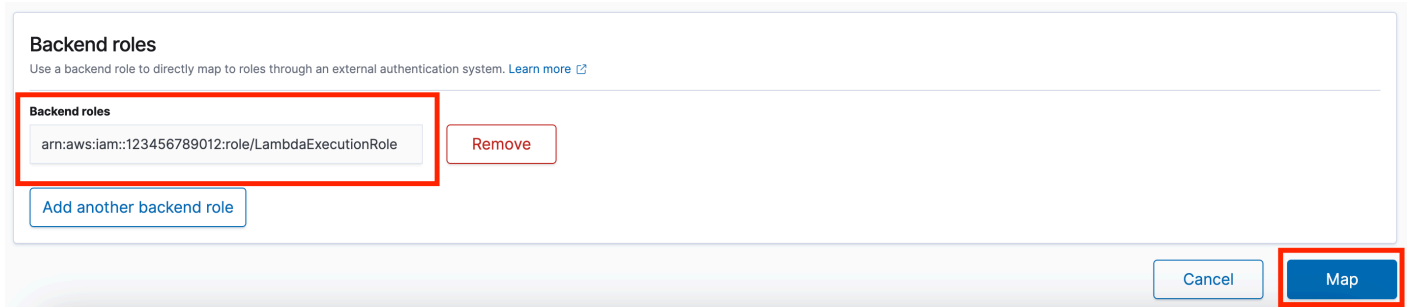
4. Jika Anda telah mengaktifkan [kontrol akses berbutir halus](#) pada kluster OpenSearch Service, pastikan bahwa LambdaExecutionRole peran arn dipetakan ke peran dengan setidaknya izin. `cluster_monitor`

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. [Learn more](#)

> • cluster_monitor



5. Pilih Jalankan.

6. Otomatisasi dimulai.

7. Runbook otomatisasi melakukan langkah-langkah berikut:

- GetClusterConfiguration:

Mengambil konfigurasi kluster OpenSearch Layanan.

- Buat AWSLambdaFunctionStack:

Membuat fungsi Lambda sementara di akun Anda menggunakan CloudFormation Fungsi Lambda digunakan untuk menjalankan Layanan OpenSearch APIs

- WaitForAWSLambdaFunctionStack:

Menunggu CloudFormation tumpukan selesai.

- GetClusterMetricsFromCloudWatch:

Mendapatkan metrik terkait kluster Amazon CloudWatch ClusterStatus CPUUtilization,, dan JVMMemory Pressure OpenSearch Service dan tanggal pembuatannya.

- RunOpenSearchAPIs:

Menggunakan fungsi Lambda untuk memanggil OpenSearch Layanan APIs dan menganalisis data metrik cluster untuk mendiagnosis penyebab status kluster merah atau kuning.

- Hapus AWSLambdaFunctionStack:

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 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.

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: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`

 Note

`iam:CreateRole`, `iam>DeleteRole`, `iam:GetRole`
`iam:PutRolePolicy` dan hanya `iam>DeleteRolePolicy`
diperlukan jika Anda tidak menggunakan peran IAM yang ada untuk parameter
`LambdaInvocationRoleForStepFunctions`

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](#).

LambdaInvocationRoleForStepFunctionsParameter memberikan izin untuk mesin AWS Step Functions status untuk menjalankan fungsi Lambda. Berikut ini adalah contoh kebijakan IAM yang memberikan izin Step Functions untuk menjalankan fungsi Lambda yang mengambil data diagnostik dari domain Layanan. OpenSearch Untuk informasi selengkapnya, lihat [Membuat peran IAM mesin status](#) di Panduan AWS Step Functions Pengembang.

JSON

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

```

        "Resource": [
            "arn:aws:lambda:us-east-1:111122223333:function:AWSSupport-
HighCPU-*"
        ]
    }
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootOpenSearchHighCPU](#) dalam 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.

- DomainName (Diperlukan):

Nama domain OpenSearch Layanan Amazon yang ingin Anda pecahkan masalah CPU 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".

- LambdaInvocationRoleForStepFunctions(Opsional):

(Opsional) ARN dari peran IAM untuk dilampirkan ke alur kerja Step Functions. Mesin status menggunakan kredensi dari peran ini untuk menjalankan fungsi Lambda yang mengambil data diagnostik dari domain Layanan. OpenSearch Jika tidak ada peran yang ditentukan, otomatisasi ini akan membuat peran IAM untuk Step Functions di akun Anda.

- **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`

The screenshot shows the AWS IAM console interface for a role. The 'Permissions' tab is selected. Under 'Cluster permissions (1)', there is a list of permissions, including 'cluster_monitor'. In the 'Backend roles' section, a role with the ARN 'arn:aws:iam::[redacted]:role/LambdaExecutionRole' is listed, and a 'Remove' button is next to it. At the bottom right, there are 'Cancel' and 'Map' buttons, with the 'Map' button highlighted.

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 CloudFormation.

- waitForStackPenciptaan:

Menunggu CloudFormation tumpukan selesai.

- describeStackResources:

Menjelaskan CloudFormation tumpukan dan mendapatkan ARN dari mesin negara.

- runStateMachine:

Memanggil fungsi Lambda pengumpul data satu kali atau lebih dengan menjalankan mesin status Step Functions.

- describeErrorsFromStackEvents:

Menjelaskan kesalahan dari CloudFormation tumpukan untuk kesalahan.

- unstageOpenSearchTinggiCPUAutomation:

Menghapus AWSSupport-TroubleshootOpenSearchHighCPU CloudFormation tumpukan.

- describeErrorsFromStackDeletion:

Menjelaskan kesalahan yang ditemui saat menghapus 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 lebih lanjut 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 sudah 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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) String deduplikasi yang ingin Anda tambahkan ke aturan.

- `RuleName`

Tipe: 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

Tipe: 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

Tipe: String

Default: default

Deskripsi: (Opsional) Bus acara yang terkait dengan aturan yang ingin Anda nonaktifkan.

- RuleName

Tipe: 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.

AWS Glue

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

Topik

- [AWSSupport-TroubleshootGlueConnection](#)

AWSSupport-TroubleshootGlueConnection

Deskripsi

AWSSupport-TroubleshootGlueConnectionsRunbook membantu memecahkan masalah koneksi AWS Glue. Target koneksi yang diuji harus dicapai melalui koneksi JDBC dan dapat berupa cluster/instance Amazon Relational Database Service (Amazon RDS), cluster Amazon Redshift, atau target lain yang dapat diakses melalui JDBC. Dalam dua kasus pertama, alat Reachability Analyzer digunakan untuk menentukan apakah konektivitas antara source AWS Glue() dan target (Amazon RDS atau Amazon Redshift) diberikan.

Jika target koneksi bukan Amazon RDS atau Amazon Redshift, konektivitas masih diuji dengan membuat AWS Lambda fungsi di subnet yang sama dengan koneksi (titik keberadaan jaringan) dan memeriksa apakah nama target dapat diselesaikan dan apakah dapat dijangkau di port target. AWS Glue

 Important

Untuk menjalankan pemeriksaan [Reachability Analyzer, Elastic Network](#) Interfaces akan dibuat di setiap subnet sumber data koneksi. Pastikan Anda memiliki cukup gratis IPs pada subnet tersebut dan bahwa konsumsi satu IP tidak akan memengaruhi beban kerja Anda sebelum menjalankan otomatisasi ini.

 Important

Semua sumber daya yang dibuat oleh otomatisasi ini ditandai sehingga dapat dengan mudah ditemukan. Tag yang digunakan adalah:

- `AWSSupport-TroubleshootGlueConnection`: benar
- `AutomationExecutionId`: *Amazon EC2 Systems Manager Execution Id*

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Menjelaskan AWS Glue koneksi untuk mendapatkan informasi sumber (subnet dan grup keamanan) untuk pemeriksaan konektivitas.
- Mengambil informasi target (subnet dan grup keamanan) dari sumber data yang direferensikan dalam URL JDBC atau dari parameter dan jika ada. `DatasourceSecurityGroups` `DatasourceSubnets`
- Jika sumber data yang ada di URL JDBC adalah instans atau kluster Amazon RDS atau kluster Amazon Redshift, otomatisasi ini dibuat menggunakan sumber dan informasi target yang dikumpulkan pada langkah sebelumnya dan ENIs menggunakan Reachability Analyzer untuk melakukan pemeriksaan konektivitas di antara keduanya.
- Fungsi Lambda (titik kehadiran jaringan, dalam konteks otomatisasi ini) digunakan untuk melakukan konektivitas L4 dan pemeriksaan resolusi nama.

- Fungsi Lambda yang sama digunakan untuk melakukan pemeriksaan terhadap titik akhir Amazon S3.
- Simulator Kebijakan digunakan untuk menentukan apakah peran IAM yang digunakan dalam koneksi memiliki izin yang diperlukan.
- Otomatisasi memeriksa apakah grup keamanan yang digunakan oleh koneksi memiliki konfigurasi yang diharapkan.
- Sebuah laporan dihasilkan yang berisi kemungkinan penyebab kegagalan dalam operasi koneksi uji and/or juga pengujian yang berhasil dilakukan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `ec2:CreateNetworkInsightsPath`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `ec2>DeleteNetworkInsightsAnalysis`
- `ec2>DeleteNetworkInsightsPath`
- `ec2>DeleteNetworkInterface`
- `ec2:StartNetworkInsightsAnalysis`
- `iam:AttachRolePolicy`

- `iam:CreateRole`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:PutRolePolicy`
- `iam:TagRole`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:TagResource`
- `logs:CreateLogGroup`
- `logs>DeleteLogGroup`
- `logs:PutRetentionPolicy`
- `logs:TagResource`
- `glue:GetConnection`
- `glue:GetDataCatalogEncryptionSettings`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `ec2:DescribeDhcpOptions`
- `ec2:DescribeNetworkInsightsPaths`
- `ec2:DescribeNetworkInsightsAnalyses`
- `ec2:DescribeSecurityGroupRules`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpcAttribute`
- `iam:GetRole`
- `iam>ListAttachedRolePolicies`
- `iam:SimulatePrincipalPolicy`
- `kms:DescribeKey`
- `lambda:InvokeFunction`

- `lambda:GetFunction`
- `s3:GetEncryptionConfiguration`
- `iam:PassRole`

Important

Selain tindakan yang disebutkan di atas, [Amazon AutomationAssumeRole](#) harus memiliki [kebijakan VPCReachability AnalyzerFullAccessPolicy terkelola terlampir](#) sehingga pengujian [Reachability Analyzer](#) berhasil dilakukan.

Berikut adalah contoh kebijakan yang dapat diberikan untuk `AutomationAssumeRole`:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "TaggedAWSResourcesPermissions",
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
      }
    },
    "Action": [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam>DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:TagRole",
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda:TagResource",
      "logs>DeleteLogGroup",
      "logs>CreateLogGroup",
      "logs:PutRetentionPolicy",
```

```

        "logs:TagResource",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack"
    ],
    "Resource": "*"
},
{
    "Sid": "TaggedEC2ResourcesPermissions",
    "Effect": "Allow",
    "Condition": {
        "StringEquals": {
            "ec2:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
        }
    },
    "Action": [
        "ec2:DeleteNetworkInterface"
    ],
    "Resource": "*"
},
{
    "Sid": "PutRolePolicy",
    "Effect": "Allow",
    "Condition": {
        "StringEquals": {
            "iam:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
        }
    },
    "Action": [
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy"
    ],
    "Resource": "*"
},
{
    "Sid": "InvokeFunction",
    "Effect": "Allow",
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": "arn:*:lambda:*:*:function:point-of-presence-*"
},
{

```

```

        "Sid": "UnTaggedActions",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateNetworkInsightsPath",
            "ec2:DeleteNetworkInsightsAnalysis",
            "ec2:DeleteNetworkInsightsPath",
            "ec2:CreateNetworkInterface",
            "ec2:CreateTags",
            "ec2:StartNetworkInsightsAnalysis",
            "glue:GetConnection",
            "glue:GetDataCatalogEncryptionSettings",
            "cloudformation:DescribeStacks",
            "cloudformation:DescribeStackEvents",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeNetworkInsightsPaths",
            "ec2:DescribeNetworkInsightsAnalyses",
            "ec2:DescribeSecurityGroupRules",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "ec2:DescribeVpcAttribute",
            "iam:GetRole",
            "iam:ListAttachedRolePolicies",
            "iam:SimulatePrincipalPolicy",
            "kms:DescribeKey",
            "lambda:GetFunction",
            "s3:GetEncryptionConfiguration"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:PassRole"
        ],
        "Resource": "arn:*:iam::*:role/point-of-presence-*",
        "Condition": {
            "StringLikeIfExists": {
                "iam:PassedToService": "lambda.amazonaws.com"
            }
        }
    }
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootGlueConnection](#) 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.

- TestConnectionRole (Diperlukan)

Nama Sumber Daya Amazon (ARN) dari peran IAM yang digunakan selama pengujian koneksi.

- ConnectionName (Diperlukan)

AWS Glue gagal menguji nama koneksi yang ingin Anda pecahkan masalah.

- PersistReachabilityAnalyzerResults(Opsional)

Bendera yang menginformasikan apakah hasil eksekusi Reachability Analyzer harus disimpan atau tidak. Default: `false`.

- PointOfPresenceLogRetentionPeriod(Opsional)

Jumlah hari log untuk titik keberadaan Lambda akan disimpan. Default: 7.

- DatasourceSubnets (Opsional)

Jika sumber data asli tidak tersedia, gunakan parameter ini untuk menyediakan subnet yang digunakan sehingga tes konektivitas masih dilakukan. Harus digunakan dengan `DatasourceSecurityGroups`. Contoh: `subnet-1`, `subnet-2`.

- DatasourceSecurityGroups (Opsional)

Jika sumber data asli tidak tersedia, gunakan parameter ini untuk menyediakan grup keamanan yang digunakan sehingga tes konektivitas masih dilakukan. Harus digunakan dengan `DatasourceSubnets`. Contoh: `sg-1, sg-2`.

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.	ConnectionName (Required) The name of the AWS Glue Connection you want to troubleshoot the failed test connection attempt. String
TestConnectionRole (Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that is used during the connection test.	PersistReachabilityAnalyzerResults (Optional) The flag informing if the results of the VPC Reachability Analyzer execution should be kept or not. Default: false. false
PointOfPresenceLogRetentionPeriod (Optional) The amount of days the logs for the point of presence AWS Lambda will be stored for. Default: 7. 7	DatasourceSubnets (Optional) If the original datasource is not available, use this parameter to provide the subnets that it used so that the connectivity tests are still performed. **Must** be used with <code>DatasourceSecurityGroups</code>. Example: <code>subnet-1, subnet-2</code>. StringList
DatasourceSecurityGroups (Optional) If the original datasource is not available, use this parameter to provide the security groups it used so that the connectivity tests are still performed. **Must** be used with <code>DatasourceSubnets</code>. Example: <code>sg-1, sg-2</code>. StringList	

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Runbook otomatisasi melakukan langkah-langkah berikut:

- **ParseInputs:**

Langkah ini memvalidasi kombinasi input. Jika keduanya `DatasourceSecurityGroups` dan `DatasourceSubnets` disediakan, mereka valid dan dikembalikan apa adanya. Jika tidak ada yang disediakan, dua daftar kosong dikembalikan. Jika hanya satu dari mereka disediakan, langkahnya memunculkan `ValueException`.

- **GetConnectionDetails:**

Langkah-langkah ini mengembalikan rincian AWS Glue koneksi yang disediakan.

- **ParseSecurityGroupList:**

Langkah ini digunakan untuk menggabungkan pemanfaatan in a for `String` future `SecurityGroupIdList` dalam otomatisasi ini.

- **GetConnectionData:**

Menentukan berdasarkan URL JDBC, jenis koneksi antara:RedShift,RdsInstance, RdsCluster dan. Other Selain itu, mengembalikan domain dan port yang digunakan dalam koneksi JDBC, Amazon VPC koneksi dan server nama domainnya.

- **GetNetworkDetails:**

Mendapatkan informasi subnet dan grup keamanan dari target Amazon RDS atau Amazon Redshift.

- **BuatENITemplate:**

Menghasilkan AWS CloudFormation template yang digunakan untuk membuat antarmuka jaringan yang digunakan untuk menguji konektivitas. Ini diperlukan untuk menjalankan alat Reachability Analyzer.

- **BuatENIStack:**

Membuat CloudFormation tumpukan dari template yang dibuat pada langkah sebelumnya.

- **GetStackDetails:**

Menjelaskan CloudFormation tumpukan yang dibuat di tumpukan sebelumnya dan mengambil TargetNetworkInterfaces informasi. SourceNetworkInterface

- **RunSourceToTargetCheck:**

Menjalankan pemeriksaan antara sumber dan target yang ENIs dibuat pada langkah sebelumnya menggunakan alat Reachability Analyzer.

- **HapusENIStack:**

Menghapus CloudFormation tumpukan yang membuat Antarmuka Jaringan

- **CreateNetworkPointOfPresence:**

CloudFormation menciptakan fungsi Lambda yang digunakan sebagai titik kehadiran jaringan.

- **GetFunctionName:**

Melakukan panggilan API stack CloudFormation describe untuk mengambil nama fungsi Lambda yang dibuat pada langkah sebelumnya.

- **RunEndpointChecks:**

Menggunakan titik kehadiran jaringan untuk menentukan apakah titik akhir yang ada dalam koneksi JDBC dapat diselesaikan dan dapat dijangkau di port yang dideklarasikan.

- **Checks3konektivitas:**

Memeriksa konektivitas jaringan dari AWS Glue koneksi ke layanan Amazon S3.

- **DeletePointOfPresence:**

Menghapus CloudFormation tumpukan yang menciptakan titik jaringan kehadiran Lambda.

- **IAMRoleIzin Uji:**

Memeriksa apakah peran IAM yang digunakan untuk pengujian memiliki izin yang diperlukan untuk menjalankannya.

- **CheckConnectionSecurityGroupReferencingRule:**

Memeriksa apakah grup keamanan yang digunakan dalam AWS Glue koneksi memungkinkan semua lalu lintas masuk dari dirinya sendiri. Ini akan mengembalikan daftar grup keamanan tanpa aturan ini, jika ada.

- **GenerateReport:**

Menghasilkan laporan yang berisi daftar temuan (kemungkinan alasan kegagalan dalam tes koneksi) dan langkah selanjutnya (upaya untuk menyelesaikan kegagalan uji koneksi).

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

- **Hasil Otomasi**

Di bagian ini, Anda akan menemukan skenario yang menjelaskan kemungkinan penyebab kegagalan operasi koneksi pengujian (temuan) dan bagaimana mereka dapat diperbaiki (langkah selanjutnya). Jika otomatisasi tidak dapat menemukan penyebab kegagalan pengujian, ini akan diinformasikan di bagian ini juga.

- **Tes yang Berhasil**

Di bagian ini, Anda akan menemukan skenario yang menginformasikan apa yang telah berhasil diuji oleh otomatisasi ini. Pengujian yang berhasil berguna jika otomatisasi tidak dapat mengidentifikasi penyebab kegagalan koneksi pengujian karena mengurangi ruang lingkup penyelidikan dengan menginformasikan apa yang tidak berkontribusi untuk masalah ini.

- **Kesalahan Otomasi**

Di bagian ini, Anda akan menemukan skenario yang menjelaskan masalah yang terjadi selama otomatisasi, yang mungkin membatasi jumlah pengujian yang dapat dilakukan otomatisasi.

Deskripsi skenario akan menginformasikan langkah mana yang gagal.

```

TroubleshootGlueConnection
-----
Automation Results
Below are possible causes for the issue being troubleshoot and their fixes.
-----

# Scenario: AWS Glue connection's VPC using Amazon Provided DNS
🔍 Findings:
- The JDBC URL's endpoint dummy-instance.c3c3tj8ogvmj.us-east-1.rds.amazonaws.com could not be resolved from the AWS Glue connection's subnet subnet-
- Glue connection's VPC (vpc- ) is using AWS DNS Resolver but no issue could be found.
➔ Next steps:
- Please check the following links for further DNS troubleshooting:
- https://repost.aws/knowledge-center/vpc-find-cause-of-failed-dns-queries.
- https://repost.aws/knowledge-center/vpc-peering-troubleshoot-dns-resolution
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-support

# Scenario: Checking AWS Glue connection IAM role trust relationship
🔍 Findings:
- The IAM role arn:aws:iam:: :role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-lLu7FYAp9bfi used for the AWS Glue connection test has no trust relationship with the AWS Glue service.
➔ Next steps:
- Please add the AWS Glue service to the arn:aws:iam:: :role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-lLu7FYAp9bfi trust relationship. More details on the following link:
- https://docs.aws.amazon.com/directoryservice/latest/admin-guide/edit_trust.html

# Scenario: Glue test connection role IAM check
🔍 Findings:
- The IAM role (arn:aws:iam:: :role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-lLu7FYAp9bfi) used to test the connection is not allowed to perform 'glue:TestConnection'.
➔ Next steps:
- Please add the 'glue:TestConnection' action to the role used for the AWS Glue connection test:
arn:aws:iam:: :role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-lLu7FYAp9bfi.

-----
✓ Successful Tests
Below are the successful tests performed by the automation, for further troubleshooting.
-----

# Scenario: Datasource security group
✓ The target's security group(s) allow(s) inbound connections from the Glue connection.

# Scenario: Checking connection security group self referencing rule
✓ The AWS Glue connection has a self referencing inbound rule allowing all traffic.

```

Referensi

Otomatisasi Systems Manager

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

Amazon FSx

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

Topik

- [AWSSupport-ValidateFSxWindowsADConfig](#)

AWSSupport-ValidateFSxWindowsADConfig

Deskripsi

AWSSupport-ValidateFSxWindowsADConfigRunbook digunakan untuk memvalidasi konfigurasi Active Directory (AD) yang dikelola sendiri dari Amazon FSx untuk Windows File Server

Bagaimana cara kerjanya?

Runbook AWSSupport-ValidateFSxWindowsADConfig mengeksekusi skrip validasi Amazon FSx pada instans Windows Amazon Elastic Compute Cloud (Amazon EC2) sementara yang diluncurkan oleh runbook di subnet Amazon. FSx Skrip melakukan beberapa pemeriksaan untuk memvalidasi konektivitas jaringan ke AD/DNS server yang dikelola sendiri dan izin akun layanan Amazon FSx . Runbook dapat memvalidasi Amazon FSx yang gagal atau salah dikonfigurasi untuk Windows File Server atau membuat FSx Amazon baru untuk Windows File Server dengan AD yang dikelola sendiri.

Secara default, runbook membuat instans Windows Amazon EC2, grup keamanan AWS Systems Manager untuk akses (SSM), peran (IAM) AWS Identity and Access Management , dan kebijakan menggunakan subnet Amazon CloudFormation FSx. Jika Anda ingin menjalankan skrip pada instans Amazon EC2 yang ada, berikan ID dalam parameter. InstanceId Pada eksekusi yang berhasil, ia menghapus CloudFormation sumber daya. Namun, untuk mempertahankan sumber daya, atur RetainCloudFormationStack parameter ke true.

CloudFormation Template membuat peran IAM atas nama Anda dengan izin yang diperlukan untuk dilampirkan ke instans Amazon EC2 untuk menjalankan skrip validasi Amazon FSx . Untuk menentukan profil instans IAM yang ada untuk instance sementara, gunakan InstanceProfileName parameter. Peran IAM terkait harus berisi izin berikut:

- `ec2:DescribeSubnets` dan `ec2:DescribeVpcs` izin serta Kebijakan AmazonSSMManagedInstanceCore Terkelola Amazon.
- Izin untuk mendapatkan nama pengguna dan kata sandi akun FSx layanan Amazon dari Systems Manager dengan memanggil `GetSecretValue` API.
- Izin untuk menempatkan objek di bucket Amazon Simple Storage Service (Amazon S3) Simple Storage S3) untuk output skrip.

Prasyarat

Subnet tempat instans Amazon EC2 sementara dibuat (atau instans yang ada yang disediakan dalam InstanceId parameter) harus mengizinkan akses ke AWS Systems Manager AWS Secrets Manager,, dan titik akhir Amazon S3 untuk menjalankan AmazonFSxADValidation skrip menggunakan SSM Run Command.

AWS Secrets Manager penyiapan

Skrip validasi terhubung ke domain Microsoft AD dengan mengambil nama pengguna dan kata sandi akun FSx layanan Amazon dengan panggilan runtime ke Secrets Manager. Ikuti langkah-langkah di [Buat AWS Secrets Manager rahasia untuk membuat rahasia Secrets Manager baru](#). Pastikan nama pengguna dan kata sandi disimpan menggunakan key/value pasangan dalam format{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}. Lihat [Otentikasi dan kontrol akses AWS Secrets Manager untuk](#) informasi tentang mengamankan akses ke rahasia.

Untuk informasi lebih lanjut tentang alat ini, lihat README.md file TROUBLESHOOTING.md dan file di FSx ADValidation file [Amazon](#).

Eksekusi Runbook

Jalankan runbook dengan parameter FSx ID Amazon atau AD. Berikut ini adalah alur kerja runbook:

- Mendapat parameter dari FSx ID Amazon atau menggunakan parameter AD input.
- Membuat instance Windows Amazon EC2 validasi sementara di subnet FSx Amazon, grup keamanan untuk akses SSM, peran dan kebijakan IAM (bersyarat) menggunakan CloudFormation. Jika InstanceId parameter ditentukan, itu digunakan.
- Mengunduh dan mengeksekusi skrip validasi pada instans Amazon EC2 target di subnet utama Amazon FSx.
- Menyediakan kode hasil validasi AD dalam output otomatisasi. Selain itu, output skrip lengkap diunggah ke bucket Amazon S3.

[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.

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackResources`
- `cloudformation:DescribeStackEvents`
- `ec2:CreateTags`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `ec2:CreateLaunchTemplate`
- `ec2>DeleteLaunchTemplate`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeLaunchTemplateVersions`
- `ec2:CreateSecurityGroup`
- `ec2>DeleteSecurityGroup`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupEgress`
- `iam:CreateRole`
- `iam:CreateInstanceProfile`
- `iam:GetInstanceProfile`

- `iam:getRolePolicy`
- `iam:DeleteRole`
- `iam:DeleteInstanceProfile`
- `iam:AddRoleToInstanceProfile`
- `iam:RemoveRoleFromInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:DetachRolePolicy`
- `iam:PutRolePolicy`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:PassRole`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetDocument`
- `ssm:GetAutomationExecution`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:ListCommandInvocations`
- `ssm:GetParameters`
- `ssm:ListCommands`
- `ssm:GetCommandInvocation`
- `fsx:DescribeFileSystems`
- `ds:DescribeDirectories`
- `s3:GetEncryptionConfiguration`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetAccountPublicAccessBlock`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketAcl`
- `s3:GetBucketLocation`

Contoh Kebijakan IAM untuk Otomasi Asumsikan Peran

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribe",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudFormation",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack"
      ],
      "Resource": "arn:*:cloudformation:*:*:stack/AWSSupport-ValidateFSxWindowsADConfig-*"
    },
    {
      "Sid": "AllowCreateLaunchTemplate",
      "Effect": "Allow",
      "Action": [

```

```

        "ec2:CreateLaunchTemplate",
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:launch-template/*"
    ]
},
{
    "Sid": "AllowEC2RunInstances",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*"
    ]
},
{
    "Sid": "AllowEC2RunInstancesWithTags",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
    ]
},
{
    "Sid": "EC2SecurityGroup",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateTags"
    ]
}

```

```

    ],
    "Resource": [
        "arn:*:ec2:*:*:security-group/*",
        "arn:*:ec2:*:*:vpc/*"
    ]
},
{
    "Sid": "EC2Remove",
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteSecurityGroup"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:*:ec2:*:*:security-group/*"
    ]
},
{
    "Sid": "IAMInstanceProfile",
    "Effect": "Allow",
    "Action": [
        "iam:CreateInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam:GetInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource": "arn:*:iam:*:*:instance-profile/*"
},
{
    "Sid": "IAM",
    "Effect": "Allow",
    "Action": [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:getRolePolicy",
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy",
        "iam:GetRole",

```

```

        "iam:TagRole"
      ],
      "Resource": "arn:*:iam:*:role/*"
    },
    {
      "Sid": "SSM",
      "Effect": "Allow",
      "Action": [
        "ssm:StartAutomationExecution",
        "ssm:GetDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:GetCommandInvocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSMSendCommand",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript"
    },
    {
      "Sid": "SSMSendCommandOnlyFsxInstance",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/CreatedBy": [
            "AWSSupport-ValidateFSxWindowsADConfig"
          ]
        }
      }
    }
  ],
}

```

```

        {
            "Sid": "AllowPassRoleToEC2",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:*:iam:*:role/AWSSupport-
ValidateFSxWindowsADConfig-*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "ec2.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation"
            ],
            "Resource": "*"
        }
    ]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-ValidateFSxWindowsADConfig](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk memvalidasi iklan yang dikelola sendiri dengan FSx Amazon yang gagal atau salah konfigurasi, masukkan parameter 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.

- **FSxId (Bersyarat):**

ID Server File Amazon FSx untuk Windows. Ini diperlukan untuk memvalidasi Amazon yang gagal atau salah konfigurasi yang ada. FSx

- **SecretArn (Diperlukan):**

ARN rahasia Secrets Manager Anda yang berisi nama pengguna dan kata sandi akun FSx layanan Amazon. Pastikan nama pengguna dan kata sandi disimpan menggunakan key/value pasangan dalam format `{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}`. CloudFormation Tumpukan membuat instance validasi dengan izin `GetSecretValue` untuk melakukan ARN ini.

- **FSxSecurityGroupId (Diperlukan):**

ID grup keamanan untuk Amazon FSx untuk Windows File Server.

- **BucketName (Diperlukan):**

Bucket Amazon S3 untuk mengunggah hasil validasi ke. Pastikan bucket dikonfigurasi dengan enkripsi sisi server (SSE) dan kebijakan bucket tidak memberikan read/write izin yang tidak perlu kepada pihak yang tidak perlu mengakses log. Juga pastikan bahwa instans Amazon EC2 Windows memiliki akses yang diperlukan ke bucket Amazon S3.

Input parameters**InstanceId**

(Optional) The ID of an existing AWS Systems Manager managed Windows Server Amazon EC2 instance where you intend to run the validation script. The instance requires the [AWS Tools for PowerShell](https://docs.aws.amazon.com/powershell/) to be installed. ****Caution****: The script will temporarily modify the DNS configuration of the instance, which may result in loss of network connectivity. To avoid disruptions, ****do not use a production instance****. Ensure the selected instance is designated for testing purposes only. Please ensure that access to the contents of the instance's volume is not exposed to parties that do not need to access the logs.

☐ Show interactive instance picker

`AWS::EC2::Instance::Id`

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.

`fsx-test`

BucketName

(Required) The Amazon S3 bucket to upload the validation results 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.

`test-for-customer`

RetainCloudFormationStack

(Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

`false`

SecretArn

(Required) The ARN of your AWS Secrets Manager secret containing the FSx service account username and password. Make sure that the username and password are stored using a key/value pair in the format `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`.

`arn:aws:secretsmanager:us-west-2:123456789012:secret:fsx-test`

FSxSecurityGroupId

(Required) The security group ID of the Amazon FSx for Windows File Server.

`sg-examplesg1234`

FSxId

(Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.

`fs-abcdef123456789`

4. Untuk memvalidasi konfigurasi AD yang dikelola sendiri untuk FSx pembuatan Amazon baru, masukkan parameter 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.

- SecretArn (Diperlukan):

ARN rahasia Secrets Manager Anda yang berisi nama pengguna dan kata sandi akun FSx layanan Amazon. Pastikan nama pengguna dan kata sandi disimpan menggunakan key/value pasangan dalam format `{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}`. CloudFormation Tumpukan membuat instance validasi dengan izin `GetSecretValue` untuk melakukan ARN ini.

- FSxSecurityGroupId (Diperlukan):

ID grup keamanan untuk Amazon FSx untuk Windows File Server.

- BucketName (Diperlukan):

Bucket Amazon S3 untuk mengunggah hasil validasi ke. Pastikan bucket dikonfigurasi dengan enkripsi sisi server (SSE) dan kebijakan bucket tidak memberikan read/write izin yang tidak

perlu kepada pihak yang tidak perlu mengakses log. Juga pastikan bahwa instans Amazon EC2 Windows memiliki akses yang diperlukan ke bucket Amazon S3.

- **FSxPreferredSubnetId**(Bersyarat):

Amazon FSx untuk Windows File Server lebih disukai subnet.

- **DomainName** (Bersyarat):

Nama domain yang sepenuhnya memenuhi syarat dari domain Microsoft AD Anda yang dikelola sendiri.

- **DnsIpAddresses** (Bersyarat):

Daftar hingga dua alamat IP server DNS atau pengontrol domain di domain AD yang dikelola sendiri. Hingga dua IPs, masukkan mereka dipisahkan dengan koma.

- **FSxAdminsGroup** (Bersyarat):

Amazon FSx untuk Windows File Server mendelegasikan grup administrator sistem file. Secara default, ini adalah `Domain Admins`.

- **FSxOrganizationalUnit**(Bersyarat):

Unit Organisasi (OU) di mana Anda ingin bergabung dengan sistem file Anda. Berikan nama jalur yang dibedakan dari OU. Contoh: `OU=org,DC=example,DC=com`.

RetainCloudFormationStack

(Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

false

TestServiceAccountPermissions

(Optional) Enable service account permission validation. This validation will create test Active Directory computer objects in the Microsoft Active Directory Organizational Unit. The resources are cleaned up by the script unless delete permissions are not properly configured on the provided service account in which case manual cleanup may be necessary.

true

DnsIpAddresses

(Conditional) A list of up to two DNS server or domain controller IP addresses in your self-managed AD domain. Required if the `FSxId` parameter is not specified. For up to two IPs, enter them separated by a comma.

10.0.1.10

FSxSecondarySubnetId

(Conditional) The Amazon FSx for Windows File Server secondary subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Optional if the `FSxId` parameter is not specified.

String

FSxOrganizationalUnit

(Conditional) The Organizational Unit (OU) within which you want to join your file system. Provide the distinguished path name of the OU. Example: `OU=org,DC=example,DC=com`. Optional if the `FSxId` parameter is not specified.

OU=testou,DC=example,DC=com

FSxId

(Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.

String

DomainName

(Conditional) The fully qualified domain name of your self-managed Microsoft Active Directory domain. Required if the `FSxId` parameter is not specified.

example.com

FSxPreferredSubnetId

(Conditional) The Amazon FSx for Windows File Server preferred subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Required if the `FSxId` parameter is not specified.

subnet-test1234example

FSxAdminsGroup

(Conditional) The Amazon FSx for Windows File Server delegated file system administrators group. Optional if the `FSxId` parameter is not specified. By default, this is `Domain Admins`.

Domain Admins

InstanceKeyPairName

(Conditional) An existing Amazon EC2 key pair you want to associate to the temporary Amazon EC2 instance. Optional when the `InstanceId` parameter is not specified.

String

5. Pilih Jalankan.

6. Otomatisasi dimulai.

7. Dokumen melakukan langkah-langkah berikut:

- `CheckBucketPublicStatus(AWS: ExecuteScript)`:

Memeriksa apakah bucket Amazon S3 target berpotensi memberikan akses publik baca and/or tulis ke objeknya.

- `BranchOnInputParameters(aws: cabang)`:

Cabang pada parameter input yang disediakan seperti parameter FSx ID Amazon atau Amazon FSx.

- `AssertFileSystemTypelsWindows(aws: assertAwsResource Properti)`:

Jika FSx ID Amazon disediakan, memvalidasi jenis sistem file Amazon FSx untuk Windows File Server.

- `GetValidationInputs(AWS: ExecuteScript)`:

Mengembalikan konfigurasi Microsoft AD yang dikelola sendiri yang diperlukan oleh CloudFormation template untuk membuat instans Amazon EC2.

- `BranchOnInstanceId (aws: cabang)`:

Cabang pada input yang disediakan `InstanceId`. Jika `InstanceId` disediakan, skrip validasi berjalan pada instans Amazon EC2 target dari otomatisasi. `step:RunValidationScript`

- `Buat EC2 InstanceStack (AWS:CreateStack)`:

Membuat instans Amazon EC2 di subnet pilihan menggunakan CloudFormation tempat `AmazonFSxADValidation` alat akan dijalankan

- `DescribeStackResources(aws:executeAwsApi)`:

Menjelaskan CloudFormation tumpukan untuk mendapatkan ID instans Amazon EC2 sementara.

- `WaitForEC2InstanceToBeManaged(aws: waitForAwsResourceProperty)`:

Menunggu hingga instans Amazon EC2 dikelola oleh Systems Manager untuk menjalankan skrip validasi menggunakan SSM Run Command.

- `GetAmazonFSxADValidationLampiran (aws:executeAwsApi)`:

Mendapat URL `AmazonFSxADValidation` alat dari lampiran runbook.

- `RunValidationScript(AWS:runcommand)`:

Menjalankan `AmazonFSxADValidation` alat pada instans Amazon EC2 sementara dan menyimpan hasilnya di bucket Amazon S3 yang ditentukan dalam parameter. `BucketName`

- `DescribeErrorsFromStackEvents(AWS: ExecuteScript)`:

Menjelaskan peristiwa CloudFormation tumpukan jika runbook gagal membuat tumpukan.

- `BranchOnRetainCloudFormationStack(aws:cabang)`:

Cabang pada `InstanceId` parameter `RetainCloudFormationStack` dan untuk menentukan apakah CloudFormation tumpukan harus dihapus.

- `DeleteCloudFormationStack(AWS>DeleteStack)`:

Menghapus CloudFormation tumpukan.

8. Setelah selesai, tinjau bagian Output untuk hasil eksekusi:

```

▼ Outputs

DescribeInstanceAndSubnet.InstanceId
i-06: [REDACTED]

CreateEC2InstanceStack.CloudFormationStackId
arn:aws:cloudformation:us-east-1:3[REDACTED]:stack/AWSSupport-ValidateFSxWindowsADConfig-3428bd96-f8ca-4c8d-9b02-57d81560bac8/67c23cc0-3585-11ef-868f-0efb7b77b54b

RunValidationScript.Output
AmazonFSxADValidation tool downloaded and extracted successfully.
RSAT-AD-PowerShell installed successfully.

Running Test-FSxADConfiguration with parameters:
DomainDNSRoot: self.msfc.com
DnsIpAddresses: 10.10.1.191
SubnetIds: subnet-0[REDACTED]
TestServiceAccountPermissions: True
TranscriptDirectory: C:\ProgramData\Amazon\AmazonFSxADValidation\3428bd96-f8ca-4c8d-9b02-57d81560bac8
AdminGroup: Domain Admins
OrganizationalUnit:

=====
The validation details and logs can be found in the bucket test-for-customer.

ERRORS: 1
- InvalidCredentials

WARNINGS: 0

For detailed information about a given warning or error, see C:\ProgramData\Amazon\AmazonFSxADValidation\AmazonFSxADValidation\TROUBLESHOOTING.md.

=====
The local DNS configuration has been reset successfully.

```

Runbook akan mengunggah hasil eksekusi skrip validasi ke bucket Amazon S3.

Referensi

Otomatisasi Systems Manager

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

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

AWS dokumentasi layanan

- [Apa itu Amazon FSx untuk Windows File Server?](#)
- [Memvalidasi konfigurasi AD yang dikelola sendiri FSx untuk Amazon untuk Windows File Server](#)

GuardDuty

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon.

GuardDuty Untuk informasi lebih lanjut 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

Tipe: 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 adalahENABLED. Status

IAM

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk. AWS Identity and Access Management Untuk informasi lebih lanjut tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSSupport-TroubleshootIAMAccessDeniedEvents](#)
- [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](#)
- [AWSSupport-ContainIAMPrincipal](#)
- [AWSSupport-TroubleshootSAMLIssues](#)

AWSSupport - Troubleshoot IAM Access Denied Events

Deskripsi

Runbook AWSSupport-TroubleshootIAMAccessDeniedEvents otomatisasi membantu pemecahan masalah AWS Identity and Access Management (IAM) akses ditolak. Kueri buku runbook CloudTrail untuk akses terbaru menolak peristiwa yang terkait dengan entitas IAM dan sumber peristiwa AWS layanan yang ditentukan. Ini menganalisis peristiwa dalam jendela waktu yang dapat dikonfigurasi hingga 24 jam, memproses hingga 10 peristiwa per eksekusi. Setiap peristiwa yang ditolak akses yang diidentifikasi diperiksa untuk membantu memahami konteks penolakan dan tindakan yang dicoba. Otomatisasi menganalisis kebijakan IAM berbasis identitas dan sumber daya. Untuk kebijakan berbasis identitas, ini memeriksa kebijakan inline dan terkelola yang dilampirkan pada entitas IAM. Untuk kebijakan berbasis sumber daya, ini mengevaluasi kebijakan di beberapa layanan AWS termasuk Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), Amazon Key Management Service (AWS KMS), Amazon Elastic Container Registry (Amazon ECR), Amazon API Gateway, Amazon Elastic File System (Amazon EFS), Amazon Simple Queue Service (Amazon SQS), Amazon IAM, dan AWS Cloud9, OpenSearch, AWS Serverless Application Repository, dan AWS Secrets Manager.

Runbook menggunakan kemampuan simulasi kebijakan IAM untuk mengevaluasi kebijakan ini terhadap tindakan yang ditolak yang ditemukan dalam peristiwa tersebut. CloudTrail

Runbook memanfaatkan kemampuan simulasi kebijakan IAM baik untuk pengguna IAM maupun [SimulatePrincipalPolicy](#) untuk peran IAM [SimulateCustomPolicy](#) untuk mengevaluasi kebijakan ini terhadap tindakan yang ditolak yang ditemukan dalam peristiwa tersebut. CloudTrail Otomatisasi menghasilkan laporan yang membantu mengidentifikasi tindakan spesifik yang ditolak, membedakan antara penolakan implisit dan eksplisit, mencantumkan kebijakan yang bertanggung jawab atas penolakan akses dan memberikan penjelasan untuk setiap penolakan. Laporan ini juga menyarankan resolusi potensial, seperti mengidentifikasi pernyataan allow yang hilang atau pernyataan penolakan yang bertentangan

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Menjelaskan dan memvalidasi `RequesterARN` (peran atau pengguna) untuk mendapatkan informasi seperti tipe entitas IAM, dan Id IAM.
- Mengambil CloudTrail peristiwa yang terkait dengan `RequesterARN`, `EventSource`, dan `ResourceARN` jika disediakan.
- Menganalisis CloudTrail peristiwa untuk mendapatkan tindakan yang dilakukan ketika kesalahan Access Denied dikembalikan, kemudian memeriksa semua kebijakan IAM seperti kebijakan inline dan terkelola yang dilampirkan pada entitas IAM, serta kebijakan berbasis sumber daya. Kemudian mensimulasikan kebijakan ini terhadap tindakan yang ditemukan dalam kesalahan Access Denied dari CloudTrail peristiwa yang dimaksud untuk menentukan penyebab kesalahan.
- Mengeluarkan laporan yang menentukan jenis kesalahan Akses Ditolak, kebijakan yang bertanggung jawab atas kesalahan, dan memberikan saran untuk solusi potensial untuk kesalahan tersebut.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `apigateway:GetRestApis`
- `cloudtrail:LookupEvents`
- `cloud9:GetEnvironment`
- `codeartifact:GetRepositoryPermissionsPolicy`
- `ecr:GetRepositoryPolicy`
- `elasticfilesystem:GetFileSystemPolicy`
- `es:DescribeDomain`
- `iam:GetPolicy`
- `iam:GetPolicyVersion`
- `iam:GetRole`
- `iam:GetRolePolicy`
- `iam:GetUser`
- `iam:GetUserPolicy`
- `iam:ListAttachedRolePolicies`
- `iam:ListAttachedUserPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`
- `iam:SimulatePrincipalPolicy`
- `iam:SimulateCustomPolicy`
- `kms:GetKeyPolicy`
- `lambda:GetPolicy`
- `secretsmanager:GetResourcePolicy`
- `serverlessrepo:GetApplication`
- `signer:GetSigningProfile`
- `sns:GetTopicAttributes`
- `ssm:StartAutomationExecution`

- `ssm:StopAutomationExecution`
- `sqs:GetQueueAttributes`
- `s3:GetBucketPolicy`

Contoh Kebijakan:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:GetUser",
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "iam:ListUserPolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetUserPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedUserPolicies",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "cloudtrail:LookupEvents",
        "iam:SimulateCustomPolicy"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetBucketPolicy",
        "kms:GetKeyPolicy",
        "lambda:GetPolicy",
        "sns:GetTopicAttributes",
        "ecr:GetRepositoryPolicy",
        "apigateway:GET",
```



```

        "codeartifact:GetRepositoryPermissionsPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "sqs:GetQueueAttributes",
        "cloud9:DescribeEnvironmentStatus",
        "es:DescribeDomain",
        "signer:GetSigningProfile",
        "serverlessrepo:GetApplication",
        "secretsmanager:GetResourcePolicy"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - Troubleshoot IAM Access Denied Events](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan SSM Automation untuk melakukan tindakan atas nama Anda. Peran tersebut perlu ditambahkan ke entri akses kluster Amazon EKS atau izin RBAC untuk mengizinkan panggilan API Kubernetes.
 - Tipe: `AWS::IAM::Role::Arn`
 - requesterARN (Diperlukan):
 - Deskripsi: (Wajib) ARN pengguna IAM atau peran yang ingin Anda selidiki izin akses pada sumber daya tertentu. AWS
 - Tipe: String
 - Izinkan Pola: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam:[0-9]{12}:(role|user)\\/[\\w+\\/=, .@-]+$`
 - ResourceArn (Opsional):

- Deskripsi: (Opsional) ARN sumber daya AWS yang aksesnya ditolak dievaluasi. Sumber daya AWS target harus ada di wilayah yang sama di mana runbook otomatisasi dijalankan.
- Tipe: String
- Izinkan Pola: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:([a-zA-Z0-9\\-]{1,63}):([a-z0-9\\-]{0,63})?:((\\d{12})?:([a-zA-Z0-9\\-_/:.]{1,1024}))$`
- EventSource (Diperlukan):
 - Deskripsi: (Wajib) Titik akhir Amazon API tempat CloudTrail kejadian berasal. Sebagai contoh: `s3.amazonaws.com`.
 - Tipe: String
 - Izinkan Pola: `^([a-zA-Z0-9.-]+)\\.amazonaws\\.com$`
- EventName (Opsional):
 - Deskripsi: (Opsional) Nama tindakan Amazon API yang terkait dengan CloudTrail acara tersebut. Sebagai contoh: `s3:CreateBucket`.
 - Tipe: String
 - Izinkan Pola: `^$|^([a-z0-9]+:[A-Za-z0-9])+$`
- LookBackHours (Opsional):
 - Deskripsi: (Opsional) Jumlah jam untuk melihat kembali CloudTrail acara saat mencari Access Denied acara. Rentang yang valid: 1 hingga 24 berjam-jam.
 - Jenis: Integer
 - Izinkan Pola: `^([1-9]|1[0-9]|2[0-4])$`
 - Default: 12
- MaxEvents (Opsional):
 - Deskripsi: (Opsional) Jumlah maksimum CloudTrail Access Denied acara yang dikembalikan saat mencari acara. Rentang yang valid: 1 ke 5 acara.
 - Jenis: Integer
 - Izinkan Pola: `^([1-9]|1[0-9]|2[0-4])$`
 - Default: 3
- UseContextEntries (Opsional):
 - Deskripsi: (Opsional) Jika Anda menentukan `true`, otomatisasi mengekstrak detail tentang konteks permintaan API dari CloudTrail peristiwa dan menyertakannya untuk simulasi kebijakan IAM.

- Jenis: Boolean
- Izinkan Pola: `^([1-9]|1[0-9]|2[0-4])$`
- Default: 3

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- `ValidateRequesterArn`

Memvalidasi dan mendekonstruksi `RequesterArn` ARN, mengambil informasi tentang pengguna atau peran IAM target.

- `GetCloudTrailEventsWithAccessDeniedError`

Menanyakan CloudTrail peristiwa untuk `Access Denied` peristiwa terbaru yang terkait dengan entitas dan AWS layanan IAM yang ditentukan. `EventSource`

- Evaluasi `IAMRequester` Kebijakan

Mengevaluasi izin IAM dari entitas IAM pemohon terhadap tindakan dari peristiwa. CloudTrail Evaluasi ini mencakup analisis kebijakan berbasis identitas dan berbasis sumber daya yang terkait dengan pemohon. Otomatisasi menggunakan kemampuan simulasi kebijakan IAM untuk menilai kebijakan ini dalam konteks tindakan yang ditolak yang diidentifikasi dalam peristiwa tersebut. CloudTrail

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

- `PermissionEvaluationResults`

Menghasilkan laporan yang membantu mengidentifikasi tindakan spesifik yang ditolak, membedakan antara penolakan implisit dan eksplisit. Ini juga mencantumkan kebijakan yang bertanggung jawab atas penolakan akses dan memberikan penjelasan untuk setiap penolakan. Laporan ini juga menyarankan resolusi potensial, seperti mengidentifikasi pernyataan `allow` yang hilang atau pernyataan penolakan yang bertentangan

Referensi

Otomatisasi Systems Manager

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

- [Menyiapkan Otomasi](#)
- [Support Automation Workflow landing page](#)

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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instance yang ingin Anda tetapkan peran IAM.

- RoleName

Tipe: 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- DisassociateInstanceProfile` - 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- AttachInstanceProfileToInstance` - Lampirkan peran profil instans IAM ke instans EC2.
 - i. 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- AttachInstanceProfileToInstanceWithRetry` - Lampirkan peran profil instans IAM ke instans EC2.

Keluaran

Lampirkan IAMProfileToInstanceWithRetry. AssociationId

GetInstanceProfile.InstanceProfileName

GetInstanceProfile.InstanceProfileArn

Lampirkan IAMProfileToInstance. 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

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Daftar terpisah koma ARNs 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

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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`

Tipe: 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.

- `IAMResourceId`

Tipe: 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

Tipe: 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.

- IAMResourceId

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama penganalysis yang akan dibuat.

- AutomationAssumeRole

Tipe: 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

Tipe: 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.

- IAMGroupName

Tipe: String

Default: ExampleSupportAndBillingGroup

Deskripsi: (Wajib) Dapat berupa grup baru atau yang sudah ada. Harus mematuhi [Batas Nama Entitas IAM](#).

- IAMUserName

Tipe: String

Default: ExampleUser

Deskripsi: (Wajib) Harus pengguna yang sudah ada.

- LambdaAssumeRole

Tipe: String

Deskripsi: (Opsional) ARN dari peran yang diasumsikan oleh lambda.

- Izin

Tipe: 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:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:*:111122223333: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 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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) ID pengguna yang ingin Anda hapus kebijakannya.

- `PolicyType`

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID pengguna, grup, atau peran IAM yang kebijakan sebarisnya 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`

Tipe: 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.

- `IAMResourceId`

Tipe: String

Deskripsi: (Wajib) ID sumber daya IAM yang ingin Anda cabut kredensialnya yang tidak digunakan.

- `MaxCredentialUsageAge`

Tipe: 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 kredensi 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`

Tipe: 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 Konsol Manajemen AWS 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 `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 `true`, kata sandi pengguna IAM harus berisi karakter numerik (0-9).

- `RequireSymbols`

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika diatur `true`, kata sandi pengguna IAM harus berisi karakter non-alfanumerik (! @ # \$ % ^ * () _ + - = [] { } | ').

- `RequireUppercaseCharacters`

Jenis: Boolean

Bawaan: salah

Deskripsi: (Opsional) Jika diatur `true`, 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

AWSSupport-ContainIAMPrincipal

Deskripsi

Jika terjadi insiden keamanan atau dugaan kompromi dari pengguna AWS Identity and Access Management (IAM) Pengguna/Peran atau Pusat AWS Identitas (IDC), isolasi cepat identitas yang terpengaruh sangat penting sambil mempertahankan konfigurasinya untuk penyelidikan. `AWSSupport-ContainIAMPrincipalRunbook` menyediakan pendekatan terstruktur dan reversibel untuk memuat identitas IAM atau IDC yang dikompromikan, secara efektif memblokir akses mereka ke AWS sumber daya dan mencegah potensi penyebaran kompromi.

Proses otomatis ini memungkinkan investigasi tanpa perubahan permanen konfigurasi identitas, memungkinkan pemulihan akses normal bila dianggap tepat. Proses penahanan mempertahankan pengguna atau peran dalam IAM atau pengguna dalam IDC, sementara secara efektif mengisolasinya dari semua aktivitas jaringan. Isolasi ini mencegah sumber daya identitas yang terkandung berkomunikasi dengan sumber daya di dalam Amazon Virtual Private Cloud Anda atau mengakses sumber daya internet. Penahanan dirancang agar dapat dibalik, memungkinkan pemulihan akses normal bila dianggap tepat.

Bagaimana cara kerjanya?

`AWSSupport-ContainIAMPrincipalRunbook` mengimplementasikan proses penahanan yang komprehensif untuk pengguna IAM, peran, dan pengguna Pusat Identitas. Saat dijalankan dalam `Contain` mode, pertama-tama memvalidasi semua parameter input dan melakukan pemeriksaan keamanan pada bucket Amazon S3 yang ditentukan. Kemudian mengumpulkan informasi rinci tentang target utama IAM dan menerapkan langkah-langkah penahanan yang sesuai berdasarkan jenis utama. Untuk pengguna IAM, ini menonaktifkan kunci akses, menghapus akses konsol, dan melampirkan kebijakan penolakan. Untuk peran IAM, ini melampirkan kebijakan penolakan yang mencabut izin untuk sesi yang dibuat sebelum penahanan. Untuk pengguna Pusat Identitas, ini menghapus set izin, keanggotaan grup, dan menerapkan kebijakan penolakan. Sepanjang proses, runbook mencadangkan konfigurasi asli ke bucket Amazon S3 untuk potensi pemulihan. Saat dijalankan dalam `Restore` mode, ia mencoba mengembalikan prinsipal ke status pra-penahanannya menggunakan konfigurasi yang dicadangkan. Runbook menyertakan `DryRun` opsi untuk melihat

pratinjau perubahan tanpa menerapkannya, dan menyediakan pelaporan komprehensif tentang operasi yang berhasil dan skenario kegagalan.

Important

- **Penggunaan Hak Istimewa Tinggi:** Dokumen SSM ini melakukan berbagai operasi yang memerlukan hak istimewa yang lebih tinggi, seperti memodifikasi kebijakan identitas IAM dan IDC dan menerapkan konfigurasi karantina. Tindakan ini berpotensi menyebabkan eskalasi hak istimewa atau berdampak pada beban kerja lain yang bergantung pada identitas yang ditargetkan. Anda harus meninjau izin yang diberikan untuk peran yang ditentukan oleh `AutomationAssumeRole` parameter dan memastikannya sesuai untuk kasus penggunaan yang dimaksudkan. Anda dapat merujuk ke AWS dokumentasi berikut untuk informasi lebih lanjut tentang izin IAM:
 - [Izin Identity and Access Management \(IAM\)](#)
 - [AWS Izin Otomasi Systems Manager](#)
- **Risiko Ketidaktersediaan Beban Kerja:** Dokumen Systems Manager ini melakukan tindakan isolasi yang berpotensi menyebabkan tidak tersedianya atau gangguan pada beban kerja Anda. Ketika dijalankan selama peristiwa keamanan, itu akan membatasi akses ke sumber daya yang terpengaruh dengan mencabut izin AWS API dari identitas IAM dan IDC yang ditentukan, mencegah mereka melakukan panggilan atau tindakan API apa pun. AWS Ini dapat memengaruhi aplikasi atau layanan apa pun yang bergantung pada identitas ini.
- **Pembuatan Sumber Daya Tambahan:** Dokumen otomatisasi dapat membuat sumber daya tambahan secara kondisional, seperti bucket Amazon Simple Storage Service (Amazon S3) dan objek Amazon S3 yang disimpan di dalamnya, tergantung pada parameter eksekusi. Sumber daya ini akan dikenakan biaya tambahan berdasarkan AWS penggunaan Anda.
- **Risiko Restorasi:** Jika parameter Action disetel ke `Restore`, dokumen SSM ini mencoba mengembalikan konfigurasi identitas IAM atau IDC ke keadaan semula. Namun, ada risiko bahwa proses restorasi mungkin gagal, meninggalkan identitas IAM atau IDC dalam keadaan tidak konsisten. Dokumen ini memberikan instruksi untuk restorasi manual jika terjadi kegagalan tersebut, tetapi Anda harus siap untuk menangani masalah potensial selama proses restorasi.

Disarankan untuk meninjau runbook secara menyeluruh, memahami potensinya, dan mengujinya di lingkungan non-produksi sebelum menjalankannya di lingkungan produksi Anda.

Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan izin berikut agar berhasil menggunakan runbook:

- s3: GetBucketLocation
- s3: GetBucket
- s3: ListBucket
- s3: GetBucketPublicAccessBlocks
- s3: GetAccountPublicAccessBlocks
- s3: GetBucketPolicyStatus
- s3: GetBucketAcl
- s3: GetObject
- s3: CreateBucket
- s3: PutObject
- saya: GetUser
- saya: GetUserPolicy
- saya: GetRole
- saya: ListUserPolicies

- saya: ListAttachedUserPolicies
- saya: ListAccessKeys
- saya: ListMfaDevices
- saya: ListVirtual MFADevices
- saya: GetLoginProfile
- saya: GetPolicy
- saya: GetRolePolicy
- saya: ListPolicies
- saya: ListAttachedRolePolicies
- saya: ListRolePolicies
- saya: UpdateAccessKey
- saya: CreateAccessKey
- saya: DeleteLoginProfile
- saya: DeleteAccessKey
- saya: PutUserPolicy
- saya: DeleteUserPolicy
- iam:Nonaktifkan MFADevice
- saya: AttachRolePolicy
- saya: AttachUserPolicy
- saya: DeleteRolePolicy
- iam:Tag MFADevice
- saya: PutRolePolicy
- saya: TagPolicy
- saya: TagRole
- saya: TagUser
- saya: UntagUser
- saya: UntagRole
- organisasi: ListAccounts
- sso: ListPermissionSetsProvisionedToAccount
- sso: GetInlinePolicyForPermissionSet

- sso: ListInstances
- sso-direktori: SearchUsers
- sso: ListPermissionSets
- sso: ListAccountAssignments
- sso-direktori: DescribeUser
- toko identitas: ListUsers
- toko identitas: ListGroups
- toko identitas: IsMemberInGroups
- toko identitas: ListGroupMemberships
- manajer rahasia: CreateSecret
- manajer rahasia: DeleteSecret
- sso: DeleteAccountAssignment
- sso: PutInlinePolicyToPermissionSet
- sso: CreateAccountAssignment
- sso: DeleteInlinePolicyFromPermissionSet
- sso: TagResource
- sso: UntagResource
- toko identitas: DeleteGroupMembership
- toko identitas: CreateGroupMembership

Berikut adalah contoh kebijakan IAM yang memberikan izin yang diperlukan untuk: AutomationAssumeRole

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
```

```

        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutObject"
    ],
    "Resource": "*"
},
{
    "Sid": "IAMPermissions",
    "Effect": "Allow",
    "Action": [
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetRole",
        "iam:ListUserPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListAccessKeys",
        "iam:ListMfaDevices",
        "iam:ListVirtualMFADevices",
        "iam:GetLoginProfile",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:ListPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:UpdateAccessKey",
        "iam:CreateAccessKey",
        "iam:DeleteLoginProfile",
        "iam:DeleteAccessKey",
        "iam:PutUserPolicy",
        "iam:DeleteUserPolicy",
        "iam:DeactivateMFADevice",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:DeleteRolePolicy",
        "iam:TagMFADevice",
        "iam:PutRolePolicy",
        "iam:TagPolicy",
        "iam:TagRole",
        "iam:TagUser",
        "iam:UntagUser",
        "iam:UntagRole"
    ]
}

```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "OrganizationsPermissions",
    "Effect": "Allow",
    "Action": [
      "organizations:ListAccounts"
    ],
    "Resource": "*"
  },
  {
    "Sid": "SSOPermissions",
    "Effect": "Allow",
    "Action": [
      "sso:ListPermissionSetsProvisionedToAccount",
      "sso:GetInlinePolicyForPermissionSet",
      "sso:ListInstances",
      "sso-directory:SearchUsers",
      "sso:ListPermissionSets",
      "sso:ListAccountAssignments",
      "sso-directory:DescribeUser",
      "sso:DeleteAccountAssignment",
      "sso:PutInlinePolicyToPermissionSet",
      "sso:CreateAccountAssignment",
      "sso:DeleteInlinePolicyFromPermissionSet",
      "sso:TagResource",
      "sso:UntagResource"
    ],
    "Resource": "*"
  },
  {
    "Sid": "IdentityStorePermissions",
    "Effect": "Allow",
    "Action": [
      "identitystore:ListUsers",
      "identitystore:ListGroups",
      "identitystore:IsMemberInGroups",
      "identitystore:ListGroupMemberships",
      "identitystore:DeleteGroupMembership",
      "identitystore:CreateGroupMembership"
    ],
    "Resource": "*"
  },
},

```

```

    {
      "Sid": "SecretsManagerPermissions",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource": "*"
    }
  ]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-ContainIAMPrincipal](#) konsol AWS Systems Manager.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - 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.
 - Tipe: `AWS::IAM::Role::Arn`
 - PrincipalType (Diperlukan):
 - Deskripsi: (Wajib) Tipe utama AWS IAM: pengguna IAM, peran IAM, atau pengguna Pusat Identitas.
 - Tipe: String
 - Nilai yang Diizinkan: `IAM user|IAM role|Identity Center user`
 - PrincipalName (Diperlukan):
 - Keterangan: (Wajib) Nama kepala sekolah IAM. Untuk pengguna Pusat Identitas, berikan nama pengguna.
 - Tipe: String
 - Pola yang Diizinkan: `^[a-zA-Z0-9\\.\\"-_\\"\\!*'()/+ =, @]{1,1024}$`

- Tindakan (Diperlukan):
 - Deskripsi: (Wajib) Pilih `Contain` untuk mengisolasi prinsipal IAM target atau `Restore` mencoba mengembalikan prinsipal IAM ke konfigurasi aslinya dari cadangan sebelumnya.
 - Tipe: String
 - Nilai yang Diizinkan: `Contain` | `Restore`
- DryRun (Opsional):
 - Deskripsi: (Opsional) Saat disetel ke `true`, otomatisasi tidak akan membuat perubahan apa pun pada prinsipal IAM target, melainkan akan menghasilkan apa yang akan dicoba diubah, merinci setiap langkah. Nilai default: `true`.
 - Jenis: Boolean
 - Nilai yang Diizinkan: `true` | `false`
- ActivateDisabledKeys(Bersyarat):
 - Deskripsi: (Bersyarat) Jika parameter input Tindakan diatur ke `Restore` dan diatur ke pengguna IAM, opsi ini menentukan apakah otomatisasi ini harus mencoba mengaktifkan kunci akses terkait jika dinonaktifkan. `PrincipalType` Harap dicatat bahwa integritas kunci akses yang dikompromikan tidak dapat diverifikasi. AWS sangat merekomendasikan untuk tidak mengaktifkan kembali kunci yang dikompromikan. Sebagai gantinya, disarankan untuk membuat kunci baru. Nilai default: `false`.
 - Jenis: Boolean
 - Nilai yang Diizinkan: `true` | `false`
- Backups3 BucketName (Bersyarat):
 - Deskripsi: (Bersyarat) Bucket Amazon S3 Amazon untuk mencadangkan konfigurasi utama IAM saat Tindakan disetel `Contain` ke atau memulihkan konfigurasi dari saat Tindakan dilakukan. `Restore` Perhatikan bahwa jika Action yang ditentukan adalah `Contain` dan runbook tidak dapat mengakses bucket atau nilai tidak disediakan, bucket baru akan dibuat di akun Anda dengan nama `awssupport-containiamprincipal-<random-string>` tersebut. Jika DryRun diatur ke parameter `true` ini diperlukan.
 - Tipe: `AWS::S3::Bucket::Name`
- Backups3 KeyName (Bersyarat):
 - Deskripsi: (Bersyarat) Jika Tindakan disetel ke `Restore`, ini menentukan kunci Amazon Amazon S3 yang akan digunakan otomatisasi untuk mencoba memulihkan konfigurasi utama IAM. Kunci Amazon Amazon S3 biasanya mengikuti format ini: `{year}/{month}/{day}/`

`{hour}/{minute}/{automation_execution_id}.json` Kuncinya dapat diperoleh dari output eksekusi otomatisasi penahanan sebelumnya.

- Tipe: String
- Pola yang Diizinkan: `^[a-zA-Z0-9\\.\_-\\\\!*'()/{0,1024}$`
- Backups3 BucketAccess (Bersyarat):
 - Deskripsi: (Bersyarat) ARN pengguna IAM atau peran yang akan diizinkan mengakses bucket Amazon Amazon S3 cadangan setelah menjalankan tindakan penahanan. Parameter ini diperlukan saat `ActionContain.AutomationAssumeRole`, atau jika tidak ada pengguna yang konteksnya otomatisasi berjalan secara otomatis ditambahkan ke daftar.
 - Jenis: StringList
 - Pola yang Diizinkan: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=, .@-]+$`
- TagIdentifier (Opsional):
 - Deskripsi: (Opsional) Tandai prinsipal IAM dengan tag pilihan Anda menggunakan format berikut: `Key=<EXAMPLE_KEY>,Value=<EXAMPLE_VALUE>`. Opsi ini memungkinkan Anda untuk melacak prinsip-prinsip IAM yang telah ditargetkan oleh runbook ini. Catatan: Kunci dan nilai tag peka huruf besar/kecil.
 - Tipe: String
 - Pola yang Diizinkan: `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\\\:\\\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\\\:\\\\/@a-zA-Z0-9]{0,128}$`

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- `ValidateRequiredInputs`

Memvalidasi parameter input otomatisasi yang diperlukan berdasarkan yang `Action` ditentukan.

- `CheckBackupS3 BucketName`

Memeriksa apakah bucket Amazon S3 target berpotensi memberikan `read` atau akses `write` publik ke objeknya. Dalam hal alur kerja penahanan, bucket Amazon Amazon S3 baru dibuat jika `BackupS3BucketName` bucket tidak ada.

Cabang otomatisasi berdasarkan nilai yang ditentukan `Action`.

- `BranchOnPrincipalTypeAndDryRun`

Cabang otomatisasi berdasarkan jenis prinsipal IAM (pengguna IAM, peran IAM, atau pengguna Pusat Identitas) dan jika berjalan dalam mode `DryRun`

- `BranchOnPrincipalTypeForContain`

Cabang otomatisasi untuk berbasis `Contain` tindakan dan tipe utama IAM (pengguna IAM, peran IAM, atau pengguna Pusat Identitas) yang ditentukan dalam input.

- Dapatkan `IAMUser`

Mendapat waktu pembuatan dan nama pengguna pengguna IAM target.

- Dapatkan `IAMUser Detail`

Mendapatkan dan menyimpan konfigurasi pengguna IAM target, termasuk kebijakan inline, kebijakan terkelola, kunci akses, perangkat MFA, dan profil login.

- Pembaruan3 `KeyForUser`

Memperbarui variabel otomatisasi '`S3Key`' dari output langkah. `GetIAMUserDetails`

- Dapatkan `IAMRole`

Mendapat waktu pembuatan, nama peran, dan jalur peran IAM target.

- Dapatkan `IAMRole Detail`

Mendapatkan dan menyimpan konfigurasi peran IAM target, termasuk kebijakan inline dan kebijakan terkelola yang dilampirkan pada peran tersebut.

- Pembaruan3 `KeyForRole`

Memperbarui variabel otomatisasi '`S3Key`' dari output langkah. `GetIAMRoleDetails`

- `GetIdentityStoreId`

Mendapat ID dari instans Pusat AWS Identitas IAM yang terkait dengan AWS akun.

- Dapatkan `IDCUser`

Mendapatkan ID pengguna pengguna Pusat Identitas target menggunakan ID Toko Identitas.

- Kumpulkan `IDCUser Detail`

Mendapatkan dan menyimpan konfigurasi pengguna Pusat Identitas target, termasuk penetapan akun, set izin terkait, dan kebijakan inline.

- `Pembaruan3 KeyFor IDCUser`

Memperbarui variabel otomatisasi 'S3Key' dari output langkah. `GatherIDCUserDetails`

- `BranchOnIdentityContain`

Cabang otomatisasi berdasarkan nilai `DryRun` dan tipe utama IAM untuk `Contain` tindakan tersebut.

- `BranchOnDisableAccessKeys`

Cabang otomatisasi berdasarkan apakah pengguna IAM memiliki kunci akses yang perlu dinonaktifkan.

- `DisableAccessKeys`

Menonaktifkan kunci akses pengguna IAM aktif.

- `BranchOnDisableConsoleAccess`

Cabang berdasarkan apakah pengguna IAM mengaktifkan akses AWS Management Console atau tidak.

- `DisableConsoleAccess`

Menghapus akses berbasis kata sandi pengguna IAM ke Konsol Manajemen. AWS

- `AttachInlineDenyPolicyToUser`

Melampirkan kebijakan penolakan ke pengguna IAM untuk mencabut izin untuk token sesi yang lebih lama.

- `AttachInlineDenyPolicyToRole`

Melampirkan kebijakan penolakan ke peran IAM untuk mencabut izin untuk token sesi yang lebih lama.

- `RemovePermissionSets`

Menghapus set izin yang terkait dengan pengguna Pusat Identitas.

- `Hapus IDCUser Dari IDCGroups`

Menghapus pengguna Pusat Identitas dari grup Pusat Identitas

- `AttachInlineDenyPolicyToPermissionSet`

Melampirkan kebijakan penolakan ke set izin yang terkait dengan pengguna Pusat Identitas.

- `BranchOnReactivateKeys`

Cabang otomatisasi berdasarkan `ActivatedDisabledKeys` parameter selama proses pemulihan.

- `DetachInlineDenyPolicy`

Menghapus kebijakan penolakan yang dilampirkan pada peran IAM selama proses penahanan.

- `DetachInlineDenyPolicyFromPermissionSet`

Menghapus kebijakan penolakan yang dilampirkan pada set izin selama proses penahanan.

- `ReportContain`

Mengeluarkan informasi rinci tentang tindakan penahanan yang akan dilakukan ketika `DryRun` diatur ke `True`

- `ReportRestore`

Mengeluarkan informasi rinci tentang tindakan restorasi yang akan dilakukan ketika `DryRun` diatur ke `True`.

- `ReportContainFailure`

Memberikan instruksi komprehensif untuk memulihkan konfigurasi asli kepala sekolah IAM secara manual selama skenario kegagalan alur kerja penahanan.

- `ReportRestoreFailure`

Memberikan instruksi terperinci untuk menyelesaikan pemulihan konfigurasi asli kepala sekolah IAM secara manual selama skenario kegagalan alur kerja pemulihan.

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

- `IAMPrincipalMengandung.Output`

Memberikan informasi rinci tentang tindakan penahanan yang dilakukan saat `Action` disetel ke `Contain` dan `DryRun` disetel ke `False`. Termasuk informasi tentang lokasi cadangan, kebijakan penolakan yang diterapkan, dan konfigurasi yang dimodifikasi.

- `Kembalikan IAMPrincipal .Output`

Memberikan informasi rinci tentang tindakan restorasi yang dilakukan saat Tindakan diatur ke Restore dan DryRun disetel ke False. Termasuk informasi tentang konfigurasi yang dipulihkan dan masalah apa pun yang dihadapi selama pemulihan.

- ReportContain.Keluaran

Mengeluarkan informasi rinci tentang tindakan penahanan yang akan dilakukan ketika Action diatur ke Contain dan DryRun disetel ke True. Termasuk perbandingan konfigurasi saat ini dan pasca-penahanan.

- ReportRestore.Keluaran

Mengeluarkan informasi rinci tentang tindakan restorasi yang akan dilakukan ketika Action diatur ke Restore dan DryRun disetel ke True. Menunjukkan konfigurasi saat ini dan konfigurasi asli yang akan dipulihkan.

- ReportContainFailure.Keluaran

Memberikan instruksi komprehensif untuk memulihkan konfigurasi asli kepala sekolah IAM secara manual selama skenario kegagalan alur kerja penahanan.

- ReportRestoreFailure.Keluaran

Memberikan instruksi terperinci untuk menyelesaikan pemulihan konfigurasi asli kepala sekolah IAM secara manual selama skenario kegagalan alur kerja pemulihan.

Keluaran

Setelah eksekusi selesai, tinjau bagian Output untuk hasil terperinci:

- IAMPrincipalMengandung.Output

Memberikan informasi rinci tentang tindakan penahanan yang dilakukan saat Action disetel ke Contain dan DryRun disetel ke False. Termasuk informasi tentang lokasi cadangan, kebijakan penolakan yang diterapkan, dan konfigurasi yang dimodifikasi.

- Kembalikan IAMPrincipal .Output

Memberikan informasi rinci tentang tindakan restorasi yang dilakukan saat Tindakan diatur ke Restore dan DryRun disetel ke False. Termasuk informasi tentang konfigurasi yang dipulihkan dan masalah apa pun yang dihadapi selama pemulihan.

- ReportContain.Keluaran

Mengeluarkan informasi rinci tentang tindakan penahanan yang akan dilakukan ketika Action diatur ke Contain dan DryRun disetel ke True. Termasuk perbandingan konfigurasi saat ini dan pasca-penahanan.

- ReportRestore.Keluaran

Mengeluarkan informasi rinci tentang tindakan restorasi yang akan dilakukan ketika Action diatur ke Restore dan DryRun disetel ke True. Menunjukkan konfigurasi saat ini dan konfigurasi asli yang akan dipulihkan.

- ReportContainFailure.Keluaran

Memberikan instruksi komprehensif untuk memulihkan konfigurasi asli kepala sekolah IAM secara manual selama skenario kegagalan alur kerja penahanan.

- ReportRestoreFailure.Keluaran

Memberikan instruksi terperinci untuk menyelesaikan pemulihan konfigurasi asli kepala sekolah IAM secara manual selama skenario kegagalan alur kerja pemulihan.

Referensi

Otomatisasi Systems Manager

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

AWSSupport-TroubleshootSAMLIssues

Deskripsi

Runbook AWSSupport-TroubleshootSAMLIssues otomatisasi membantu mendiagnosis masalah terkait Security Assertion Markup Language (SAMP) dengan menganalisis file respons SAMP yang disimpan di Amazon Simple Storage Service (Amazon S3). Ini melakukan validasi komprehensif termasuk verifikasi skema, validasi tanda tangan, pemeriksaan pembatasan audiens, dan verifikasi waktu kedaluwarsa. Runbook menerjemahkan dan mengekstrak elemen SAMP kunci termasuk penerbit, pernyataan, subjek, kondisi, tanda tangan, dan atribut dari respons SAMP. Untuk lingkungan di mana SAMP digunakan untuk mengakses AWS sumber daya (seperti Amazon Connect

atau Amazon WorkSpaces Applications) melalui Penyedia Identitas IAM, itu memverifikasi apakah sertifikat dalam tanda tangan respons SAMP cocok dengan sertifikat yang dikonfigurasi dalam Penyedia Identitas IAM.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Memvalidasi format respons SAMP dan elemen yang diperlukan.
- Mendekode dan mengekstrak komponen respons SAMP (penerbit, pernyataan, subjek, kondisi, tanda tangan, atribut).
- Memverifikasi tanda tangan digital terhadap sertifikat Penyedia Identitas IAM saat disediakan.
- Memeriksa batasan audiens dan validitas waktu.
- Memberikan informasi diagnostik terperinci yang menunjukkan struktur SAMP yang diurai dan hasil validasi.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `s3:GetBucketLocation`
- `s3:ListBucket`
- `s3:GetBucketPublicAccessBlock`

- s3:GetAccountPublicAccessBlock
- s3:GetObject
- s3:GetBucketPolicyStatus
- s3:GetEncryptionConfiguration
- s3:GetBucketOwnershipControls
- s3:GetBucketAcl
- s3:GetBucketPolicy
- s3:PutObject
- iam:GetSAMLProvider
- sts:AssumeRole

Contoh Kebijakan:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "iam:GetSAMLProvider",
        "sts:AssumeRole"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

```
    ]
}
```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Sebelum menggunakan runbook ini, Anda perlu menangkap dan menyimpan respons SAMP yang dikodekan Base64 (file txt) di bucket S3. [Petunjuk untuk menangkap tanggapan SAMP dapat ditemukan dalam dokumen ini](#)
2. Arahkan ke [AWSSupport-TroubleshootSAMLIssues](#) Systems Manager di bawah Documents.
3. Pilih Jalankan otomatisasi.
4. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran AWS Identity and Access Management (IAM) yang memungkinkan SSM Automation untuk melakukan tindakan atas nama Anda. Jika tidak ada peran yang ditentukan, Systems Manager Automation menggunakan izin pengguna yang memulai runbook ini.
 - Tipe: `AWS::IAM::Role::Arn`
 - InputFileS3URI (Diperlukan):
 - Deskripsi: (Diperlukan) Amazon Simple Storage Service (Amazon S3) URI dari file txt SAML Response (misalnya, `s3://bucket - .txt`). `name/path/to/file`
 - Tipe: String
 - Izinkan Pola: `^s3://[a-z0-9][a-z0-9.-][a-z0-9](/. )?.$`
 - S3 OutputPrefix (Opsional):
 - `<executionID of the runbook>` Deskripsi: (Opsional) File keluaran analisis disimpan dalam ember input dengan nama `'saml_analysis_ .json'`. Anda dapat menggunakan parameter ini jika Anda ingin menampilkan file dengan awalan tertentu. `<executionID of the runbook>` Nilai defaultnya adalah `"output"`, dalam hal ini URI file yang menampilkan hasilnya adalah `'s3:// bucket - name/output/saml _analysis_ .json'`.
 - Tipe: String
 - Izinkan Pola: `^[a-zA-Z0-9+=, .@\\-_/]*/$`
 - ExpectedAudience (Opsional):

- Deskripsi: (Opsional) Nilai audiens yang diharapkan dalam respons SAMP. Jika tidak ditentukan, kami menggunakan `urn:amazon:webservices`. Jika Anda telah mengonfigurasi nilai audiens tertentu dalam pengaturan IDP dan SP Anda, berikan format yang tepat (misalnya, `urn:amazon:webservices,https://signin.aws.amazon.com/saml`).
- Tipe: String
- Default: `urn:amazon:webservices`
- `IamIdProviderArn` (Opsional):
 - Deskripsi: (Opsional) Jika Anda menggunakan entitas Penyedia ID IAM untuk secara langsung menautkan IDP Anda AWS dengan IAM, harap berikan ARN-nya (mis., `arn:aws:iam::<account-id>saml-provider/<provider-name>`).
 - Tipe: String
 - Izinkan Pola: `^$|^arn:aws:iam::[0-9]{12}:saml-provider/[a-zA-Z0-9_-]+$`
- `SAMLAuthenticationWaktu` (Opsional):
 - Deskripsi: (Opsional) Tanggal dan waktu ketika otentikasi SAMP dilakukan. Zona waktu harus UTC. Harus dalam YYYY-MM-DDThh format:mm: ss (mis., `2025-02-01T 10:00:00`). Jika parameter ini tidak disediakan, pemeriksaan kedaluwarsa akan dilakukan terhadap stempel waktu saat ini.
 - Tipe: String
 - Izinkan Pola: `^$|^\\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[12]\\d|3[01])T(?:[01]\\d|2[0-3]):[0-5]\\d:[0-5]\\d$`
- `S3 BucketOwnerRoleArn` (Opsional):
 - Deskripsi: (Opsional) IAM Role ARN untuk mengakses bucket Amazon S3. ARN peran IAM dengan izin untuk mendapatkan bucket Amazon S3 dan pengaturan pemblokiran akun akses publik, konfigurasi enkripsi bucket, bucket, status kebijakan bucket ACLs, dan mengunggah objek ke bucket. Jika parameter ini tidak ditentukan, runbook menggunakan `AutomationAssumeRole` (jika ditentukan) atau pengguna yang memulai runbook ini (jika `AutomationAssumeRole` tidak ditentukan).
 - Tipe: `AWS::IAM::Role::Arn`

5. Pilih Jalankan.

6. Otomatisasi dimulai.

7. Dokumen melakukan langkah-langkah berikut:

- Validasi IAMIDProvider

Memvalidasi ARN Penyedia ID IAM yang disediakan dengan memeriksa apakah ada dan dapat diakses. Jika tidak ada ARN yang disediakan, validasi dilewati dan langkahnya berhasil diselesaikan.

- Ceks3 BucketPublicStatus

Memeriksa apakah bucket Amazon S3 mengizinkan izin akses baca atau tulis anonim, atau publik. Jika bucket mengizinkan izin ini, otomatisasi berhenti pada langkah ini.

- Ceks3 ObjectExistence

Memvalidasi akses ke bucket Amazon S3. Memeriksa apakah bucket dan objek ada dan apakah otomatisasi memiliki izin yang diperlukan untuk membaca dari sumber dan menulis ke tujuan.

- Menganalisis SAMLResponse

Menganalisis file respons SAMP dengan melakukan pemeriksaan (validasi skema, verifikasi tanda tangan, validasi audiens, pemeriksaan kedaluwarsa). Menghasilkan laporan JSON terperinci dan menyimpannya ke lokasi Amazon S3 yang ditentukan.

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

- Bagian output berisi informasi tentang objek Amazon S3 tempat hasil analisis dijelaskan.

9. Objek Amazon S3 dalam hasil analisis adalah file Json yang berisi informasi berikut:

- validation_result: berisi hasil validasi dasar dari respons SAMP.
 - saml_info: informasi SAMP kunci termasuk penerbit, tanda tangan, dan pernyataan.
 - schema_validation: hasil validasi skema SAMP.
- verification_result: memberikan hasil diagnostik yang lebih rinci.
 - tanda tangan: hasil verifikasi tanda tangan.
 - audiens: hasil validasi pembatasan audiens.
 - kedaluwarsa: hasil verifikasi waktu kedaluwarsa.

Referensi

Otomatisasi Systems Manager

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

Deteksi dan Respon Insiden

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Deteksi dan AWS Respons Insiden. Untuk informasi lebih lanjut tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSPremiumSupport-OnboardWorkloadToIDR](#)

AWSPremiumSupport-OnboardWorkloadToIDR

Deskripsi

AWSPremiumSupport-OnboardWorkloadToIDRRunbook ini membantu pelanggan AWS Enterprise Support dalam beban kerja untuk pemantauan dan manajemen insiden kritis menggunakan Deteksi dan Respons AWS Insiden. Beban kerja dapat didefinisikan sebagai kumpulan AWS sumber daya yang terkait dengan Grup AWS Sumber Daya atau AppRegistry aplikasi AWS Service Catalog. Jika Grup AWS Sumber Daya atau AppRegistry aplikasi AWS Service Catalog tidak ditentukan, runbook akan membuat Grup Sumber Daya atas nama Anda menggunakan filter tag atau ID AWS CloudFormation tumpukan yang sumber dayanya ingin disertakan dalam grup. Jika Anda mengatur parameter `CreateApplicationInsights` ke `Yes`, maka otomatisasi menyediakan aplikasi Amazon CloudWatch Application Insights menggunakan AWS CloudFormation. CloudWatch Wawasan Aplikasi menyiapkan metrik dan log yang direkomendasikan untuk sumber daya aplikasi yang dipilih menggunakan CloudWatch metrik Amazon, Log, dan Peristiwa untuk pemberitahuan tentang masalah yang terdeteksi.

Important

Runbook ini melakukan tindakan berikut di akun Anda tergantung pada parameter input yang disediakan:

- Membuat Grup AWS Sumber Daya baru menggunakan AWS CloudFormation jika `ResourceGroupName` atau `AppRegistryApplication` tidak ditentukan. Setelah tumpukan dibuat, runbook mencoba mengatur perlindungan terminasi.
- Menandai Grup AWS Sumber Daya terkait beban kerja, termasuk `aws_idr` tag.

- Membuat aplikasi berbasis grup Amazon CloudWatch Application Insights Resource jika parameter `CreateApplicationInsights` input disetel ke. `Yes` Setelah tumpukan dibuat, runbook mencoba mengatur perlindungan terminasi untuk tumpukan.
- Menginstal peran `AWSServiceRoleForHealth_EventProcessor` terkait layanan (SLR) untuk menyediakan akses untuk konsumsi peringatan ke Deteksi dan Respons Insiden jika parameter input disetel ke. `InstallServiceLinkedRole Yes`
- Membuat kasus AWS dukungan dengan Deteksi dan Respons AWS Insiden.

Important

Untuk menggunakan runbook ini dan onboard untuk Deteksi dan Respons AWS Insiden, Anda memerlukan AWS Dukungan Perusahaan (dengan biaya tambahan) atau Langganan Operasi Terpadu. Untuk informasi selengkapnya, lihat [Bandingkan Dukungan Paket](#).

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah tingkat tinggi berikut:

- Memeriksa apakah Rencana Dukungan AWS Akun saat ini adalah Perusahaan; jika tidak, otomatisasi berakhir.
- Menentukan apakah akan menggunakan Grup AWS Sumber Daya yang ada atau membuat yang baru berdasarkan parameter yang disediakan.
- Jika membuat Grup Sumber Daya baru, buat AWS CloudFormation template dan buat tumpukan dengan tag yang sesuai.
- Menandai Grup Sumber Daya dengan tag Deteksi dan Respons AWS Insiden yang diperlukan.
- Secara opsional menginstal peran terkait layanan untuk Deteksi dan Respons AWS Insiden.
- Secara opsional membuat aplikasi Amazon CloudWatch Application Insights untuk pemantauan yang ditingkatkan.
- Membuat kasus AWS dukungan untuk menyelesaikan proses orientasi.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `cloudformation:CreateStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateTerminationProtection`
- `iam:CreateServiceLinkedRole`
- `resource-groups:CreateGroup`
- `resource-groups:GetGroup`
- `resource-groups:TagResource`
- `servicecatalog-appregistry:GetApplication`
- `support:CreateCase`
- `support:DescribeSeverityLevels`
- `support:DescribeServices`
- `support:DescribeSupportLevel`

Contoh Kebijakan:

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

```

        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "iam:CreateServiceLinkedRole",
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:TagResource",
        "servicecatalog-appregistry:GetApplication",
        "support:CreateCase",
        "support:DescribeSeverityLevels",
        "support:DescribeServices",
        "support:DescribeSupportLevel"
    ],
    "Resource": "*"
}
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSPremiumSupport-OnboardWorkloadToIDR](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - 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.
 - Tipe: `AWS::IAM::Role::Arn`
 - WorkloadName (Diperlukan):
 - Deskripsi: (Wajib) Nama beban kerja. Jika tidak ResourceGroupName disediakan, nama beban kerja digunakan untuk menyiapkan Grup AWS Sumber Daya baru dengan nama IDR-AWS-<WorkloadName> tersebut.
 - Tipe: `String`
 - Izinkan Pola: `^[a-zA-Z0-9_-]{1,128}$`

- **WorkloadDescription (Diperlukan):**
 - Deskripsi: (Wajib) Deskripsi beban kerja. Masukkan deskripsi singkat untuk merinci kasus penggunaan beban kerja ini. Harap sertakan pengguna akhir utama dan fungsi beban kerja ini.
 - Tipe: String
 - Izinkan Pola: `^[a-zA-Z0-9.:;,-_&() ]{1,1024}$`
- **AppRegistryApplication (Opsional):**
 - Deskripsi: (Opsional) Nama atau ID AppRegistry aplikasi AWS Service Catalog. Jika tidak disediakan, Anda harus memberikan masukan untuk `ResourceGroupName`.
 - Tipe: String
 - Izinkan Pola: `^$|^[a-zA-Z0-9.-_]{1,128}$`
 - Default: ""
- **ResourceGroupName (Opsional):**
 - Deskripsi: (Opsional) Nama Grup AWS Sumber Daya yang `AppRegistryApplication` ada jika tidak disediakan. Jika Anda ingin membuat Grup Sumber Daya, Anda harus memberikan masukan untuk `TagFilters` dan secara opsional `ResourceTypeFilters` untuk membuat Grup AWS Sumber Daya baru.
 - Tipe: String
 - Izinkan Pola: `^$|^[a-zA-Z0-9_.-]{1,128}$`
 - Default: ""
- **TagFilters (Bersyarat):**
 - Deskripsi: (Bersyarat) Daftar pasangan key/values (string/daftar string) yang dibandingkan dengan tag yang dilampirkan ke sumber daya Anda. AWS Parameter ini digunakan untuk membuat Grup AWS Sumber Daya baru jika Anda tidak menentukan yang sudah ada `ResourceGroupName` atau `AppRegistryApplication`.
 - Tipe: StringMap
- **ResourceTypeFilters (Bersyarat):**
 - Deskripsi: (Bersyarat) Daftar jenis sumber daya yang didukung oleh Resource Groups.
 - Tipe: StringList
 - Item Maks: 10
 - Default: `AWS::AllSupported`
- **InstallServiceLinkedRole (Opsional):**

- Deskripsi: (Opsional) Pilih Yes untuk menginstal peran `AWSServiceRoleForHealth_EventProcessor` terkait layanan (SLR).
- Tipe: `String`
- Nilai yang Diizinkan: `[Yes, No]`
- Default: `No`
- `CreateApplicationInsights` (Opsional):
 - Deskripsi: (Opsional) Pilih Yes untuk membuat aplikasi berbasis grup Amazon CloudWatch Application Insights Resource.
 - Tipe: `String`
 - Nilai yang Diizinkan: `[Yes, No]`
 - Default: `No`
- `ComplianceAndRegulatoryRequirements` (Diperlukan):
 - Deskripsi: (Wajib) Persyaratan and/or peraturan kepatuhan yang berlaku untuk beban kerja ini dan tindakan apa pun yang diperlukan AWS setelah insiden.
 - Tipe: `String`
 - Izinkan Pola: `^[a-zA-Z0-9.:;,\ \- _&() ]{1,1024}$`
- `Non AWSComponents` (Opsional):
 - Deskripsi: (Opsional) Detail apakah ada di lokasi atau AWS non-komponen untuk beban kerja ini? Jika demikian, apa itu dan fungsi apa yang mereka lakukan.
 - Tipe: `String`
 - Izinkan Pola: `^$|^[a-zA-Z0-9.:;,\ \- _&() ]{1,1024}$`
 - Default: `""`
- `UpstreamDownstreamDependencies` (Opsional):
 - Deskripsi: (Opsional) Detail upstream/downstream komponen apa pun yang tidak di-onboard, yang dapat memengaruhi beban kerja ini jika mengalami pemadaman.
 - Tipe: `String`
 - Izinkan Pola: `^$|^[a-zA-Z0-9.:;,\ \- _&() ]{1,1024}$`
 - Default: `""`
- `FailoverDisasterRecoveryPlan` (Opsional):
 - Deskripsi: (Opsional) Berikan rincian rencana failover/disaster pemulihan manual atau otomatis di AZ dan tingkat regional.

- Tipe: String
- Izinkan Pola: `^[a-zA-Z0-9.;,\-_\&() ]{1,1024}$`
- Default: ""
- BridgeDetails (Opsional):
 - Deskripsi: (Opsional) Jembatan incident/crisis manajemen statis yang didirikan oleh perusahaan Anda. Jika Anda menggunakan jembatan non-statis, tentukan aplikasi pilihan Anda dan AWS akan meminta rincian ini selama insiden.
 - Tipe: String
 - Nilai yang Diizinkan: [Amazon Chime bridge, Non-Static bridge, Static bridge]
 - Default: Amazon Chime bridge
- SubscriptionStartDate (Diperlukan):
 - Deskripsi: (Wajib) Tanggal dalam YYYY-MM-DD format yang Anda inginkan untuk memulai langganan Deteksi dan Respons AWS Insiden.
 - Tipe: String
 - Izinkan Pola: `^(20[2-9]|20[3-9][0-9])-(0[1-9]|1[0-2])-(0[1-9]|[12][0-9]|3[01])$`

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- Periksa AWSSupport Rencana:

Memeriksa apakah Rencana Dukungan AWS Akun saat ini adalah Perusahaan; jika tidak, otomatisasi berakhir.

- BranchOnResourceGroup:

Memcabangkan otomatisasi apakah Grup AWS Sumber Daya yang ada disediakan. Jika tidak disediakan, otomatisasi membuat Grup AWS Sumber Daya baru.

- GetAppRegistryApplication:

Mendapat informasi metadata tentang AppRegistry aplikasi AWS Service Catalog jika disediakan.

- GenerateResourceGroupTemplate:

Menghasilkan AWS CloudFormation template untuk Grup AWS Sumber Daya dengan filter tag yang ditentukan.

- `CreateResourceGroup`:

Membuat Grup AWS Sumber Daya baru dengan menggunakan AWS CloudFormation.

- `TagResourceGroup`:

Menandai grup sumber daya dengan tag AWS Incident Detection and Response (IDR) yang diperlukan.

- `InstallServiceLinkedRole`:

Menginstal peran terkait layanan Deteksi dan Respons AWS Insiden (IDR) jika diminta.

- `CreateApplicationInsightsApplication`:

Membuat aplikasi Amazon CloudWatch Application Insights jika diminta.

- `CreateAwsSupportCase`:

Membuat kasus AWS dukungan dengan Deteksi dan Respons AWS Insiden.

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

Referensi

Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)
- [Support Automation Workflow](#)
- [Memulai Deteksi dan Respons AWS Insiden](#)
- [Penemuan beban kerja dalam Deteksi dan Respons Insiden](#)

Amazon Kinesis Data Streams

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Kinesis Data Streams. Untuk informasi lebih lanjut 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama aliran yang ingin Anda aktifkan enkripsi.

- KeyId

Tipe: 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:waitForAwsResourceProperty)` - 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:assertAwsResourceProperty)` - Memverifikasi enkripsi diaktifkan untuk Kinesis Data Streams.

AWS KMS

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk AWS Key Management Service. Untuk informasi lebih lanjut 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

Tipe: 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**

Tipe: String

Deskripsi: (Wajib) ID kunci terkelola pelanggan yang ingin Anda batalkan penghapusannya.

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

Tipe: 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

Tipe: 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 untuk AWS Lambda. Untuk informasi lebih lanjut 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

Tipe: 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`

Tipe: 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-DeleteLambdaFunctionRunbook` menghapus AWS Lambda fungsi yang Anda tentukan.

Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: 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`

Tipe: 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**

Tipe: String

Deskripsi: (Wajib) Nama atau ARN dari fungsi Lambda yang variabel lingkungannya ingin Anda enkripsi.

- **KMSKeyArn**

Tipe: 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-MoveLambdaToVPCRunbook 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama fungsi Lambda untuk pindah ke VPC Amazon.

- SecurityGroupIds

Tipe: String

Deskripsi: (Wajib) Grup keamanan yang ingin IDs Anda tetapkan ke antarmuka jaringan elastis (ENIs) yang terkait dengan fungsi Lambda Anda.

- SubnetIds

Tipe: String

Deskripsi: (Wajib) Subnet yang ingin IDs Anda buat antarmuka jaringan elastis (ENIs) 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ARN dari fungsi Lambda.

- S3 BucketName

Tipe: String

Deskripsi: (Wajib) Nama bucket Amazon S3 yang notifikasi kejadiannya memicu fungsi Lambda.

- Tindakan

Tipe: 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

`CheckOutput.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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama fungsi Lambda yang ingin Anda pecahkan masalah akses internet.

- destinationIp

Tipe: String

Deskripsi: (Wajib) Alamat IP tujuan yang ingin Anda buat koneksi keluar.

- destinationPort

Tipe: 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` - Subnet tempat IDs 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. `LambdaIpRules` objek 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ARN dari fungsi Lambda yang dipicu oleh notifikasi peristiwa Amazon S3.

- S3 BucketName

Tipe: 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

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Alur Kerja Terkelola Amazon untuk Apache Airflow. Untuk informasi lebih lanjut 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 for Apache Airflow (Amazon MWAA) masalah pembuatan lingkungan, 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

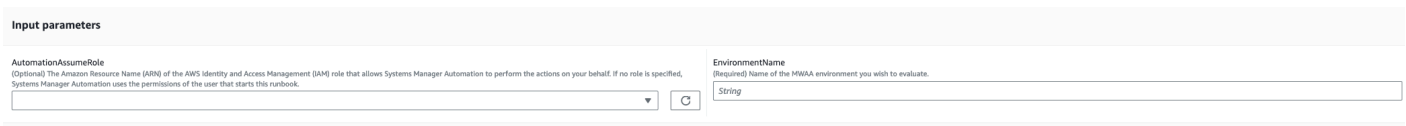
Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

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 Automation console. It contains two fields: 'AutomationAssumeRole' and 'EnvironmentName'. The 'AutomationAssumeRole' field is optional and has a dropdown menu. The 'EnvironmentName' field is required and has a text input box.

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, jaringan, subnet ACLs, 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 MWAA Block 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 MWAA:

Memverifikasi apakah peran eksekusi memiliki izin yang diperlukan untuk sumber daya Amazon MWAA, 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 MWAA:

Memverifikasi apakah peran eksekusi memiliki izin yang diperlukan untuk sumber daya Amazon MWAA, 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 MWAA:

Memeriksa apakah Grup CloudWatch Log yang diperlukan untuk lingkungan Amazon MWAA ada. Jika tidak, otomatisasi kemudian CloudTrail memeriksa lokasi CreateLogGroup dan DeleteLogGroup acara.

- Memeriksa Tabel Rute lingkungan Amazon MWAA:

Memeriksa apakah tabel rute VPC Amazon di lingkungan Amazon MWAA dikonfigurasi dengan benar.

- Memeriksa Grup Keamanan lingkungan Amazon MWAA:

Memeriksa apakah lingkungan Amazon MWAA Grup keamanan Amazon VPC dikonfigurasi dengan benar.

- Memeriksa Jaringan lingkungan Amazon MWAA: ACLs

Memeriksa apakah grup keamanan Amazon VPC di lingkungan Amazon MWAA dikonfigurasi dengan benar.

- Memeriksa Subnet lingkungan Amazon MWAA:

Memverifikasi apakah subnet lingkungan Amazon MWAA 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

```

GenerateReportAutomationReport
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] DAGProcessing - 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 lebih lanjut 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

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) ID sumber daya cluster DB Neptune 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 Neptune.
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`) - Memverifikasi jenis mesin Neptune DB adalah. `neptune`
- `EnableNeptuneDbAuditLogs` (`aws:executeAwsApi`) - Mengaktifkan log audit untuk cluster DB Neptune untuk dikirim Log. CloudWatch
- `VerifyNeptuneDbStatus` (`aws:waitAwsResourceProperty`) - Memverifikasi status cluster Neptune DB adalah. `available`
- `VerifyNeptuneDbAuditLogs` (`aws:executeScript`) - Memverifikasi bahwa log audit berhasil dikonfigurasi untuk dikirim ke CloudWatch Log.

AWS-EnableNeptuneDbBackupRetentionPeriod

Deskripsi

`AWS-EnableNeptuneDbBackupRetentionPeriodRunbook` membantu Anda mengaktifkan pencadangan otomatis dengan periode retensi cadangan antara 7 dan 35 hari untuk cluster DB Amazon Neptune.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) ID sumber daya cluster DB Neptune yang ingin Anda aktifkan pencadangan.

- `BackupRetentionPeriod`

Jenis: Integer

Nilai yang valid: 7-35

Deskripsi: (Wajib) Jumlah hari cadangan dipertahankan.

- `PreferredBackupWindow`

Tipe: 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:assertAwsResourceProperty`) - Memverifikasi jenis mesin Neptunus DB adalah. `neptune`
- `VerifyNeptuneDbStatus` (`aws:waitAwsResourceProperty`) - Memverifikasi status cluster Neptunus DB 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 klaster Amazon Neptunus yang Anda tentukan.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID cluster Neptune 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 adalah `neptune`.
- `VerifyNeptuneStatus` (`aws:waitForAwsResourceProperty`) - Memverifikasi bahwa status cluster adalah `available`.
- `EnableNeptuneDbDeletionProtection` (`aws:executeAwsApi`) - Memungkinkan 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 lebih lanjut 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-EnableMinorVersionUpgradeOnRDSDBInstance](#)
- [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

Tipe: 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.

- DBInstancePengidentifikasi

Tipe: String

Deskripsi: (Wajib) ID instans Amazon RDS yang ingin Anda buat snapshot.

- DBSnapshotPengidentifikasi

Tipe: String

Deskripsi: (Opsional) Template nama untuk snapshot Amazon RDS. Template nama default adalah *DBInstanceIdentifier-yyyymmddhhmmss*.

- Pengenal Terenkripsi DBSnapshot

Tipe: String

Deskripsi: (Opsional) Nama untuk snapshot terenkripsi. Nama default adalah nilai yang Anda tentukan untuk DBSnapshotIdentifier parameter yang ditambahkan. -encrypted

- InstanceTags

Tipe: String

Deskripsi: (Opsional) Tag untuk ditambahkan ke instans DB. (Contoh: key=tagkey1, value = tagValue1; key=tagkey2, value = tagValue2) '

- KmsKeyId

Tipe: 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`

Tipe: 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

Tipe: 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.

- DBInstancePengidentifikasi

Tipe: String

Deskripsi: (Wajib) DBInstance ID dari Instans RDS untuk membuat Snapshot dari.

- DBSnapshotPengidentifikasi

Tipe: String

Deskripsi: (Opsional) ID DBSnapshot Pengenal snapshot RDS yang akan dibuat.

- InstanceTags

Tipe: String

Deskripsi: (Opsional) Tag untuk membuat misalnya.

- SnapshotTags

Tipe: String

Deskripsi: (Opsional) Tag yang akan dibuat untuk snapshot.

Langkah Dokumen

create RDSSnapshot - Membuat snapshot RDS dan mengembalikan ID snapshot.

verifikasi RDSSnapshot — Memeriksa apakah snapshot yang dibuat pada langkah sebelumnya ada.

Keluaran

buatRDSSnapshot. SnapshotId — ID dari 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

Tipe: 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.

- DBClusterId

Tipe: 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

Tipe: 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.

- DBClusterSnapshotId

Tipe: 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 cluster 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

Tipe: 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

Tipe: 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 `DbResourceId` parameter.
- `aws:branch`- Cabang berdasarkan nilai yang Anda tentukan dalam `SkipFinalSnapshot` parameter.
- `aws:executeAwsApi`- Menghapus instans DB yang Anda tentukan dalam `DbResourceId` parameter.

- `aws:executeAwsApi`- Menghapus instans DB yang Anda tentukan dalam `DbResourceId` 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`

Tipe: 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`

Tipe: 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

Tipe: 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

Tipe: 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`

Tipe: 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`

Tipe: 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-EnableCopyTagsToSnapshotOnRDSDBInstance` Runbook 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`

Tipe: 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`

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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-EnableMinorVersionUpgradeOnRDSDBInstance

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

Tipe: 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

Tipe: 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 mengatur `ApplyImmediately` parameter ke `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`

Tipe: 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`

Tipe: 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` adalah `available`.
- `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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda aktifkan Performance Insights.

- PerformanceInsightsKMSKeyId

Tipe: 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, awalan 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`

Tipe: 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`

Tipe: 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-EnableRDSInstanceBackupRunbook 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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Pengidentifikasi sumber daya untuk instans DB yang ingin Anda aktifkan pencadangan.

- `PreferredBackupWindow`

Tipe: String

Deskripsi: (Opsional) Rentang waktu harian (dalam UTC) selama pencadangan dibuat.

Batas:

- 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`

Tipe: 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`

Tipe: 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`

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Nomor port yang Anda inginkan instans DB untuk menerima koneksi.

- RDSDBInstanceResourceId

Tipe: 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

Tipe: 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) Akun yang ingin Anda bagikan snapshot dengan. IDs Parameter ini diperlukan jika Anda memasukkan No nilai Private parameter.

- AccountPermissionOperation

Tipe: String

Nilai yang valid: tambahkan | hapus

Default: tidak ada

Deskripsi: (Opsional) Jenis operasi yang harus dilakukan.

- Privat

Tipe: 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 izinnya 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 snapshot yang disediakan dalam parameter. IDs `SnapshotIdentifiers` Setelah memverifikasi IDs, 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 `Public` ke `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 Dukungan 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 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. Dukungan

- 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, 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. Dukungan

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 Dukungan Perusahaan Runbook ini dan Diagnostik dan Ulasan Beban Kerja Layanan Proaktif memerlukan Langganan Dukungan Perusahaan. Sebelum menggunakan runbook ini, hubungi Manajer Akun Teknis (TAM) atau Spesialis TAM (STAM) Anda untuk mendapatkan instruksi. Untuk informasi selengkapnya, lihat [Layanan Dukungan Proaktif](#).
- Akun dan Wilayah AWS kuota Pastikan Anda belum mencapai jumlah maksimum instans Amazon EC2 VPCs atau 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` `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 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 I/O level 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 I/O waktu 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 kredensi 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://amzn-s3-demo-bucket/automation execution id/queries/`

Skrip ini mengumpulkan data yang digunakan oleh AWS Spesialis untuk meninjau indikator kinerja utama pada tingkat objek. Script 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` parameternya, 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` parameternya, 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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/automation-execution-  
id/*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
```

```

    "Resource": "arn:aws:secretsmanager:us-
east-1:111122223333: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.

JSON

```

{
  "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:us-east-1:111122223333:instance/temporary-instance-  

        id",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:111122223333:automation-execution/*"
    ],
    "Effect": "Allow"
},
{
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "ssm.amazonaws.com"
        },
        "ArnLike": {
            "iam:AssociatedResourceARN": "arn:aws:ssm:*:*:document/AWS-*"
        }
    },
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::111122223333:role/SSM-*",
    "Effect": "Allow"
}
]
}

```

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AutomationAssumeRole

Tipe: 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.

- DBInstancePengidentifikasi

Tipe: String

Deskripsi: (Wajib) ID instans DB Anda.

- DatabaseName

Tipe: String

Deskripsi: (Wajib) Nama database yang dihosting pada instans DB Anda.

- SecretId

Tipe: String

Deskripsi: (Wajib) ARN rahasia Secrets Manager Anda yang berisi pasangan nilai kunci nama pengguna dan kata sandi. CloudFormation Tumpukan membuat kebijakan IAM dengan izin untuk `GetSecretValue` operasi ke ARN ini. Kredensial digunakan untuk memungkinkan instance sementara untuk mengumpulkan statistik database. Hubungi TAM atau STAM Anda untuk mendiskusikan izin minimum yang diperlukan.

- Akui

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Nomor Dukungan 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 Dukungan API. Anda harus mengatur `AllowVpcInternetAccess` parameter ke `true`. Subjek kasus harus berisi frasa `AWSPremiumSupport-PostgreSQLWorkloadReview`.

- **S3 BucketName**

Tipe: 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**

Tipe: 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**

Tipe: 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**

Tipe: String

Deskripsi: (Opsional) Awalan dan tag nama sumber daya CloudFormation tumpukan. Runbook membuat sumber daya 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: AWSPostgre SQLWorkload Ulasan

- **Jadwal**

Tipe: 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**

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Jika disetel ke `true`, runbook akan membuat gateway NAT untuk menyediakan konektivitas internet ke instans Amazon EC2 sementara untuk berkomunikasi dengan Dukungan 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

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Jika disetel ke `true`, volume root instans Amazon EC2 sementara akan dihapus setelah runbook selesai dan menghapus tumpukan. 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 CloudFormation template dari lampiran Runbook Otomasi yang digunakan untuk membuat AWS sumber daya sementara di Anda Akun AWS.
5. `aws:createStack`- Menciptakan sumber daya CloudFormation tumpukan.
6. `aws:waitForAwsResourceProperty`- Menunggu sampai instans Amazon EC2 yang dibuat oleh template CloudFormation berjalan.
7. `aws:executeAwsApi`- Mendapatkan ID untuk instans Amazon EC2 sementara dan koneksi peering VPC yang dibuat oleh. 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 CloudFormation template siap.
- 16 `aws:executeAwsApi`- Mendapat jendela IDs untuk pemeliharaan dan mengubah kalender yang dibuat oleh 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.
 - a. `aws:changeInstanceState`- Memulai instans Amazon EC2 sementara dan menunggu pemeriksaan status lulus sebelum mengunggah laporan.

- b. `aws:waitForAwsResourceProperty`- Menunggu hingga instans Amazon EC2 sementara dikelola oleh Systems Manager. Jika batas waktu langkah ini atau gagal, maka runbook me-reboot instance.
 - i. `aws:executeAwsApi`- Mem-boot ulang instans Amazon EC2 sementara jika langkah sebelumnya gagal atau habis waktu.
 - ii. `aws:waitForAwsResourceProperty`- Menunggu hingga instans Amazon EC2 sementara dikelola oleh Systems Manager setelah reboot.
 - c. `aws:runCommand`- Melampirkan laporan metadata ke Dukungan kasus jika Anda memberikan nilai untuk parameter. SupportCase Skrip mengompres dan membagi laporan menjadi file 5 MB. Jumlah maksimum file yang dilampirkan skrip ke Dukungan kasing adalah 12.
22. `aws:changeInstanceState`- Menghentikan instans Amazon EC2 sementara jika CloudFormation tumpukan gagal dihapus.
23. `aws:executeAwsApi`- Menjelaskan peristiwa CloudFormation tumpukan jika runbook gagal membuat atau memperbarui CloudFormation tumpukan.
24. `aws:waitForAwsResourceProperty`- Menunggu sampai CloudFormation tumpukan berada dalam status terminal sebelum menghapus.
25. `aws:executeAwsApi`- Menghapus 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-RebootRdsInstanceRunbook 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

Tipe: 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

Tipe: 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-ShareRDSSnapshotRunbook 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 akun yang dipisahkan koma IDs untuk berbagi snapshot.

- AutomationAssumeRole

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) lengkap dari kunci terkelola AWS KMS pelanggan yang digunakan untuk mengenkripsi snapshot.

- SnapshotName

Tipe: 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`
- `kms:CreateGrant`
- `kms:DescribeKey`

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.

- 14aws:executeAwsApi- Memeriksa apakah nilai yang disediakan untuk Database parameter adalah cluster DB.
- 15aws:executeAwsApi- Mengambil daftar snapshot untuk yang ditentukan. Database
- 16aws:executeScript- Menentukan snapshot terbaru yang tersedia dari daftar yang dirakit pada langkah sebelumnya.
- 17aws:executeAwsApi- Menyalin snapshot instance DB menggunakan yang ditentukanKMSKey.
- 18aws:waitForAwsResourceProperty- Menunggu operasi snapshot salin selesai.
- 19aws:executeAwsApi- Berbagi snapshot baru dengan yang AccountIds ditentukan.
- 20aws:executeAwsApi- Mengambil daftar snapshot untuk yang ditentukan. Database
- 21aws:executeScript- Menentukan snapshot terbaru yang tersedia dari daftar yang dirakit pada langkah sebelumnya.
- 22aws:executeAwsApi- Menyalin snapshot instance DB menggunakan yang ditentukanKMSKey.
- 23aws:waitForAwsResourceProperty- Menunggu operasi snapshot salin selesai.
- 24aws:executeAwsApi- Berbagi snapshot baru dengan yang AccountIds ditentukan.
- 25aws: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 instance Amazon Relational Database Service (Amazon RDS).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AutomationAssumeRole

Tipe: 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.

- Instanceld

Tipe: 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 v1 Aurora Serverless, cluster multi-master Aurora, bagian dari database global Aurora, atau cluster yang menggunakan query paralel Aurora. Runbook dapat digunakan untuk menghentikan dan memulai cluster Aurora Serverless v2.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama cluster Aurora yang ingin Anda hentikan atau mulai.

- Tindakan

Tipe: 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`

Tipe: 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

Tipe: 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 (jaringan ACLs), dan tabel rute untuk potensi masalah konektivitas.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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.

- DBInstancePengidentifikasi

Tipe: String

Deskripsi: (Wajib) ID instans DB untuk menguji konektivitas ke.

- SourceInstance

Tipe: 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 jaringan instans DB ACLs.
- `aws:executeAwsApi`- Mendapat contoh DB subnet CIDR.
- `aws:executeAwsApi`- Mendapat informasi tentang instans EC2.
- `aws:executeAwsApi`- Mendapat informasi tentang jaringan ACLs 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 jaringan ACLs.
- `aws:executeScript`- Mengevaluasi tabel rute.
- `aws:sleep`- Mengakhiri otomatisasi.

Keluaran

dapatkan RDSInstance Properti. DBInstanceIdentifier - Instans DB yang digunakan dalam otomatisasi.

dapatkan RDSInstance Properti. DBInstanceStatus - 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 SourceInstance jaringan dengan jaringan ACLs instans DB ACLs.

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 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 EC2 Disediakan`: Memverifikasi apakah ID Instans Amazon EC2 sumber disediakan dalam parameter input.
- Langkah 3: `memvalidasiRDSConnectivity`: Memvalidasi konektivitas Amazon RDS dari sumber instans Amazon EC2 jika disediakan.
- Langkah 4: `memvalidasiRDSIAMAuthentication`: Memvalidasi jika fitur Autentikasi IAM diaktifkan.
- Langkah 5: `memvalidasiIAMPolicies`: 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

Tipe: 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.

- RDSType

Tipe: String

Deskripsi: (Wajib): Pilih jenis database relasional yang Anda coba sambungkan dan autentikasi.

Nilai yang Diizinkan: Amazon RDS atau Amazon Aurora Cluster.

- DBInstancePengenal

Tipe: 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: ""

- DBIAMRoleNama

Tipe: 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: ""

- DBIAMUserName

Tipe: 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: ""

- DBUserName

Tipe: String

Deskripsi: (Opsional) Nama pengguna database dipetakan ke IAM role/user 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 AWS Systems Manager Konsol.
2. Pilih Jalankan Otomasi
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole(Optional):

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.

- **RDSType(Diperlukan):**

Pilih jenis Amazon RDS yang Anda coba sambungkan dan autentikasi. Pilih dari dua nilai yang diizinkan: `Amazon RDS` atau `Amazon Aurora Cluster`.

- **DBInstancePengidentifikasi (Diperlukan):**

Masukkan pengenalan 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.

- **DBIAMRoleName (Opsional):**

Masukkan nama Peran IAM yang digunakan untuk otentikasi berbasis IAM. Berikan hanya jika tidak `DBIAMUserName` disediakan; jika tidak, biarkan kosong. Entah `DBIAMRoleName` atau `DBIAMUserName` harus disediakan.

- **DBIAMUserName (Opsional):**

Masukkan Pengguna IAM yang digunakan untuk otentikasi berbasis IAM. Berikan hanya jika tidak `DBIAMRoleName` disediakan, jika tidak, biarkan kosong. Entah `DBIAMRoleName` atau `DBIAMUserName` harus disediakan.

- **DBUserName (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.

RDSType
(Required) The type of Relational Database.

DBInstanceIdentifier
(Required) The identifier of the target Amazon RDS DB instance or Amazon Aurora DB cluster.

DBIAMRoleName
(Optional) The IAM role name being used for IAM-based authentication. Provide only if the parameter 'DBIAMUserName' is not provided, otherwise leave it empty. Either 'DBIAMRoleName' or 'DBIAMUserName' must be provided.

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 EC2 Disediakan:

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: memvalidasiRDSConnectivity:

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: `memvalidasiRDSIAMAuthentication`:

Memvalidasi jika fitur Autentikasi IAM diaktifkan pada instans Amazon RDS atau Aurora Cluster.

- Langkah 5: `memvalidasiIAMPolicies`:

Memverifikasi apakah izin IAM yang diperlukan ada di IAM yang user/role 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 apakah izin IAM yang diperlukan ada di IAM yang user/role 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

Zel[REDACTED]a4

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 klaster Amazon Aurora /Amazon DocumentDB, pastikan Anda menggunakannya. `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:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ValidateRdsNetwork",
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "servicequotas:GetServiceQuota",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets"
      ],
      "Resource": [
        "arn:aws:rds:us-east-1:111122223333:db:db-instance-name"
      ]
    }
  ]
}
```

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.

- DBInstancePengidentifikasi (Diperlukan):

Masukkan Pengenal Instans Layanan Amazon Relational Database Service.

The screenshot shows the 'Input parameters' section of an AWS Systems Manager console. It contains two input fields: 'AutomationAssumeRole' and 'DBInstanceIdentifier'. The 'AutomationAssumeRole' field has a dropdown menu with 'AutomationAssumeRoleSSM' selected. The 'DBInstanceIdentifier' field has a text input with 'my-rds-instance-01' entered.

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`) VPC Amazon disetel ke `true` (atau tidak jika instans Amazon RDS). `PubliclyAccessible`

- Langkah 5: `validateSubnetAttributes`:

Memvalidasi keberadaan subnet di `DBSubnetGroup` dan memeriksa tersedia IPs 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](#)

AWS dokumentasi 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 lebih lanjut 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`

Tipe: 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`

Tipe: 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`

Tipe: 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`

Tipe: 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 klaster Amazon Redshift yang Anda tentukan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Basis Data

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama bucket Amazon Simple Storage Service (Amazon S3) Simple Storage S3 yang ingin Anda unggah log.

- ClusterIdentifier

Tipe: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda aktifkan log audit.

- S3 KeyPrefix

Tipe: 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`

Tipe: 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`

Tipe: 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 klaster 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda aktifkan enkripsi.

- KMSKeyARN

Tipe: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari kunci terkelola AWS KMS pelanggan yang ingin Anda gunakan untuk mengenkripsi data klaster.

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

Tipe: 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

Tipe: 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`

Tipe: 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`

Tipe: 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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang ingin Anda aktifkan perutean VPC yang disempurnakan.

- `PreferredMaintenanceWindow`

Tipe: 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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Pengidentifikasi unik cluster yang tipe simpulnya ingin Anda modifikasi.

- `ClusterType`

Tipe: String

Nilai yang valid: `simpul tunggal` | `multi-node`

Deskripsi: (Wajib) Jenis cluster yang ingin Anda tetapkan ke cluster Anda.

- `NodeType`

Tipe: 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 lebih lanjut 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](#)
- [AWSSupport-ConfigureS3ReplicationSameAndCrossAccount](#)
- [AWSSupport-EmptyS3Bucket](#)
- [AWSSupport-TroubleshootS3EventNotifications](#)
- [AWSSupport-ContainS3Resource](#)

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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama bucket S3 yang ingin Anda buat konfigurasi tiering cerdas.

- ConfigurationId

Tipe: String

Deskripsi: (Wajib) ID untuk konfigurasi tingkatan cerdas. Ini bisa berupa ID konfigurasi baru, atau ID dari konfigurasi yang ada.

- **NumberOfDaysToArchive**

Tipe: 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**

Tipe: 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**

Tipe: String

Deskripsi: (Opsional) Awalan nama kunci dari objek yang ingin Anda terapkan konfigurasinya.

- **Tanda**

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).

Important

Perhatikan informasi penting berikut mengenai ACL Penerima Email untuk Amazon S3 [PutBucketLogging](#) API, yang digunakan oleh runbook ini:

Pemberitahuan akhir dukungan: Mulai 1 Oktober 2025, Amazon S3 akan menghentikan dukungan untuk membuat Daftar Kontrol Akses Penerima Email (ACL) baru. Penerima Email yang ACLs dibuat sebelum tanggal ini akan terus berfungsi dan tetap dapat diakses melalui, (AWS CLI CLI) Konsol Manajemen AWS,, dan REST API SDKs. Namun, Anda tidak akan lagi dapat membuat Penerima Email baru. ACLs Antara 15 Juli 2025 dan 1 Oktober 2025, Anda akan mulai melihat peningkatan tingkat kesalahan HTTP 405 untuk permintaan ke Amazon S3 saat mencoba membuat Penerima Email baru. ACLs

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama Bucket Amazon S3 yang ingin Anda konfigurasi logging.

- GrantedPermission

Tipe: String

Nilai yang valid: FULL_CONTROL | BACA | TULIS

Deskripsi: (Wajib) Izin pencatatan yang diberikan kepada penerima hibah untuk bucket.

- GranteeEmailAddress

Tipe: String

(Opsional) Alamat email penerima hibah.

- GranteeId

Tipe: String

Deskripsi: (Opsional) ID pengguna kanonik penerima hibah.

- GranteeType

Tipe: String

Nilai yang valid: CanonicalUser | AmazonCustomerByEmail | Grup

Keterangan: (Wajib) Jenis penerima hibah.

- GranteeUri

Deskripsi: (Opsional) URI dari kelompok penerima hibah.

- TargetBucket

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama bucket Amazon S3 yang ingin Anda konfigurasikan untuk pembuatan versi.

- VersioningState

Tipe: 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 keSuspended, 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

Tipe: 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 (ACLs) 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

Tipe: String

Deskripsi: (Wajib) Nama bucket S3 yang ingin Anda konfigurasikan.

- IgnorePublicAcls

Jenis: Boolean

Default: `betul`

Deskripsi: (Opsional) Jika disetel ke `true`, Amazon S3 mengabaikan semua publik ACLs 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`

Izin IAM yang diperlukan

`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`

Tipe: String

Deskripsi: (Wajib) ID pemilik Akun AWS bucket S3 yang Anda konfigurasi.

- `AutomationAssumeRole`

Tipe: 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 (ACLs) 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 public ACLs untuk bucket S3 yang dimiliki oleh yang Akun AWS Anda tentukan dalam 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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Nama bucket S3 yang ingin Anda konfigurasikan.

- `DaysUntilExpire`

Jenis: Integer

Deskripsi: (Wajib) Jumlah hari Amazon S3 menunggu sebelum menghapus semua bagian unggahan secara permanen.

- `RuleId`

Tipe: String

Deskripsi: (Wajib) ID yang digunakan untuk mengidentifikasi aturan bucket siklus hidup. Ini harus menjadi nilai yang unik.

- `S3Prefix`

Tipe: 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`

Tipe: 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: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama bucket S3 tempat Anda ingin mengenkripsi konten.

- SSEAlgorithm

Tipe: String

Default: AES256

Deskripsi: (Opsional) Algoritma enkripsi sisi server yang 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

Tipe: 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**

Tipe: String

Deskripsi: (Wajib) Nama bucket S3 yang ingin Anda aktifkan Kunci Bucket.

- **KMSKeyId**

Tipe: 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 AES256 enkripsi.
- `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

Tipe: 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

Tipe: 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`

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Aliran CloudWatch 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 ke `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 ke `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`

Tipe: String

Deskripsi: (Wajib) Nama bucket S3 untuk memecahkan masalah.

- S3 PrefixName

Tipe: String

Deskripsi: (Opsional) Awalan nama kunci objek yang ingin Anda analisis di bucket S3 Anda.

Untuk informasi selengkapnya, lihat [Kunci objek](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

- StartAfter

Tipe: 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 disetel ke `false`.

Izin IAM yang diperlukan

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

logs:PutLogEvents, logs:CreateLogGroup, logs:CreateLogStream, dan hanya diperlukan jika Anda ingin otomatisasi mengirim data CloudWatch log ke Log.

JSON

```
{
  "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:::amzn-s3-demo-bucket1/*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPolicy",
        "s3:GetBucketAcl"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "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 setelan 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 ke `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 mengonfirmasi bahwa kelas penyimpanan didukung.
- Memeriksa setelan 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`

AWSSupport-ConfigureS3ReplicationSameAndCrossAccount

Deskripsi

Runbook `AWSSupport-ConfigureS3ReplicationSameAndCrossAccount` otomatisasi mengonfigurasi replikasi bucket Amazon Simple Storage Service (Amazon S3) antara bucket sumber dan tujuan untuk akun yang sama atau lintas akun. Otomatisasi ini mendukung replikasi bucket yang dienkripsi dengan Enkripsi Sisi Server dengan Amazon S3-Managed Keys (SSE-S3) dan Enkripsi Sisi Server dengan (SSE-KMS). AWS Key Management Service ini juga mendukung pemfilteran replikasi selektif berbasis awalan dan tag, Kontrol Waktu Replikasi Amazon S3 (Amazon S3 RTC) dengan SLA 15 menit, dan hapus replikasi penanda. Otomatisasi melakukan tindakan berikut:

- Memvalidasi parameter input dan konfigurasi bucket untuk kompatibilitas.
- Memeriksa pengaturan enkripsi pada bucket sumber dan tujuan.
- Membuat peran baru AWS Identity and Access Management (IAM) dengan izin yang sesuai untuk replikasi jika tidak disediakan sebagai input.

- Mengkonfigurasi aturan replikasi berdasarkan parameter tertentu (awalan, tag, atau seluruh bucket).
- Mengaktifkan pembuatan versi bucket jika belum diaktifkan.
- Menyiapkan konfigurasi replikasi dengan fitur opsional seperti Replication Time Control (RTC) dan hapus replikasi penanda.

Important

- Otomatisasi ini tidak mendukung bucket dengan aturan replikasi yang ada. Bucket sumber tidak boleh memiliki konfigurasi replikasi yang ada.
- Otomatisasi ini menciptakan peran IAM baru dengan izin yang sesuai untuk replikasi jika ReplicationRole input S3 tidak disediakan.
- Otomatisasi ini tidak mereplikasi objek yang ada. Replikasi Amazon S3 hanya berlaku untuk objek uploaded/created setelah konfigurasi replikasi diaktifkan.
- Untuk replikasi lintas akun, Anda harus memberikan peran IAM di akun tujuan dengan izin yang sesuai untuk operasi dan AWS KMS operasi Amazon S3 (jika bucket menggunakan enkripsi). AWS KMS
- Otomatisasi ini menggunakan `aws:approve` tindakan, yang menghentikan sementara eksekusi hingga kepala sekolah yang ditunjuk menyetujui perubahan konfigurasi. Lihat [Menjalankan otomatisasi dengan pemberi persetujuan](#) untuk informasi selengkapnya.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- `ValidateInputParameters`: Memvalidasi semua parameter input untuk kebenaran dan kompatibilitas untuk memastikan konfigurasi replikasi yang tepat.
- `PrepareApprovalMessage`: Menyiapkan pesan persetujuan dengan semua parameter konfigurasi replikasi untuk tinjauan pengguna.
- `RequestApproval`: Meminta persetujuan dari pengguna yang berwenang sebelum menambahkan konfigurasi replikasi Amazon S3 pada bucket sumber.
- `CheckBucketEncryption`: Memeriksa konfigurasi enkripsi untuk bucket Amazon S3 sumber dan tujuan untuk menentukan pengaturan replikasi yang kompatibel.

- **BranchOnEncryptionType:** Eksekusi cabang berdasarkan jenis enkripsi bucket Amazon S3 untuk menerapkan konfigurasi replikasi yang sesuai untuk bucket terenkripsi SSE-S3 atau SSE-KMS.
- **Konfigurasi SSES3 Replikasi:** Mengonfigurasi replikasi Amazon S3 untuk bucket yang dienkripsi dengan Enkripsi Sisi Server dengan Amazon S3-Managed Keys (SSE-S3), termasuk peran IAM dan aturan replikasi.
- **Konfigurasi SSEKMSReplication:** Mengonfigurasi replikasi Amazon S3 untuk bucket yang dienkripsi dengan Enkripsi Sisi Server AWS KMS dengan (SSE-KMS), termasuk peran IAM, izin kunci KMS, dan aturan replikasi.
- **CleanupResources:** Membersihkan peran IAM yang dibuat selama konfigurasi replikasi gagal saat S3 tidak ReplicationRole disediakan sebagai input.

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

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- s3: ListBucket
- s3: GetBucketVersioning
- s3: GetEncryptionConfiguration
- s3: GetBucketLocation
- s3: GetReplicationConfiguration
- s3: PutBucketVersioning
- s3: PutReplicationConfiguration
- saya: ListRoles
- saya: GetRole
- saya: GetRolePolicy
- saya: ListRoleTags
- saya: ListAttachedRolePolicies
- saya: ListRolePolicies
- saya: SimulatePrincipalPolicy
- saya: CreateRole
- saya: TagRole

- saya: PassRole
- saya: DeleteRole
- saya: DeleteRolePolicy
- saya: DetachRolePolicy
- saya: PutRolePolicy
- sts: GetCallerIdentity
- SNS:Publish
- kms: GetKeyPolicy (saat bucket menggunakan SSE-KMS, replikasi akun yang sama)
- kms: DescribeKey (saat bucket menggunakan SSE-KMS, replikasi akun yang sama)
- kms: PutKeyPolicy (saat bucket menggunakan SSE-KMS, replikasi akun yang sama)
- sts: AssumeRole (untuk replikasi lintas akun)

CrossAccountReplicationRole (untuk skenario lintas akun):

Untuk replikasi lintas akun, Anda harus memberikan CrossAccountReplicationRole izin berikut di akun tujuan:

- s3: ListBucket
- s3: GetBucketVersioning
- s3: GetBucketLocation
- s3: GetBucketPolicy
- s3: GetEncryptionConfiguration
- s3: PutBucketVersioning
- s3: PutBucketPolicy
- kms: GetKeyPolicy (saat bucket tujuan lintas akun menggunakan SSE-KMS)
- kms: DescribeKey (saat bucket tujuan lintas akun menggunakan SSE-KMS)
- kms: PutKeyPolicy (saat bucket tujuan lintas akun menggunakan SSE-KMS)

S3 ReplicationRole (peran yang disediakan pelanggan):

Jika Anda memberikan S3 yang adaReplicationRole, itu harus memiliki izin berikut:

- s3: ListBucket

- s3: GetBucketLocation
- s3: GetReplicationConfiguration
- s3: GetObjectVersionAcl
- s3: GetObjectVersionTagging
- s3: GetObjectVersionForReplication
- s3: GetObjectTagging
- s3: ReplicateObject
- s3: ReplicateDelete
- s3: ReplicateTags
- s3: ObjectOwnerOverrideToBucketOwner
- KMS: Dekripsi (untuk skenario SSE-KMS, kunci KMS sumber)
- KMS: Enkripsi (untuk skenario SSE-KMS, kunci KMS tujuan)
- kms: GenerateDataKey (untuk skenario SSE-KMS, kunci KMS tujuan)
- kms: ReEncrypt * (untuk skenario SSE-KMS, kunci KMS tujuan)

Contoh AutomationAssumeRolekebijakan untuk replikasi akun yang sama:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::SOURCE_BUCKET",
        "arn:aws:s3:::DESTINATION_BUCKET"
      ]
    }
  ]
}
```



```

    },
    {
      "Sid": "IAMReadOperations",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRoleTags",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMListRolesForCleanup",
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "*"
    },
    {
      "Sid": "IAMCreateAndTagRole",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AWSSupport-ConfigureS3ReplicationSameAndCrossAccount": "*"
        }
      }
    },
    {
      "Sid": "IAMPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "s3.amazonaws.com"
        }
      }
    }
  ]
}

```

```

    }
  },
  {
    "Sid": "TaggedIAMRoleModifyAndDeleteOperations",
    "Effect": "Allow",
    "Action": [
      "iam:DeleteRole",
      "iam:DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
    "Condition": {
      "StringLike": {
        "aws:ResourceTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
      }
    }
  },
  {
    "Sid": "STSGetCallerIdentity",
    "Effect": "Allow",
    "Action": "sts:GetCallerIdentity",
    "Resource": "*"
  },
  {
    "Sid": "SNSPublish",
    "Effect": "Allow",
    "Action": "sns:Publish",
    "Resource": "SNS_TOPIC_ARN"
  },
  {
    "Sid": "KMSKeyReadOperations",
    "Effect": "Allow",
    "Action": [
      "kms:GetKeyPolicy",
      "kms:DescribeKey"
    ],
    "Resource": [
      "arn:aws:kms:REGION:ACCOUNT_ID:key/SOURCE_KMS_KEY_ID",
      "arn:aws:kms:REGION:ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
    ]
  },
  {
    {

```

```

        "Sid": "KMSKeyMutatingOperations",
        "Effect": "Allow",
        "Action": "kms:PutKeyPolicy",
        "Resource": [
            "arn:aws:kms:REGION:ACCOUNT_ID:key/SOURCE_KMS_KEY_ID",
            "arn:aws:kms:REGION:ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
        ],
        "Condition": {
            "StringEquals": {
                "kms:CallerAccount": "ACCOUNT_ID"
            }
        }
    }
}

```

Note

Pernyataan Kebijakan (KMSKeyReadOperations dan KMSKeyMutatingOperations) hanya diperlukan ketika bucket menggunakan enkripsi SSE-KMS.

Contoh AutomationAssumeRolekebijakan untuk replikasi lintas akun:

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3SourceBucketOperations",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketVersioning",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:PutBucketVersioning",
                "s3:PutReplicationConfiguration"
            ],
            "Resource": "arn:aws:s3:::SOURCE_BUCKET"
        }
    ]
}

```

```

    },
    {
      "Sid": "IAMReadOperations",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRoleTags",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMListRolesForCleanup",
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "*"
    },
    {
      "Sid": "IAMCreateAndTagRole",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AWSSupport-ConfigureS3ReplicationSameAndCrossAccount": "*"
        }
      }
    },
    {
      "Sid": "IAMPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "s3.amazonaws.com"
        }
      }
    }
  ]
}

```

```

    }
  },
  {
    "Sid": "TaggedIAMRoleModifyAndDeleteOperations",
    "Effect": "Allow",
    "Action": [
      "iam:DeleteRole",
      "iam:DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
    "Condition": {
      "StringLike": {
        "aws:ResourceTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
      }
    }
  },
  {
    "Sid": "CrossAccountRoleAssumption",
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "CROSS_ACCOUNT_REPLICATION_ROLE_ARN"
  },
  {
    "Sid": "STSGetCallerIdentity",
    "Effect": "Allow",
    "Action": "sts:GetCallerIdentity",
    "Resource": "*"
  },
  {
    "Sid": "SNSPublish",
    "Effect": "Allow",
    "Action": "sns:Publish",
    "Resource": "SNS_TOPIC_ARN"
  },
  {
    "Sid": "KMSSourceKeyReadOperations",
    "Effect": "Allow",
    "Action": [
      "kms:GetKeyPolicy",
      "kms:DescribeKey"
    ],
  },

```

```

        "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID"
    },
    {
        "Sid": "KMSSourceKeyMutatingOperations",
        "Effect": "Allow",
        "Action": "kms:PutKeyPolicy",
        "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID",
        "Condition": {
            "StringEquals": {
                "kms:CallerAccount": "SOURCE_ACCOUNT_ID"
            }
        }
    }
]
}

```

Note

- Pernyataan Kebijakan (KMSSourceKeyReadOperations dan KMSSourceKeyMutatingOperations) hanya diperlukan jika bucket sumber menggunakan enkripsi SSE-KMS.
- Ganti CROSS_ACCOUNT_REPLICATION_ROLE_ARN dengan nilai parameter aktual yang Anda berikan ke otomatisasi. CrossAccountReplicationRole

Contoh CrossAccountReplicationRolekebijakan:

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3DestinationBucketReadOperations",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketVersioning",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy",

```

```

        "s3:GetEncryptionConfiguration",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "s3:PutBucketPolicy"
    ],
    "Resource": "arn:aws:s3:::DESTINATION_BUCKET"
},
{
    "Sid": "KMSDestinationKeyReadOperations",
    "Effect": "Allow",
    "Action": [
        "kms:GetKeyPolicy",
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
},
{
    "Sid": "KMSDestinationKeyMutatingOperations",
    "Effect": "Allow",
    "Action": "kms:PutKeyPolicy",
    "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "DESTINATION_ACCOUNT_ID"
        }
    }
}
]
}

```

Note

Pernyataan KMS (KMSDestinationKeyReadOperations dan KMSDestinationKeyMutatingOperations) hanya diperlukan jika bucket tujuan menggunakan enkripsi SSE-KMS. Hapus pernyataan ini untuk skenario SSE-S3.

Contoh kebijakan CrossAccountReplicationRole kepercayaan:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "AUTOMATION_ASSUME_ROLE_ARN"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Note

Ganti AUTOMATION_ASSUME_ROLE_ARN dengan nilai parameter aktual yang Anda berikan ke otomatisasi. AutomationAssumeRole

Contoh ReplicationRole kebijakan S3:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3SourceBucketPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetReplicationConfiguration",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::SOURCE_BUCKET",
        "arn:aws:s3:::SOURCE_BUCKET/*"
      ]
    }
  ]
}
```



```

    ]
  },
  {
    "Sid": "S3DestinationBucketPermissions",
    "Effect": "Allow",
    "Action": [
      "s3:ReplicateObject",
      "s3:ReplicateDelete",
      "s3:ReplicateTags"
    ],
    "Resource": "arn:aws:s3:::DESTINATION_BUCKET/*"
  },
  {
    "Sid": "S3CrossAccountPermissions",
    "Effect": "Allow",
    "Action": "s3:ObjectOwnerOverrideToBucketOwner",
    "Resource": "arn:aws:s3:::DESTINATION_BUCKET/*"
  },
  {
    "Sid": "KMSSourceKeyPermissions",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID"
  },
  {
    "Sid": "KMSDestinationKeyPermissions",
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:GenerateDataKey",
      "kms:ReEncrypt*"
    ],
    "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/
DESTINATION_KMS_KEY_ID"
  }
]
}

```

 Note

- Pernyataan KMS (KMSSourceKeyPermissions dan KMSDestinationKeyPermissions) hanya diperlukan ketika bucket menggunakan enkripsi SSE-KMS.
- CrossAccountPermissions Pernyataan S3 hanya diperlukan untuk replikasi bucket lintas akun.

Contoh kebijakan ReplicationRole kepercayaan S3:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSsupport-ConfigureS3ReplicationSameAndCrossAccount](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Diperlukan):
 - 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 memulai runbook ini.

- Tipe: `AWS::IAM::Role::Arn`
- SourceBucket (Diperlukan):
 - Deskripsi: (Wajib) Nama bucket Amazon S3 sumber tempat aturan replikasi akan dibuat atau diperbarui.
 - Tipe: `AWS::S3::Bucket::Name`
- DestinationBucket (Diperlukan):
 - Deskripsi: (Wajib) Nama bucket Amazon S3 tujuan tempat objek akan direplikasi.
 - Tipe: `String`
 - Pola yang Diizinkan: `^[0-9a-z][a-z0-9\\-\\.]{3,63}$`
- SourceAccountId (Diperlukan):
 - Deskripsi: (Wajib) ID AWS Akun tempat bucket sumber berada.
 - Tipe: `String`
 - Pola yang Diizinkan: `^[0-9]{12,13}$`
- DestinationAccountId (Diperlukan):
 - Deskripsi: (Wajib) ID AWS Akun tempat bucket tujuan berada.
 - Tipe: `String`
 - Pola yang Diizinkan: `^[0-9]{12,13}$`
- SnsNotificationArn (Diperlukan):
 - Deskripsi: (Wajib) ARN dari Amazon Simple Notification Service (Amazon SNS) topik untuk persetujuan Otomasi.
 - Tipe: `String`
 - Pola yang Diizinkan: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):sns:[a-z]{2}(-gov)?(-iso[a-z])?-[a-z]{2,10}-[0-9]{1,2}:\\d{12}:([0-9a-zA-Z-_.]{1,256})(.fifo)?$`
- Penyetuju (Wajib):
 - Deskripsi: (Wajib) Daftar IAM yang user/role ARNs berwenang untuk menyetujui eksekusi otomatisasi.
 - Tipe: `StringList`
 - Pola yang Diizinkan: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam:\\d{12}:(user|role)/[\\w+=,\\.@\\-\\/]+$`

- Deskripsi: (Opsional) ARN dari peran IAM yang ada untuk digunakan untuk operasi replikasi Amazon S3. Peran ini harus memiliki izin untuk membaca dari bucket sumber dan menulis ke bucket tujuan, termasuk izin KMS jika bucket menggunakan enkripsi SSE-KMS. Jika tidak disediakan, otomatisasi akan membuat peran baru dengan izin yang sesuai.
- Tipe: String
- Pola yang Diizinkan: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::\d{12}:role/[\w+=,.\@\\-/+]+$`
- Default: ""
- CrossAccountReplicationRole (Opsional):
 - Deskripsi: (Opsional) ARN peran IAM dalam akun tujuan yang dapat diasumsikan oleh otomatisasi. Ini diperlukan untuk replikasi lintas akun. Untuk replikasi akun yang sama, biarkan ini kosong.
 - Tipe: String
 - Pola yang Diizinkan: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::\d{12}:role/[\w+=,.\@\\-/+]+$`
 - Default: ""
- ReplicateEntireBucket (Opsional):
 - Deskripsi: (Opsional) Jika disetel ke `true`, seluruh bucket akan direplikasi dan Awalan dan Tag harus kosong. Jika salah, replikasi akan didasarkan pada awalan atau tag yang ditentukan.
 - Tipe: Boolean
 - Nilai yang Diizinkan: `[true, false]`
 - Default: `true`
- ReplicationRuleStatus (Opsional):
 - Deskripsi: (Opsional) Jika diatur ke `true`, aturan replikasi yang dibuat akan diaktifkan. Jika disetel ke `false`, aturan replikasi yang dibuat akan disetel ke Dinonaktifkan.
 - Tipe: Boolean
 - Nilai yang Diizinkan: `[true, false]`
 - Default: `true`
- DeleteMarkerReplicationStatus (Opsional):
 - Deskripsi: (Opsional) Jika disetel ke `true`, otomatisasi memungkinkan replikasi penanda

- Tipe: Boolean
- Nilai yang Diizinkan: `[true, false]`
- Default: `false`
- ReplicationTimeControl (Opsional):
 - Deskripsi: (Opsional) Jika disetel ke `true`, aktifkan Kontrol Waktu Replikasi Amazon S3 (Amazon S3 RTC) dengan SLA 15 menit untuk waktu replikasi yang dapat diprediksi.
 - Tipe: Boolean
 - Nilai yang Diizinkan: `[true, false]`
 - Default: `false`
- ReplicaModifications (Opsional):
 - Deskripsi: (Opsional) Jika disetel ke `true`, memungkinkan replikasi perubahan metadata yang dibuat ke objek replika, memungkinkan modifikasi pada objek yang direplikasi untuk disinkronkan kembali ke sumber.
 - Tipe: Boolean
 - Nilai yang Diizinkan: `[true, false]`
 - Default: `false`
- Awalan (Opsional):
 - Deskripsi: (Opsional) Filter awalan untuk replikasi selektif objek dengan awalan kunci tertentu. Awalan harus diakhiri dengan garis miring (/) untuk pemfilteran awalan Amazon S3 yang tepat.
 - Tipe: String
 - Pola yang Diizinkan: `^$|^([a-zA-Z0-9!_'\(\)\-\-]*\/+)$`
 - Default: `""`
- Tag (Opsional):
 - Deskripsi: (Opsional) JSON array tag untuk memfilter objek untuk direplikasi. Format untuk tag tunggal: `[{"Key": "TagKey", "Value": "TagValue"}]` dan untuk beberapa tag: `[{"Key": "TagKey 1", "Value": "TagValue 1"}, {"Key": "TagKey 2", "Value": "TagValue 2"}]`.
 - Tipe: String
 - Pola yang Diizinkan: `^\\[\\(\\(\\{\\\"Key\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{1,128}\\\", \\\"Value\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{0,256}\\\"\\}\\}\\(,\\{\\\"Key\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{1,128}\\\", \\\"Value\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{0,256}\\\"\\}\\}\\)*\\)?\\$`

- Default: []

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- `ValidateInputParameters`:

Memvalidasi semua parameter input untuk kebenaran dan kompatibilitas untuk memastikan konfigurasi replikasi yang tepat.

- `PrepareApprovalMessage`:

Menyiapkan pesan persetujuan dengan semua parameter konfigurasi replikasi untuk tinjauan pengguna.

- `RequestApproval`:

Meminta persetujuan dari pengguna yang berwenang sebelum melanjutkan dengan perubahan konfigurasi replikasi Amazon S3.

- `CheckBucketEncryption`:

Memeriksa konfigurasi enkripsi untuk bucket Amazon S3 sumber dan tujuan untuk menentukan pengaturan replikasi yang kompatibel.

- `BranchOnEncryptionType`:

Eksekusi cabang berdasarkan jenis enkripsi bucket Amazon S3 untuk menerapkan konfigurasi replikasi yang sesuai untuk bucket terenkripsi SSE-S3 atau SSE-KMS.

- Konfigurasi SSES3 Replikasi:

Mengonfigurasi replikasi Amazon S3 untuk bucket yang dienkripsi dengan Enkripsi Sisi Server dengan Amazon S3-Managed Keys (SSE-S3), termasuk peran IAM dan aturan replikasi.

- Konfigurasi SSEKMSReplication:

Mengonfigurasi replikasi Amazon S3 untuk bucket yang dienkripsi dengan Enkripsi Sisi Server AWS KMS dengan (SSE-KMS), termasuk peran IAM, izin kunci KMS, dan aturan replikasi.

- `CleanupResources`:

Membersihkan peran IAM yang dibuat selama konfigurasi replikasi gagal saat S3 tidak disediakan `ReplicationRole` oleh pelanggan.

7. Setelah selesai, tinjau output dari langkah Configure SSES3 Replication (untuk bucket terenkripsi SSE-S3) atau SSEKMSReplication langkah Configure (untuk bucket terenkripsi SSE-KMS) untuk hasil eksekusi, termasuk status konfigurasi replikasi bersama dengan peran IAM yang digunakan untuk Replikasi.

Referensi

Otomatisasi Systems Manager

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

AWSSupport-EmptyS3Bucket

Deskripsi

Runbook AWSSupport-EmptyS3Bucket otomatisasi mengosongkan bucket Amazon Simple Storage Service (Amazon S3) yang sudah ada dengan menggunakan aturan konfigurasi kedaluwarsa siklus hidup.

Important

- Bucket Amazon S3 dengan Otentikasi Multi-faktor (MFA) diaktifkan tidak didukung.
- Aturan siklus hidup yang dimodifikasi oleh runbook ini secara permanen menghapus semua objek dan versinya di bucket Amazon S3 yang ditentukan. Anda tidak dapat memulihkan objek yang dihapus secara permanen. Untuk informasi lebih lanjut, tinjau [Objek Kedaluwarsa](#).

Bagaimana cara kerjanya?

Runbook AWSSupport-EmptyS3Bucket melakukan langkah-langkah tingkat tinggi berikut:

- Menangguhkan versi bucket, jika diaktifkan.
- Memperbarui kebijakan bucket untuk menolak panggilan s3:PutObject API apa pun (untuk mencegah unggahan baru saat sedang dikosongkan).

- Memperbarui aturan siklus hidup untuk menghapus semua objek sesuai dengan hari kedaluwarsa yang ditentukan dalam parameter input.

 Note

- Versi objek yang dilindungi dengan Amazon S3 Object Lock tidak dihapus atau ditimpa oleh konfigurasi siklus hidup.
- Proses penghapusan tidak sinkron dan mungkin memerlukan waktu untuk diselesaikan setelah eksekusi runbook selesai.

Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

AutomationAssumeRole Parameter memerlukan tindakan berikut agar berhasil menggunakan runbook:

- ssm: DescribeAutomationExecutions
- ssm: GetAutomationExecution
- s3: GetBucketVersioning
- s3: PutBucketVersioning
- s3: GetBucketPolicy

- s3: GetBucketLifecycleConfiguration
- s3: GetLifecycleConfiguration
- s3: PutBucketPolicy
- s3: PutBucketLifecycleConfiguration
- s3: PutLifecycleConfiguration
- s3: DeleteBucketPolicy
- s3: DeleteBucketLifecycle

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-EmptyS3Bucket](#) 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.

- S3BucketName:

Nama bucket Amazon S3 yang ingin Anda kosongkan.

- SNSTopicArn:

Berikan ARN Topik Amazon SNS untuk pemberitahuan persetujuan. Topik Amazon SNS ini digunakan untuk mengirim pemberitahuan persetujuan selama diperlukan selama eksekusi otomatisasi.

- ApproverIAM:

Berikan daftar kepala sekolah yang AWS diautentikasi yang dapat menyetujui atau menolak tindakan tersebut. Jumlah maksimum pemberi persetujuan adalah 10. Anda dapat menentukan prinsipal dengan menggunakan salah satu format ini, nama pengguna AWS Identity and Access Management (IAM), ARN pengguna IAM, ARN peran IAM, atau ARN pengguna peran IAM.

- MinimumRequiredApprovals(Opsional):

Jumlah minimum persetujuan yang diperlukan untuk melanjutkan otomatisasi. Jika Anda tidak menentukan nilai, sistem default ke. 1 Nilai untuk parameter ini harus berupa angka positif. Nilai untuk parameter ini tidak dapat melebihi jumlah pemberi persetujuan yang ditentukan oleh parameter ApproverIAM.

- NoncurrentVersionExpirationDays(Optional):

Tentukan jumlah hari ketika versi objek noncurrent kedaluwarsa. Setelah kedaluwarsa, Amazon S3 menghapus versi objek noncurrent secara permanen.

- Default: 1
- Nilai Maksimum: 365
- ExpirationDays (Optional):

Tentukan kedaluwarsa untuk siklus hidup objek dalam bentuk hari.

- Default: 1
- Nilai Maksimum: 365
- AbortIncompleteMultipartUpload(Optional):

Tentukan hari sejak dimulainya unggahan multibagian yang tidak lengkap yang akan ditunggu Amazon S3 sebelum menghapus semua bagian unggahan secara permanen.

- Default: 1
- Nilai Maksimum: 365
- Pengakuan:

Harap baca detail lengkap tindakan yang dilakukan oleh runbook otomatisasi ini dan berikan persetujuan Yes, I understand and acknowledge jika Anda mengakui langkah-langkahnya.

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.

SNSTopicArn
(Required) The ARN of the Amazon Simple Notification Service (Amazon SNS) Topic for approval notification. This SNS topic is used to send the approval notifications required during the automation execution.

MinimumRequiredApprovals
(Optional) The minimum number of approvals required to resume the automation. If you don't specify a value, the system defaults to one. The value for this parameter must be a positive number. The value for this parameter can't exceed the number of approvers defined in the 'ApproverIAM' parameter.

ExpirationDays
(Optional) Specify the expiration for the lifecycle of the object in days. Default value is 1 and max value is 365.

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. ****Important:**** You cannot recover permanently removed objects. For more information please review [Expiring objects] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-expire-general-considerations.html>).

S3BucketName
(Required) The name of the Amazon S3 bucket you want to empty.

ApproverIAM
(Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats, 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN.

NoncurrentVersionExpirationDays
(Optional) Specify the number of days when noncurrent object versions expire. Upon expiration, Amazon S3 permanently deletes the noncurrent object versions. Default value is 1 and max value is 365.

AbortIncompleteMultipartUpload
(Optional) Specify the days since the initiation of an incomplete multipart upload that Amazon S3 will wait before permanently removing all parts of the upload. Default value is 1 and max value is 365.

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **checkConcurrency:**

Memastikan hanya ada satu eksekusi runbook ini yang menargetkan bucket Amazon S3 yang ditentukan. Jika runbook menemukan eksekusi lain dalam proses yang menargetkan nama bucket yang sama, itu akan mengembalikan kesalahan dan berakhir.

- **getBucketVersioningConfiguration:**

Mengambil status pembuatan versi bucket Amazon S3 yang ditentukan.

- **branchOnStoppingIfMFADeleteEnabled(bersyarat):**

Menghentikan otomatisasi jika Otentikasi Multi-faktor (MFA) diaktifkan pada bucket Amazon S3 yang ditentukan.

- **approvalToMakeChangesToTheProvidedS3Bucket:**

Menunggu persetujuan kepala sekolah yang ditentukan untuk menonaktifkan pembuatan versi bucket dan memperbarui kebijakan bucket dan konfigurasi aturan siklus hidup untuk bucket Amazon S3 yang ditentukan.

- **branchOnBucketVersioningStatus**(bersyarat):

Jika pembuatan versi diaktifkan pada bucket Amazon S3 yang ditentukan, nonaktifkan, jika tidak, lanjutkan perbarui kebijakan bucket dan konfigurasi siklus hidup.

- **suspendBucketVersioning**:

Menangguhkan status pembuatan versi bucket Amazon S3 yang ditentukan.

- **updateBucketPolicyAndLifecycleConfiguration**:

Menambahkan atau memperbarui kebijakan bucket untuk menolak semua `s3:PutObject` permintaan dan memperbarui konfigurasi siklus hidup untuk objek kedaluwarsa berdasarkan parameter input yang diberikan pengguna.

- **branchOnFailingIfBucketPropertiesNotUpdated**(bersyarat):

Memeriksa status `updateBucketPolicyAndLifecycleConfiguration` langkah dan mencoba mengembalikan status pembuatan versi bucket asli jika diubah oleh otomatisasi.

- **branchOnFailureOriginalVersioningStatus**(bersyarat):

Pada kegagalan, cabang untuk menentukan status versi asli. Jika diaktifkan dan ditangguhkan oleh otomatisasi ini, coba aktifkan lagi.

- **onFailureRestoreBucketVersioning**

Mengembalikan status pembuatan versi yang diaktifkan dari bucket Amazon S3 yang ditentukan.

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

✓ Execution has been initiated.
✕

Execution detail: AWSSupport-EmptyS3Bucket Cancel execution Actions ▾

▶ Execution description

▼ Outputs

updateBucketPolicyAndLifecycleConfiguration.Message

===== Execution Result =====

INFO: Getting the configured lifecycle rules for the S3 Bucket: sample-not-empty-bucket
 INFO: Getting bucket policy for S3 Bucket: sample-not-empty-bucket
 INFO: Creating new bucket policy to deny any s3:PutObject API calls (to prevent new uploads while it is being emptied).
 INFO: Creating a new lifecycle rule to delete all the objects according to the expiration days specified in the input parameters
 INFO: The bucket updates have been successfully completed.
 Upon the expiration of items, as specified in the parameters, the bucket will be emptied.
 Meanwhile, S3 'put object' requests are denied by the bucket policy to prevent the upload of new items.

Execution status

Overall status

✓ Success

Failed

0

All executed steps

7

Cancelled

0

Succeeded

7

TimedOut

0

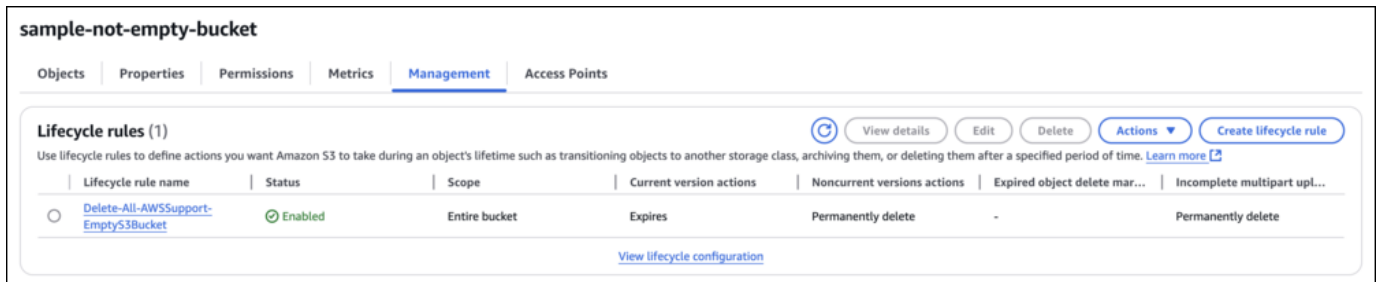
Executed steps (10)

< 1 >

Step ID	Step #	Step name	Action	Status	Start time
17e09354-6a90-4216-9797-a9d6fa18d57c	1	checkConcurrency	aws:executeScript	✓ Success	Wed, 18 Dec 2024 08:01:54 GM
44bc75db-0bd9-44c1-9537-0b9ff9eea87a	2	getBucketVersioningConfiguration	aws:executeAwsApi	✓ Success	Wed, 18 Dec 2024 08:02:08 GM
1e942013-e886-4fce-b685-bc8e578bcb2a	3	branchOnStoppingIfMFADeleteEnabled	aws:branch	✓ Success	Wed, 18 Dec 2024 08:02:09 GM
742066ac-39a8-4699-8aa4-13a7a8b0239f	4	approvalToMakeChangesToTheProvidedS3Bucket	aws:approve	✓ Success	Wed, 18 Dec 2024 08:02:09 GM
34c276bb-f7e3-43f8-a89f-8d457040cc31	5	branchOnBucketVersioningStatus	aws:branch	✓ Success	Wed, 18 Dec 2024 08:03:24 GM
5f3efb16-d6f8-441e-b090-ab6c88ab2a9d	6	updateBucketPolicyAndLifecycleConfiguration	aws:executeScript	✓ Success	Wed, 18 Dec 2024 08:03:25 GM
739dd72a-e7de-42d9-900a-7a0aa5e826d0	7	branchOnFailingIfBucketPropertiesNotUpdated	aws:branch	✓ Success	Wed, 18 Dec 2024 08:03:29 GM
f97fc493-3d62-4884-901f-dcc2a2a3bcd0	8	suspendBucketVersioning	aws:executeAwsApi	⌚ Pending	-
4b02a204-8de7-49c8-b079-e94741c40a37	9	branchOnFailureOriginalVersioningStatus	aws:branch	⌚ Pending	-
92645daf-8587-4947-bc53-b4c440d07f84	10	onFailureRestoreBucketVersioning	aws:executeAwsApi	⌚ Pending	-

- Eksekusi yang berhasil

Alur kerja ini memperbarui aturan siklus hidup bucket. Objek akan dihapus sesuai dengan kebijakan Delete-All-AWSSupport-EmptyS3-Bucket siklus hidup.



- Eksekusi kegagalan

Penghapusan sebagian tidak akan dilakukan. Jika eksekusi gagal, siklus hidup dan pengaturan bucket lainnya akan digulung kembali.

Referensi

Otomatisasi Systems Manager

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

Untuk informasi selengkapnya tentang mengelola bucket dan objek Amazon S3, lihat [Mengosongkan bucket](#).

AWSSupport-TroubleshootS3EventNotifications

Deskripsi

Runbook AWSSupport-TroubleshootS3EventNotifications AWS Systems Manager otomatisasi membantu memecahkan masalah Pemberitahuan Acara Bucket Simple Storage Service Amazon (Amazon S3) yang dikonfigurasi AWS Lambda dengan Fungsi, Topik Simple Notification Service Amazon (Amazon SNS), atau Amazon Simple Queue Service (Amazon SQS) Antrian. Ini menyediakan laporan pengaturan konfigurasi dari berbagai sumber daya yang dikonfigurasi dengan Amazon S3 Bucket sebagai pemberitahuan acara tujuan.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Memeriksa apakah Bucket Amazon S3 ada di akun yang sama tempat `AWSSupport-TroubleshootS3EventNotifications` dijalankan.
- Mengambil sumber daya tujuan (AWS Lambda Fungsi, atau Topik Amazon SNS atau antrean Amazon SQS) yang dikonfigurasi sebagai Pemberitahuan Peristiwa untuk Bucket Amazon S3 menggunakan API. [GetBucketNotificationConfiguration](#)
- Memvalidasi bahwa sumber daya tujuan ada, lalu meninjau kebijakan sumber daya tujuan berbasis sumber daya untuk menentukan apakah Amazon S3 diizinkan untuk mempublikasikan ke tujuan.
- Jika Anda mengenkripsi tujuan dengan kunci AWS Key Management Service (AWS KMS), kebijakan kunci akan diperiksa untuk menentukan apakah akses Amazon S3 diizinkan.
- Menghasilkan laporan dari semua pemeriksaan sumber daya tujuan.

Important

- Runbook ini hanya dapat mengevaluasi konfigurasi notifikasi peristiwa jika pemilik bucket Amazon S3 sama Akun AWS dengan pemilik tempat runbook otomatisasi dijalankan.
- Selain itu, buku runbook ini tidak dapat mengevaluasi kebijakan tentang sumber daya tujuan yang di-host di tempat lain Akun AWS.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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.

- S3 BucketName

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

Deskripsi: (Wajib) Nama bucket Amazon S3 yang dikonfigurasi dengan notifikasi peristiwa.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:GetBucketNotification`
- `sqs:GetQueueAttributes`
- `sqs:GetQueueUrl`
- `sns:GetTopicAttributes`
- `kms:GetKeyPolicy`
- `kms:DescribeKey`
- `kms:ListAliases`
- `lambda:GetPolicy`
- `lambda:GetFunction`
- `iam:GetContextKeysForCustomPolicy`
- `iam:SimulateCustomPolicy`
- `iam:ListRoles`
- `ssm:DescribeAutomationStepExecutions`

Contoh Kebijakan IAM untuk Otomasi Asumsikan Peran

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permission",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3PermissionGetBucketNotification",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketNotification"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "SQSPermission",
      "Effect": "Allow",
      "Action": [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource": "arn:aws:sqs:us-east-1:111122223333:*"
    },
    {
      "Sid": "SNSPermission",
      "Effect": "Allow",
      "Action": [
        "sns:GetTopicAttributes"
      ],
      "Resource": "arn:aws:sns:us-east-1:111122223333:*"
    }
  ]
}

```

```

        "Sid": "KMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey",
            "kms:ListAliases"
        ],
        "Resource": "arn:aws:kms:us-  

east-1:111122223333:key/key-id"
    },
    {
        "Sid": "LambdaPermission",
        "Effect": "Allow",
        "Action": [
            "lambda:GetPolicy",
            "lambda:GetFunction"
        ],
        "Resource": "arn:aws:lambda:us-  

east-1:111122223333:function:*"
    },
    {
        "Sid": "IAMPermission",
        "Effect": "Allow",
        "Action": [
            "iam:GetContextKeysForCustomPolicy",
            "iam:SimulateCustomPolicy",
            "iam:ListRoles"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SSMPermission",
        "Effect": "Allow",
        "Action": [
            "ssm:DescribeAutomationStepExecutions"
        ],
        "Resource": "*"
    }
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

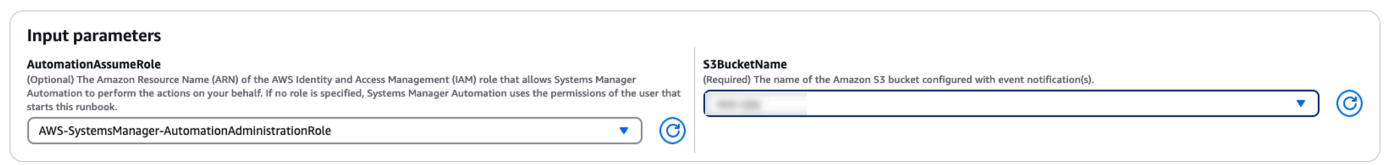
1. Arahkan ke [AWS Support - Troubleshoot S3 Event Notifications](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:

- 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.

- S3 BucketName (Diperlukan):

Nama bucket Amazon S3 dikonfigurasi dengan notifikasi acara.



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.

AWS-SystemsManager-AutomationAdministrationRole

S3BucketName
(Required) The name of the Amazon S3 bucket configured with event notification(s).

4. Pilih Jalankan.
5. Otomatisasi dimulai.
6. Dokumen melakukan langkah-langkah berikut:

- ValidateInputs

Memvalidasi bucket Amazon S3 yang disediakan milik akun yang sama tempat otomatisasi dijalankan dan mengambil wilayah tempat bucket di-host.

- GetBucketNotificationConfiguration

Memanggil GetBucketNotificationConfiguration API untuk meninjau Pemberitahuan Acara yang dikonfigurasi dengan bucket Amazon S3 dan output format.

- BranchOnSQSResourceKebijakan

Cabang tentang apakah ada sumber daya Amazon SQS dalam pemberitahuan acara.

- Kebijakan Validasi SQSResource

Memvalidasi kebijakan sumber daya pada atribut Antrian Amazon SQS sqs:SendMessage memiliki izin untuk Amazon S3. Jika sumber daya Amazon SQS dienkripsi, periksa apakah

enkripsi tidak menggunakan AWS KMS kunci default yaitu `aws/sqs` dan memeriksa bahwa kebijakan AWS KMS kunci memiliki izin untuk Amazon S3.

- `BranchOnSNSResourceKebijakan`

Cabang tentang apakah ada sumber daya Amazon SNS dalam pemberitahuan acara.

- `Kebijakan Validasi SNSResource`

Memvalidasi kebijakan sumber daya pada atribut Topik Amazon SNS `sns:Publish` memiliki izin untuk Amazon S3. Jika sumber daya Amazon SNS dienkripsi, periksa apakah enkripsi tidak menggunakan AWS KMS kunci default yaitu `aws/sns` dan memeriksa bahwa kebijakan AWS KMS kunci memiliki izin untuk Amazon S3.

- `BranchOnLambdaFunctionResourcePolicy`

Cabang tentang apakah ada AWS Lambda fungsi dalam pemberitahuan acara.

- `ValidateLambdaFunctionResourcePolicy`

Memvalidasi kebijakan sumber daya pada AWS Lambda fungsi memiliki `lambda:InvokeFunction` izin untuk Amazon S3.

- `GenerateReport`

Mengembalikan detail keluaran langkah runbook, dan rekomendasi untuk menyelesaikan masalah apa pun dengan notifikasi acara yang dikonfigurasi dengan bucket Amazon S3.

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

- `Pemberitahuan Acara Amazon SQS`

Jika ada notifikasi tujuan Amazon SQS yang dikonfigurasi dengan bucket Amazon S3, daftar Antrian Amazon SQS ditampilkan di samping hasil pemeriksaan. Laporan tersebut mencakup pemeriksaan sumber daya Amazon SQS, pemeriksaan kebijakan akses Amazon SQS AWS KMS, pemeriksaan kunci, pemeriksaan status kunci AWS KMS, AWS KMS dan pemeriksaan kebijakan kunci.

- `Pemberitahuan Acara Amazon SNS`

Jika ada notifikasi tujuan Amazon SNS yang dikonfigurasi dengan bucket Amazon S3, daftar Topik Amazon SNS ditampilkan di samping hasil pemeriksaan. Laporan tersebut mencakup pemeriksaan sumber daya Amazon SNS, pemeriksaan kebijakan akses Amazon SNS AWS KMS, pemeriksaan kunci, pemeriksaan status kunci AWS KMS, AWS KMS dan pemeriksaan kebijakan kunci.

- AWS Lambda Pemberitahuan Acara

Jika ada notifikasi AWS Lambda tujuan yang dikonfigurasi dengan bucket Amazon S3, daftar fungsi Lambda ditampilkan di samping hasil pemeriksaan. Laporan tersebut mencakup pemeriksaan sumber daya Lambda dan pemeriksaan kebijakan akses Lambda.

▼ Outputs

generateReport.Output

```

-----
| Amazon S3 Event Notification Troubleshooting Results for S3 Bucket |
-----
| Amazon SQS Event Notifications |
-----
| SQS Queue: 1. arn:aws:sqs:us-east-1:123456789012:SAW-Core-TroubleshootS3EventNotification-EncryptedQueue | KMS Key: |
| SQS resource check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| SQS access policy check | ✓ [PASSED]: The resource policy is properly configured for use with S3 Bucket. |
| KMS key check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| KMS key status check | ✗ [FAILED]: The KMS key is disabled. |
| KMS key policy check | ✓ [PASSED]: The resource policy is properly configured for use with S3 Bucket. |
-----
| Amazon SNS Event Notifications |
-----
| SNS Topic: 1. arn:aws:sns:us-east-1:123456789012:SAW-Core-TroubleshootS3EventNotification-EncryptedTopic | KMS Key: alias/aws/sns |
| SNS resource check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| SNS access policy check | ✓ [PASSED]: The resource policy is properly configured for use with S3 Bucket. |
| KMS key check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| KMS key status check | ✓ [PASSED]: Not Applicable. |
| KMS key policy check | ✗ [FAILED]: Amazon S3 Event Notifications does not support using SQS or SNS targets encrypted using AWS managed keys, i.e., aws/sns or aws/sqs respectively. |
-----
| AWS Lambda Event Notifications |
-----
| Lambda Function: 1. arn:aws:lambda:us-east-1:123456789012:function:SAW-Core-TroubleshootS3EventNotification-LambdaFunction |
| Lambda resource check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| Lambda access policy check | ✗ [FAILED]: No resource policies found on the resource. Please update the resource with a valid policy using this guide: https://docs.aws.amazon.com/AmazonS3/latest/userguide/grant-destin
-----

```

Referensi

Otomatisasi Systems Manager

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

AWSSupport-ContainS3Resource

Deskripsi

AWSSupport-ContainS3ResourceRunbook menyediakan solusi otomatis untuk prosedur yang diuraikan dalam artikel [Support Automation Workflow \(SAW\) Runbook: Mengandung Bucket Amazon S3 yang disusupi AWS](#)

Important

- Runbook ini menjalankan berbagai operasi yang memerlukan hak istimewa yang ditingkatkan, seperti memodifikasi kebijakan bucket Amazon S3, tag, dan konfigurasi akses publik. Tindakan ini berpotensi menyebabkan eskalasi hak istimewa atau memengaruhi beban kerja lain yang bergantung pada bucket Amazon S3 yang ditargetkan. Anda harus meninjau izin yang diberikan untuk peran yang ditentukan oleh `AutomationAssumeRole` parameter dan memastikannya sesuai untuk kasus penggunaan yang dimaksudkan. Anda dapat merujuk ke AWS dokumentasi berikut untuk informasi lebih lanjut tentang izin IAM: [Identity and Access Management \(IAM\) PermissionsAWS AWS Systems Manager Automation Permissions](#)
- Runbook ini melakukan tindakan mutatif yang berpotensi menyebabkan tidak tersedianya atau gangguan pada beban kerja Anda. Secara khusus, `Contain` tindakan memblokir semua akses ke bucket Amazon S3 yang ditentukan, kecuali untuk peran yang ditentukan dalam parameter. `SecureRoles` Ini dapat memengaruhi aplikasi atau layanan apa pun yang mengandalkan bucket Amazon S3 yang ditargetkan.
- Selama `Contain` aksi, runbook ini dapat membuat bucket Amazon S3 tambahan (ditentukan oleh `BackupS3BucketName` parameter) untuk menyimpan cadangan konfigurasi bucket asli, jika belum ada.
- Jika `Action` parameter disetel ke `Restore`, runbook ini mencoba mengembalikan konfigurasi bucket Amazon S3 ke status semula berdasarkan cadangan yang disimpan di `BackupS3BucketName` bucket. Namun, ada risiko bahwa proses restorasi mungkin gagal, meninggalkan bucket Amazon S3 dalam keadaan tidak konsisten. Runbook memberikan instruksi untuk restorasi manual jika terjadi kegagalan tersebut, tetapi Anda harus siap untuk menangani masalah potensial selama proses restorasi.

Disarankan untuk meninjau runbook secara menyeluruh, memahami potensi dampaknya, dan mengujinya di lingkungan non-produksi sebelum menjalankannya di lingkungan produksi Anda.

Bagaimana cara kerjanya?

Runbook ini beroperasi secara berbeda berdasarkan jenis dan tindakan sumber daya:

- Untuk Bucket Tujuan Umum Amazon S3Containment: Otomatisasi memblokir akses publik ke bucket, menonaktifkan konfigurasi ACL, memberlakukan kepemilikan Objek Pemilik Bucket, dan menempatkan kebijakan bucket terbatas yang menolak semua tindakan Amazon S3 ke bucket kecuali untuk mengizinkan Peran IAM yang terdaftar.
- Untuk Objek Tujuan Umum Amazon S3Containment: Otomatisasi memblokir Akses Publik ke bucket, menonaktifkan konfigurasi ACL, memberlakukan kepemilikan Objek Pemilik Bucket, dan menempatkan kebijakan bucket terbatas yang menolak semua tindakan Amazon S3 pada objek kecuali untuk mengizinkan Peran IAM yang terdaftar.
- Untuk Bucket Direktori Amazon S3Containment: Otomatisasi menempatkan kebijakan bucket terbatas yang menolak semua tindakan Amazon S3 ke bucket kecuali untuk mengizinkan Peran IAM yang terdaftar.
- Untuk Bucket Tujuan Umum Amazon S3Restore: Otomatisasi mengembalikan konfigurasi Blokir Akses Publik, konfigurasi Bucket ACL, kepemilikan Objek Pemilik Bucket, dan Kebijakan Bucket ke konfigurasi awal sebelum penahanan.
- Untuk Objek Tujuan Umum Amazon S3Restore: Otomatisasi mengembalikan konfigurasi Blokir Akses Publik, konfigurasi Bucket ACL, Konfigurasi Objek ACL, kepemilikan Objek Pemilik Bucket, dan Kebijakan Bucket ke konfigurasi awal sebelum penahanan.
- Untuk Bucket Direktori Amazon S3Restore: Otomatisasi mengembalikan kebijakan bucket ke konfigurasi awal sebelum penahanan.

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

Jenis Dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang Diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- s3: CreateBucket
- s3: DeleteBucketPolicy
- s3: DeleteObjectTagging
- s3: GetAccountPublicAccessBlock
- s3: GetBucketAcl
- s3: GetBucketLocation
- s3: GetBucketOwnershipControls
- s3: GetBucketPolicy
- s3: GetBucketPolicyStatus
- s3: GetBucketTagging
- s3: GetEncryptionConfiguration
- s3: GetObject
- s3: GetObjectAcl
- s3: GetObjectTagging
- s3: GetReplicationConfiguration
- s3: ListBucket
- s3: PutAccountPublicAccessBlock
- s3: PutBucket ACL
- s3: PutBucketOwnershipControls
- s3: PutBucketPolicy
- s3: PutBucketPublicAccessBlock
- s3: PutBucketTagging
- s3: PutBucketVersioning
- s3: PutObject
- s3: PutObjectAcl
- s3express: CreateSession
- s3express: DeleteBucketPolicy
- s3express: GetBucketPolicy
- s3express: PutBucketPolicy
- ssm: DescribeAutomationExecutions

Berikut adalah contoh kebijakan IAM yang memberikan izin yang diperlukan untuk: AutomationAssumeRole

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetEncryptionConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketACL",
        "s3:PutBucketOwnershipControls",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ExpressPermissions",
      "Effect": "Allow",
```

```

        "Action": [
            "s3express:CreateSession",
            "s3express>DeleteBucketPolicy",
            "s3express:GetBucketPolicy",
            "s3express:PutBucketPolicy"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SSMPermissions",
        "Effect": "Allow",
        "Action": [
            "ssm:DescribeAutomationExecutions"
        ],
        "Resource": "*"
    }
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-ContainS3Resource](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - BucketName (Diperlukan):
 - Deskripsi: (Wajib) Nama bucket Amazon S3.
 - Tipe: `AWS::S3::Bucket::Name`
 - Tindakan (Diperlukan):
 - Deskripsi: (Diperlukan) Pilih Contain untuk mengisolasi sumber daya Amazon S3 Restore atau mencoba mengembalikan konfigurasi sumber daya ke keadaan semula dari cadangan sebelumnya.
 - Tipe: String
 - Nilai yang Diizinkan: `Contain|Restore`
 - DryRun (Opsional):

- Deskripsi: (Opsional) Jika disetel ke true, otomatisasi tidak akan membuat perubahan apa pun pada sumber daya Amazon S3 target, melainkan akan menampilkan apa yang akan dicoba diubah. Nilai default: true.
- Jenis: Boolean
- Nilai yang Diizinkan: `true | false`
- BucketKeyName (Opsional):
 - Deskripsi: (Opsional) Kunci objek Amazon S3 yang ingin Anda isi atau pulihkan. Digunakan selama penahanan tingkat objek.
 - Tipe: String
 - Pola yang Diizinkan: `^[a-zA-Z0-9\\.\_-\\\\!*'()/{0,1024}]$`
- BucketRestrictAccess(Bersyarat):
 - Deskripsi: (Bersyarat) ARN pengguna IAM atau peran yang akan diizinkan mengakses sumber daya Amazon S3 target setelah menjalankan tindakan penahanan. Parameter ini diperlukan ketika Action diatur ke `Contain`.
 - Jenis: StringList
 - Pola yang Diizinkan: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam:[0-9]{12}:(role|user)\\/[\\w+\\/=, .@-]+$`
- TagIdentifier (Opsional):
 - Deskripsi: (Opsional) Tag dalam format `Key=BatchId, Value=78925` yang akan ditambahkan ke sumber daya yang dibuat atau dimodifikasi oleh runbook ini selama alur kerja penahanan.
 - Tipe: String
 - Pola yang Diizinkan: `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{0,128}$`
- Backups3 BucketName (Bersyarat):
 - Deskripsi: (Bersyarat) Bucket Amazon S3 untuk mencadangkan konfigurasi sumber daya target saat Action disetel `Contain` ke atau memulihkan konfigurasi dari saat disetel Action ke `Restore`
 - Tipe: `AWS::S3::Bucket::Name`
- Backups3 KeyName (Bersyarat):

- Deskripsi: (Bersyarat) Jika Action disetel ke Restore, ini menentukan kunci Amazon S3 yang akan digunakan otomatisasi untuk mencoba memulihkan konfigurasi sumber daya target.
 - Tipe: String
 - Pola yang Diizinkan: `^[a-zA-Z0-9\\.\_-\\\\!*'()/{0,1024}$`
 - Backups3 BucketAccess (Bersyarat):
 - Deskripsi: (Bersyarat) ARN pengguna IAM atau peran yang akan diizinkan mengakses bucket Amazon S3 cadangan setelah menjalankan tindakan penahanan. Parameter ini Action diperlukan kapanContain.
 - Jenis: StringList
 - Pola yang Diizinkan: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.-]+$`
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (Opsional) Nama Sumber Daya Amazon (ARN) dari peran IAM yang memungkinkan Otomasi Systems Manager untuk melakukan tindakan atas nama Anda.
 - Tipe: `AWS::IAM::Role::Arn`
4. Pilih Jalankan.
 5. Otomatisasi dimulai.
 6. Dokumen melakukan langkah-langkah berikut:
 - validateRequiredInputs

Memvalidasi parameter input otomatisasi yang diperlukan berdasarkan Tindakan yang ditentukan.
 - assertBucketExists

Memeriksa apakah bucket Amazon S3 target ada dan dapat diakses.
 - backupBucketPreCek

Memeriksa apakah bucket Amazon S3 cadangan berpotensi memberikan akses baca atau tulis publik ke objeknya.
 - backupTargetBucketMetadata

Menjelaskan konfigurasi bucket Amazon S3 target saat ini dan mengunggah cadangan ke bucket Amazon S3 cadangan yang ditentukan.

- `ContainBucket`

Melakukan operasi tingkat bucket untuk memuat bucket Amazon S3 target.

- `BranchOnActionAndMode`

Cabang otomatisasi berdasarkan parameter input Tindakan dan `DryRun`.

- `RestoreInstanceConfiguration`

Mengembalikan konfigurasi bucket Amazon S3 dari cadangan.

- `containFinalOutput`

Mengkonsolidasikan aktivitas penahanan dalam format yang dapat dibaca.

- `ReportContain`

Menghasilkan detail dry run untuk tindakan penahanan.

- `ReportRestore`

Menghasilkan detail dry run untuk tindakan pemulihan.

- `ReportRestoreFailure`

Memberikan petunjuk untuk memulihkan konfigurasi asli bucket Amazon S3 selama skenario kegagalan alur kerja pemulihan.

- `ReportContainmentFailure`

Memberikan petunjuk untuk memulihkan konfigurasi asli bucket Amazon S3 selama skenario kegagalan alur kerja penahanan.

- `FinalOutput`

Menghasilkan detail tindakan penahanan.

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

- `ContainFinalOutput.Keluaran`

Mengeluarkan detail tindakan penahanan yang dilakukan oleh runbook ini saat `DryRun` disetel ke `False`.

- `RestoreFinalOutput.Keluaran`

Mengeluarkan detail tindakan pemulihan yang dilakukan oleh runbook ini saat `DryRun` disetel ke `False`.

- `Mengandung3 ResourceDryRun .Output`

Mengeluarkan detail tindakan penahanan yang dilakukan oleh runbook ini saat DryRun disetel ke True.

- `Pulihkan3 ResourceDryRun .Output`

Mengeluarkan detail tindakan pemulihan yang dilakukan oleh runbook ini saat DryRun disetel ke True.

- `ReportContainmentFailure.Keluaran`

Memberikan instruksi untuk memulihkan konfigurasi asli sumber daya Amazon S3 target selama skenario kegagalan alur kerja penahanan.

- `ReportRestoreFailure.Keluaran`

Memberikan instruksi untuk memulihkan konfigurasi asli sumber daya Amazon S3 target selama skenario kegagalan alur kerja pemulihan.

Referensi

Otomatisasi Systems Manager

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

Amazon SES

AWS Systems Manager Automation menyediakan runbook standar untuk Amazon Simple Email Service. Untuk informasi lebih lanjut tentang runbook, lihat [Bekerja dengan runbook](#). Untuk informasi tentang cara melihat konten buku runbook, lihat [Lihat konten runbook](#).

Topik

- [AWSSupport-AnalyzeSESMessagesSendingStatus](#)
- [AWSSupport-DeploySESSendingLogsToCloudWatchLogs](#)

AWSSupport-AnalyzeSESMessagesSendingStatus

Deskripsi

Runbook `AWSSupport-AnalyzeSESMessagesSendingStatus` otomatisasi merangkum status pengiriman email dari pesan email yang tidak terkirim dan memberi Anda saran untuk memecahkan mengapa itu tidak terkirim. Runbook mengambil peristiwa pengiriman email Amazon Simple Email Service (Amazon SES) yang disimpan dalam grup Amazon CloudWatch Logs yang diterbitkan oleh Amazon SES. Untuk detail penerbitan acara Amazon SES, silakan merujuk ke [Pemantauan menggunakan penerbitan acara Amazon Simple Email Service](#). Runbook juga menyediakan ringkasan dan garis waktu pengiriman email serta rekomendasi yang berpotensi memengaruhi pesan email yang tidak terkirim. Anda dapat menemukan pesan-pesan tersebut di bagian output dari setiap eksekusi. Harap dicatat bahwa runbook ini hanya dapat memecahkan masalah peristiwa setelah penyebaran toko acara.

Bagaimana cara kerjanya?

Runbook melakukan langkah-langkah berikut:

- Memeriksa eksekusi otomatisasi bersamaan untuk grup CloudWatch Log yang sama.
- Analisis peristiwa Amazon SES yang sesuai dengan pesan yang IDs diberikan oleh parameter otomatisasi.
- Ringkasan pengiriman output ke bagian output dari eksekusi otomatisasi.

Important

- Sebelum menjalankan runbook ini, Anda harus menyimpan peristiwa Amazon SES yang dipublikasikan ke grup CloudWatch log Log yang ditentukan oleh parameter otomatisasi. Runbook ini hanya menganalisis peristiwa Amazon SES yang disimpan dalam grup log.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

- logs:StartQuery
- logs:GetQueryResults
- ses:GetIdentityMailFromDomainAttributes
- ses:GetSendQuota
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - Analyze SES Message Sending Status](#) 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 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.

- MessageIds (Diperlukan)

Pesan Amazon Simple Email Service dipisahkan koma IDs dari peristiwa Amazon Simple Email Service yang ingin Anda analisis.

- **CloudWatchLogsGroup** (Opsional)

Grup Amazon CloudWatch Logs yang menyimpan acara Amazon Simple Email Service. Nama grup log default adalah `/ses/sending_event_logs`. Jika Anda ingin menggunakan grup log lain selain grup log default, masukkan nama grup log Anda di bidang ini. “,

- **QueryStartTime** (Opsional)

Waktu mulai rentang waktu untuk analisis peristiwa. Format waktu yang valid adalah ISO8601 (misalnya ``yyyy-mm-ddthh:mm:ss``, ``1970-01-01T 00:00:00``). Waktu tanggal default adalah 30 hari yang lalu.

- **QueryEndTime** (Opsional)

Waktu akhir rentang waktu untuk analisis peristiwa. Format waktu yang valid adalah ISO8601 (misalnya ``yyyy-mm-ddthh:mm:ss``, ``1970-01-01T 00:00:00``). Waktu tanggal default adalah waktu saat ini.

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.



CloudWatchLogsGroup

(Optional) The Amazon CloudWatch Logs group which stores Amazon SES events. The default log group name is `/ses/sending_event_logs`. If you would like to utilize another log group than the default log group, please enter your log group name in this field.

QueryEndTime

(Optional) The end time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is the current time.

MessageIds

(Required) Comma separated Amazon SES message IDs of the Amazon SES events that you would like to analyze.

QueryStartTime

(Optional) The start time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is 30 days ago.

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **CheckConcurrency:**

Memastikan bahwa hanya ada satu eksekusi runbook ini yang menargetkan grup Amazon CloudWatch Logs. Jika runbook menemukan eksekusi lain yang menargetkan grup log yang sama, ia mengembalikan kesalahan dan berakhir.

- **AnalyzeSesEvents:**

Analisis peristiwa Amazon Simple Email Service yang disimpan dalam grup Amazon CloudWatch Logs yang ditentukan oleh parameter otomatisasi.

- **OutputFailureReason:**

Keluarkan pesan kegagalan langkah eksekusi saat `AnalyzeSESMessagesSendingStatus` langkah gagal.

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

- Output analisis pada pesan email yang tidak terkirim karena pantulan

Output eksekusi otomatisasi untuk pesan email yang tidak mencapai kotak pesan tujuan karena bouncing.

```
▼ Outputs

OutputFailureReason.FailureReason
No output available yet because the step is not successfully executed

AnalyzeSesEvents.ResultMessage
==== Delivery summary of the message ID [REDACTED] ====
SES received bounces or complaints.

==== Timeline of [REDACTED] =====
[2024-08-21 06:22:58.193000+00:00] Your email message was sent from SES.
[2024-08-21 06:22:58.193000+00:00] SES received a bounce from [REDACTED].
Bounce type: Permanent(general)
Bounce sources:
- email address: [REDACTED] diagnostic code: "smtp; 550 5.1.1 user unknown"

==== Next Action ====
Please fix the issues described in the delivery error messages returned from the destination email servers in the Timeline section. In the case you received s

==== Recommendations for arn:aws:ses:[REDACTED] =====
- The SES account in this region seems to be in the sandbox environment. If you haven't requested the production access, please consider to move out of the san
```

Referensi

Otomatisasi Systems Manager

- [Jalankan Otomasi ini \(konsol\)](#)
- [Jalankan otomatisasi](#)
- [Menyiapkan Otomasi](#)

- [Support Automation Workflow landing page](#)

AWSSupport-DeploySESSendingLogsToCloudWatchLogs

Deskripsi

Runbook AWSSupport-DeploySESSendingLogsToCloudWatchLogs otomatisasi membantu mengonfigurasi infrastruktur yang diperlukan untuk penerbitan acara Amazon Simple Email Service (Amazon SES) ke CloudWatch Amazon Logs CloudWatch (Log). Runbook ini menyiapkan komponen yang diperlukan untuk menangkap peristiwa pengiriman email dan menyimpannya di CloudWatch Log untuk pemantauan dan analisis. Untuk informasi selengkapnya tentang penerbitan acara Amazon SES, lihat [Memantau pengiriman email menggunakan penerbitan acara Amazon SES](#).

Saat ApproveDeployAnalyticEnvironment parameter disetel keapprove, buku runbook ini membuat AWS sumber daya baru di AWS akun Anda. CloudFormation Tumpukan secara otomatis dihapus setelah waktu yang ditentukan dalam SleepTime parameter kecuali diatur ke0.

Bagaimana cara kerjanya?

Runbook ini melakukan tindakan berikut:

- Daftar set konfigurasi yang ada yang memiliki tujuan acara yang dikonfigurasi untuk topik atau aliran pengiriman Amazon Simple Notification Service (Amazon SNS).
- Membuat infrastruktur yang diperlukan untuk penerbitan acara Amazon SES ke CloudWatch Log saat ApproveDeployAnalyticEnvironment parameter disetel keapprove.

Ketika ApproveDeployAnalyticEnvironment parameter disetel keapprove, runbook akan membuat sumber daya berikut:

- CloudFormation Tumpukan bernama AWSSupport-SESSendingLogsToCloudWatchLogs yang mencakup:
 - Topik Amazon SNS dengan enkripsi AWS Key Management Service (AWS KMS)
 - Antrean Amazon Simple Queue Service (Amazon SQS)
 - AWS Lambda fungsi untuk memproses acara pengiriman email
 - AWS Identity and Access Management (IAM) peran eksekusi dengan izin untuk Amazon SQS dan Log CloudWatch
 - CloudWatch Grup log log

- AWS KMS kunci untuk enkripsi
- Konfigurasi Amazon SES diatur dengan tujuan acara
- Infrastruktur memproses peristiwa pengiriman email dalam alur berikut: Acara Pengiriman Email Amazon SES → Set Konfigurasi Amazon SES → Topik Amazon SNS → Antrian Amazon SQS → Fungsi Lambda → Log CloudWatch
- Mengaitkan set konfigurasi yang dibuat sebagai set konfigurasi default untuk identitas Amazon SES tertentu saat `SesIdentity` parameter disediakan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

/

Izin IAM yang diperlukan

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

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStackEvents`
- `cloudformation:DescribeStacks`
- `iam:CreateRole`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `kms:CreateKey`
- `kms:CreateAlias`

- `lambda:CreateFunction`
- `lambda:AddPermission`
- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `ses:CreateConfigurationSet`
- `ses:CreateConfigurationSetEventDestination`
- `ses:ListConfigurationSets`
- `ses:PutEmailIdentityConfigurationSetAttributes`
- `sns:CreateTopic`
- `sns:Subscribe`
- `sqs:CreateQueue`
- `sqs:SetQueueAttributes`
- `ssm:DescribeAutomationExecutions`

Contoh Kebijakan:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "kms:CreateKey",
        "kms:CreateAlias",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "ses:CreateConfigurationSet",
```

```

        "ses:CreateConfigurationSetEventDestination",
        "ses:ListConfigurationSets",
        "ses:PutEmailIdentityConfigurationSetAttributes",
        "sns:CreateTopic",
        "sns:Subscribe",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "ssm:DescribeAutomationExecutions"
    ],
    "Resource": "*"
}
]
}

```

Instruksi

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWS Support - Deploy SES Sending Logs To CloudWatch Logs](#) Systems Manager di bawah Documents.
2. Pilih Jalankan otomatisasi.
3. Untuk parameter input, masukkan yang berikut ini:
 - AutomationAssumeRole (Opsional):
 - Deskripsi: (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.
 - Tipe: `AWS::IAM::Role::Arn`
 - ApproveDeployAnalyticEnvironment (Opsional):
 - Deskripsi: (Opsional) Persetujuan untuk menerapkan infrastruktur penerbitan acara Amazon SES. Masuk approve untuk membuat CloudFormation tumpukan dan sumber daya terkait. Jika dibiarkan kosong, runbook hanya menampilkan set konfigurasi yang ada dengan atau tujuan acara Amazon SNS di wilayah saat ini.
 - Tipe: `String`
 - Izinkan Pola: `^$|^approve$`
 - Default: `""`
 - SesIdentity (Opsional):

- Deskripsi: (Opsional) Identitas Amazon SES (alamat email atau domain) untuk dikaitkan dengan konfigurasi yang baru dibuat yang ditetapkan sebagai set konfigurasi default. Ini akan menimpa set konfigurasi default yang ada untuk identitas yang ditentukan.
- Tipe: String
- Default: ""
- CloudWatchLogGroupName (Opsional):
 - Deskripsi: (Opsional) Nama grup CloudWatch log Log yang akan dibuat untuk menyimpan peristiwa pengiriman email Amazon SES.
 - Tipe: String
 - Izinkan Pola: `^[0-9a-zA-Z_.#/\-]{1,512}$`
 - Default: `/ses/sending_event_logs`
- Topeng PIIData (Opsional):
 - Deskripsi: (Opsional) Tentukan apakah akan menutupi data informasi identitas pribadi (PII) seperti alamat email tujuan dan subjek email di Log. CloudWatch Setel `False` untuk menyertakan informasi ini di log.
 - Tipe: String
 - Nilai yang Diizinkan: `[True, False]`
 - Default: `True`
- SleepTime (Opsional):
 - Deskripsi: (Opsional) Jumlah menit untuk menunggu sebelum secara otomatis menghapus CloudFormation tumpukan. Standarnya adalah 24 jam (1.440 menit), maksimum 7 hari (10.080 menit). Setel `0` untuk mencegah penghapusan otomatis.
 - Tipe: String
 - Izinkan Pola: `^(?:[0-9]|[1-9]\d{1,3}|100[0-7][0-9])$`
 - Default: `1440`
- RetainCloudWatchLogsOnDeletion (Opsional):
 - Deskripsi: (Opsional) Tentukan apakah akan mempertahankan grup CloudWatch log Log saat CloudFormation tumpukan dihapus. Setel `False` untuk menghapus grup log bersama dengan tumpukan.
 - Tipe: String
 - Nilai yang Diizinkan: `[True, False]`
 - Default: `True`

- **Uniqueld (Opsional):**
 - Deskripsi: (Opsional) Pengidentifikasi unik untuk alur kerja.
 - Tipe: String
 - Izinkan Pola: `\\{\\{ automation:EXECUTION_ID \\}\\}\\}|[a-zA-Z0-9-]+`
 - Default: `{ automation:EXECUTION_ID }`
 - Karakter kapak: 64

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- **BranchOnValueOfParameterApproveDeployAnalyticEnvironment**

Menentukan apakah akan menerapkan infrastruktur penerbitan acara Amazon SES berdasarkan nilai `ApproveDeployAnalyticEnvironment` parameter.

- **GetEligibleConfigurationSets**

Mengambil set konfigurasi Amazon SES yang ada dan mengidentifikasi set dengan tujuan acara yang dikonfigurasi untuk aliran pengiriman atau topik Amazon SNS.

- **CheckConcurrency**

Memverifikasi bahwa tidak ada tumpukan yang ada dan tidak ada eksekusi bersamaan lainnya dari runbook ini yang membuat tumpukan yang sama.

- **DeploySesEventDestinations**

Membuat CloudFormation tumpukan yang berisi infrastruktur penerbitan acara Amazon SES termasuk topik Amazon SNS, antrian Amazon SQS, fungsi Lambda, dan grup log Log CloudWatch

- **RelateConfigurationSetAsDefaultConfigurationSet**

Mengaitkan set konfigurasi Amazon SES yang baru dibuat sebagai set konfigurasi default untuk identitas Amazon SES yang ditentukan (jika disediakan).

- **SleepBeforeDeleteCloudFormationStack**

Menunggu durasi yang ditentukan dalam `SleepTime` parameter sebelum melanjutkan untuk menghapus tumpukan. CloudFormation

Menghapus CloudFormation tumpukan setelah periode waktu yang ditentukan.

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

Referensi

Otomatisasi Systems Manager

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

SageMaker AI

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan untuk Amazon SageMaker AI. Untuk informasi lebih lanjut 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 notebook Amazon SageMaker AI. Selama otomatisasi, instance notebook dihentikan untuk membuat perubahan yang diperlukan. SageMaker Instans notebook AI Studio tidak didukung.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Nama instance notebook SageMaker AI untuk menonaktifkan akses root.

- `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: waitAwsResourceProperty): Memverifikasi instancinya `stopped`
- `UpdateNotebookInstance` (aws:executeAwsApi): Menonaktifkan akses root pada instance notebook.
- `WaitForNotebookUpdate` (aws: waitAwsResourceProperty): 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: assertAwsResource Properti): Memverifikasi setelah akses root instance notebook berhasil dinonaktifkan.

Secrets Manager

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk. AWS Secrets Manager Untuk informasi lebih lanjut 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 defaultnya menjadi 30 hari.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama Sumber Daya Amazon (ARN) dari AWS Lambda function yang dapat memutar rahasia.

- SecretId

Tipe: String

Deskripsi: (Wajib) 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 CSPM

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk AWS Security Hub CSPM. Untuk informasi lebih lanjut 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 CSPM (Security Hub CSPM) untuk Akun AWS dan Wilayah AWS di mana Anda menjalankan otomatisasi. Untuk informasi tentang Security Hub CSPM, lihat [Apa itu? AWS Security Hub CSPM](#) dalam AWS Security Hub User Guide.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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: (Wajib) Jika disetel ke `true`, standar keamanan default yang ditetapkan oleh Security Hub CSPM 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 CSPM di akun saat ini dan Wilayah.
- `aws:executeAwsApi`- Memverifikasi bahwa Security Hub CSPM telah diaktifkan.

AWS Shield

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk AWS Shield. Untuk informasi lebih lanjut 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 AWS Elastic IPs untuk pengaturan konfigurasi mereka 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 Business + Support, Enterprise Support, atau Unified Operations Subscription. Untuk informasi selengkapnya, lihat [Bandingkan AWS Dukungan Paket](#).
- Runbook ini membutuhkan ACTIVE [AWS Shield Advanced langganan](#).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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`

Tipe: 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

Tipe: 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

Tipe: 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

JSON

```
{
  "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::111122223333:role/automation-assume-role-name",
      "Effect": "Allow"
    }
  ]
}

```

Instruksi

1. Arahkan ke [AWSPremiumSupport-DDoSResiliencyAssessment](#) di AWS Systems Manager Konsol.

2. Pilih Jalankan Otomasi

3. Untuk parameter input, masukkan yang berikut ini:

- AutomationAssumeRole(Optional):

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(Optional):

Menentukan jenis sumber daya untuk dievaluasi untuk 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 AWS ID bucket Amazon S3 untuk verifikasi kepemilikan. Akun AWS ID 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	
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 ssm-admin arn:aws:iam::[redacted]:role/ssm-admin	ResourceType (Required) Determines the type of resources to be evaluated for DDoS resiliency assessment. By default, the runbook will evaluate both global and regional resources. Global and Regional Resources
S3BucketName (Required) The name of the Amazon S3 bucket to save the assessment report in HTML format. Select an existing S3 Bucket [redacted]	S3BucketOwner (Required) The Account ID of the Amazon S3 bucket for ownership verification. [redacted]
S3BucketPrefix (Optional) Any prefix for the path inside Amazon S3 for storing the results. Example path with prefix: S3://<BucketName>/<Prefix> String	

4. Pilih Jalankan.

5. Otomatisasi dimulai.

6. Dokumen melakukan langkah-langkah berikut:

- CheckShieldAdvancedState:

Memverifikasi Akun AWS apakah berlangganan AWS Shield Advanced dan apakah runbook memiliki akses ke 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 Berlangganan Status Kepemilikan Bucket and/or Amazon S3.

- **ShieldAdvancedConfigurationReview:**

Ulasan Shield Konfigurasi lanjutan 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 Balancers, Classic Load Balancers, Amazon Elastic Compute Cloud (Amazon EC2) Instances (Elastic). IPs

- **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

SendReportToS3.AssessmentReportS3Uri
S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html

Execution status

Overall status 🟢 Success	All executed steps 9	# Succeeded 9
# Failed 0	# Cancelled 0	# TimedOut 0

Referensi

Otomatisasi Systems Manager

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

AWS dokumentasi layanan

- [AWS Shield Advanced](#)

Amazon SNS

AWS Systems Manager Automation menyediakan runbook standar untuk Amazon Simple Notification Service. Untuk informasi lebih lanjut 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

Tipe: 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

Tipe: String

Nilai valid:

- HTTP
- Firehouse
- Lambda
- Aplikasi
- SQS

Deskripsi: (Wajib) Jenis titik akhir topik Amazon SNS yang ingin Anda log pesan pemberitahuan status pengiriman.

- TopicArn

Tipe: String

Deskripsi: (Wajib) ARN dari topik Amazon SNS yang ingin Anda konfigurasi pencatatan status pengiriman.

- SuccessFeedbackRoleArn

Tipe: String

Deskripsi: (Wajib) ARN dari peran IAM yang digunakan Amazon SNS untuk mengirim log agar pesan notifikasi berhasil. CloudWatch

- SuccessFeedbackSampleRate

Tipe: String

Nilai yang valid: 0-100

Deskripsi: (Wajib) Persentase pesan yang berhasil diambil sampel untuk topik Amazon SNS yang ditentukan.

- FailureFeedbackRoleArn

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama Sumber Daya Amazon (ARN) dari kunci terkelola AWS KMS pelanggan yang ingin Anda gunakan untuk mengenkripsi topik Amazon SNS.

- TopicArn

Tipe: 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`

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Pesan untuk disertakan dalam notifikasi SNS.

- TopicArn

Tipe: String

Deskripsi: (Wajib) ARN dari topik SNS untuk mempublikasikan pemberitahuan ke.

Amazon SQS

AWS Systems Manager Automation menyediakan runbook yang telah ditentukan sebelumnya untuk Amazon Simple Queue Service (Amazon SQS). Untuk informasi lebih lanjut 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

Tipe: 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.

- QueueUrl

Tipe: String

Deskripsi: (Wajib) URL antrian Amazon SQS yang ingin Anda aktifkan enkripsi.

- KmsKeyId

Tipe: 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

Tipe: 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:assertAwsResourceProperty)` - Memverifikasi enkripsi diaktifkan pada antrian Amazon SQS.
- `VerifySqsEncryptionDefault (aws:assertAwsResourceProperty)` - Memverifikasi enkripsi diaktifkan pada antrian Amazon SQS.

Step Functions

AWS Systems Manager Automation menyediakan runbook standar untuk AWS Step Functions (Step Functions). Untuk informasi lebih lanjut 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 keALL,ERROR, atauFATAL.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Nilai yang valid: SEMUA | KESALAHAN | FATAL

Deskripsi: (Wajib) URL antrian Amazon SQS yang ingin Anda aktifkan enkripsi.

- LogGroupArn

Tipe: String

Deskripsi: (Diperlukan) ARN dari grup CloudWatch log Amazon Logs yang ingin Anda kirim log mesin status.

- StateMachineArn

Tipe: 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 yang telah ditentukan untuk Systems Manager. Untuk informasi lebih lanjut 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-BulkDeleteAssociationRunbook 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

Tipe: 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 terpisah koma dari IDs 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`

Tipe: 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`

Tipe: 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 terpisah koma yang ingin OpsItems IDs Anda edit (misalnya, OI-xxxxxxxxxxxxx, OI-xxxxxxxxxxxxx).

- Prioritas

Tipe: 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

Tipe: String

- Tidak ada perubahan
- 1
- 2
- 3
- 4

Default: Tidak ada perubahan

Deskripsi: (Opsional) Tingkat keparahan yang diedit. OpsItems

- WaitTimeBetweenEditsInSecs

Tipe: String

Nilai yang valid: 0.0-2.0

Default: 0.8

Deskripsi: (Opsional) Waktu otomatisasi menunggu antara memanggil UpdateOpsItems operasi.

- Status

Tipe: 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

Tipe: 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.

- `Penyaring`

Tipe: 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`

Tipe: String

Deskripsi: (Opsional) Pengidentifikasi sumber daya terkait yang ingin Anda tambahkan untuk diselesaikan OpsItems.

- `S3 BucketName`

Tipe: String

Deskripsi: (Opsional) Nama bucket Amazon S3 yang ingin Anda kirim ringkasan hasilnya.

- `SnsMessage`

Tipe: String

Deskripsi: (Opsional) Pemberitahuan yang Anda inginkan untuk dikirim oleh Amazon Simple Notification Service (Amazon SNS) saat otomatisasi selesai.

- `SnsTopicArn`

Tipe: 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

Tipe: 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 jendela pemeliharaan yang IDs dipisahkan koma yang ingin Anda aktifkan atau nonaktifkan.

- MaintenanceWindowsStatus

Tipe: String

Nilai yang valid: "Benar" | "Salah"

Default: "Salah"

Deskripsi: (Wajib) Menentukan apakah jendela pemeliharaan diaktifkan atau dinonaktifkan. Tentukan "Benar" 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`

Tipe: String

Deskripsi: (Wajib) AMI ID yang akan digunakan untuk meluncurkan instance.

- `AutomationAssumeRole`

Tipe: 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`

Tipe: String

Default: `SSMSecurity GroupForLinuxInstances`

Deskripsi: (Diperlukan) Nama grup keamanan untuk dibuat.

- `HttpTokens`

Tipe: 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 IMDSv2 apakah opsional atau diperlukan.

- `InstanceType`

Tipe: String

Default: `t2.medium`

Deskripsi: (Wajib) Jenis instance yang akan diluncurkan. Defaultnya adalah `t2.medium`.

- `KeyPairName`

Tipe: String

Deskripsi: (Wajib) Pasangan kunci yang akan digunakan saat membuat instance.

- `RemoteAccessCidr`

Tipe: String

Default `0.0.0.0/0`

Deskripsi: (Diperlukan) Membuat grup Keamanan dengan port untuk SSH (Rentang port 22) terbuka untuk IPs 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`

Tipe: String

Default: `SSMManaged InstanceProfileRole`

Deskripsi: (Wajib) Nama peran untuk membuat.

- StackName

Tipe: String

Default: CreateManagedInstanceStack {{Automation:Execution_ID}}

Deskripsi: (Opsional) Tentukan nama tumpukan yang digunakan oleh runbook ini

- SubnetId

Tipe: String

Default: Default

Deskripsi: (Diperlukan) Instance baru akan digunakan ke subnet ini atau di subnet default jika tidak ditentukan.

- VpcId

Tipe: 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**

Tipe: 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**

Tipe: 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**

Tipe: String

Default: `SSMSecurity GroupForLinuxInstances`

Deskripsi: (Diperlukan) Nama grup keamanan untuk dibuat.

- **HttpTokens**

Tipe: 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 IMDSv2 apakah opsional atau diperlukan.

- InstanceType

Tipe: String

Default: t2.medium

Deskripsi: (Wajib) Jenis instance yang akan diluncurkan. Defaultnya adalah t2.medium.

- KeyPairName

Tipe: String

Deskripsi: (Wajib) Pasangan kunci yang akan digunakan saat membuat instance.

- RemoteAccessCidr

Tipe: String

Default 0.0.0.0/0

Deskripsi: (Wajib) Membuat grup keamanan dengan port untuk RDP (Rentang port 3389) terbuka untuk IPs 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

Tipe: String

Default: SSMMManaged InstanceProfileRole

Deskripsi: (Wajib) Nama peran untuk membuat.

- StackName

Tipe: String

Default: CreateManagedInstanceStack {{Automation:Execution_ID}}

Deskripsi: (Opsional) Tentukan nama tumpukan yang digunakan oleh runbook ini

- SubnetId

Tipe: String

Default: Default

Deskripsi: (Diperlukan) Instance baru akan digunakan ke subnet ini atau di subnet default jika tidak ditentukan.

- VpcId

Tipe: 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

Tipe: 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

Tipe: 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 mengeksportnya 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

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Filter untuk getOpsSummary permintaan.

- resultAttribute

Tipe: String

Deskripsi: (Opsional) Atribut hasil untuk getOpsSummary permintaan.

- s3 BucketName

Tipe: String

Deskripsi: (Wajib) Bucket S3 tempat Anda ingin mengunduh file output.

- snsSuccessMessage

Tipe: String

Deskripsi: (Opsional) Pesan untuk dikirim saat runbook selesai.

- snsTopicArn

Tipe: String

Deskripsi: (Diperlukan) Amazon Simple Notification Service (Amazon SNS) topik ARN untuk memberi tahu saat unduhan selesai.

- syncName

Tipe: 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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Bucket S3 tempat Anda ingin mengunduh file output.

- `snsTopicArn`

Tipe: String

Deskripsi: (Opsional) Tema Amazon Simple Notification Service (Amazon SNS) Nama Sumber Daya Amazon (ARN) untuk memberi tahu kapan unduhan selesai.

- `snsSuccessMessage`

Tipe: String

Deskripsi: (Opsional) Teks pesan yang akan dikirim saat runbook selesai.

- `sasaran`

Tipe: 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 mengekspornya 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

Tipe: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan metadata tentang aplikasi yang diinstal.

- AssociatedDocName

Tipe: String

Default: AWS-GatherSoftwareInventory

Deskripsi: (Opsional) Nama runbook yang digunakan untuk mengumpulkan Inventaris dari instance terkelola.

- AssociationName

Tipe: String

Deskripsi: (Opsional) Nama untuk asosiasi Inventaris yang akan ditetapkan ke instance.

- AssocWaitTime

Tipe: String

Standar: PT5 M

Deskripsi: (Opsional) Jumlah waktu pengumpulan Inventaris harus berhenti sejenak ketika waktu mulai asosiasi Inventaris tercapai. Waktu menggunakan format ISO 8601.

- AutomationAssumeRole

Tipe: 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

Tipe: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan metadata untuk AWS Komponen seperti. amazon-ssm-agent

- CustomInventory

Tipe: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan metadata inventaris khusus.

- Berkas

Tipe: 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

Tipe: String

Default: Diaktifkan

Deskripsi: (Opsional) Kumpulkan informasi tambahan tentang instance, termasuk model CPU, kecepatan, dan jumlah inti, untuk beberapa nama.

- InstanceIds

Tipe: String

Default: *

Deskripsi: (Diperlukan) instans EC2 yang ingin Anda inventarisasi.

- LambdaAssumeRole

Tipe: 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

Tipe: String

Default: Diaktifkan

~~Deskripsi: (Opsional) Kumpulkan metadata tentang konfigurasi jaringan.~~

- Keluaran3 BucketName

Tipe: String

Deskripsi: (Opsional) Nama bucket Amazon S3 tempat Anda ingin menulis data log Inventaris.

- Keluaran3 KeyPrefix

Tipe: String

Deskripsi: (Opsional) Sebuah key prefix Amazon S3 (subfolder) tempat Anda ingin menulis data log Inventaris.

- Keluaran3wilayah

Tipe: String

Deskripsi: (Opsional) Nama Wilayah AWS tempat Amazon S3 ada.

- Jadwal

Tipe: String

Default: cron (0 */30 * * * ? *)

Deskripsi: (Opsional) Ekspresi cron untuk jadwal asosiasi Inventaris. Defaultnya adalah setiap 30 menit.

- Layanan

Tipe: String

Default: Diaktifkan

Deskripsi: (Opsional, hanya OS Windows, memerlukan SSMAgent versi 2.2.64.0 ke atas) Kumpulkan data untuk konfigurasi layanan.

- WindowsRegistry

Tipe: 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\ "," " : [ " " ]} MachinelImage ValueNames AMIName`

- WindowsRoles

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instans EC2 untuk dikonfigurasi

- LambdaAssumeRole

Tipe: 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

Tipe: String

Default: SSMRole ForManagedInstance

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 SSMManged InstanceCore Terkelola Amazon.

AWS-SetupManagedRoleOnEC2Instance

Deskripsi

Konfigurasi instance dengan peran IAM SSMRole ForManagedInstance terkelola untuk akses Systems Manager.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instans EC2 untuk dikonfigurasi

- LambdaAssumeRole

Tipe: 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

Tipe: String

Default: SSMMRole ForManagedInstance

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 SSMMManaged InstanceCore Terkelola Amazon.

AWSSupport-TroubleshootManagedInstance

Deskripsi

AWSSupport-TroubleshootManagedInstanceRunbook membantu Anda menentukan mengapa instans Amazon Elastic Compute Cloud EC2 (Amazon) 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 IPv6 aturan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) ID EC2 instans Amazon 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 Patch Manager, alat di dalamnya. 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/Command ID instance pasangan yang Anda berikan 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 AL2023
- 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]

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.
Choose an option ▼

RunCommandId
(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.
42[REDACTED]e

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

GenerateReportOutput
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/awss-sm-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/awss-sm-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 alat di AWS Systems Manager. Runbook ini memeriksa hal-hal berikut:

- Memeriksa apakah instance 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-AnalyzeAWSEndpointReachabilityFromEC2` Runbook 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`

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instans Amazon EC2 yang tidak dapat Anda sambungkan menggunakan Pengelola Sesi.

- SessionPreferenceDocument

Tipe: 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 lebih lanjut 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

Tipe: String

Deskripsi: (Opsional) Nama pengguna orang yang menjadi masalah harus ditetapkan.

- DueDate

Tipe: String

Deskripsi: (Opsional) Tanggal jatuh tempo untuk masalah dalam yyyy-mm-dd format.

- IssueDescription

Tipe: String

Deskripsi: (Wajib) Penjelasan rinci tentang masalah ini.

- IssueSummary

Tipe: String

Deskripsi: (Wajib) Ringkasan singkat tentang masalah ini.

- IssueTypeName

Tipe: String

Deskripsi: (Wajib) Nama jenis masalah yang ingin Anda buat (misalnya, Tugas, Sub-tugas, Bug, dll.).

- JiraURL

Tipe: String

Deskripsi: (Wajib) Url contoh Jira.

- JiraUsername

Tipe: String

Deskripsi: (Wajib) Nama pengguna yang akan dibuat dengan masalah tersebut.

- PriorityName

Tipe: String

Deskripsi: (Opsional) Nama prioritas masalah.

- ProjectKey

Tipe: String

Deskripsi: (Wajib) Kunci proyek yang harus dibuat masalah.

- **SSMParameterName**

Tipe: 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

Issued: 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**

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Kategori insiden.

Nilai yang valid: Tidak Ada | Inquiry/Help | Perangkat Lunak | Perangkat Keras | Jaringan | Database

Nilai Default: Tidak ada

- Deskripsi

Tipe: String

Deskripsi: (Wajib) Penjelasan rinci tentang insiden tersebut.

- Dampak

Tipe: String

Deskripsi: (Opsional) Efek suatu insiden terhadap bisnis.

Nilai yang valid: Tinggi | Sedang | Rendah

Nilai Default: Rendah

- ServiceNowInstanceUsername

Tipe: String

Deskripsi: (Wajib) Nama pengguna yang akan dibuat dengan insiden tersebut.

- ServiceNowInstancePassword

Tipe: String

Deskripsi: (Wajib) Nama Parameter SSM terenkripsi yang berisi kata sandi untuk pengguna. ServiceNow

- ServiceNowInstanceURL

Tipe: String

Deskripsi: (Wajib) URL ServiceNow contoh

- ShortDescription

Tipe: String

Deskripsi: (Wajib) Deskripsi singkat tentang insiden tersebut.

- Subkategori

Tipe: String

Deskripsi: (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 | MS SQL Server DB2 | 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 IPv4 publik subnet Anda, Anda juga harus menyetel `associate_public_ip_address` ke `true`.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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.

- Modus

Tipe: String

Deskripsi: Mode, atau perintah, di mana untuk menggunakan Packer saat memvalidasi terhadap template. Pilihan termasuk `Build`, `Validate`, dan `Fix`.

- `TemplateFileName`

Tipe: String

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

- `Template3 BucketName`

Tipe: 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 lebih lanjut 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`

Tipe: 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`

Tipe: 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 penyelesai, lihat Pencatatan kueri [DNS Publik dan pencatatan kueri Resolver](#).

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Opsional) Jenis kueri yang ingin Anda log.

Nilai yang valid: Publik | Resolver/Pribadi

Default: Publik

- ResourceId

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Diperlukan) Elastic network interface yang ingin Anda konfigurasi untuk mirroring lalu lintas.

- Target

Tipe: 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

Tipe: 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.Target IDOutput`

AWSsupport-ConnectivityTroubleshooter

Deskripsi

`AWSsupport-ConnectivityTroubleshooterRunbook` mendiagnosis masalah konektivitas antara yang berikut ini:

- AWS sumber daya dalam Amazon Virtual Private Cloud (Amazon VPC)
- AWS sumber daya di Amazon yang berbeda VPCs 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

Tipe: 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.

- DestinasIP

Tipe: String

Deskripsi: (Wajib) IPv4 Alamat sumber daya yang ingin Anda sambungkan.

- DestinationPort

Tipe: String

Default: betul

Deskripsi: (Wajib) Nomor port yang ingin Anda sambungkan pada sumber daya tujuan.

- DestinationVpc

Tipe: String

Default: Semua

Deskripsi: (Opsional) ID VPC Amazon yang ingin Anda uji konektivitas.

- SourceIP

Tipe: String

Deskripsi: (Wajib) IPv4 Alamat pribadi AWS sumber daya di VPC Amazon yang ingin Anda uji konektivitas.

- SourcePortRange

Tipe: String

Deskripsi: (Opsional) Rentang port yang digunakan oleh AWS sumber daya di VPC Amazon yang ingin Anda uji konektivitas.

- SourceVpc

Tipe: 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 (NACLs) yang terkait dengan subnet untuk sumber daya sumber dan tujuan.
- `aws:executeScript`- Mengonfirmasi apakah NACLs 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 yang NACLs terkait dengan subnet untuk sumber daya sumber.
- `aws:executeScript`- Mengonfirmasi apakah NACLs memungkinkan lalu lintas yang dibutuhkan dari sumber daya sumber.
- `aws:executeAwsApi`- Mengumpulkan rincian tentang gateway NAT.
- `aws:executeAwsApi`- Mengumpulkan yang NACLs terkait dengan subnet untuk gateway NAT.
- `aws:executeScript`- Mengonfirmasi apakah NACLs memungkinkan 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 keduanya VPCs berada di Wilayah yang sama dan bahwa ID yang dikembalikan untuk VPC tujuan cocok dengan nilai yang ditentukan, jika ada, dalam parameter. `DestinationVpc`
- `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 pencatatan VPN.

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Id AWS Site-to-Site VPN koneksi yang akan dipecahkan masalah.

Pola yang Diizinkan: `^vpn-[0-9a-f]{8,17}$`

- Terowongan AIPAddress

Tipe: String

Deskripsi: (Wajib) Alamat terowongan nomor 1 yang terkait dengan IPv4 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}$`

- Terowongan BIPAddress

Tipe: String

Deskripsi: (Opsional) Alamat terowongan nomor 2 yang terkait dengan IPv4 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

Tipe: 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

Tipe: 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

Tipe: 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: `^(\\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 pencatatan terowongan VPN Anda, ketika format Output logging adalah JSON.

Ikuti langkah-langkah ini untuk mengonfigurasi otomatisasi:

1. Arahkan ke [AWSSupport-TroubleshootVPN](#) dalam AWS Systems Manager konsol.
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.

- 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.

- Terowongan AIPAddress (Diperlukan):

Terowongan Alamat IP yang terkait dengan AWS Site-to-Site VPN koneksi Anda.

- Terowongan BIPAddress (Opsional):

Alamat IP terowongan B yang terkait dengan AWS Site-to-Site VPN koneksi Anda.

- IKEVersion (Diperlukan):

Pilih apa yang IKEVersion Anda gunakan. Nilai yang diizinkan: IKEv1, IKEv2.

- StartTimeEpoch (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.

- EndTimeEpoch (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 StartTimeEpoch EndTimeEpoch,, atau LookBackPeriod untuk memperbaiki rentang waktu untuk analisis log. Berikan angka dua digit dalam beberapa jam untuk memeriksa kesalahan di masa lalu dari waktu mulai otomatisasi. Atau, jika kesalahan di masa lalu dalam rentang waktu tertentu, sertakan StartTimeEpoch dan EndTimeEpoch, alih-alih LookBackPeriod.

Input parameters	
AutomationAssumeRole (Optional) The ARN of the role that allows Automation to perform the actions on your behalf. Choose an option	LogGroupName (Required) The Amazon CloudWatch log group name to be validated. This must be the CloudWatch log group which is destined for VPN logs vpnlog
VpnConnectionId (Required) The AWS Site-to-Site VPN connection id to be validated. vpn-123abc456xyz	TunnelAPIAddress (Required) The tunnel number 1 IP address associated with your AWS Site-to-Site VPN to be validated. 1.1.1.1
TunnelBIPAddress (Optional) The tunnel number 2 IP address associated with your AWS Site-to-Site VPN to be validated. String	IKEVersion (Required) Select what IKE Version you are using. Allowed values : IKEv1, IKEv2 or both IKEv1
StartTimeEpoch (Optional) Start time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis String	EndTimeEpoch (Optional) End time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis String
LookBackPeriod (Required) Time in hours to look back for log analysis 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

traceError.Tunnel1IKEv2
(1IKEv2ErrorCount=0)

traceError.Tunnel2IKEv2
(1IKEv2ErrorCount=0)

traceError.Tunnel1IKEv1
{"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](#)

AWS dokumentasi layanan

- [Isi log Site-to-Site VPN](#)

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Deskripsi

AWSConfigRemediation-DeleteEgressOnlyInternetGatewayRunbook menghapus gateway internet khusus egres yang Anda tentukan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID ENI yang ingin Anda hapus.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter 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`

Tipe: 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

Tipe: 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`

Tipe: 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`

Tipe: 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`

Tipe: 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`

Tipe: 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 virtual private cloud (VPC) Anda memiliki alamat IP elastis atau IPv4 alamat publik yang terkait dengannya, runbook gagal.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- `AutomationAssumeRole`

Tipe: 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

Tipe: 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 tertentu.
- 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

Tipe: 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

Tipe: 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 tertentu.
- 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`

Tipe: 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`

Tipe: String

Deskripsi: (Wajib) Daftar terpisah koma dari grup keamanan yang ingin Anda batasi lalu lintas SSH. IDs

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 kelompok keamanan IDs yang memiliki aturan SSH inbound 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 Tiongkok.

Jalankan Otomasi ini (konsol)

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID grup keamanan tempat port harus dinonaktifkan.

- IpAddressToBlock

Tipe: String

Deskripsi: (Opsional) IPv4 Alamat tambahan dari mana akses harus diblokir, dalam format 1.2.3.4/32.

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Deskripsi

AWSConfigRemediation-DisableSubnetAutoAssignPublicIPRunbook menonaktifkan atribut pengalamatan IPv4 publik untuk subnet yang Anda tentukan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID subnet tempat Anda ingin menonaktifkan atribut IPv4 alamat publik penetapan 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 IPv4 alamat publik penetapan 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 di file Anda. VPCs 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 \(konsol\)](#)

 Note

Saat memilih s3 sebagai tujuan log, pastikan kebijakan bucket memungkinkan akses layanan pengiriman log ke bucket. Untuk informasi selengkapnya, lihat [izin bucket Amazon S3](#) untuk log aliran

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: 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

Tipe: 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.

 Important

Saat memilih `s3` sebagai `LogDestinationType` Anda harus memastikan bahwa bucket yang dipilih mengikuti [praktik terbaik keamanan Amazon S3 Bucket](#), dan Anda mengikuti undang-undang privasi data untuk organisasi dan wilayah geografis Anda.

- `LogDestinationType`

Tipe: 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`

Tipe: 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`

Tipe: String

Deskripsi: (Opsional) Nama grup CloudWatch log log tempat data log aliran diterbitkan. Jika Anda menentukan `s3` `LogDestinationType` parameter, jangan berikan nilai untuk parameter ini.

- `ResourceIds`

Jenis: StringList

Deskripsi: (Wajib) Daftar subnet yang dipisahkan koma, antarmuka jaringan elastis, atau VPC yang ingin Anda buat log alirannya. IDs

- TrafficType

Tipe: 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:GetBucketLocation
- s3:GetBucketAcl
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:ListBucket
- s3:PutObject

Kebijakan Sampel

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSMExecutionPermissions",
      "Effect": "Allow",
      "Action": [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EC2FlowLogsPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateFlowLogs",
```

```

        "ec2:DeleteFlowLogs",
        "ec2:DescribeFlowLogs"
    ],
    "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:subnet/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:vpc/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:transit-gateway/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:transit-gateway-
attachment/resource-id"
    ]
},
{
    "Sid": "IAMCreateRolePermissions",
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:GetPolicy",
        "iam:GetRole",
        "iam:TagRole",
        "iam:PassRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole"
    ],
    "Resource": [
        "arn:aws:iam:111122223333:role/role-name",
        "arn:aws:iam:111122223333:role/AWSSupportCreateFlowLogsRole"
    ]
},
{
    "Sid": "CloudWatchLogsPermissions",
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:DeleteLogDelivery",
        "logs:DeleteLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
    ]
}

```

```

    ],
    "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:log-group-name",
        "arn:aws:logs:us-east-1:111122223333:log-group:log-group-name:*"
    ]
},
{
    "Sid": "S3Permissions",
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:ListBucket",
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3::amzn-s3-demo-bucket",
        "arn:aws:s3::amzn-s3-demo-bucket/*"
    ]
}
]
}

```

Langkah Dokumen

- `aws:branch`- Cabang berdasarkan nilai yang ditentukan untuk `LogDestinationType` parameter.
- `aws:executeScript`- Memeriksa apakah target Amazon Simple Storage Service (Amazon S3) berpotensi memberikan akses baca atau public tulis ke objeknya.
- `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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama grup CloudWatch log Log yang ingin Anda publikasikan data log aliran.

- DeliverLogsPermissionArn

Tipe: 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

Tipe: 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

Tipe: 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`

Tipe: 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.

- **Destinasi3 BucketArn**

Tipe: String

Deskripsi: (Wajib) ARN bucket Amazon S3 yang ingin Anda publikasikan data log alur.

- **FlowLogId**

Tipe: 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**

Tipe: 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 diterbitkan 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`

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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`

Tipe: 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`

Tipe: 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 IPs target IPv4 (IPv6 atau) yang dipilih dengan terus menjalankan pengujian ping, MTR, traceroute, dan tracertcp. 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 pattern/trends. Additionally, you can configure CloudWatch alarms with Amazon SNS notifications when packet loss and/or latensi mencapai ambang batas. Data juga dapat digunakan saat membuka kasus dengan AWS Dukungan, untuk membantu mengisolasi masalah dengan cepat dan mengurangi waktu penyelesaian saat menyelidiki masalah jaringan.

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

Jenis dokumen

Otomatisasi

Pemilik

Amazon

Platform

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Tipe: 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

Tipe: String

Default: /AWSSupport-SetupIPMonitoringFromVPC

Deskripsi: (Opsional) Awalan yang digunakan untuk setiap grup CloudWatch log yang dibuat untuk hasil pengujian.

- CloudWatchLogGroupRetentionInDays

Tipe: 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

Tipe: 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: t3.micro

Deskripsi: (Opsional) Jenis instans EC2 untuk instance EC2 Rescue. Ukuran yang disarankan: t3.micro.

- SubnetId

Tipe: 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).

- Target IPs

Tipe: String

Deskripsi: (Wajib) Daftar terpisah koma IPv4s dan/atau IPv6s 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.

- TestInstanceSecurityGroupId

Tipe: String

Deskripsi: (Opsional) ID grup keamanan untuk contoh pengujian. Jika tidak ditentukan, otomatisasi membuatnya selama pembuatan instance. Pastikan grup keamanan mengizinkan akses keluar ke pemantauan IPs.

- TestInstanceProfileName

Tipe: String

Deskripsi: (Opsional) Nama profil instans IAM yang ada untuk instance pengujian. Jika tidak ditentukan, otomatisasi membuatnya selama pembuatan instance. Peran harus memiliki izin berikut: `logs:CreateLogStream`, `logs:DescribeLogGroups`, `logs:DescribeLogStreams`, `logs:PutLogEvents` dan Kebijakan AWS AmazonSSMManagedInstanceCore Terkelola.

- TestInterval

Tipe: String

Deskripsi: (Opsional) Jumlah menit antara interval tes. Nilai default adalah 1 menit dan maksimum adalah 10 menit.

- RetainDashboardAndLogsOnDeletion

Tipe: String

Deskripsi: (Opsional) Tentukan `False` untuk menghapus CloudWatch dasbor Amazon dan Log saat menghapus AWS CloudFormation tumpukan. Nilai default-nya adalah `True`. Secara default, dasbor dan log dipertahankan dan perlu dihapus secara manual ketika tidak lagi diperlukan.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Warning

Disarankan untuk melewati `TestInstanceProfileName` parameter atau memastikan pagar pembatas keamanan di tempat untuk mencegah penyalahgunaan izin IAM yang dapat diubah.

Disarankan agar pengguna yang menjalankan otomatisasi memiliki kebijakan terkelola IAM `SSMAutomationPeran` Amazon yang dilampirkan. Selain itu, pengguna harus memiliki kebijakan berikut yang dilampirkan ke akun pengguna, grup, atau peran mereka:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
```

```

        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "iam:AddRoleToInstanceProfile",
        "iam:GetRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteInstanceProfile",
        "iam:PutRolePolicy",
        "iam:TagRole"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/SetupIPMonitoringFromVPC*",
        "arn:aws:iam::111122223333:instance-profile/
SetupIPMonitoringFromVPC*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudwatch:PutDashboard",
        "cloudwatch>DeleteDashboards",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateLaunchTemplate",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcs",
        "ec2>DeleteLaunchTemplate",
        "ec2>DeleteSecurityGroup",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",

```

```

        "ec2:AssignIpv6Addresses",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeLaunchTemplates",
        "ec2:RevokeSecurityGroupEgress",
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:SendCommand",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations"
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow"
}
]
}
```

Jika `TestInstanceProfileName` parameter disediakan, izin IAM berikut tidak diperlukan untuk menjalankan runbook:

- saya: `CreateRole`
- saya: `CreateInstanceProfile`
- saya: `DetachRolePolicy`
- saya: `AttachRolePolicy`
- saya: `AddRoleToInstanceProfile`
- saya: `RemoveRoleFromInstanceProfile`
- saya: `DeleteRole`
- saya: `DeleteRolePolicy`
- saya: `DeleteInstanceProfile`

Langkah Dokumen

1. **aws:executeAwsApi**- jelaskan subnet yang disediakan untuk mendapatkan ID VPC IPv6 dan status asosiasi blok CIDR.
2. **aws:executeScript**- memvalidasi target IPs yang disediakan secara sintaksis benar IPv4 dan/ atau IPv6 alamat, dapatkan arsitektur jenis instance yang dipilih, dan verifikasi subnet memiliki asosiasi IPv6 kumpulan jika ada IP target. IPv6
3. **aws:createStack**- buat AWS CloudFormation tumpukan yang menyediakan instance Amazon EC2 pengujian, profil instans IAM (jika tidak disediakan), grup keamanan (jika tidak disediakan), grup CloudWatch log, dan dasbor. CloudWatch

(Pembersihan) Jika langkah gagal:

aws:executeScript- jelaskan peristiwa CloudFormation tumpukan untuk mengidentifikasi alasan kegagalan.

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

4. **aws:waitForAwsResourceProperty**- tunggu CloudFormation tumpukan untuk menyelesaikan pembuatan.

(Pembersihan) Jika langkah gagal:

aws:executeScript- jelaskan peristiwa CloudFormation tumpukan untuk mengidentifikasi alasan kegagalan.

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

5. **aws:executeScript**- jelaskan sumber daya CloudFormation tumpukan untuk mendapatkan ID instance pengujian, ID grup keamanan, peran IAM, profil instance, dan nama dasbor.

(Pembersihan) Jika langkah gagal:

aws:executeScript- jelaskan peristiwa CloudFormation tumpukan untuk mengidentifikasi alasan kegagalan.

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

6. **aws:waitForAwsResourceProperty**- tunggu instance pengujian menjadi instance terkelola.

(Pembersihan) Jika langkah gagal:

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

7. **aws:runCommand**- instal CloudWatch agen pada contoh pengujian.

(Pembersihan) Jika langkah gagal:

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

8. **aws:runCommand**- tentukan skrip pengujian jaringan (MTR, ping, tracepath, dan traceroute) untuk masing-masing yang disediakan. IPs

(Pembersihan) Jika langkah gagal:

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

9. **aws:runCommand**- memulai tes jaringan dan menjadwalkan eksekusi berikutnya menggunakan cronjobs yang berjalan setiap menit. TestInterval

(Pembersihan) Jika langkah gagal:

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

- 10 **aws:runCommand**- konfigurasi CloudWatch agen untuk mendorong hasil tes dari /home/ec2-user/logs/ ke CloudWatch Log.

(Pembersihan) Jika langkah gagal:

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

- 11 **aws:runCommand**- konfigurasi rotasi log untuk hasil tes di /home/ec2-user/logs/.

- 12 **aws:executeScript**- atur kebijakan retensi untuk semua grup CloudWatch log yang dibuat oleh CloudFormation tumpukan.

- 13 **aws:executeScript**- buat filter metrik grup CloudWatch log untuk latensi ping dan kehilangan paket ping.

(Pembersihan) Jika langkah gagal:

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

- 14 **aws:executeScript**- Perbarui CloudWatch dasbor untuk menyertakan widget untuk latensi ping dan statistik kehilangan paket ping.

(Pembersihan) Jika langkah gagal:

aws:executeAwsApi- hapus CloudWatch dasbor, jika ada.

aws:deleteStack- hapus CloudFormation tumpukan dan semua sumber daya terkait.

15**aws:branch**- mengevaluasi SleepTime parameter. Jika disetel ke0, otomatisasi berakhir tanpa menghapus tumpukan.

16**aws:sleep**- tunggu SleepTime durasi yang ditentukan sebelum menghapus CloudFormation tumpukan.

17**aws:deleteStack**- Hapus CloudFormation tumpukan. Berdasarkan RetainDashboardAndLogsOnDeletion parameter, CloudWatch dasbor dan grup log dipertahankan atau dihapus.

(Pembersihan) Jika penghapusan tumpukan gagal:

aws:executeScript- jelaskan peristiwa CloudFormation tumpukan untuk mengidentifikasi alasan kegagalan penghapusan.

Keluaran

updateCloudWatchDasbor. StackUrl - URL CloudFormation tumpukan.

updateCloudWatchDasbor. DashboardUrl - URL CloudWatch dasbor.

updateCloudWatchDasbor. DashboardName - nama CloudWatch dasbor.

updateCloudWatchDasbor. LogGroups - daftar grup CloudWatch log yang dibuat.

describeStackResources. HelperInstanceid - ID contoh uji.

describeStackResources. StackName - nama CloudFormation tumpukan.

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

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID instans untuk instance monitor.

- SubnetId

Tipe: String

Deskripsi: (Wajib) ID subnet untuk contoh monitor.

Izin IAM yang diperlukan

AutomationAssumeRoleParameter memerlukan tindakan berikut untuk menggunakan runbook dengan sukses.

Disarankan agar pengguna yang menjalankan otomatisasi memiliki kebijakan terkelola IAM SSMAutomationPeran Amazon yang dilampirkan. Selain itu, pengguna harus memiliki kebijakan berikut yang melekat pada pengguna, grup, atau peran mereka:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:DetachRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteRole",
        "iam:DeleteInstanceProfile",
        "iam:DeleteRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::111122223333:role/AWSSupport/SetupIPMonitoringFromVPC_*",
        "arn:aws:iam::111122223333: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 SSMManged InstanceCore terkelola Amazon 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 untuk AWS WAF. Untuk informasi lebih lanjut 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

Tipe: 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID untuk aturan yang ingin Anda tambahkan ke grup aturan regional Anda.

- RuleAction

Tipe: 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

- Get WAFChange Token (`aws:executeAwsApi`) - Mengambil token AWS WAF perubahan untuk memastikan runbook tidak mengirimkan permintaan yang bertentangan ke layanan.
- Add WAFRule To WAFRegional RuleGroup (`AWS:ExecuteScript`) - Menambahkan aturan yang ditentukan ke grup aturan regional. AWS WAF
- VerifyChangeTokenPropagating (`aws:waitForAwsResourceProperty`) - Memverifikasi token perubahan memiliki status PENDING atau INSYNC.
- 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

Tipe: 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.

- Web ACLId

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID untuk aturan reguler, aturan berbasis tarif, atau grup yang ingin Anda tambahkan ke ACL web.

- `ActivatedRuleAction`

Tipe: String

Nilai yang valid: IZINKAN | BLOK | HITUNG

Deskripsi: (Opsional) Menentukan tindakan yang AWS WAF diambil ketika permintaan web cocok dengan kondisi aturan.

- `ActivatedRuleType`

Tipe: 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

- `DetermineWebACLNotDalam FMSAnd RulePriority` (AWS:ExecuteScript) - Memverifikasi apakah ACL AWS WAF web 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

- `DetermineWebACLNotDalam FMSAndRulePriority`. `PrereqResponse`: Keluaran dari `DetermineWebACLNotInFMSAndRulePriority` langkah.
- `VerifyRuleOrRuleGroupAddedToWebAcl`. `VerifyRuleOrRuleGroupAddedToWebACLResponse`: Keluaran dari `AddRuleOrRuleGroupToWebACL` langkah.
- `VerifyRuleOrRuleGroupAddedToWebAcl`. `ListActivatedRulesOrRuleGroupsInWebACLResponse`: Output dari `VerifyRuleOrRuleGroupAddedToWebAcl` langkah.

AWSConfigRemediation-EnableWAFCClassicLogging

Deskripsi

AWSConfigRemediation-EnableWAFCClassicLoggingRunbook 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) Nama aliran pengiriman Firehose yang ingin Anda kirim log.

- Web ACLId

Tipe: 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-EnableWAFCClassicRegionalLogging

Deskripsi

AWSConfigRemediation-EnableWAFCClassicRegionalLoggingRunbook 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`

Tipe: 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`

Tipe: String

Deskripsi: (Diperlukan) Nama Sumber Daya Amazon (ARN) dari aliran pengiriman Firehose yang ingin Anda kirim log.

- `Web ACLId`

Tipe: 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

Tipe: 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

Tipe: 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

Tipe: 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 lebih lanjut 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

Tipe: 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

Tipe: String

Deskripsi: (Wajib) ID bundel yang akan digunakan untuk file WorkSpace.

- ComputeTypeName

Tipe: String

Nilai yang valid: NILAI | STANDAR | KINERJA | DAYA | GRAFIK | POWERPRO | GRAPHICSPRO

Deskripsi: (Opsional) Jenis komputasi untuk Anda WorkSpace.

- DirectoryId

Tipe: 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

Tipe: String

Nilai yang valid: ALWAYS_ON | AUTO_STOP

Deskripsi: (Wajib) Mode berjalan dari WorkSpace.

- RunningModeAutoStopTimeoutInMinutes

Jenis: Integer

Deskripsi: (Opsional) Waktu setelah pengguna log off ketika WorkSpaces berhenti. Tentukan nilai dalam interval 60 menit.

- Tanda

Tipe: String

Deskripsi: (Opsional) Tag yang ingin Anda terapkan pada WorkSpace.

- UserName

Tipe: 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

Tipe: 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 adalahAVAILABLE.

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 `diamUNHEALTHY`, 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

Tipe: 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

Tipe: 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.

- Boot ulang

Tipe: String

Nilai yang valid: Ya | Tidak

Default: Ya

Deskripsi: (Wajib) Menentukan WorkSpace apakah reboot.

- Membangun kembali

Tipe: String

Nilai yang valid: Ya | Tidak

Default: tidak

Deskripsi: (Wajib) Menentukan WorkSpace apakah dibangun kembali.

- Memulihkan

Tipe: String

Nilai yang valid: Ya | Tidak

Default: tidak

Deskripsi: (Wajib) Menentukan WorkSpace apakah dipulihkan.

- WorkspaceId

Tipe: 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`- Memulai 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 menjadiREBOOTING.
- `aws:waitForAwsResourceProperty`- Menunggu Workspace status berubah menjadiAVAILABLE,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 menjadiRESTORING.
- `aws:waitForAwsResourceProperty`- Menunggu Workspace negara berubah menjadiAVAILABLE,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 menjadiREBUILDING.
- `aws:waitForAwsResourceProperty`- Menunggu Workspace negara berubah menjadiAVAILABLE,ERROR, atau UNHEALTHY setelah dibangun kembali.
- `aws:executeAwsApi`- Mengumpulkan keadaan Workspace setelah dibangun kembali.
- `aws:assertAwsResourceProperty`- Mengonfirmasi keadaan Workspace adalahAVAILABLE.

X-Ray

AWS Systems Manager Otomasi menyediakan runbook yang telah ditentukan untuk. AWS X-Ray Untuk informasi lebih lanjut 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 dienkripsi 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

Tipe: 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

Tipe: 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.