aws

Benutzer-Leitfaden

AWS Systems Manager Referenz zum Automatisierungs-Runbook

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Systems Manager Referenz zum Automatisierungs-Runbook: Benutzer-Leitfaden

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Runbook-Referenz für Automation 1
Runbook-Inhalte anzeigen 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 35
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS 36
CloudTrail 38
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail 38
AWS-EnableCloudTrail 40
AWS-EnableCloudTrailCloudWatchLogs 41
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS 43
AWS-EnableCloudTrailKmsEncryption 45
AWSConfigRemediation-EnableCloudTrailLogFileValidation 46
AWS-EnableCloudTrailLogFileValidation 48
AWS-QueryCloudTrailLogs 49
CloudWatch 51
AWS-ConfigureCloudWatchOnEC2Instance 51
AWS-EnableCWAlarm 53
AWSSupport-TroubleshootCloudWatchAgent 55

AWSSupport-TroubleshootCloudWatchAlarm ... 62
Amazon DocumentDB ... 70
AWS-EnableDocDbClusterBackupRetentionPeriod ... 70
CodeBuild ... 72
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK ... 73
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject ... 75
AWS CodeDeploy ... 76
AWSSupport-TroubleshootCodeDeploy ... 76
AWS Config ... 78
AWSSupport-SetupConfig ... 79
Amazon Connect ... 82
AWSSupport-AssociatePhoneNumbersToConnectContactFlows ... 82
AWSSupport-CollectAmazonConnectContactFlowLog ... 91
AWS Directory Service ... 97
AWS-CreateDSManagementInstance ... 97
AWSSupport-TroubleshootADConnectorConnectivity ... 102
AWSSupport-TroubleshootDirectoryTrust ... 106
AWS AppSync ... 110
AWS-EnableAppSyncGraphQLApiLogging ... 110
Amazon Athena ... 112
AWS-EnableAthenaWorkGroupEncryptionAtRest ... 113
DynamoDB ... 115
AWS-ChangeDDBRWCapacityMode ... 116
AWS-CreateDynamoDBBackup ... 118
AWS-DeleteDynamoDbBackup ... 119
AWSConfigRemediation-DeleteDynamoDbTable ... 120
AWS-DeleteDynamoDbTableBackups ... 121
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable ... 123
AWSConfigRemediation-EnablePITRForDynamoDbTable ... 124
AWS-EnableDynamoDbAutoscaling ... 126
AWS-RestoreDynamoDBTable ... 129
AWS Database Migration Service ... 132
AWSSupport-TroubleshootDMSTableErrors ... 132
AWSSupport-TroubleshootDMSEndpointConnection ... 138
Amazon EBS ... 149
AWSSupport-AnalyzeEBSResourceUsage ... 149

AWS-ArchiveEBSSnapshots ... 156
AWS-AttachEBSVolume ... 159
AWSSupport-CalculateEBSPerformanceMetrics ... 160
AWS-CopySnapshot ... 167
AWS-CreateSnapshot ... 168
AWS-DeleteSnapshot ... 169
AWSConfigRemediation-DeleteUnusedEBSVolume ... 170
AWS-DeregisterAMIs ... 172
AWS-DetachEBSVolume ... 174
AWSConfigRemediation-EnableEbsEncryptionByDefault ... 175
AWS-ExtendEbsVolume ... 176
AWSSupport-ModifyEBSSnapshotPermission ... 178
AWSConfigRemediation-ModifyEBSVolumeType ... 181
Amazon EC2 ... 182
AWS-ASGEnterStandby ... 185
AWS-ASGExitStandby ... 186
AWS-CreateImage ... 187
AWS-DeleteImage ... 188
AWS-PatchAsgInstance ... 190
AWS-PatchInstanceWithRollback ... 192
AWS-QuarantineEC2Instance ... 195
AWS-ResizeInstance ... 197
AWS-RestartEC2Instance ... 198
AWS-SetupJupyter ... 199
AWS-StartEC2Instance ... 202
AWS-StopEC2Instance ... 203
AWS-TerminateEC2Instance ... 204
AWS-UpdateLinuxAmi ... 205
AWS-UpdateWindowsAmi ... 209
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck ... 213
AWSConfigRemediation-EnforceEC2InstanceIMDSv2 ... 215
AWSEC2-CloneInstanceAndUpgradeSQLServer ... 216
AWSEC2-CloneInstanceAndUpgradeWindows ... 220
AWSEC2-PatchLoadBalancerInstance ... 224
AWSEC2-SQLServerDBRestore ... 226
AWSSupport-ActivateWindowsWithAmazonLicense ... 232

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 235
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD 240
AWSSupport-CheckXenToNitroMigrationRequirements 246
AWSSupport-CloneXenEC2InstanceAndMigrateToNitro 249
AWSSupport-ConfigureEC2Metadata 256
AWSSupport-ContainEC2Instance 260
AWSSupport-CopyEC2Instance 271
AWSPremiumSupport-DiagnoseDiskUsageOnLinux 277
AWSSupport-EnableWindowsEC2SerialConsole 281
AWSPremiumSupport-ExtendVolumesOnWindows 289
AWSSupport-ExecuteEC2Rescue 294
AWSSupport-ListEC2Resources 297
AWSSupport-ManageRDPSettings 300
AWSSupport-ManageWindowsService 302
AWSSupport-MigrateEC2ClassicToVPC 304
AWSSupport-MigrateXenToNitroLinux 311
AWSSupport-ResetAccess 324
AWSSupport-ResetLinuxUserPassword 327
AWSSupport-RunEC2RescueForWindowsTool 334
AWSPremiumSupport-ResizeNitroInstance 338
AWSSupport-ShareEncryptedAMIOrEBSSnapshot 346
AWSSupport-RestoreEC2InstanceFromSnapshot 351
AWSSupport-SendLogBundleToS3Bucket 355
AWSSupport-StartEC2RescueWorkflow 357
AWSSupport-TroubleshootActiveDirectoryReplication 368
AWSPremiumSupport-TroubleshootEC2DiskUsage 374
AWSSupport-TroubleshootEC2InstanceConnect 379
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs 385
AWSSupport-TroubleshootRDP 388
AWSSupport-TroubleshootSSH 394
AWSSupport-TroubleshootSUSERegistration 398
AWSSupport-TroubleshootWindowsPerformance 400
AWSSupport-TroubleshootWindowsUpdate 408
AWSSupport-UpgradeWindowsAWSDrivers 415
Amazon ECS 419
AWSSupport-CollectECSInstanceLogs 420

AWS-InstallAmazonECSAgent ... 423
AWS-ECSRunTask ... 424
AWSSupport-TroubleshootECSContainerInstance ... 428
AWSSupport-TroubleshootECSTaskFailedToStart ... 430
AWS-UpdateAmazonECSAgent ... 435
Amazon EFS ... 437
AWSSupport-CheckAndMountEFS ... 437
Amazon EKS ... 441
AWS-CreateEKSClusterWithFargateProfile ... 442
AWS-CreateEKSClusterWithNodegroup ... 445
AWS-DeleteEKSCluster ... 449
AWS-MigrateToNewEKSSelfManagedNodeGroup ... 452
AWSPremiumSupport-TroubleshootEKSCluster ... 458
AWSSupport-TroubleshootEKSWorkerNode ... 462
AWS-UpdateEKSCluster ... 465
AWS-UpdateEKSManagedNodeGroup ... 466
AWS-UpdateEKSSelfManagedLinuxNodeGroups ... 470
AWSSupport-CollectEKSLinuxNodeStatistics ... 474
AWSSupport-CollectEKSInstanceLogs ... 480
AWSSupport-SetupK8sApiProxyForEKS ... 484
AWSSupport-TroubleshootEbsCsiDriversForEks ... 495
AWSSupport-TroubleshootEKSALBControllerIssues ... 505
Elastic Beanstalk ... 517
AWSSupport-CollectElasticBeanstalkLogs ... 517
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ... 520
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications ... 522
AWSSupport-TroubleshootElasticBeanstalk ... 524
Elastic Load Balancing ... 527
AWSConfigRemediation-DropInvalidHeadersForALB ... 527
AWS-EnableCLBAccessLogs ... 529
AWS-EnableCLBConnectionDraining ... 531
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing ... 533
AWSConfigRemediation-EnableELBDeletionProtection ... 534
AWSConfigRemediation-EnableLoggingForALBAndCLB ... 535
AWSSupport-TroubleshootCLBConnectivity ... 537
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing ... 540

AWS-UpdateALBDesyncMitigationMode ... 542
AWS-UpdateCLBDesyncMitigationMode ... 544
AWSSupport-TroubleshootELBHealthChecks ... 545
Amazon EMR ... 550
AWSSupport-AnalyzeEMRLogs ... 551
AWSSupport-DiagnoseEMRLogsWithAthena ... 557
OpenSearch Amazon-Dienst ... 566
AWSConfigRemediation-DeleteOpenSearchDomain ... 567
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain ... 568
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups ... 569
AWSSupport-TroubleshootOpenSearchRedYellowCluster ... 571
AWSSupport-TroubleshootOpenSearchHighCPU ... 577
EventBridge ... 584
AWS-AddOpsItemDedupStringToEventBridgeRule ... 585
AWS-DisableEventBridgeRule ... 586
AWS Glue ... 588
AWSSupport-TroubleshootGlueConnection ... 588
Amazon FSx ... 599
AWSSupport-ValidateFSxWindowsADConfig ... 600
GuardDuty ... 614
AWSConfigRemediation-CreateGuardDutyDetector ... 615
IAM ... 616
AWSSupport-TroubleshootIAMAccessDeniedEvents ... 617
AWS-AttachIAMToInstance ... 624
AWS-DeleteIAMInlinePolicy ... 626
AWSConfigRemediation-DeleteIAMRole ... 627
AWSConfigRemediation-DeleteIAMUser ... 629
AWSConfigRemediation-DeleteUnusedIAMGroup ... 631
AWSConfigRemediation-DeleteUnusedIAMPolicy ... 633
AWSConfigRemediation-DetachIAMPolicy ... 634
AWSConfigRemediation-EnableAccountAccessAnalyzer ... 635
AWSSupport-GrantPermissionsToIAMUser ... 637
AWSConfigRemediation-RemoveUserPolicies ... 642
AWSConfigRemediation-ReplaceIAMInlinePolicy ... 644
AWSConfigRemediation-RevokeUnusedIAMUserCredentials ... 646
AWSConfigRemediation-SetIAMPasswordPolicy ... 648

AWSSupport-ContainIAMPrincipal 651
AWSSupport-TroubleshootSAMLIssues 666
Erkennung und Reaktion auf Vorfälle 672
AWSPremiumSupport-OnboardWorkloadToIDR 672
Amazon Kinesis Data Streams 680
AWS-EnableKinesisStreamEncryption 680
AWS KMS 682
AWSConfigRemediation-CancelKeyDeletion 682
AWSConfigRemediation-EnableKeyRotation 684
Lambda 685
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing 685
AWSConfigRemediation-DeleteLambdaFunction 687
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK 688
AWSConfigRemediation-MoveLambdaToVPC 690
AWSSupport-RemediateLambdaS3Event 692
AWSSupport-TroubleshootLambdaInternetAccess 694
AWSSupport-TroubleshootLambdaS3Event 698
Von Amazon verwaltete Workflows für Apache Airflow 700
AWSSupport-TroubleshootMWAAEnvironmentCreation 700
Neptune 707
AWS-EnableNeptuneDbAuditLogsToCloudWatch 707
AWS-EnableNeptuneDbBackupRetentionPeriod 709
AWS-EnableNeptuneClusterDeletionProtection 711
Amazon RDS 712
AWS-CreateEncryptedRdsSnapshot 713
AWS-CreateRdsSnapshot 716
AWSConfigRemediation-DeleteRDSCluster 717
AWSConfigRemediation-DeleteRDSClusterSnapshot 719
AWSConfigRemediation-DeleteRDSInstance 720
AWSConfigRemediation-DeleteRDSInstanceSnapshot 722
AWSConfigRemediation-DisablePublicAccessToRDSInstance 723
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster 725
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance 727
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance 729
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance 731
AWSConfigRemediation-EnableMultiAZOnRDSInstance 732

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance 734
AWSConfigRemediation-EnableRDSClusterDeletionProtection 736
AWSConfigRemediation-EnableRDSInstanceBackup 738
AWSConfigRemediation-EnableRDSInstanceDeletionProtection 740
AWSConfigRemediation-ModifyRDSInstancePortNumber 741
AWSSupport-ModifyRDSSnapshotPermission 743
AWSPremiumSupport-PostgreSQLWorkloadReview 746
AWS-RebootRdsInstance 762
AWSSupport-ShareRDSSnapshot 764
AWS-StartRdsInstance 768
AWS-StartStopAuroraCluster 768
AWS-StopRdsInstance 770
AWSSupport-TroubleshootConnectivityToRDS 771
AWSSupport-TroubleshootRDSIAMAuthentication 774
AWSSupport-ValidateRdsNetworkConfiguration 782
Amazon Redshift 788
AWSConfigRemediation-DeleteRedshiftCluster 788
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster 790
AWSConfigRemediation-EnableRedshiftClusterAuditLogging 791
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot 793
AWSConfigRemediation-EnableRedshiftClusterEncryption 795
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting 796
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster 798
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings 799
AWSConfigRemediation-ModifyRedshiftClusterNodeType 801
Amazon S3 803
AWS-ArchiveS3BucketToIntelligentTiering 804
AWS-ConfigureS3BucketLogging 806
AWS-ConfigureS3BucketVersioning 809
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock 810
AWSConfigRemediation-ConfigureS3PublicAccessBlock 812
AWS-CreateS3PolicyToExpireMultipartUploads 815
AWS-DisableS3BucketPublicReadWrite 817
AWS-EnableS3BucketEncryption 818
AWS-EnableS3BucketKeys 819
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy 821

AWSConfigRemediation-RestrictBucketSSLRequestsOnly ... 822
AWSSupport-TroubleshootS3PublicRead ... 824
AWSSupport-ConfigureS3ReplicationSameAndCrossAccount ... 830
AWSSupport-EmptyS3Bucket ... 849
AWSSupport-TroubleshootS3EventNotifications ... 856
AWSSupport-ContainS3Resource ... 863
Amazon SES ... 873
AWSSupport-AnalyzeSESMessageSendingStatus ... 873
AWSSupport-DeploySESSendingLogsToCloudWatchLogs ... 877
SageMaker KI ... 884
AWS-DisableSageMakerNotebookRootAccess ... 884
Secrets Manager ... 886
AWSConfigRemediation-DeleteSecret ... 886
AWSConfigRemediation-RotateSecret ... 888
Security Hub CSPM ... 890
AWSConfigRemediation-EnableSecurityHub ... 890
AWS Shield ... 891
AWSPremiumSupport-DDoSResiliencyAssessment ... 892
Amazon SNS ... 901
AWS-EnableSNSTopicDeliveryStatusLogging ... 901
AWSConfigRemediation-EncryptSNSTopic ... 904
AWS-PublishSNSNotification ... 906
Amazon SQS ... 907
AWS-EnableSQSEncryption ... 907
Step Functions ... 909
AWS-EnableStepFunctionsStateMachineLogging ... 909
Systems Manager ... 912
AWS-BulkDeleteAssociation ... 912
AWS-BulkEditOpsItems ... 914
AWS-BulkResolveOpsItems ... 917
AWS-ConfigureMaintenanceWindows ... 919
AWS-CreateManagedLinuxInstance ... 921
AWS-CreateManagedWindowsInstance ... 923
AWSConfigRemediation-EnableCWLoggingForSessionManager ... 926
AWS-ExportOpsDataToS3 ... 927
AWS-ExportPatchReportToS3 ... 929

AWS-SetupInventory 931
AWS-SetupManagedInstance 935
AWS-SetupManagedRoleOnEC2Instance 937
AWSSupport-TroubleshootManagedInstance 938
AWSSupport-TroubleshootPatchManagerLinux 940
AWSSupport-TroubleshootSessionManager 944
Drittanbieter 950
AWS-CreateJiraIssue 950
AWS-CreateServiceNowIncident 952
AWS-RunPacker 955
Amazon VPC 957
AWS-CloseSecurityGroup 958
AWSSupport-ConfigureDNSQueryLogging 959
AWSSupport-ConfigureTrafficMirroring 962
AWSSupport-ConnectivityTroubleshooter 965
AWSSupport-TroubleshootVPN 969
AWSConfigRemediation-DeleteEgressOnlyInternetGateway 975
AWSConfigRemediation-DeleteUnusedENI 976
AWSConfigRemediation-DeleteUnusedSecurityGroup 978
AWSConfigRemediation-DeleteUnusedVPCNetworkACL 979
AWSConfigRemediation-DeleteVPCFlowLog 980
AWSConfigRemediation-DetachAndDeleteInternetGateway 982
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway 984
AWS-DisableIncomingSSHOnPort22 986
AWS-DisablePublicAccessForSecurityGroup 987
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP 988
AWSSupport-EnableVPCFlowLogs 990
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch 996
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket 999
AWS-ReleaseElasticIP 1001
AWS-RemoveNetworkACLUnrestrictedSSHRDP 1002
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules 1003
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules 1005
AWSSupport-SetupIPMonitoringFromVPC 1006
AWSSupport-TerminateIPMonitoringFromVPC 1015
AWS WAF 1018

AWS-AddWAFRegionalRuleToRuleGroup 1019
AWS-AddWAFRegionalRuleToWebAcl 1021
AWSConfigRemediation-EnableWAFClassicLogging 1024
AWSConfigRemediation-EnableWAFClassicRegionalLogging 1025
AWSConfigRemediation-EnableWAFV2Logging 1027
Amazon WorkSpaces 1029
AWS-CreateWorkSpace 1029
AWSSupport-RecoverWorkSpace 1032
X-Ray 1036
AWSConfigRemediation-UpdateXRayKMSKey 1037
..... mxxxix

Runbook-Referenz für Systems Manager Automation

AWS Systems Manager Stellt vordefinierte Runbooks bereit, damit Sie schnell loslegen können. Diese Runbooks werden von Amazon Web Services verwaltet, AWS Support, und AWS Config. Die Runbook-Referenz beschreibt jedes der vordefinierten Runbooks, die von Systems Manager Support, und bereitgestellt werden. AWS Config

> **Important**
>
> Wenn Sie einen automatisierten Workflow ausführen, der andere Services mithilfe einer AWS Identity and Access Management -(IAM)-Servicerolle aufruft, muss die Servicerolle mit der Berechtigung zum Aufrufen dieser Services konfiguriert sein. Diese Anforderung gilt für alle AWS Automation-Runbooks (`AWS-*`-Runbooks), wie zum Beispiel `AWS-ConfigureS3BucketLogging`, `AWS-CreateDynamoDBBackup` und `AWS-RestartEC2Instance`-Runbooks, um nur einige zu nennen. Diese Anforderung gilt auch für alle benutzerdefinierten Automatisierungs-Runbooks, die Sie erstellen und die andere Dienste mithilfe von Aktionen aufrufen, die andere AWS Dienste aufrufen. Wenn Sie unter anderem `aws:executeAwsApi`-, `aws:createStack`- oder `aws:copyImage`-Aktionen verwenden, dann müssen Sie die Servicerolle mit der Berechtigung zum Aufrufen solcher Services konfigurieren. Sie können Berechtigungen für andere AWS Dienste aktivieren, indem Sie der Rolle eine IAM-Inline-Richtlinie hinzufügen. Weitere Informationen finden Sie unter Hinzufügen einer Automatisierungs-Inline-Richtlinie zum Aufrufen anderer AWS Dienste.

Diese Referenz enthält Themen, in denen die einzelnen Systems Manager Manager-Runbooks beschrieben werden, deren Eigentümer AWS AWS Support, und AWS Config sind. Runbooks sind nach den jeweiligen Benutzern geordnet. AWS-Service Jede Seite enthält eine Erläuterung der erforderlichen und optionalen Parameter, die Sie bei der Verwendung des Runbooks angeben können. Auf jeder Seite sind auch die Schritte im Runbook und gegebenenfalls die Ergebnisse der Automatisierung aufgeführt.

Diese Referenz enthält keine separate Seite für Runbooks, für die eine Genehmigung erforderlich ist, wie z. B. das Runbook `AWS-CreateManagedLinuxInstanceWithApproval` oder`AWS-StopEC2InstanceWithApproval`. Jeder Runbook-Name, der die Aktion enthält`WithApproval`, bedeutet, dass das Runbook die Aktion enthält. `aws:approve` Durch diese Aktion wird eine Automatisierung vorübergehend angehalten, bis bestimmte Hauptbenutzer die Aktion entweder

genehmigen oder ablehnen. Nach Erreichen der erforderlichen Anzahl an Genehmigungen wird die Automatisierung fortgesetzt.

Informationen zum Ausführen von Automatisierungen finden Sie unter Einfache Automatisierung ausführen. Informationen zum Ausführen von Automatisierungen auf mehreren Zielen finden Sie unter Ausführen von Automatisierungen, die Ziele und Ratensteuerungen verwenden.

Themen

- Runbook-Inhalte anzeigen
- 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 Amazon-Dienst
- EventBridge
- AWS Glue
- Amazon FSx
- GuardDuty
- IAM
- Erkennung und Reaktion auf Vorfälle
- Amazon Kinesis Data Streams
- AWS KMS
- Lambda
- Von Amazon verwaltete Workflows für Apache Airflow
- Neptune
- Amazon RDS
- Amazon Redshift
- Amazon S3
- Amazon SES
- SageMaker KI
- Secrets Manager
- Security Hub CSPM
- AWS Shield
- Amazon SNS
- Amazon SQS
- Step Functions
- Systems Manager
- Drittanbieter
- Amazon VPC
- AWS WAF
- Amazon WorkSpaces
- X-Ray

Runbook-Inhalte anzeigen

Sie können den Inhalt für Runbooks in der Systems Manager Manager-Konsole anzeigen.

Um Runbook-Inhalte anzuzeigen

1. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/
2. Wählen Sie im Navigationsbereich die Option Dokumente aus.

   –oder–

   Wenn die AWS Systems Manager Startseite zuerst geöffnet wird, wählen Sie das Menüsymbol (☰), um den Navigationsbereich zu öffnen, und wählen Sie dann im Navigationsbereich Dokumente aus.
3. Wählen Sie im Abschnitt Kategorien die Option Automatisierungsdokumente aus.
4. Wählen Sie ein Runbook aus und anschließend die Option View details.
5. Wählen Sie die Registerkarte Content aus.

API Gateway

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon API Gateway bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-DeleteAPIGatewayStage
- AWSConfigRemediation-EnableAPIGatewayTracing
- AWSConfigRemediation-UpdateAPIGatewayMethodCaching
- AWSSupport-TroubleshootAPIGatewayHttpErrors

`AWSConfigRemediation-DeleteAPIGatewayStage`

Beschreibung

Das `AWSConfigRemediation-DeleteAPIGatewayStage` Runbook löscht eine Amazon API Gateway Gateway-Stufe (API Gateway). AWS Config muss dort aktiviert sein, AWS-Region wo Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- StageArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der API Gateway Gateway-Stufe, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `config:GetResourceConfigHistory`
- `apigateway:GET`
- `apigateway:DELETE`

Dokumentschritte

- `aws:executeScript`— Löscht den im `StageArn` Parameter angegebenen API-Gateway-Schritt.

AWSConfigRemediation-EnableAPIGatewayTracing

Beschreibung

Das `AWSConfigRemediation-EnableAPIGatewayTracing` Runbook ermöglicht die Ablaufverfolgung auf einer Amazon API Gateway Gateway-Stufe (API Gateway). AWS Config muss dort aktiviert sein, AWS-Region wo Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- StageArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der API Gateway Gateway-Stufe, für die Sie die Ablaufverfolgung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`— Aktiviert die Ablaufverfolgung auf der im `StageArn` Parameter angegebenen API-Gateway-Stufe.

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

Beschreibung

Das `AWSConfigRemediation-UpdateAPIGatewayMethodCaching` Runbook aktualisiert die Einstellung der Cache-Methode für eine Amazon API Gateway Gateway-Staging-Ressource.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- CachingAuthorizedMethods

  Typ: StringList

  Beschreibung: (Erforderlich) Die Methoden, die für die Aktivierung von Caching autorisiert sind. Die Liste muss eine Kombination aus`DELETE`,`GET`,`HEAD`, `OPTIONS` `PATCHPOST`, und `PUT` sein. Das Caching ist für ausgewählte Methoden aktiviert und für nicht ausgewählte Methoden deaktiviert. Das Zwischenspeichern ist für alle Methoden aktiviert, wenn `ANY` es ausgewählt ist, und für alle Methoden deaktiviert, wenn `NONE` es ausgewählt ist.
- StageArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der API Gateway Gateway-Staging-ARN für die `REST` API.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`— Akzeptiert die Staging-Ressourcen-ID als Eingabe, aktualisiert die Cache-Methodeneinstellung für einen API-Gateway-Schritt mithilfe der `UpdateStage` API-Aktion und verifiziert das Update.

AWSSupport-TroubleshootAPIGatewayHttpErrors

Beschreibung

Das AWSSupport-TroubleshootAPIGatewayHttpErrorsRunbook hilft bei der Behebung von 5XX/4XX-Fehlern beim Aufrufen einer bereitgestellten Amazon API Gateway Gateway-REST-API, indem es and/or Zugriffsausführungsprotokolle analysiert und Fehler analysiert, um anhand von Re:POST-Artikeln und der Dokumentation Korrekturmaßnahmen bereitzustellen. AWS

Important

Dieses Runbook hat die folgenden Einschränkungen:

- Die Protokollierung muss aktiviert sein. Weitere Informationen finden Sie unter Amazon CloudWatch API-Protokollierung mithilfe der API Gateway Gateway-Konsole einrichten.
- Die Protokolle müssen aktiviert worden sein, bevor der oder die Fehler aufgetreten sind. Die Erfassung und Analyse von Protokollen kann nicht rückwirkend durchgeführt werden.
- Behandelte Fehler: 500, 502, 503, 504, 401, 403, 429.
- Nur REST wird APIs unterstützt. WebSocket und HTTP (v2) werden in diesem Runbook nicht behandelt.

Important

Bei der Verwendung dieses Runbooks können zusätzliche Gebühren für Ihr AWS Konto für die von Ihrer REST-API erfassten Amazon CloudWatch Logs und für Logs Insights, die in der CloudWatch Analyse verwendet wurden, anfallen. Weitere Informationen zu den möglicherweise anfallenden Gebühren finden Sie unter CloudWatch Amazon-Preise. Wenn der `aws:deletestack` Schritt fehlschlägt, wechseln Sie zur CloudFormation Konsole, um den Stack manuell zu löschen. Der von diesem Runbook erstellte Stack-Name beginnt mit`AWSSupport-TroubleshootAPIGatewayHttpErrors`. Informationen zum Löschen

von CloudFormation Stacks finden Sie unter Löschen eines Stacks im AWS CloudFormation Benutzerhandbuch.

Wie funktioniert es?

Das Runbook führt die folgenden Validierungs- und Analyseschritte durch:

- Überprüft, ob die angegebene REST-API vorhanden ist und Sie über die erforderlichen Berechtigungen verfügen.
- Überprüft, ob die angegebene Phase in der API vorhanden ist.
- Überprüft, ob der angegebene Ressourcenpfad in der API vorhanden ist.
- Überprüft, ob die angegebene HTTP-Methode für die Ressource existiert.
- Analysiert CloudWatch Protokolle für die angegebenen Parameter und den angegebenen Zeitraum, um Fehler zu identifizieren und Empfehlungen zur Behebung zu geben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:PutLogEvents
- logs:StartQuery
- logs:GetQueryResults

Beispiel für eine IAM-Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-TroubleshootAPIGatewayHttpErrorsim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

  - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es SSM Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet SSM Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
  - Typ: `AWS::IAM::Role::Arn`
- RestApiId (Erforderlich):
  - Beschreibung: (Erforderlich) Die API-ID für die API, für die eine Fehlerbehebung erforderlich ist. Muss eine 10-stellige alphanumerische Zeichenfolge sein.
  - Typ: `String`
  - Zulässiges Muster: `^[a-zA-Z0-9]{10}$`
- StageName (Erforderlich):
  - Beschreibung: (Erforderlich) Der Name der bereitgestellten Phase. Muss aus 1—128 Zeichen bestehen und Buchstaben, Zahlen, Unterstriche oder Bindestriche enthalten.
  - Typ: `String`
  - Zulässiges Muster: `^[a-zA-Z0-9_\\-]{1,128}$`
- ResourcePath (Fakultativ):
  - Beschreibung: (Optional) Der Ressourcenpfad, für den die Methode konfiguriert ist. Beispiele: `/`, `/store/items`, `/{resource}`.
  - Typ: `String`
  - Standard: `/`
- HttpMethod (Optional):
  - Beschreibung: (Optional) Die Methode für den konfigurierten Ressourcenpfad.
  - Typ: `String`
  - Zulässige Werte: `[ANY, DELETE, HEAD, OPTIONS, GET, POST, PUT, PATCH]`
  - Standard: `GET`
- StartTime (Fakultativ):
  - Beschreibung: (Optional) Das Startdatum und die Startzeit für die Abfrage der CloudWatch Protokolle. Format: `yyyy-MM-ddTHH:mm:ss` in der UTC-Zeitzone. Wenn nicht angegeben, wird standardmäßig 3 Tage vor der aktuellen Uhrzeit angezeigt.
  - Typ: `String`
  - Zulässiges Muster: `^$|^[0-9]{4}-(0[1-9]|1[0-2])-(0[1-9]|[1-2][0-9]|3[0-1])T(2[0-3]|[01][0-9]):[0-5][0-9]:[0-5][0-9]$`

- Standard: ""
- EndTime (Fakultativ):
  - Beschreibung: (Optional) Das Enddatum und die Endzeit für die Abfrage der CloudWatch Protokolle. Format: `yyyy-MM-ddTHH:mm:ss` in der UTC-Zeitzone. Wenn nicht angegeben, wird standardmäßig die aktuelle Uhrzeit verwendet.
  - Typ: `String`
  - Zulässiges Muster: `^$|^[0-9]{4}-(0[1-9]|1[0-2])-(0[1-9]|[1-2][0-9]|3[0-1])T(2[0-3]|[01][0-9]):[0-5][0-9]:[0-5][0-9]$`
  - Standard: ""
- AccessLogs (Fakultativ):
  - Beschreibung: (Optional) Ob Zugriffsprotokolle analysiert werden sollen.
  - Typ: `Boolean`
  - Zulässige Werte: `[true, false]`
  - Standard: `false`
- RequestId (Fakultativ):
  - Beschreibung: (Optional) Die Anforderungs-ID für die Anfrage, bei der ein Fehler beobachtet wurde. Muss ein gültiges UUID-Format haben.
  - Typ: `String`
  - Zulässiges Muster: `^$|^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$`
  - Standard: ""

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - CheckApiExists:

     Überprüft, ob die bereitgestellte REST-API existiert und Sie über die erforderlichen Zugriffsberechtigungen verfügen.
   - CheckStageExists:

     Überprüft, ob der angegebene Staging-Name in der angegebenen API vorhanden ist, und ruft Informationen zur Zugriffsprotokollgruppe ab.
   - CheckResourceExists:

Überprüft, ob der angegebene Ressourcenpfad in der API vorhanden ist, und ruft die Ressourcen-ID ab.

- CheckMethodExists:

  Überprüft, ob die angegebene HTTP-Methode für die angegebene Ressource existiert.

- AnalyseLogs:

  Sucht anhand der angegebenen Parameter nach Protokollen und gibt Empfehlungen zurück, die auf den gefundenen Fehlern basieren. In diesem Schritt werden sowohl Ausführungs- als auch Zugriffsprotokolle (falls aktiviert) analysiert, um 4XX- und 5XX-Fehler zu identifizieren, und es werden spezifische Hinweise zur Problembehebung bereitgestellt.

7. Nach Abschluss des Vorgangs finden Sie im Abschnitt Ergebnisse die detaillierten Ergebnisse der Ausführung, einschließlich der Fehleranalyse und Empfehlungen zur Problembehebung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

AWS Batch

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS Batch Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-TroubleshootAWSBatchJob

`AWSSupport-TroubleshootAWSBatchJob`

Beschreibung

Das `AWSSupport-TroubleshootAWSBatchJob` Runbook hilft Ihnen bei der Behebung von Problemen, die verhindern, dass ein AWS Batch Job vom aktuellen Status abweicht`RUNNABLE`. `STARTING`

Wie funktioniert es?

Dieses Runbook führt die folgenden Prüfungen durch:

- Wenn sich die Rechenumgebung im `DISABLED` Status `INVALID` Oder befindet.
- Wenn der `Max vCPU` Parameter der Rechenumgebung groß genug ist, um das Auftragsvolumen in der Auftragswarteschlange aufzunehmen.
- Wenn die Jobs mehr V CPUs - oder Speicherressourcen benötigen, als die Instanztypen der Rechenumgebung bereitstellen können.
- Wenn die Jobs auf GPU-basierten Instanzen ausgeführt werden sollen, die Rechenumgebung jedoch nicht für die Verwendung GPU-basierter Instanzen konfiguriert ist.
- Wenn die Auto Scaling Scaling-Gruppe für die Rechenumgebung keine Instances starten konnte.
- Wenn die gestarteten Instances dem zugrunde liegenden Amazon Elastic Container Service (Amazon ECS) -Cluster beitreten können; andernfalls wird das AWSSupport-TroubleshootECSContainerInstanceRunbook ausgeführt.
- Wenn aufgrund eines Berechtigungsproblems bestimmte Aktionen blockiert werden, die zur Ausführung des Jobs erforderlich sind.

Important

- Dieses Runbook muss in derselben AWS Region initiiert werden wie Ihr Job, der im `RUNNABLE` Status „hängengeblieben“ ist.
- Dieses Runbook kann für AWS Batch Jobs initiiert werden, die auf Amazon ECS AWS Fargate - oder Amazon Elastic Compute Cloud (Amazon EC2) -Instances geplant sind. Wenn die Automatisierung für einen AWS Batch Job auf Amazon Elastic Kubernetes Service (Amazon EKS) initiiert wird, wird die Initiierung gestoppt.
- Wenn Instances für die Ausführung des Jobs verfügbar sind, der Amazon ECS-Cluster jedoch nicht registriert werden kann, initiiert dieses Runbook das `AWSSupport-TroubleshootECSContainerInstance` Automatisierungs-Runbook, um herauszufinden, warum. Weitere Informationen finden Sie im Runbook. AWSSupport-TroubleshootECSContainerInstance

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- JobId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des AWS Batch Job, der im `RUNNABLE` Status hängengeblieben ist.

  Zulässiges Muster: `^[a-f0-9]{8}(-[a-f0-9]{4}){3}-[a-f0-9]{12}(:[0-9]+)?(#[0-9]+)?$`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

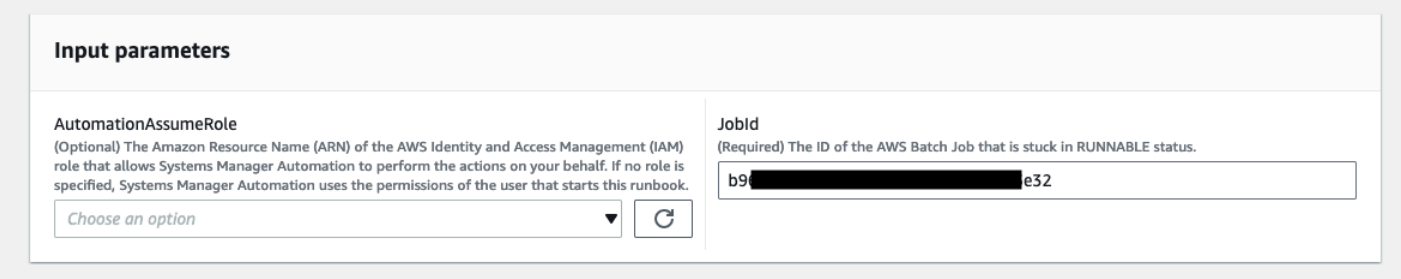
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sts:GetCallerIdentity`

Anweisungen

1. Navigieren Sie AWSSupport-TroubleshootAWSBatchJobin der AWS Systems Manager Konsole zu.
2. Wählen Sie Automatisierung ausführen
3. Geben Sie für Eingabeparameter Folgendes ein:
   - AutomationAssumeRole(Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - JobId(Erforderlich):

     Die ID des AWS Batch Job, der im `RUNNABLE` Status hängengeblieben ist.



4. Wählen Sie Ausführen aus.
5. Beachten Sie, dass die Automatisierung initiiert wird.
6. Das Dokument führt die folgenden Schritte aus:
   - PreflightPermissionChecks:

     Führt Preflight-IAM-Berechtigungsprüfungen für den Benutzer/die Rolle durch, die den Vorgang initiiert hat. Wenn Berechtigungen fehlen, werden in diesem Schritt die API-Aktionen angezeigt, die im globalen Ausgabebereich fehlen.
   - ProceedOnlyIfUserHasPermission:

Verzweigungen basieren darauf, ob Sie über Berechtigungen für alle erforderlichen Aktionen für das Runbook verfügen.

- AWSBatchJobEvaluation:

  Führt Prüfungen anhand des AWS Batch Job durch, um zu überprüfen, ob er vorhanden ist und sich im `RUNNABLE` Status befindet.

- ProceedOnlyIfBatchJobExistsAndIsinRunnableStatus:

  Branches basieren darauf, ob der Job existiert und ob er sich im `RUNNABLE` Status befindet.

- BatchComputeEnvironmentEvaluation:

  Führt Prüfungen anhand der AWS Batch Rechenumgebung durch.

- ProceedOnlyIfComputeEnvironmentChecksAreOK:

  Verzweigungen, die darauf basieren, ob die Prüfungen der Rechenumgebung erfolgreich waren.

- UnderlyingInfraEvaluation:

  Führt Prüfungen anhand der zugrunde liegenden Auto Scaling Group oder Spot Fleet Request durch.

- ProceedOnlyIfInstancesNotJoiningEcsCluster:

  Branches basieren darauf, ob es Instances gibt, die dem Amazon ECS-Cluster nicht beitreten.

- EcsAutomationRunner:

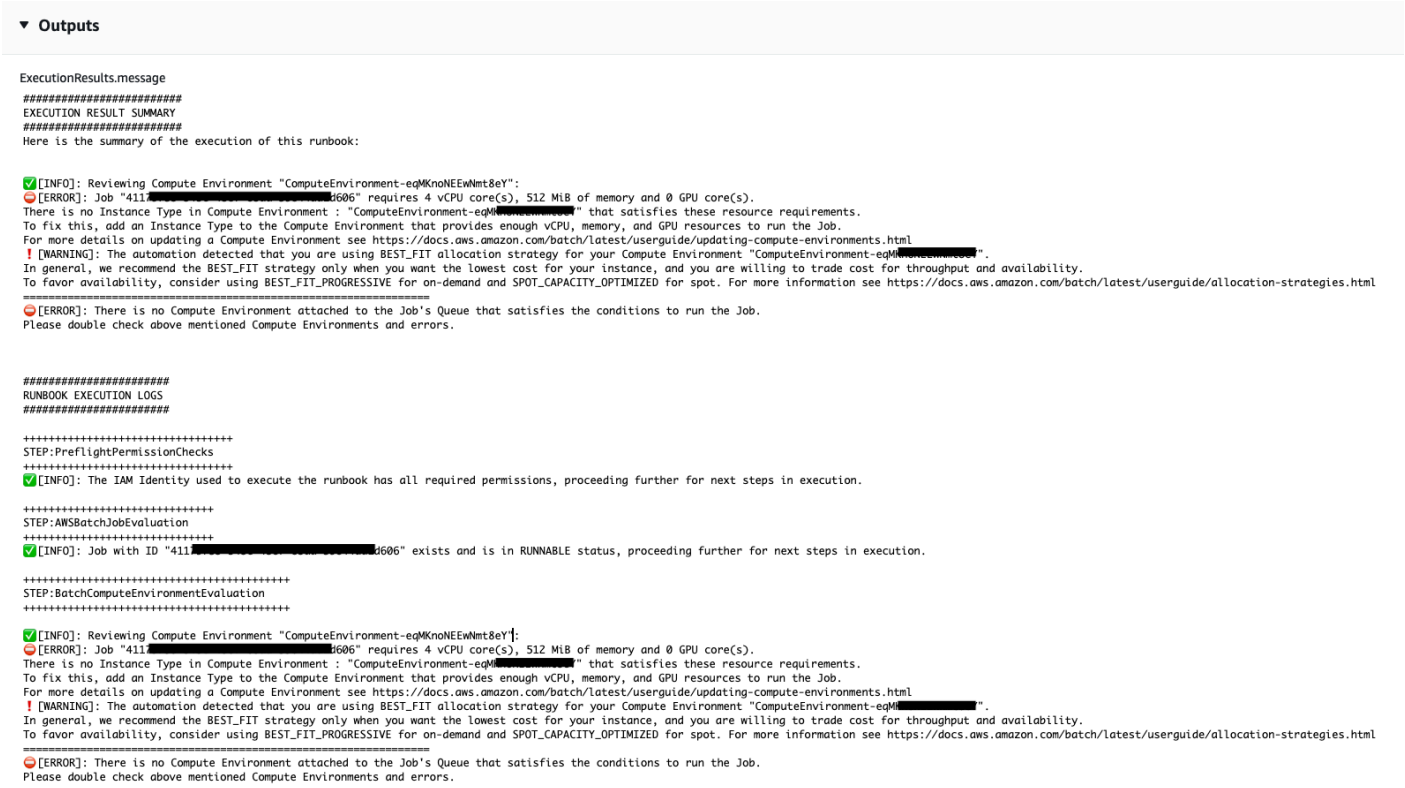
  Führt die Amazon ECS-Automatisierung für die Instances aus, die dem Cluster nicht beitreten.

- ExecutionResults:

  Generiert eine Ausgabe auf der Grundlage der vorherigen Schritte.

7. Nach Abschluss des Vorgangs wird der URI für die HTML-Datei des Bewertungsberichts bereitgestellt:

   S3-Konsolenlink und Amazon S3 S3-URI für den Bericht über die erfolgreiche Ausführung des Runbooks



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

CloudFormation

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS CloudFormation Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-DeleteCloudFormationStack

- AWS-EnableCloudFormationSNSNotification
- AWS-RunCfnLint
- AWSSupport-TroubleshootCFNCustomResource
- AWS-UpdateCloudFormationStack

AWS-DeleteCloudFormationStack

Beschreibung

Löscht einen CloudFormation Stapel.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- StackNameOrId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name oder eindeutige ID des zu CloudFormation löschenden Stacks

AWS-EnableCloudFormationSNSNotification

Beschreibung

Das `AWS-EnableCloudFormationSNSNotification` Runbook aktiviert Amazon Simple Notification Service (Amazon SNS) -Benachrichtigungen für den von Ihnen angegebenen AWS CloudFormation (CloudFormation) -Stack.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- StackArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN oder Name des CloudFormation Stacks, für den Sie Amazon SNS SNS-Benachrichtigungen aktivieren möchten.
- NotificationArn

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der ARN des Amazon SNS SNS-Themas, das Sie dem CloudFormation Stack zuordnen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- ssm: GetAutomationExecution
- ssm: StartAutomationExecution
- Wolkenbildung: DescribeStacks
- Wolkenbildung: UpdateStack
- kms:Decrypt
- km: GenerateDataKey
- sns:Publish
- sqs: GetQueueAttributes

Dokumentschritte

- CheckCfnSnsLimits (`aws:executeScript`) — Überprüft, ob die maximale Anzahl von Amazon SNS SNS-Themen noch nicht mit dem von Ihnen angegebenen CloudFormation Stack verknüpft wurde.
- EnableCfnSnsNotification (`aws:executeAwsApi`) — Aktiviert Amazon SNS SNS-Benachrichtigungen für den CloudFormation Stack.
- VerificationCfnSnsNotification (`aws:executeScript`) — Überprüft, ob Amazon SNS SNS-Benachrichtigungen für den CloudFormation Stack aktiviert wurden.

Ausgaben

CheckCfnSnsLimits. NotificationArnList - Eine Liste von Personen ARNs , die Amazon SNS SNS-Benachrichtigungen für den CloudFormation Stack erhalten.

VerificationCfnSnsNotification. VerifySnsTopicsResponse — Antwort des API-Vorgangs, die bestätigt, dass Amazon SNS SNS-Benachrichtigungen für den CloudFormation Stack aktiviert wurden.

AWS-RunCfnLint

Beschreibung

Dieses Runbook verwendet einen AWS CloudFormation Linter (`cfn-python-lint`), um YAML- und JSON-Vorlagen anhand der Ressourcenspezifikation zu validieren. CloudFormation Das `AWS-RunCfnLint` Runbook führt zusätzliche Prüfungen durch und stellt beispielsweise sicher, dass gültige Werte für Ressourceneigenschaften eingegeben wurden. Wenn die Validierung nicht erfolgreich ist, schlägt der `RunCfnLintAgainstTemplate`-Schritt fehl und die Ausgabe des Lintertools wird in einer Fehlermeldung bereitgestellt. Dieses Runbook verwendet cfn-lint v0.24.4.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ConfigureRuleFlag

  Typ: Zeichenfolge

  Beschreibung (optional): Konfigurationsoptionen für eine Regel, die an den `--configure-rule`-Parameter übergeben werden soll.

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

- FormatFlag

  Typ: Zeichenfolge

  Beschreibung (optional): Wert, der an den `--format`-Parameter übergeben wird, um das Ausgabeformat anzugeben.

  Gültige Werte: Standard | quiet | parseable | json

  Standard: Standard

- IgnoreChecksFlag

  Typ: Zeichenfolge

  Beschreibung: (Optional) IDs von Regeln, die an den Parameter --ignore-checks übergeben werden sollen. Diese Regeln werden nicht überprüft.

  Beispiel: E1001, E1003, W7001

- IncludeChecksFlag

  Typ: Zeichenfolge

  Beschreibung: (Optional) IDs der Regeln, die an den Parameter übergeben werden sollen. `--include-checks` Diese Regeln werden überprüft.

  Beispiel: E1001, E1003, W7001

- InfoFlag

  Typ: Zeichenfolge

  Beschreibung (optional): Option für den `--info`-Parameter. Fügen Sie die Option hinzu, um zusätzliche Protokollierungsinformationen zur Vorlagenverarbeitung zu aktivieren.

  Standard: false

- TemplateFileName

  Typ: Zeichenfolge

  Beschreibung: der Name oder der Schlüssel der Vorlagendatei im S3-Bucket.

- Vorlagen (3) BucketName

  Typ: Zeichenfolge

  Beschreibung: der Name des S3-Buckets, der die Packer-Vorlage enthält.
- RegionsFlag

  Typ: Zeichenfolge

  Beschreibung: (Optional) Werte, die an den `--regions` Parameter for übergeben werden, um die Vorlage anhand der angegebenen Werte zu testen. AWS-Regionen

  Beispiel: us-east-1,us-west-1

Dokumentschritte

RunCfnLintAgainstTemplate — Führt das `cfn-python-lint` Tool anhand der angegebenen CloudFormation Vorlage aus.

Ausgaben

RunCfnLintAgainstTemplate.output — Die Standardausgabe aus dem Tool. `cfn-python-lint`

AWSSupport-TroubleshootCFNCustomResource

Beschreibung

Das `AWSSupport-TroubleshootCFNCustomResource` Runbook hilft bei der Diagnose, warum ein AWS CloudFormation Stack beim Erstellen, Aktualisieren oder Löschen einer benutzerdefinierten Ressource fehlgeschlagen ist. Das Runbook überprüft das für die benutzerdefinierte Ressource verwendete Diensttoken und die zurückgegebene Fehlermeldung. Nachdem Sie die Details für die benutzerdefinierte Ressource überprüft haben, enthält die Runbook-Ausgabe eine Erläuterung des Stapelverhaltens und der Schritte zur Fehlerbehebung für die benutzerdefinierte Ressource.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- StackName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des CloudFormation Stacks, bei dem die benutzerdefinierte Ressource ausgefallen ist.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `validateCloudFormationStack`- Überprüft, ob der CloudFormation Stapel im selben AWS-Konto und vorhanden ist. AWS-Region
- `checkCustomResource`- Analysiert den CloudFormation Stapel, überprüft die ausgefallene benutzerdefinierte Ressource und gibt Informationen zur Problembehandlung bei der ausgefallenen benutzerdefinierten Ressource aus.

AWS-UpdateCloudFormationStack

Beschreibung

Aktualisieren Sie einen AWS CloudFormation Stack mithilfe einer CloudFormation Vorlage, die in einem Amazon S3 S3-Bucket gespeichert ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LambdaAssumeRole

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der ARN der von Lambda übernommenen Rolle

- StackNameOrId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name oder eindeutige ID des zu CloudFormation aktualisierenden Stacks

- TemplateUrl

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) S3-Bucket-Speicherort, der die aktualisierte CloudFormation Vorlage enthält (z. B. `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`)

CloudFront

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon CloudFront bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-EnableCloudFrontDefaultRootObject
- AWSConfigRemediation-EnableCloudFrontAccessLogs
- AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity
- AWSConfigRemediation-EnableCloudFrontOriginFailover
- AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

`AWSConfigRemediation-EnableCloudFrontDefaultRootObject`

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontDefaultRootObject` Runbook konfiguriert das Standard-Root-Objekt für die Amazon CloudFront (CloudFront) -Distribution, die Sie angeben.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- CloudFrontDistributionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront Distribution, für die Sie das Standard-Root-Objekt konfigurieren möchten.
- DefaultRootObject

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Das Objekt, das Sie zurückgeben CloudFront möchten, wenn eine Viewer-Anfrage auf Ihre Stamm-URL verweist.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

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

Dokumentschritte

- `aws:executeScript`- Konfiguriert das Standard-Stammobjekt für die CloudFront Verteilung, die Sie im `CloudFrontDistributionId` Parameter angeben.

AWSConfigRemediation-EnableCloudFrontAccessLogs

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontAccessLogs` Runbook ermöglicht die Zugriffsprotokollierung für die von Ihnen angegebene Amazon CloudFront (CloudFront) -Distribution.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BucketName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name des Amazon Simple Storage Service (Amazon S3) - Buckets, in dem Sie Zugriffs-Logs speichern möchten. Buckets in af-south-1, ap-east-1, eu-south-1 und me-south-1 werden nicht unterstützt. AWS-Region

- CloudFrontId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Distribution, für die Sie die Zugriffsanmeldung aktivieren möchten. CloudFront

- IncludeCookies

  Typ: Boolesch

  Zulässige Werte: true | false

  Beschreibung: (Erforderlich) Setzen Sie diesen Parameter auf`true`, wenn Cookies in die Zugriffsprotokolle aufgenommen werden sollen.

- Präfix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine optionale Zeichenfolge, der Sie dem Zugriffsprotokoll `filenames` für Ihre Distribution als Präfix hinzufügen möchten CloudFront , `myprefix/` z. B.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `s3:GetBucketAcl`
- `s3:PutBucketAcl`

> **Note**
>
> Die `s3:GetBucketLocation` API kann nur für S3-Buckets im selben Konto verwendet werden. Sie können sie nicht für kontoübergreifende S3-Buckets verwenden.

Dokumentschritte

- `aws:executeScript`- Aktiviert die Zugriffsprotokollierung für die CloudFront Verteilung, die Sie im `CloudFrontDistributionId` Parameter angeben.

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity` Runbook aktiviert die Ursprungszugriffsidentität für die von Ihnen angegebene Amazon CloudFront (CloudFront) - Distribution. Diese Automatisierung weist allen Origins des CloudFront Origin-Origin-Typs Amazon Simple Storage Service (Amazon S3) ohne Ursprungszugriffsidentität für die von Ihnen angegebene CloudFront Distribution dieselbe Origin-Zugriffsidentität zu. Diese Automatisierung gewährt der ursprünglichen Zugriffsidentität keine Leseberechtigung für den CloudFront Zugriff auf Objekte in Ihrem Amazon S3 S3-Bucket. Sie müssen Ihre Amazon S3 S3-Bucket-Berechtigungen aktualisieren, um Zugriff zu gewähren.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- CloudFrontDistributionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront Distribution, für die Sie das Origin-Failover aktivieren möchten.
- OriginAccessIdentityId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront ursprünglichen Zugriffsidentität, die dem Ursprung zugeordnet werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert die ursprüngliche Zugriffsidentität für die CloudFront Verteilung, die Sie im `CloudFrontDistributionId` Parameter angeben, und überprüft, ob die ursprüngliche Zugriffsidentität zugewiesen wurde.

AWSConfigRemediation-EnableCloudFrontOriginFailover

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontOriginFailover` Runbook ermöglicht Origin-Failover für die von Ihnen angegebene Amazon CloudFront (CloudFront) -Distribution.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- CloudFrontDistributionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront Distribution, für die Sie das Origin-Failover aktivieren möchten.
- OriginGroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Ursprungsgruppe.

- PrimaryOriginId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des primären Ursprungs in der Ursprungsgruppe.
- SecondaryOriginId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des sekundären Ursprungs in der Ursprungsgruppe.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert das Origin-Failover für die CloudFront Verteilung, die Sie im `CloudFrontDistributionId` Parameter angeben, und überprüft, ob das Failover aktiviert wurde.

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

Beschreibung

Das `AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS` Runbook aktiviert die Viewer-Protokollrichtlinie für die von Ihnen angegebene Amazon CloudFront (CloudFront) - Distribution.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- CloudFrontDistributionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der CloudFront Distribution, für die Sie die Viewer-Protokollrichtlinie aktivieren möchten.
- ViewerProtocolPolicy

  Typ: Zeichenfolge

  Gültige Werte: nur https, redirect-to-https

  Beschreibung: (Erforderlich) Das Protokoll, mit dem Zuschauer auf die Dateien im Ursprung zugreifen können.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`
- `cloudfront:GetDistribution`

Dokumentschritte

- `aws:executeScript`- Aktiviert die Viewer-Protokollrichtlinie für die CloudFront Verteilung, die Sie im `CloudFrontDistributionId` Parameter angeben, und überprüft, ob die Richtlinie zugewiesen wurde.

CloudTrail

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS CloudTrail Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-CreateCloudTrailMultiRegionTrail
- AWS-EnableCloudTrail
- AWS-EnableCloudTrailCloudWatchLogs
- AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS
- AWS-EnableCloudTrailKmsEncryption
- AWSConfigRemediation-EnableCloudTrailLogFileValidation
- AWS-EnableCloudTrailLogFileValidation
- AWS-QueryCloudTrailLogs

`AWSConfigRemediation-CreateCloudTrailMultiRegionTrail`

Beschreibung

Das `AWSConfigRemediation-CreateCloudTrailMultiRegionTrail` Runbook erstellt einen AWS CloudTrail (CloudTrail) -Trail, der Protokolldateien von mehreren AWS-Regionen an den Amazon Simple Storage Service (Amazon S3) -Bucket Ihrer Wahl übermittelt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, in den Sie Protokolle hochladen möchten.
- KeyPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Amazon S3 S3-Schlüsselpräfix, das nach dem Namen des Buckets steht, den Sie für die Protokolldateizustellung bestimmt haben.
- TrailName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des zu erstellenden CloudTrail Trails.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:CreateTrail`
- `cloudtrail:StartLogging`
- `cloudtrail:GetTrail`
- `s3:PutObject`
- `s3:GetBucketAcl`
- `s3:PutBucketLogging`
- `s3:ListBucket`

Dokumentschritte

- `aws:executeAwsApi`- Akzeptiert den Trail-Namen und den Amazon S3 S3-Bucket-Namen als Eingabe und erstellt einen CloudTrail Trail.
- `aws:executeAwsApi`- Aktiviert die Protokollierung für den erstellten Trail und startet die Protokollzustellung an den von Ihnen angegebenen Amazon S3 S3-Bucket.
- `aws:assertAwsResourceProperty`- Überprüft, ob der CloudTrail Trail erstellt wurde.

AWS-EnableCloudTrail

Beschreibung

Erstellen Sie einen AWS CloudTrail Trail und konfigurieren Sie die Protokollierung in einem S3-Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name des S3-Buckets für die Veröffentlichung von Protokolldateien.

  > **Note**
  >
  > Der S3-Bucket muss existieren und die Bucket-Richtlinie muss die CloudTrail Schreibberechtigung dafür gewähren. Weitere Informationen finden Sie unter Amazon S3 S3-Bucket-Richtlinie für CloudTrail.

- TrailName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des neuen Trails.

AWS-EnableCloudTrailCloudWatchLogs

Beschreibung

Dieses Runbook aktualisiert die Konfiguration eines oder mehrerer AWS CloudTrail Trails, um Ereignisse an eine Amazon CloudWatch Logs-Protokollgruppe zu senden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- CloudWatchLogsLogGroupArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der CloudWatch Logs-Protokollgruppe, an die die CloudTrail Logs übermittelt werden.
- CloudWatchLogsRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle CloudWatch Logs Logs geht davon aus, in die angegebene Protokollgruppe zu schreiben.
- TrailNames

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der Namen der CloudTrail Trails, deren Ereignisse Sie an Logs senden möchten CloudWatch .

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktualisiert die angegebenen CloudTrail Pfade, um Ereignisse an die angegebene Protokollgruppe „ CloudWatch Logs“ zu übermitteln.

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

Beschreibung

Das `AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS` Runbook verschlüsselt einen AWS CloudTrail (CloudTrail) Trail mit dem von Ihnen angegebenen AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssel. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass Ihre CloudTrail Trails gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Trails mit unterschiedlichen KMS-Schlüsseln zu verschlüsseln. CloudTrail Digest-Dateien sind nicht verschlüsselt. Wenn Sie den `EnableLogFileValidation` Parameter `true` für den Trail zuvor auf gesetzt haben, finden Sie weitere Informationen im Abschnitt „Serverseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln verwenden“ des Themas Bewährte Methoden zur CloudTrail präventiven Sicherheit im AWS CloudTrail Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- KMSKeyID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN, die Schlüssel-ID oder der Schlüsselalias des vom Kunden verwalteten Schlüssels, den Sie zur Verschlüsselung des im `TrailName` Parameter angegebenen Trails verwenden möchten.
- TrailName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN oder der Name des Trails, den Sie aktualisieren möchten, der verschlüsselt werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die Verschlüsselung auf dem Pfad, den Sie im `TrailName` Parameter angeben.

- `aws:executeAwsApi`- Sammelt den ARN für den vom Kunden verwalteten Schlüssel, den Sie im `KMSKeyId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft, ob die Verschlüsselung auf dem CloudTrail Trail aktiviert wurde.

AWS-EnableCloudTrailKmsEncryption

Beschreibung

Dieses Runbook aktualisiert die Konfiguration eines oder mehrerer AWS CloudTrail Trails, sodass die Verschlüsselung AWS Key Management Service (AWS KMS) verwendet wird.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- KMSKeyID

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die Schlüssel-ID des vom Kunden verwalteten Schlüssels, den Sie zur Verschlüsselung des im `TrailName` Parameter angegebenen Trails verwenden möchten. Der Wert kann ein Aliasname mit dem Präfix „alias/“, ein vollständig spezifizierter ARN für einen Alias oder ein vollständig spezifizierter ARN für einen Schlüssel sein.

- TrailNames

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der Trails, deren Verschlüsselung Sie aktualisieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert die AWS KMS Verschlüsselung auf den Pfaden, die Sie im `TrailName` Parameter angeben.

AWSConfigRemediation-EnableCloudTrailLogFileValidation

Beschreibung

Das `AWSConfigRemediation-EnableCloudTrailLogFileValidation` Runbook ermöglicht die Validierung von Protokolldateien für deinen AWS CloudTrail Trail.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- TrailName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name oder der Amazon-Ressourcenname (ARN) des Trails, für den Sie die Protokollvalidierung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die Protokollvalidierung für den AWS CloudTrail Trail, den Sie im `TrailName` Parameter angeben.

- `aws:assertAwsResourceProperty`- Überprüft, ob die Protokollvalidierung für Ihren Trail aktiviert ist.

AWS-EnableCloudTrailLogFileValidation

Beschreibung

Das `AWS-EnableCloudTrailLogFileValidation` Runbook ermöglicht die Überprüfung der Protokolldateien für die von Ihnen angegebenen AWS CloudTrail Pfade.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- TrailNames

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste mit den Namen der CloudTrail Pfade, für die Sie die Protokollvalidierung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert die Protokollvalidierung für die AWS CloudTrail Pfade, die Sie im `TrailNames` Parameter angeben.

AWS-QueryCloudTrailLogs

Beschreibung

Das `AWS-QueryCloudTrailLogs` Runbook erstellt eine Amazon Athena Athena-Tabelle aus dem Amazon Simple Storage Service (Amazon S3) -Bucket Ihrer Wahl, der AWS CloudTrail (CloudTrail) -Protokolle enthält. Nach dem Erstellen der Tabelle führt die Automatisierung von Ihnen angegebene SQL-Abfragen aus und löscht dann die Tabelle.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Abfrage

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die SQL-Abfrage, die Sie ausführen möchten.

- SourceBucketPath

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, der die CloudTrail Protokolldateien enthält, die Sie abfragen möchten.

- TableName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der Athena-Tabelle, die durch die Automatisierung erstellt wurde.

  Standard: cloudtrail_logs

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:executeAwsApi`- Erzeugt eine Athena-Tabelle.
- `aws:executeAwsApi`- Führt die Abfragezeichenfolge aus, die Sie im `Query` Parameter angeben.
- `aws:executeScript`- Fragt ab und wartet, bis die Abfrage abgeschlossen ist.
- `aws:executeAwsApi`- Ruft die Ergebnisse der Abfrage ab.
- `aws:executeAwsApi`- Löscht die durch die Automatisierung erstellte Tabelle.

CloudWatch

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon CloudWatch bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-ConfigureCloudWatchOnEC2Instance
- AWS-EnableCWAlarm
- AWSSupport-TroubleshootCloudWatchAgent
- AWSSupport-TroubleshootCloudWatchAlarm

`AWS-ConfigureCloudWatchOnEC2Instance`

Beschreibung

Aktivieren oder deaktivieren Sie die CloudWatch detaillierte Amazon-Überwachung für verwaltete Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der EC2 Amazon-Instance, auf der Sie die CloudWatch Überwachung aktivieren möchten.
- Eigenschaften

  Typ: Zeichenfolge

  Beschreibung: (Optional) Dieser Parameter wird nicht unterstützt. Er ist hier aus Gründen der Abwärtskompatibilität aufgeführt.
- Status

  Gültige Werte: Aktiviert | Deaktiviert

  Beschreibung: (Optional) Gibt an, ob CloudWatch aktiviert oder deaktiviert werden soll.

Standard: Aktiviert

Dokumentschritte

configureCloudWatch - Konfiguriert CloudWatch auf der EC2 Amazon-Instance mit dem angegebenen Status.

Ausgaben

Diese Automatisierung hat keine Ausgabe.

AWS-EnableCWAlarm

Beschreibung

Das `AWS-EnableCWAlarm` Runbook erstellt Amazon CloudWatch (CloudWatch) -Alarme für AWS Ressourcen in Ihrem AWS-Konto , die noch keinen haben. CloudWatch Alarme werden für die folgenden AWS Ressourcen erstellt:

- Amazon Elastic Compute Cloud (Amazon EC2) -Instanzen
- Amazon Elastic Block Store (Amazon EBS)-Volumes
- Buckets für Amazon Simple Storage Service (Amazon S3)
- Cluster des Amazon Relational Database Service (Amazon RDS)

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ComparisonOperator

  Typ: Zeichenfolge

  Gültige Werte: GreaterThanOrEqualToThreshold | GreaterThanThreshold | GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpperThreshol | LessThanLowerThreshold | LessThanOrEqualToThreshold LessThanThreshold

  Beschreibung: (Erforderlich) Die arithmetische Operation, die beim Vergleich der angegebenen Statistik und des Schwellenwerts verwendet werden soll.

- MetricName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Metrik, die dem Alarm zugeordnet ist.

- Intervall

  Typ: Ganzzahl

  Gültige Werte: 10 | 30 | 60 | Ein Vielfaches von 60

  Beschreibung: (Erforderlich) Der Zeitraum in Sekunden, über den die Statistik angewendet wird.

- Ressource ARNs

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste ARNs der Ressourcen, für die ein CloudWatch Alarm erstellt werden soll

- Statistik

  Typ: Zeichenfolge

  Gültige Werte: Durchschnitt | Maximum | Minimum | SampleCount | Summe

Beschreibung: (Erforderlich) Die Statistik für die dem Alarm zugeordnete Metrik.

- Threshold

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Der Wert, der mit der angegebenen Statistik verglichen werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `cloudwatch:PutMetricAlarm`

Dokumentschritte

- `aws:executeScript`- Erstellt einen CloudWatch Alarm entsprechend den in den Runbook-Parametern angegebenen Werten für die Ressourcen, die Sie im `ResourceARNs` Parameter angeben.

Ausgaben

Aktiviert. CWAlarm FailedResources: Eine Zuordnungsliste der Ressourcen, ARNs für die kein CloudWatch Alarm erstellt wurde, und der Grund für den Fehler.

Aktiviert. CWAlarm SuccessfulResources: Eine Liste der Ressourcen, ARNs für die erfolgreich ein CloudWatch Alarm erstellt wurde.

AWSSupport-TroubleshootCloudWatchAgent

Beschreibung

Das AWSSupport-TroubleshootCloudWatchAgentRunbook automatisiert die Fehlerbehebung beim Amazon CloudWatch Agent auf Ihren Amazon Elastic Compute Cloud (Amazon EC2) -Instances. Das Runbook führt diese Fehlerbehebung durch eine Reihe grundlegender und (optionaler) erweiterter Prüfungen durch.

Die grundlegenden Prüfungen umfassen Folgendes:

- Suchen Sie nach einem AWS Identity and Access Management (IAM-) Instanzprofil
- Überprüfen Sie, ob die erforderlichen Amazon CloudWatch Agent IAM-Berechtigungen mit der Amazon EC2 EC2-Instance verknüpft sind

Die erweiterten Prüfungen werden nur durchgeführt, wenn es sich bei der angegebenen Amazon EC2-Instance-ID um eine von Systems Manager verwaltete Instance handelt. Diese erweiterten Prüfungen beinhalten Folgendes:

- Überprüfen Sie den Status des CloudWatch Amazon-Agenten auf der Instance
- Analysieren Sie die Protokolle des CloudWatch Amazon-Agenten auf häufig auftretende Probleme und relevante Schritte zur Fehlerbehebung
- Komprimieren Sie die relevanten Protokolle und Konfigurationsdateien auf der Amazon EC2 EC2-Instance und laden Sie sie optional in einen Amazon Simple Storage Service (Amazon S3) -Bucket Ihrer Wahl hoch
- Führen Sie eine Konnektivitätsprüfung zwischen der Instance und den erforderlichen Endpunkten durch

Important

Wenn der `RunVpcReachabilityAnalyzer` Parameter auf gesetzt ist`true`, bestimmt dieses Runbook, ob das untergeordnete Runbook, aufgerufen werden muss. `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Das untergeordnete Runbook verwendet VPC Reachability Analyzer, was mit Kosten verbunden ist. Weitere Informationen zur Preisgestaltung finden Sie in der Amazon VPC-Preisdokumentation.

Important

Dieses Runbook überprüft nur Ihre IAM-Instance-Profilrolle auf die erforderlichen Berechtigungen. Wenn Sie sich stattdessen auf die in einer `.aws/credentials` Datei definierten Anmeldeinformationen verlassen, sind die Ergebnisse dieses `verifyIamPermissions` Schritts möglicherweise ungenau.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- getInstanceProfile: Überprüft, ob an die bereitgestellte Amazon EC2 EC2-Instance ein IAM-Instance-Profil angehängt ist.
- verifyIamPermissions: Überprüft das mit der Instance verknüpfte Instance-Profil, um festzustellen, ob die erforderlichen IAM-Berechtigungen angewendet wurden.
- getInstanceInformation: Prüft, ob die Instanz über einen aktiven Systems Manager Manager-Agenten verfügt, und ruft den Betriebssystemtyp der Instanz ab.
- getAgentStatus: Prüft den Status des CloudWatch Amazon-Agenten auf der Instance (erweiterte Prüfung).
- AnalyzeLogs/ analyzeLogsWindows: Analysiert und gibt Ergebnisse von Amazon CloudWatch Agent-Protokollen basierend auf dem Betriebssystemtyp aus.
- CollectLogs/ collectLogsWindows: Bündelt und gibt die relevanten Amazon CloudWatch Agent-Fehlerbehebungsdateien basierend auf dem Betriebssystemtyp aus.
- checkEndpointReachability/checkEndpointReachabilityWindows: Prüft je nach Betriebssystemtyp, ob die Instance die erforderlichen Endpunkte erreichen kann.
- analyzeAwsEndpointReachabilityFromEC2: Ruft das untergeordnete Automatisierungs-Runbook auf, um die Erreichbarkeit der ausgewählten Instanz für die erforderlichen Endpunkte zu überprüfen (falls aktiviert).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- ec2: DescribeInstances
- ich bin: GetInstanceProfile
- ich bin: GetRole
- ich bin: ListAttachedRolePolicies
- ich bin: ListRolePolicies
- ich bin: GetRolePolicy
- ich bin: GetPolicy
- ich bin: GetPolicyVersion
- ich bin: SimulatePrincipalPolicy
- ssm: DescribeInstanceInformation
- ssm: SendCommand
- ssm: GetCommandInvocation
- ssm: DescribeInstanceAssociationsStatus
- ssm: StartAutomationExecution

Beispiel für eine Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootCloudWatchAgent`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der ARN der IAM-Rolle, der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - InstanceId (Erforderlich):
     - Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, auf der Sie Fehler beim Amazon CloudWatch Agent beheben möchten.
     - Typ: `AWS::EC2::Instance::Id`
     - Muster zulassen: `^i-[0-9a-f]{8,17}$`
   - S3 UploadBucket (fakultativ):
     - Beschreibung: (Optional) Der Name eines Amazon S3 S3-Buckets zum Hochladen der gesammelten Amazon CloudWatch Agent-Protokolle. Das Amazon EC2 EC2-Instance-Profil muss über die richtigen Berechtigungen verfügen, um Dateien in diesen Bucket hochzuladen. Dies erfordert auch, dass es sich bei der Amazon EC2 EC2-Zielinstanz um eine von Systems Manager verwaltete Instance handelt.
     - Typ: `AWS::S3::Bucket::Name`
     - Muster zulassen: `^$|^[a-z0-9][a-z0-9.-]{1,61}[a-z0-9]$`
     - Standard: `""`
   - S3 BucketOwnerAccountId (fakultativ):

    - Beschreibung: (Optional) Die AWS Kontonummer, der der Amazon S3 S3-Bucket gehört, in den Sie die Amazon CloudWatch Agent-Logs hochladen möchten. Wenn Sie diesen Parameter nicht ändern, verwenden die Runbooks die AWS Konto-ID des Benutzers oder der Rolle, in der die Automatisierung ausgeführt wird.
    - Typ: `String`
    - Muster zulassen: `^\\{\\{ global:ACCOUNT_ID \\}\\}$|^[0-9]{12}$`
    - Standard: `{{ global:ACCOUNT_ID }}`
- EC2Endpunkt überprüfen (optional):
    - Beschreibung: (Optional) Geben Sie an, `true` ob Ihre Agentenkonfiguration die Option verwendet`append_dimensions`, Amazon EC2-Metrikdimensionen an die vom Agenten gesammelten Metriken anzuhängen. Wenn der Amazon CloudWatch Agent verwendet `append_dimensions` wird, benötigt er Konnektivität zum Amazon EC2 EC2-API-Endpunkt, sodass zusätzliche Konnektivitätstests im Rahmen der erweiterten Prüfungen durchgeführt werden.
    - Typ: `String`
    - Zulässige Werte: `[true, false]`
    - Standard: `false`
- RunVpcReachabilityAnalyzer (Fakultativ):
    - Beschreibung: (Optional) Geben Sie `true` an, dass die `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` untergeordnete Automatisierung ausgeführt werden soll, wenn durch die erweiterten Prüfungen ein Netzwerkproblem festgestellt wurde oder wenn es sich bei der angegebenen Instanz-ID nicht um eine verwaltete Instanz handelt.
    - Typ: `Boolean`
    - Standard: `false`
- RetainVpcReachabilityAnalysis (Optional):
    - Beschreibung: (Optional) Nur relevant, wenn `RunVpcReachabilityAnalyzer` es ist`true`. Geben Sie `true` an, dass der Netzwerkerkenntpfad und die zugehörigen Analysen, die von VPC Reachability Analyzer erstellt wurden, beibehalten werden sollen. Standardmäßig werden diese Ressourcen nach erfolgreicher Analyse gelöscht.
    - Typ: `Boolean`
    - Standard: `false`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.

6. Das Dokument führt die folgenden Schritte aus:

- getInstanceProfile:

  Überprüft, ob an die bereitgestellte Amazon EC2 EC2-Instance ein IAM-Instance-Profil angehängt ist.

- branchOnInstanceProfileStatus:

  Verzweigt die Automatisierung, um zu überprüfen, ob die erforderlichen Berechtigungen für das Instance-Profil erforderlich sind, wenn das Instance-Profil an die Instance angehängt ist.

- verifyIamPermissions:

  Überprüft das mit der Instanz verknüpfte Instanzprofil, um festzustellen, ob die erforderlichen IAM-Berechtigungen angewendet wurden.

- getInstanceInformation:

  Überprüft, ob die Instanz über einen aktiven Systems Manager Manager-Agenten verfügt, und ruft den Betriebssystemtyp der Instanz ab.

- branchOnManagedInstanz:

  Verzweigt die Automatisierung, um erweiterte Prüfungen durchzuführen, ob die Instanz verwaltet wird.

- getAgentStatus:

  Prüft den Status des CloudWatch Amazon-Agenten auf der Instance.

- branchOnInstanceOsType:

  Verzweigt die Automatisierung so, dass sie je nach Betriebssystem einen bestimmten collection/ analysis Protokollbefehl ausführt.

- Protokolle analysieren/: analyzeLogsWindows

  Analysiert und gibt Ergebnisse von Amazon CloudWatch Agent-Protokollen basierend auf dem Betriebssystemtyp aus.

- CollectLogs/ collectLogsWindows:

  Bündelt und gibt die relevanten Amazon CloudWatch Agent-Fehlerbehebungsdateien basierend auf dem Betriebssystemtyp aus.

- checkEndpointReachability/checkEndpointReachabilityWindows:

Überprüft, ob die Instanz je nach Betriebssystemtyp die erforderlichen Endpunkte erreichen kann.

- branchOnRunVpcReachabilityAnalyzer:

  Verzweigt die Automatisierung, um eine VPC-Erreichbarkeitsanalyse durchzuführen, falls diese Option aktiviert ist und Netzwerkprobleme erkannt werden.

- Endpunkte generieren:

  Generiert einen Endpunkt zur Überprüfung anhand der Fehler bei erweiterten Prüfungen und dem Wert von. `CheckEC2Endpoint`

- analyzeAwsEndpointReachabilityFromEC2:

  Ruft das Automatisierungs-Runbook `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` auf, um die Erreichbarkeit der ausgewählten Instanz für die erforderlichen Endpunkte zu überprüfen.

- Ergebnisse ausgeben:

  Gibt die Ergebnisse der Schritte zur Ausführung der Automatisierung aus.

7. Nach Abschluss des Vorgangs finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

`AWSSupport-TroubleshootCloudWatchAlarm`

Beschreibung

Das `AWSSupport-TroubleshootCloudWatchAlarm` Runbook hilft bei der Identifizierung und Behebung von Problemen mit falsch konfigurierten oder problematischen Amazon CloudWatch (CloudWatch) -Alarmen. Es nutzt öffentliche AWS APIs und bekannte Alarmauswertungslogik,

um verzögerte oder fehlende Datenpunkte in den überwachten Messwerten zu erkennen, was zu verpassten oder verzögerten Alarmaktionen führen kann. Dieses Runbook bietet einen strukturierten Ansatz zur Untersuchung und Lösung von Problemen im Zusammenhang mit Amazon CloudWatch (CloudWatch) Alarm.

Wie funktioniert es?

Das Runbook `AWSSupport-TroubleshootCloudWatchAlarm` führt die folgenden Schritte aus:

- Überprüft die Amazon CloudWatch (CloudWatch) -Alarmdetails und den Wert des `AlarmTriggerTimestamp` Parameters, um zu überprüfen, ob er innerhalb von 2.592.000 Sekunden (30 Tagen) eintrifft.
- Überprüft, ob ein Alarm auf einer metrischen oder metrischen Berechnung basiert oder ob es sich um einen Alarm mit einem Anomaliedetektor handelt.
- Prüft, ob der Datenstatus eines Alarms unzureichend ist.
- Überprüft, ob die im Alarm verwendete (n) Metrik (en) mit dem `ListMetrics` Wert übereinstimmt.
- Überprüft, ob bei einer Metrik zu einem bestimmten Zeitstempel Datenpunkt (e) fehlten.
- Ruft den neuesten Verlauf für einen bestimmten Zeitstempel ab.
- Prüft, ob aufgrund verzögerter oder verpasster Metrik (en) kein Alarm ausgelöst wurde.
- Prüft, ob die für einen Alarm aktivierten Aktion (en) ausgelöst was/were wurden.
- Generiert einen Bericht zur Fehlerbehebung, in dem alle Diagnoseergebnisse zusammengefasst sind.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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": "*"
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootCloudWatchAlarm`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).

3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Typ: `String`
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - CloudWatchMetricAlarmName(Erforderlich):
     - Typ: `String`
     - Beschreibung: (Erforderlich) Der Name des Amazon CloudWatch (CloudWatch) -Metrikalarms für die Fehlerbehebung.
     - Zulässiges Muster: `^[a-zA-Z0-9.:;,\\-_&() ]{1,255}$`
   - AlarmTriggerTimestamp (Erforderlich):
     - Typ: `String`
     - Beschreibung: (Erforderlich) Der UTC-Zeitstempel, als das Alarmproblem aufgetreten ist. Diese Informationen sind wichtig, um das Problem zu beheben und den Kontext zu verstehen, in dem es aufgetreten ist. Der Zeitstempelwert sollte eine Uhrzeit innerhalb der letzten 30 Tage ab heute sein und das Format `YYYY-MM-DDTHH:mm:ssZ` haben. Beispiel: `2024-10-29T09:04:00Z`
     - Zulässiges Muster: `^(\\d{4})-(\\d{2})-(\\d{2})T(\\d{2}):(\\d{2}):(\\d{2})Z$`
4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - **`VerifyRunbookInputs`**

     Überprüft die Amazon CloudWatch (CloudWatch) -Alarmdetails und den Wert des `AlarmTriggerTimestamp` Parameters, um zu überprüfen, ob er innerhalb von 2.592.000 Sekunden (30 Tagen) eintrifft.
   - **`UpdateSSMDocumentInputChecksVariable`**

     Aktualisiert die Variable `SSMDocumentInputChecks` mit dem Wert `SSMDocumentInputChecks` aus Schritt. `VerifyRunbookInputs`
   - **`BranchOnAlarmIsVerified`**

Verzweigt bei der Überprüfung der Eingaben von Runbook `AlarmTriggerTimestamp` und`CloudWatchAlarmName`.

- **`CheckMetricAlarmType`**

  Überprüft, ob ein Alarm auf einer metrischen oder metrischen Mathematik basiert oder ob es sich um einen Alarm mit einem Anomaliedetektor handelt.

- **`CheckAlarmInInsufficientDataState`**

  Prüft, ob der Datenstatus eines Alarms unzureichend ist.

- **`UpdateInsufficientDataChecksVariable`**

  Aktualisiert die Variable `InsufficientDataChecks` mit dem Wert `InsufficientDataChecks` aus `CheckAlarmInInsufficientDataState` Schritt 1.

- **`BranchOnAlarmHasInsufficientData`**

  Verzweigt nach dem `AlarmHasInsufficientData` Wert aus `CheckAlarmInInsufficientDataState` Schritt, der Standardschritt ist`CheckMetricMismatch`.

- **`CheckMetricMismatch`**

  Überprüft, ob die im Alarm verwendete (n) Metrik (en) mit dem `ListMetrics` Wert übereinstimmt.

- **`UpdateMetricMismatchChecksVariable`**

  Aktualisiert die Variable `MetricMismatchChecks` mit dem Wert `MetricMismatchChecks` aus `CheckMetricMismatch` Schritt.

- **`BranchOnMetricsMatched`**

  Verzweigt nach dem `MetricsMatched` Wert aus `CheckMetricMismatch` Schritt, der Standardschritt ist`CheckMissingDatapoint`.

- **`CheckMissingDatapoint`**

  Überprüft, ob bei einer Metrik zu einem bestimmten Zeitstempel Datenpunkt (e) fehlten.

- **`UpdateMetricMissingDatapointsChecksVariable`**

  Aktualisiert die Variable `MetricMissingDatapointsChecks` mit dem Wert aus Schritt. `MetricMissingDatapointsChecks` `CheckMissingDatapoint`

- **BranchOnMetricMissingDatapoint**

  Verzweigt nach dem `MetricMissingDatapoint` Wert aus `CheckMissingDatapoint` Schritt, der Standardschritt ist`GetAlarmHistoryDetails`.

- **GetAlarmHistoryDetails**

  Ruft den neuesten Verlauf für einen bestimmten Zeitstempel ab.

- **UpdateAlarmHistoryChecksVariable**

  Aktualisiert die Variable `AlarmHistoryChecks` mit dem Wert `AlarmHistoryChecks` aus `GetAlarmHistoryDetails` Schritt.

- **BranchOnAlarmHistoryFound**

  Verzweigt nach dem `AlarmHistoryFound` Wert aus `GetAlarmHistoryDetails` Schritt, der Standardschritt ist`CheckDelayedMetric`.

- **CheckDelayedMetric**

  Prüft, ob aufgrund verzögerter oder verpasster Metrik (en) kein Alarm ausgelöst wurde.

- **UpdateDelayedMetricChecksVariable**

  Aktualisiert die Variable `DelayedMetricChecks` mit dem Wert `DelayedMetricChecks` aus `CheckDelayedMetric` Schritt.

- **BranchOnMetricDelayedAndDatapointsMeetThreshold**

  Verzweigt nach dem Schritt `MetricDelayed` und den `DatapointsMeetThreshold` Werten aus `CheckDelayedMetric` Schritt, der Standardschritt ist`GenerateReport`.

- **CheckActionDelivered**

  Überprüft, ob die für einen Alarm aktivierten Aktion (en) ausgelöst was/were wurden.

- **UpdateActionDeliveredChecksVariable**

  Aktualisiert die Variable `ActionDeliveredChecks` mit der Ausgabe `ActionDeliveredChecks` aus `CheckActionDelivered` Schritt.

- **GenerateReport**

  Kompiliert die Ausgabe der vorherigen Schritte und gibt einen Bericht aus.

7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   - GenerateReport. Bericht

     Ein Bericht über den bereitgestellten Amazon CloudWatch (CloudWatch) -Metrik-Alarm.

```
---------------------------------------------------------------------------------------
               |                     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.
```

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung (Konsole) aus
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

Amazon DocumentDB

AWS Systems Manager Automation bietet vordefinierte Runbooks für Amazon DocumentDB (mit MongoDB-Kompatibilität). Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableDocDbClusterBackupRetentionPeriod

`AWS-EnableDocDbClusterBackupRetentionPeriod`

Beschreibung

Das `AWS-EnableDocDbClusterBackupRetentionPeriod` Runbook ermöglicht eine Aufbewahrungsfrist für Backups für den von Ihnen angegebenen Amazon DocumentDB-Cluster. Diese Funktion legt die Gesamtzahl der Tage fest, für die ein automatisiertes Backup aufbewahrt wird. Um einen Cluster zu ändern, muss sich der Cluster im verfügbaren Status mit dem Engine-Typ befinden`docdb`.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DBClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für den Amazon DocumentDB-Cluster, für den Sie die Aufbewahrungsfrist für Backups aktivieren möchten.
- BackupRetentionPeriod

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Anzahl der Tage, für die automatische Backups aufbewahrt werden. Muss ein Wert zwischen 7 und 35 Tagen sein.
- PreferredBackupWindow

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein täglicher Zeitbereich in UTC (Universal Time Coordinated) im Format hh24:mm-hh24:mm, zum Beispiel 07:14-07:44. Der Wert muss mindestens 30 Minuten betragen und darf nicht mit dem bevorzugten Wartungsfenster in Konflikt geraten.

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

Dokumentschritte

- GetDocDbClusterIdentifier (`aws:executeAwsApi`) — Gibt die Amazon DocumentDB-Cluster-ID unter Verwendung der angegebenen Ressourcen-ID zurück.
- VerifyDocDbEngine (`aws:assertAwsResourceProperty`) — Überprüft, ob der Amazon DocumentDB DocumentDB-Engine-Typ unbeabsichtigte Änderungen `docdb` an anderen Amazon RDS-Engine-Typen verhindern soll.
- VerifyDocDbStatus (`aws:waitAwsResourceProperty`) — Überprüft, ob der Amazon DocumentDB-Clusterstatus lautet. `available`
- ModifyDocDbRetentionPeriod (`aws:executeAwsApi`) — Legt die Aufbewahrungsdauer anhand der angegebenen Werte für den angegebenen Amazon DocumentDB-Cluster fest.
- VerifyDocDbBackupsEnabled (`aws:executeScript`) — Überprüft, ob der Aufbewahrungszeitraum für den Amazon DocumentDB-Cluster und das bevorzugte Backup-Fenster, falls angegeben, erfolgreich festgelegt wurden.

Ausgaben

ModifyDocDbRetentionPeriod. ModifyDbClusterResponse - Antwort vom `ModifyDBCluster` API-Vorgang.

VerifyDocDbBackupsEnabled. VerifyDbClusterBackupsEnabledResponse — Ausgabe des `VerifyDocDbBackupsEnabled` Schritts zur Bestätigung der erfolgreichen Änderung des Amazon DocumentDB-Clusters.

CodeBuild

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS CodeBuild Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with

runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK
- AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

Beschreibung

Das `AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK` Runbook verschlüsselt die Build-Artefakte eines AWS CodeBuild (CodeBuild) -Projekts mithilfe des von Ihnen angegebenen AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels. AWS Config muss an dem Ort aktiviert sein AWS-Region , an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- KMSKeyID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des vom AWS KMS Kunden verwalteten Schlüssels, den Sie zur Verschlüsselung des CodeBuild Projekts verwenden möchten, das Sie im `ProjectId` Parameter angeben.
- ProjectId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des CodeBuild Projekts, dessen Build-Artefakte Sie verschlüsseln möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Ermittelt den CodeBuild Projektnamen aus der Projekt-ID.
- `aws:executeAwsApi`- Aktiviert die Verschlüsselung für das CodeBuild Projekt, das Sie im `ProjectId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft, ob die Verschlüsselung für das CodeBuild Projekt aktiviert wurde.

Ausgaben

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Antwort auf den `UpdateFunctionConfiguration` API-Aufruf.

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

Beschreibung

Das `AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject` Runbook löscht die Umgebungsvariablen `AWS_ACCESS_KEY_ID` und die `AWS_SECRET_ACCESS_KEY` Umgebungsvariablen aus dem von Ihnen AWS CodeBuild angegebenen (CodeBuild) -Projekt. AWS Config muss an dem Ort aktiviert sein AWS-Region , an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des CodeBuild Projekts, dessen Zugriffsschlüssel-Umgebungsvariablen Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Löscht die Zugriffsschlüssel-Umgebungsvariablen für das im CodeBuild Parameter angegebene Projekt. `ResourceId`

AWS CodeDeploy

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS CodeDeploy Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-TroubleshootCodeDeploy

`AWSSupport-TroubleshootCodeDeploy`

Beschreibung

Das `AWSSupport-TroubleshootCodeDeploy` Runbook hilft bei der Diagnose, warum eine AWS CodeDeploy Bereitstellung auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance fehlgeschlagen ist. Das Runbook gibt Schritte aus, die Ihnen helfen, das Problem zu lösen oder weitere Fehler zu beheben. CodeDeploy Es werden auch bewährte Verfahren für bereitgestellt, um Ihnen zu helfen, ähnliche Probleme in future zu vermeiden.

Dieses Runbook kann Ihnen helfen, die folgenden Probleme zu lösen:

- Der CodeDeploy Agent ist nicht installiert oder läuft nicht auf der EC2 Amazon-Instance

- Der EC2 Amazon-Instance ist kein AWS Identity and Access Management (IAM-) Instance-Profil angehängt
- Das mit der Amazon-Instance verknüpfte EC2 IAM-Instance-Profil verfügt nicht über die erforderlichen Amazon Simple Storage Service (Amazon S3) -Berechtigungen
- Eine in Amazon S3 gespeicherte Revision fehlt, oder der verwendete Amazon S3 S3-Bucket befindet sich in einem AWS-Region anderen als der EC2 Amazon-Instance
- Probleme mit der Anwendungsspezifikationsdatei (AppSpec)
- Fehler „Datei ist bereits am Speicherort vorhanden“
- Fehler bei CodeDeploy verwalteten Lebenszyklus-Event-Hooks
- Fehlgeschlagene, vom Kunden verwaltete Lifecycle
- Scale-in-Ereignisse während der Bereitstellung

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DeploymentId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der fehlgeschlagenen Bereitstellung.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der EC2 Amazon-Instance, bei der die Bereitstellung fehlgeschlagen ist.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Überprüft die für die Parameter `DeploymentId` und `InstanceId` angegebenen Werte.
- `aws:executeScript`- Sammelt Informationen von der EC2 Amazon-Instance, z. B. den Status der Instance und Details zum IAM-Instance-Profil.
- `aws:executeScript`— Überprüft die angegebene Bereitstellung und gibt eine Analyse zurück, warum die Bereitstellung fehlgeschlagen ist.

AWS Config

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS Config Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-SetupConfig

AWSSupport-SetupConfig

Beschreibung

Das `AWSSupport-SetupConfig` Runbook erstellt eine AWS Identity and Access Management (IAM) -Serviceverknüpfte Rolle, einen Konfigurationsrekorder, der von unterstützt wird AWS Config, und einen Lieferkanal mit einem Amazon Simple Storage Service (Amazon S3) -Bucket, über den Konfigurations-Snapshots und Konfigurationsverlaufsdateien AWS Config gesendet werden. Wenn Sie Werte für die `AggregatorAccountRegion` Parameter `AggregatorAccountId` und angeben, erstellt das Runbook auch Autorisierungen für die Datenaggregation, um AWS Config Konfigurations- und Compliance-Daten von mehreren und mehreren zu sammeln. AWS-Konten AWS-RegionenWeitere Informationen zum Aggregieren von Daten aus mehreren Konten und Regionen finden Sie unter Datenaggregation für mehrere Konten und Regionen im Entwicklerhandbuch.AWS Config

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AggregatorAccountId

Typ: Zeichenfolge

Beschreibung: (Optional) Die ID der AWS-Konto Stelle, an der ein Aggregator hinzugefügt wird, um die AWS Config Konfigurations- und Compliance-Daten aus mehreren Konten zu aggregieren, und. AWS-Regionen Dieses Konto wird auch vom Aggregator verwendet, um die Quellkonten zu autorisieren.

- AggregatorAccountRegion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Region, in der ein Aggregator hinzugefügt wird, um AWS Config Konfigurations- und Compliance-Daten aus mehreren Konten und Regionen zu aggregieren.

- IncludeGlobalResourcesRegion

  Typ: Zeichenfolge

  Standard: us-east-1

  Beschreibung: (Erforderlich) Um zu vermeiden, dass globale Ressourcendaten in jeder Region aufgezeichnet werden, geben Sie eine Region an, aus der globale Ressourcendaten aufgezeichnet werden sollen.

- Partition

  Typ: Zeichenfolge

  Standard: `aws`

  Beschreibung: (Erforderlich) Die Partition, von der Sie AWS Config Konfigurations- und Kompatibilitätsdaten sammeln möchten.

- S3 BucketName

  Typ: Zeichenfolge

  Standard: `aws-config-delivery-channel`

  Beschreibung: (Optional) Der Name, den Sie für den Amazon S3 S3-Bucket verwenden möchten, der für den Lieferkanal erstellt wurde. Die Konto-ID wird an das Ende des Namens angehängt.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:executeScript`— Erstellt eine serviceverknüpfte IAM-Rolle für den AWS Config Fall, dass noch keine vorhanden ist.
- `aws:executeScript`— Erstellt einen Konfigurationsrekorder, falls noch keiner vorhanden ist.
- `aws:executeScript`- Erstellt einen Amazon S3 S3-Bucket, der vom Lieferkanal verwendet werden kann, falls noch keiner vorhanden ist.
- `aws:executeScript`- Erstellt einen Lieferkanal unter Verwendung der vom Runbook erstellten Ressourcen.
- `aws:executeAwsApi`- Startet den Konfigurationsrekorder.
- `aws:executeScript`- Wenn Sie Werte für die `AggregatorAccountRegion` Parameter `AggregatorAccountId` und angegeben haben, werden Autorisierungen für die Datenaggregation mit mehreren Konten und mehreren Regionen konfiguriert.

Amazon Connect

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Connect bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-AssociatePhoneNumbersToConnectContactFlows
- AWSSupport-CollectAmazonConnectContactFlowLog

AWSSupport-AssociatePhoneNumbersToConnectContactFlows

Beschreibung

Das `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` hilft Ihnen, Telefonnummern mit Kontaktabläufen in Ihrer Amazon Connect Connect-Instance zu verknüpfen. Durch die Bereitstellung der Zuordnungen von Telefonnummern und Kontaktabläufen in einer CSV-Datei (Comma Separated Values) ordnet das Runbook innerhalb von 14,5 Minuten so viele Telefonnummern wie möglich den Kontaktabläufen zu. Das Runbook erstellt eine CSV-Datei mit allen Telefonnummern- und Kontaktflusspaaren, die innerhalb des Zeitlimits nicht zugeordnet werden konnten, sodass Sie sie beim nächsten Lauf eingeben können.

Wie funktioniert es?

Das Runbook `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` hilft Ihnen dabei, Telefonnummern mit Kontaktabläufen in Ihrer Amazon Connect Connect-Instance zu verknüpfen, indem Sie eine CSV-Datei mit Zuordnungsdaten verwenden, die in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert ist. Die CSV-Eingabedatei sollte dem folgenden Format entsprechen, mit `PhoneNumber` Werten im E.164-Format.

Beispiel für die CSV-Eingabedatei

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

Das Automatisierungs-Runbook erstellt außerdem die folgenden Dateien an dem im `DestinationFileBucket` und `DestinationFilePath` angegebenen Zielverzeichnis.

- **`automation:EXECUTION_ID/ResourceIdList.csv`**: Eine temporäre Datei, die die `PhoneNumberId` und `ContactFlowId` -Paare enthält, die für die `AssociatePhoneNumberContactFlow` API erforderlich sind.
- **`automation:EXECUTION_ID/ErrorResourceList.csv`**: Eine Datei, die die Telefonnummern- und Kontaktflusspaare enthält, die aufgrund eines Fehlers nicht verarbeitet werden konnten, z. B. `ResourceNotFoundException` im Format von`PhoneNumber,ContactFlowName,ErrorMessage`.
- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`**: Eine Datei, die die Telefonnummer und die Kontaktflusspaare enthält, die nicht verarbeitet wurden. Das Runbook versucht, innerhalb von 14,5 Minuten (15 Minuten AWS Lambda Funktions-Timeout — 30 Sekunden Puffer) so viele Telefonnummern und Kontaktflüsse wie möglich zu verarbeiten. Falls es einige Telefonnummern/Kontaktflüsse gibt, die aufgrund der Zeitbeschränkung nicht verarbeitet werden konnten, nimmt das Runbook sie in eine CSV-Datei auf, die als Eingabe für die nächste Runbook-Ausführung verwendet werden kann.

Typ des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Wenn ein `LambdaRoleArn` Parameter angegeben wird, erfordert die Rolle die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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"
  }
 ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-AssociatePhoneNumbersToConnectContactFlowsim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ)

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ConnectInstanceId (Erforderlich)

  Die ID Ihrer Amazon Connect Connect-Instance.

- SourceFileBucket (Erforderlich)

  Der Amazon S3 S3-Bucket, in dem die CSV-Datei gespeichert wird, die die Telefonnummern- und Kontaktflusspaare enthält.

- SourceFilePath (Erforderlich)

  Der Amazon S3 S3-Objektschlüssel der CSV-Datei, der die Telefonnummern- und Kontaktflusspaare enthält. Beispiel, `path/to/input.csv`.

- DestinationFileBucket (Erforderlich)

  Der Amazon S3 S3-Bucket, in den die Automatisierung eine Zwischendatei und einen Ergebnisbericht einfügt.

- DestinationFilePath (Fakultativ)

  Der Amazon S3 S3-Objektpfad, `DestinationFileBucket` unter dem eine Zwischendatei und ein Ergebnisbericht gespeichert werden sollen. Wenn Sie beispielsweise angeben`path/to/files/`, werden Dateien unter gespeichert`s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`.

- S3 BucketOwnerAccount (fakultativ)

  Die AWS Kontonummer, der der Amazon S3 S3-Bucket gehört, in den Sie das Contact Flow Log hochladen möchten. Wenn Sie diesen Parameter nicht angeben, verwenden die Runbooks die AWS Konto-ID des Benutzers oder der Rolle, in der die Automatisierung ausgeführt wird.

- S3 BucketOwnerRoleArn (optional)

  Der ARN der IAM-Rolle mit den Berechtigungen zum Abrufen der Einstellungen für den öffentlichen Zugriff auf den Amazon S3 S3-Bucket und das Konto, zur Konfiguration der Bucket-Verschlüsselung, zum Bucket, zum Bucket ACLs, zum Bucket-Richtlinienstatus und zum Hochladen von Objekten in den Bucket. Wenn dieser Parameter nicht angegeben ist, verwendet das Runbook den `AutomationAssumeRole` (falls angegeben) oder den Benutzer, der dieses Runbook startet (falls nicht `AutomationAssumeRole` angegeben). Weitere Informationen finden Sie im Abschnitt „Erforderliche Berechtigungen“ in der Runbook-Beschreibung.

- LambdaRoleArn (Fakultativ)

Der ARN der IAM-Rolle, der es der AWS Lambda Funktion ermöglicht, auf die erforderlichen AWS Dienste und Ressourcen zuzugreifen. Wenn keine Rolle angegeben ist, erstellt diese Automatisierung eine IAM-Rolle für Lambda in Ihrem Konto.

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - CheckConnectInstanceExistance

     Prüft, ob die in bereitgestellte Amazon Connect Connect-Instanz `ConnectInstanceId` existiert.
   - Prüft 3 BucketPublicStatus

     Überprüft, ob die in `SourceFileBucket` und angegebenen Amazon S3 S3-Buckets anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen `DestinationFileBucket` zulassen.
   - CheckSourceFileExistenceAndSize

     Überprüft, ob die in der angegebene CSV-Quelldatei `SourceFilePath` existiert und ob die Dateigröße das Limit von 25 MiB überschreitet.
   - GenerateResourceIdMap

     Lädt die CSV-Quelldatei herunter, die in `SourceFilePath` und identify `PhoneNumberId` und `ContactFlowId` für jede Ressource angegeben ist. Danach wird eine CSV-Datei, die,, und `ContactFlowId` enthält `PhoneNumberPhoneNumberId`, in den Amazon S3 S3-Ziel-Bucket hochgeladen`ContactFlowName`, der in `DestinationFileBucket` angegeben ist. Wenn für eine bestimmte Nummer `PhoneNumberId` nicht identifiziert werden kann, ist das Feld in der CSV-Datei leer.
   - AssociatePhoneNumbersToContactFlows

     Erstellt mithilfe eines AWS CloudFormation Stacks eine AWS Lambda Funktion in Ihrem Konto. Die AWS Lambda Funktion ordnet jede Zahl einem Kontaktfluss zu, der in der in und angegebenen CSV-Quelldatei aufgeführt ist, `SourceFileBucket` `SourceFilePath` und der AWS CloudFormation Stapel ruft die Funktion auf. Die AWS Lambda Funktion ordnet so viele Telefonnummern wie möglich den Kontaktströmen zu, bevor das Zeitlimit überschritten wird (15 Minuten). Die Liste der Telefonnummern und Kontaktabläufe, die aufgrund eines Fehlers nicht verarbeitet werden konnten, wird

hochgeladen`[automation:EXECUTION_ID]/ErrorResourceList.csv`. Diejenigen, die aufgrund einer Überschreitung der maximalen Anzahl von Telefonnummern, die in einer einzigen Ausführung verarbeitet werden können, nicht verarbeitet werden konnten, werden hochgeladen`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. Schlägt dieser Schritt fehl, wird mit dem `DescribeCloudFormationErrorFromStackEvents` Schritt fortgefahren, in dem angegeben wird, warum er aufgrund von AWS CloudFormation Stack-Ereignissen fehlgeschlagen ist.

- WaitForPhoneNumberContactFlowAssociationCompletion

  Wartet, bis die AWS Lambda Funktion, die Telefonnummern Kontaktabläufen zuordnet, erstellt wurde und der AWS CloudFormation Stack seinen Aufruf abgeschlossen hat.

- GenerateReport

  Generiert den Bericht, der die Anzahl der Telefonnummern enthält, die Kontaktabläufen zugeordnet sind, diejenigen, die aufgrund eines Fehlers nicht verarbeitet werden konnten, und die, die aufgrund einer Überschreitung der maximalen Anzahl von Telefonnummern, die in einer einzigen Ausführung verarbeitet werden können, nicht verarbeitet werden konnten. Der Bericht zeigt auch den Standort (Amazon S3 S3-URI und Amazon S3 S3-Konsolen-URL) für `[automation:EXECUTION_ID]/ErrorResourceList.csv` oder`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`, falls zutreffend.

- **`DeleteCloudFormationStack`**

  Löscht den AWS CloudFormation Stack, einschließlich der Lambda-Funktion für das Mapping.

- **`DescribeCloudFormationErrorFromStackEvent`**

  Beschreibt Fehler aus dem AWS CloudFormation Stack des Schritts`AssociatePhoneNumbersToContactFlows`.

7. Wenn Sie den Vorgang abgeschlossen haben, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   - GenerateReport.OutputPayload

     Ausgabe der Verknüpfungen zwischen Telefonnummer und Kontaktfluss. Dieser Bericht enthält die folgenden Informationen:

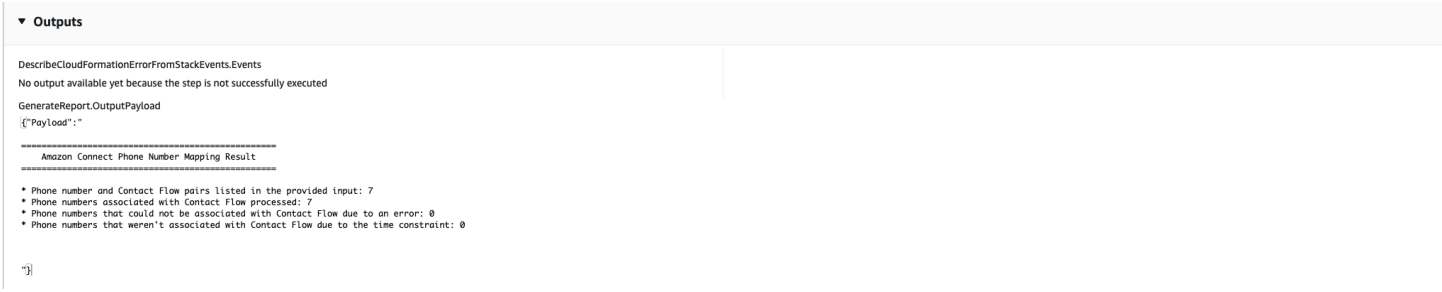
     - Die Anzahl der Telefonnummern- und Kontaktflusspaare, die in der CSV-Eingabedatei aufgeführt sind

- Die Anzahl der Telefonnummern, die mit Kontaktströmen verknüpft sind, wie in der CSV-Eingabedatei angegeben
- Die Anzahl der Telefonnummern, die aufgrund eines Fehlers nicht mit Kontaktabläufen verknüpft werden konnten
- Die Anzahl der Telefonnummern, die aus Zeitgründen nicht mit Kontaktabläufen verknüpft wurden
- Der Speicherort (Amazon S3 S3-URI und Amazon S3 S3-Konsolen-URL) der CSV-Datei, die die Telefonnummern- und Kontaktflusspaare enthält, die aufgrund eines Fehlers nicht verknüpft werden konnten
- Der Speicherort (Amazon S3 S3-URI und Amazon S3 S3-Konsolen-URL) der CSV-Datei, die die Telefonnummern- und Kontaktflusspaare enthält, die aus Zeitgründen nicht verknüpft wurden

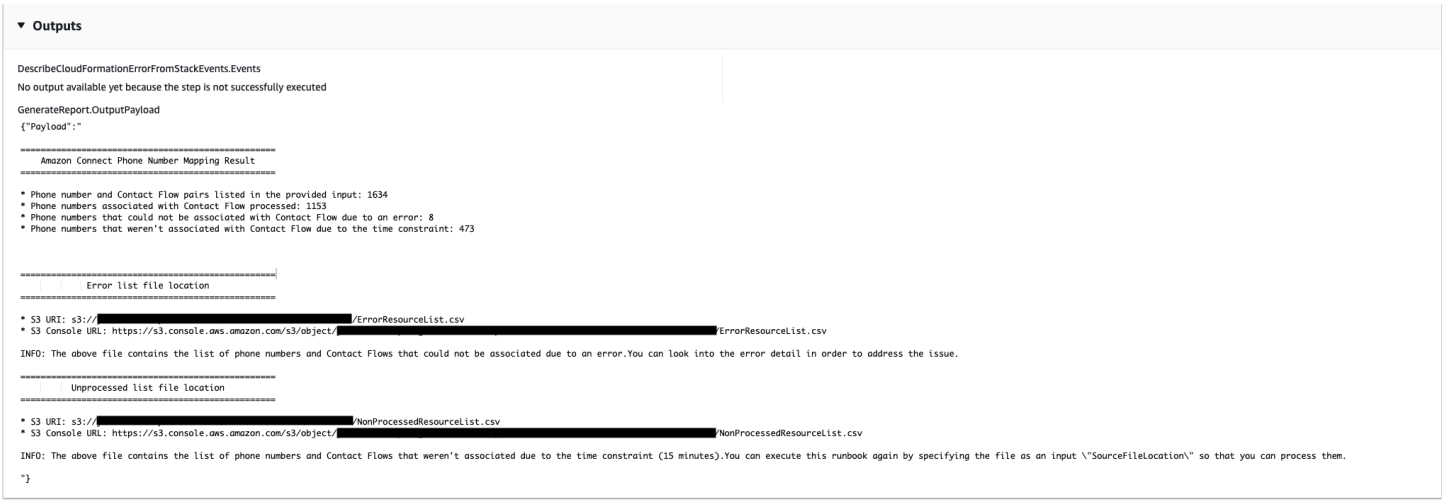
- DescribeCloudFormationErrorFromStackEvents.Ereignisse

  Ausgabe, die AWS CloudFormation Stack-Ereignisse anzeigt, falls der `AssociatePhoneNumbersToContactFlows` Schritt fehlschlägt.

Ausgabe der Ausführung mit einer kleinen Anzahl von Telefonnummern und Kontaktabläufen



Ergebnis der Ausführung mit einer großen Anzahl von Telefonnummern und Kontaktabläufen sowie Telefonnummern, die aufgrund eines Fehlers oder einer Zeitbeschränkung nicht verknüpft wurden



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWSSupport-CollectAmazonConnectContactFlowLog

Beschreibung

Das `AWSSupport-CollectAmazonConnectContactFlowLog` Automations-Runbook wird verwendet, um die Amazon Connect Connect-Kontaktflussprotokolle für eine bestimmte Kontakt-ID zu sammeln. Durch Angabe Ihrer Amazon Connect Connect-Instance-ID und Kontakt-ID durchsucht das Runbook die Kontaktflussprotokolle nach dem Kontakt aus der CloudWatch Amazon-Protokollgruppe und lädt sie in den Amazon Simple Storage Service (Amazon S3) -Bucket hoch, der im Anforderungsparameter angegeben ist. Das Runbook generiert eine Ausgabe, die eine Amazon S3 S3-Konsolen-URL und einen AWS CLI-Befehl bereitstellt, mit dem Sie die Protokolle herunterladen können.

Wie funktioniert es?

Das `AWSSupport-CollectAmazonConnectContactFlowLog` Automation-Runbook hilft dabei, die Amazon Connect Connect-Kontaktflussprotokolle für eine bestimmte Kontakt-ID zu

sammeln, die in der konfigurierten CloudWatch Protokollgruppe gespeichert ist, und lädt sie in einen bestimmten Amazon S3 S3-Bucket hoch. Um die Sicherheit der aus Ihrem Amazon Connect Connect-Kontaktablauf gesammelten Protokolle zu gewährleisten, bewertet die Automatisierung die Amazon S3 S3-Bucket-Konfiguration, um festzustellen, ob der Bucket öffentliche `read` oder `write` Zugriffsberechtigungen gewährt und dem im `S3BucketOwnerAccountId` Parameter angegebenen AWS Konto gehört. Wenn Ihr Amazon S3 S3-Bucket serverseitige Verschlüsselung mit AWS Key Management Service Schlüsseln (SSE-KMS) verwendet, stellen Sie sicher, dass der Benutzer oder die AWS Identity and Access Management (IAM-) Rolle, die diese Automatisierung ausführt, über die `kms:GenerateDataKey` Berechtigungen für den Schlüssel verfügt. AWS KMS Weitere Informationen zu den von Ihrer Amazon Connect Connect-Instance generierten Protokollen finden Sie unter In einer CloudWatch Amazon-Protokollgruppe gespeicherte Flow-Protokolle.

> **Important**
>
> Für die CloudWatch Logs Insights-Abfragen fallen Gebühren an, die auf der abgefragten Datenmenge basieren. Kunden, die über ein kostenloses Kontingent verfügen, wird lediglich die Nutzung berechnet, die die Service-Kontingente überschreitet. Weitere Informationen finden Sie unter Amazon CloudWatch – Preise.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-CollectAmazonConnectContactFlowLogim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - ConnectInstanceId (Erforderlich):

     Die ID Ihrer Amazon Connect Connect-Instance.
   - ContactId (Erforderlich):

     Die ID des Kontakts, für den Sie das Kontaktflussprotokoll erfassen möchten.
   - S3 BucketName (erforderlich):

     Der Amazon S3 S3-Bucket-Name in Ihrem Konto, in das Sie das Kontaktflussprotokoll hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie Parteien, die keinen Zugriff auf die gesammelten Protokolle benötigen, keine unnötigen Lese-/Schreibberechtigungen gewährt.
   - S3 ObjectPrefix (optional):

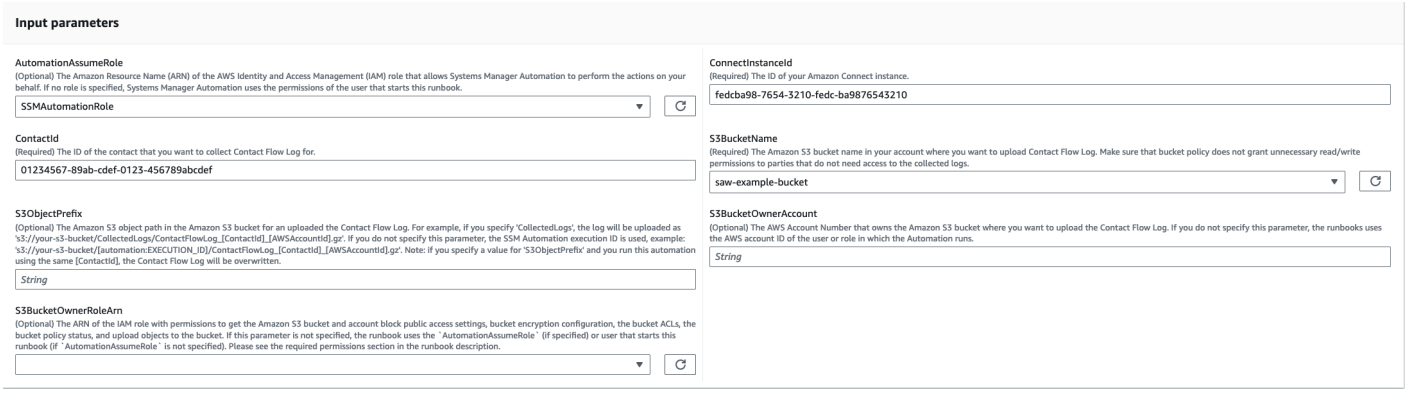
     Der Amazon S3 S3-Objektpfad im Amazon S3 S3-Bucket für ein hochgeladenes Kontaktflussprotokoll. Wenn Sie beispielsweise angeben`CollectedLogs`, wird das Protokoll als hochgeladen`s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId]_[AWSAccountId].gz`. Wenn Sie diesen Parameter nicht angeben, wird die Ausführungs-ID von Systems Manager Automation verwendet, zum Beispiel:`s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz`. Hinweis: Wenn Sie einen Wert für diese Automatisierung angeben `S3ObjectPrefix` und diese Automatisierung mit demselben [ContactId] ausführen, wird das Kontaktflussprotokoll überschrieben.
   - S3 BucketOwnerAccount (optional):

     Die AWS Kontonummer, der der Amazon S3 S3-Bucket gehört, in den Sie das Kontaktflussprotokoll hochladen möchten. Wenn Sie diesen Parameter nicht angeben,

verwendet das Runbook die AWS Konto-ID des Benutzers oder der Rolle, in der die Automatisierung ausgeführt wird.

- S3 BucketOwnerRoleArn (optional):

  Der ARN der IAM-Rolle mit den Berechtigungen zum Abrufen der Einstellungen für den öffentlichen Zugriff auf den Amazon S3 S3-Bucket und das Konto, zur Konfiguration der Bucket-Verschlüsselung, zum Bucket ACLs, zum Bucket-Richtlinienstatus und zum Hochladen von Objekten in den Bucket. Wenn dieser Parameter nicht angegeben ist, verwendet das Runbook den `AutomationAssumeRole` (falls angegeben) oder den Benutzer, der dieses Runbook startet (falls nicht `AutomationAssumeRole` angegeben). Weitere Informationen finden Sie im Abschnitt „Erforderliche Berechtigungen“ in der Runbook-Beschreibung.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - CheckConnectInstanceExistance

     Prüft, ob die in der bereitgestellte Amazon Connect Connect-Instanz `ConnectInstanceId` ist`ACTIVE`.

   - Prüft 3 BucketPublicStatus

     Prüft, ob der im angegebene Amazon S3 S3-Bucket anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen `S3BucketName` zulässt.

   - GenerateLogSearchTimeRange

     Generiert `StartTime` und `EndTime` für den `StartQuery` Schritt, der auf der API basiert `InitiationTimestamp` und von der `DescribeContact` API `LastUpdateTimestamp` zurückgegeben wird. `StartTime`wird eine Stunde davor `InitiationTimestamp` und `EndTime` eine Stunde danach sein`LastUpdateTimestamp`.

- StartQuery

  Startet ein Abfrageprotokoll für die `ContactId` in der CloudWatch Logs-Protokollgruppe angegebene Protokollgruppe, die mit der Amazon Connect Connect-Instance verknüpft ist, bereitgestellt unter`ConnectInstanceId`. Bei Abfragen läuft das Timeout nach 60 Minuten Laufzeit ab. Wenn bei Ihrer Abfrage ein Timeout auftritt, reduzieren Sie den Zeitraum, in dem gesucht wird. Sie können die aktuell ausgeführten Abfragen sowie den Verlauf Ihrer letzten Abfragen in der CloudWatch Konsole einsehen. Weitere Informationen finden Sie unter Laufende Abfragen oder Abfrageverlauf anzeigen.

- WaitForQueryCompletion

  Wartet darauf, dass das CloudWatch Log-Abfrageprotokoll abgeschlossen ist, `ContactId` bis das bereitgestellte Protokoll abgeschlossen ist. Beachten Sie, dass bei der Abfrage nach 60 Minuten Laufzeit ein Timeout auftritt. Wenn bei Ihrer Abfrage ein Timeout auftritt, reduzieren Sie den Zeitraum, in dem gesucht wird. Sie können die aktuell laufenden Abfragen sowie Ihren aktuellen Abfrageverlauf in der Amazon Connect Connect-Konsole einsehen. Weitere Informationen finden Sie unter Laufende Abfragen oder Abfrageverlauf anzeigen.

- UploadContactFlowLog

  Ruft das Abfrageergebnis ab und lädt das Kontaktflussprotokoll in `S3BucketName` den unter angegebenen Amazon S3 S3-Bucket hoch.

- GenerateReport

  Gibt die URL der Amazon S3 S3-Konsole zurück, in die das Kontaktflussprotokoll hochgeladen wurde, und einen AWS CLI-Beispielbefehl, mit dem Sie die Protokolldatei herunterladen können.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   - GenerateReport.OutputPayload

     Ausgabe, die Ihnen mitteilt, dass das Runbook die Kontaktflussprotokolle für den angegebenen Kontakt erfolgreich abgerufen hat. Dieser Bericht enthält auch die URL der Amazon S3 S3-Konsole und einen AWS CLI-Beispielbefehl, mit dem Sie die Protokolldatei herunterladen können.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS Directory Service

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS Directory Service Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-CreateDSManagementInstance
- AWSSupport-TroubleshootADConnectorConnectivity
- AWSSupport-TroubleshootDirectoryTrust

`AWS-CreateDSManagementInstance`

Beschreibung

Das `AWS-CreateDSManagementInstance` Runbook erstellt eine Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instance, mit der Sie Ihr AWS Directory Service Verzeichnis verwalten können. Die Verwaltungsinstanz kann nicht zur Verwaltung von AD Connector Connector-Verzeichnissen verwendet werden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AmiID

  Typ: Zeichenfolge

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

  Beschreibung: (Optional) Amazon Machine Image (AMI) ID, die zum Starten der Instance verwendet werden soll. Standardmäßig wird die Instance mit dem neuesten Microsoft Windows Server 2019 Base AMI gestartet.
- DirectoryId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die Verzeichnis-ID Ihres Directory Service Verzeichnisses.

- IamInstanceProfileName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Profilname der IAM-Instanz. Wenn kein Instance-Profil mit dem Namen Amazon existiert SSMDirectoryServiceInstanceProfileRole, SSMDirectory ServiceInstanceProfileRole wird standardmäßig ein Instance-Profil mit dem Namen Amazon erstellt.

  Standard: Amazon SSMDirectory ServiceInstanceProfileRole

- InstanceType

  Typ: Zeichenfolge

  Standard: t3.medium

  Zulässige Werte:

  - 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

  Beschreibung: (Optional) Typ der Instanz, die gestartet werden soll. Die Standardeinstellung ist t3.medium.

- KeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Schlüsselpaar, das beim Starten der Instance verwendet werden soll. Windows unterstützt keine ED25519 Schlüsselpaare. Standardmäßig wird die Instance ohne ein key pair (NoKeyPair) gestartet.

  Standard: NoKeyPair

- RemoteAccessCidr

  Typ: Zeichenfolge

  Beschreibung: (Optional) Erstellt eine Sicherheitsgruppe mit einem durch CIDR IPs angegebenen Port für RDP (Portbereich 3389) (Standard ist 0.0.0.0/0). Wenn die Sicherheitsgruppe bereits vorhanden ist, wird sie nicht modifiziert, und auch die Regeln werden nicht geändert.

  Standard: 0.0.0.0/0

- SecurityGroupName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Name der Sicherheitsgruppe. Wenn keine Sicherheitsgruppe mit dem Namen Amazon existiert SSMDirectoryServiceSecurityGroup, SSMDirectory ServiceSecurityGroup wird standardmäßig eine Sicherheitsgruppe mit dem Namen Amazon erstellt.

  Standard: Amazon SSMDirectory ServiceSecurityGroup

- Tags (Markierungen)

  Typ: MapList

  Beschreibung: (Optional) Ein Schlüssel-Wert-Paar, das Sie auf die durch die Automatisierung erstellten Ressourcen anwenden möchten.

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

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeAwsApi- Sammelt Details zu dem Verzeichnis, das Sie im DirectoryId Parameter angeben.
- aws:executeAwsApi- Ruft den CIDR-Block der Virtual Private Cloud (VPC) ab, in der das Verzeichnis gestartet wurde.
- aws:executeAwsApi- Erstellt eine Sicherheitsgruppe mit dem Wert, den Sie im SecurityGroupName Parameter angeben.
- aws:executeAwsApi- Erstellt eine eingehende Regel für die neu erstellte Sicherheitsgruppe, die RDP-Verkehr von dem CIDR zulässt, den Sie im Parameter angeben. RemoteAccessCidr
- aws:executeAwsApi- Erstellt eine IAM-Rolle und ein Instanzprofil unter Verwendung des Werts, den Sie im Parameter angeben. IamInstanceProfileName
- aws:executeAwsApi— Startet eine Amazon EC2 EC2-Instance auf der Grundlage der Werte, die Sie in den Runbook-Parametern angeben.
- aws:executeAwsApi- Erstellt ein AWS Systems Manager Dokument, um die neu gestartete Instance Ihrem Verzeichnis hinzuzufügen.
- aws:runCommand- Fügt die neue Instanz Ihrem Verzeichnis hinzu.
- aws:runCommand- Installiert Tools zur Remoteserververwaltung auf der neuen Instanz.

AWSSupport-TroubleshootADConnectorConnectivity

Beschreibung

Das `AWSSupport-TroubleshootADConnectorConnectivity` Runbook überprüft die folgenden Voraussetzungen für einen AD Connector:

- Überprüft, ob der erforderliche Datenverkehr durch die Sicherheitsgruppen- und ACL-Regeln (Network Access Control List) zulässig ist, die Ihrem AD Connector zugeordnet sind.
- Überprüft AWS Systems Manager AWS -Security-Token-Service, ob die VPC-Endpunkte der CloudWatch Amazon-Schnittstelle, und in derselben Virtual Private Cloud (VPC) wie der AD Connector vorhanden sind.

Wenn die Prüfungen der Voraussetzungen erfolgreich abgeschlossen wurden, startet das Runbook zwei Amazon Elastic Compute Cloud (Amazon EC2) Linux t2.micro-Instances in denselben Subnetzen wie Ihr AD Connector. Anschließend werden die Netzwerkkonnektivitätstests mit den Dienstprogrammen und durchgeführt. `netcat` `nslookup`

Führen Sie diese Automatisierung aus (Konsole)

> **Important**
>
> Wenn Sie dieses Runbook verwenden, können zusätzliche Gebühren AWS-Konto für Ihre EC2 Amazon-Instances, Amazon Elastic Block Store-Volumes und Amazon Machine Image (AMI), die während der Automatisierung erstellt wurden. Weitere Informationen finden Sie unter Amazon Elastic Compute Cloud-Preise und Amazon Elastic Block Store-Preise. Wenn der `aws:deletestack` Schritt fehlschlägt, wechseln Sie zur AWS CloudFormation Konsole, um den Stack manuell zu löschen. Der von diesem Runbook erstellte Stack-Name beginnt mit`AWSSupport-TroubleshootADConnectorConnectivity`. Informationen zum Löschen von CloudFormation Stacks finden Sie unter Löschen eines Stacks im AWS CloudFormation Benutzerhandbuch.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DirectoryId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des AD Connector Connector-Verzeichnisses, für das Sie Verbindungsprobleme beheben möchten.
- Ec2 InstanceProfile

  Typ: Zeichenfolge

  Maximale Anzahl an Zeichen: 128

  Beschreibung: (Erforderlich) Der Name des Instanzprofils, das Sie den Instances zuweisen möchten, die zur Durchführung von Konnektivitätstests gestartet werden. Dem von Ihnen angegebenen Instanzprofil müssen die `AmazonSSMManagedInstanceCore` Richtlinie oder gleichwertige Berechtigungen zugewiesen sein.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:assertAwsResourceProperty— Bestätigt, dass es sich bei dem im DirectoryId Parameter angegebenen Verzeichnis um einen AD Connector handelt.
- aws:executeAwsApi- Sammelt Informationen über den AD Connector.
- aws:executeAwsApi- Sammelt Informationen über die Sicherheitsgruppen, die dem AD Connector zugeordnet sind.
- aws:executeAwsApi- Sammelt Informationen über die Netzwerk-ACL-Regeln, die den Subnetzen für den AD Connector zugeordnet sind.
- aws:executeScript— Wertet die AD Connector-Sicherheitsgruppenregeln aus, um sicherzustellen, dass der erforderliche ausgehende Datenverkehr zulässig ist.
- aws:executeScript— Wertet die AD Connector Connector-Netzwerk-ACL-Regeln aus, um sicherzustellen, dass der erforderliche ausgehende und eingehende Netzwerkverkehr zulässig ist.
- aws:executeScript- Überprüft AWS Systems Manager, ob die Endpunkte AWS -Security-Token-Service und die CloudWatch Amazon-Schnittstelle in derselben VPC wie der AD Connector vorhanden sind.

- `aws:executeScript`- Kompiliert die Ausgaben der in den vorherigen Schritten durchgeführten Prüfungen.
- `aws:branch`- Verzweigt die Automatisierung in Abhängigkeit von den Ergebnissen der vorherigen Schritte. Die Automatisierung stoppt hier, wenn die erforderlichen Regeln für ausgehende und eingehende Nachrichten für die Sicherheitsgruppen und das Netzwerk fehlen. ACLs
- `aws:createStack`- Erstellt einen CloudFormation Stack zum Starten von EC2 Amazon-Instances zur Durchführung von Konnektivitätstests.
- `aws:executeAwsApi`- Sammelt die IDs neu gestarteten EC2 Amazon-Instances.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die erste neu gestartete EC2 Amazon-Instance als verwaltet von AWS Systems Manager gemeldet wird.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die zweite neu gestartete EC2 Amazon-Instance als verwaltet von AWS Systems Manager gemeldet wird.
- `aws:runCommand`- Führt Netzwerkverbindungstests für die IP-Adressen des lokalen DNS-Servers von der ersten EC2 Amazon-Instance aus durch.
- `aws:runCommand`- Führt Netzwerkverbindungstests zu den IP-Adressen des lokalen DNS-Servers von der zweiten EC2 Amazon-Instance aus durch.
- `aws:changeInstanceState`- Stoppt die EC2 Amazon-Instances, die für die Konnektivitätstests verwendet wurden.
- `aws:deleteStack`- Löscht den CloudFormation Stapel.
- `aws:executeScript`- Gibt Anweisungen zum manuellen Löschen des CloudFormation Stacks aus, falls die Automatisierung den Stapel nicht löschen kann.

`AWSSupport-TroubleshootDirectoryTrust`

Beschreibung

Das `AWSSupport-TroubleshootDirectoryTrust` Runbook diagnostiziert Probleme bei der Vertrauensbildung zwischen einem AWS Managed Microsoft AD und einem Microsoft Active Directory. Die Automatisierung stellt sicher, dass der Verzeichnistyp Vertrauensstellungen unterstützt, und überprüft dann die zugehörigen Sicherheitsgruppenregeln, Netzwerkzugriffskontrolllisten (Netzwerk ACLs) und Routingtabellen auf mögliche Verbindungsprobleme.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DirectoryId

  Typ: Zeichenfolge

  Zulässiges Muster: ^d- [a-z0-9] {10} $

  Beschreibung: (Erforderlich) Die ID von, mit der die Fehlerbehebung durchgeführt werden soll. AWS Managed Microsoft AD
- RemoteDomainCidrs

  Typ: StringList

  Zulässiges Muster: ^ (([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] [0-9] |1 [0-9] {2} |2 [0-4] [0-9] |25 [0-5]) (\/(3 [0-2] | [1-2] [0-9] | [1-9])) $

  Beschreibung: (Erforderlich) Die CIDR(s) der Remotedomäne, mit der Sie eine Vertrauensstellung einrichten möchten. Sie können mehrere hinzufügen, CIDRs indem Sie kommagetrennte Werte verwenden. Zum Beispiel 172.31.48.0/20, 192.168.1.10/32.
- RemoteDomainName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der vollqualifizierte Domänenname der Remotedomäne, mit der Sie eine Vertrauensstellung einrichten.

- RequiredTrafficACL

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Standard-Portanforderungen für AWS Managed Microsoft AD. In den meisten Fällen sollten Sie den Standardwert nicht ändern.

  Standard: {"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]]},"outbound":{"-1":[[0,65535]]}}

- RequiredTrafficSG

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Standard-Portanforderungen für AWS Managed Microsoft AD. In den meisten Fällen sollten Sie den Standardwert nicht ändern.

  Standard: {"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]]},"outbound":{"-1":[[0,65535]]}}

- TrustId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Vertrauensstellung für die Fehlerbehebung.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ds:DescribeConditionalForwarders`
- `ds:DescribeDirectories`
- `ds:DescribeTrusts`
- `ds:ListIpRoutes`

- `ec2:DescribeNetworkAcls`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`

Dokumentschritte

- `aws:assertAwsResourceProperty`- Bestätigt, dass der Verzeichnistyp ist AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Ruft Informationen über die ab AWS Managed Microsoft AD.
- `aws:branch`- Verzweigt die Automatisierung, wenn ein Wert für den `TrustId` Eingabeparameter angegeben wird.
- `aws:executeAwsApi`- Ruft Informationen über die Vertrauensbeziehung ab.
- `aws:executeAwsApi`- Ruft die bedingten Forwarder-DNS-IP-Adressen für die `RemoteDomainName` ab.
- `aws:executeAwsApi`- Ruft Informationen über IP-Routen ab, die dem AWS Managed Microsoft AD hinzugefügt wurden.
- `aws:executeAwsApi`- Ruft CIDRs die AWS Managed Microsoft AD Subnetze ab.
- `aws:executeAwsApi`- Ruft Informationen über die Sicherheitsgruppen ab, die dem AWS Managed Microsoft AD zugeordnet sind.
- `aws:executeAwsApi`- Ruft Informationen über das Netzwerk ab, das dem ACLs zugeordnet ist AWS Managed Microsoft AD.
- `aws:executeScript`- Bestätigt, dass `RemoteDomainCidrs` es sich um gültige Werte handelt. Bestätigt, dass der AWS Managed Microsoft AD über bedingte Weiterleitungen für die `RemoteDomainCidrs` verfügt und dass die erforderlichen IP-Routen zu den IP-Adressen hinzugefügt wurden, AWS Managed Microsoft AD falls es sich nicht um RFC 1918-IP-Adressen `RemoteDomainCidrs` handelt.
- `aws:executeScript`- Wertet Sicherheitsgruppenregeln aus.
- `aws:executeScript`- Wertet das Netzwerk aus. ACLs

Ausgaben

evalDirectorySecurityGroup.output — Ergebnisse der Bewertung, ob die zugehörigen Sicherheitsgruppenregeln den für die AWS Managed Microsoft AD Vertrauensbildung erforderlichen Datenverkehr zulassen.

evalAclEntries.output — Ergebnisse der Bewertung, ob das ACLs zugeordnete Netzwerk den für die AWS Managed Microsoft AD Vertrauensbildung erforderlichen Datenverkehr zulässt.

evaluateRemoteDomainCIDR.Output — Ergebnisse der Bewertung, ob es sich um gültige Werte handelt. `RemoteDomainCidrs` Bestätigt, dass der AWS Managed Microsoft AD über bedingte Weiterleitungen für die verfügt und dass die erforderlichen IP-Routen zu den IP-Adressen hinzugefügt wurden`RemoteDomainCidrs`, AWS Managed Microsoft AD falls es sich nicht um RFC 1918-IP-Adressen `RemoteDomainCidrs` handelt.

AWS AppSync

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS AppSync Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableAppSyncGraphQLApiLogging

`AWS-EnableAppSyncGraphQLApiLogging`

Beschreibung

Das `AWS-EnableAppSyncGraphQLApiLogging` Runbook ermöglicht die Protokollierung auf Feldebene und die Protokollierung auf Anforderungsebene für die AWS AppSync von Ihnen angegebene GraphQL-API. Das Runbook wendet Änderungen an der angegebenen GraphQL-API an, auch wenn die Protokollierung bereits aktiviert wurde.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ApiId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der API, für die Sie die Protokollierung aktivieren möchten.
- FieldLogLevel

  Typ: Zeichenfolge

  Gültige Werte: ERROR | ALL

  Beschreibung: (Erforderlich) Die Ebene der Feldprotokollierung.
- CloudWatchLogsRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der Servicerolle, die AWS AppSync davon ausgeht, in Amazon CloudWatch Logs zu veröffentlichen.
- ExcludeVerboseContent

  Typ: Boolesch

  Standard: False

  Beschreibung: (Optional) Legt fest, `True` dass Informationen wie Header, Kontext und evaluierte Zuordnungsvorlagen unabhängig von der Protokollierungsstufe ausgeschlossen werden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `appsync:GetGraphqlApi`
- `appsync:UpdateGraphqlApi`
- `iam:PassRole`

Dokumentschritte

- aws: executeAwsApi — Sammelt den Authentifizierungstyp und die Konfigurationsinformationen, die für den primären Authentifizierungstyp relevant sind.
- aws:branch — Verzweigt auf der Grundlage des Authentifizierungstyps.
- aws: executeAwsApi - Aktualisiert die Logging-Konfiguration für die AWS AppSync GraphQL-API auf der Grundlage der Werte, die für die Eingabeparameter des Runbooks angegeben wurden.

Ausgaben

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Antwort auf den `UpdateGraphqlApi` Anruf.
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Antwort auf den `UpdateGraphqlApi` Anruf.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Antwort auf den `UpdateGraphqlApi` Anruf.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Antwort auf den `UpdateGraphqlApi` Anruf.

Amazon Athena

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Athena bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableAthenaWorkGroupEncryptionAtRest

AWS-EnableAthenaWorkGroupEncryptionAtRest

Beschreibung

Das `AWS-EnableAthenaWorkGroupEncryptionAtRest` Runbook aktiviert die Verschlüsselung im Ruhezustand für die von Ihnen angegebene Amazon Athena Athena-Arbeitsgruppe.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- WorkGroup

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Arbeitsgruppe, für die Sie die Verschlüsselung im Ruhezustand aktivieren möchten.

- EncryptionOption

  Typ: Zeichenfolge

  Gültige Werte: SSE_S3 | SSE_KMS | CSE_KMS

  Beschreibung: (Erforderlich) Gibt an, welche Verschlüsselungsoption verwendet wird. Sie können zwischen serverseitiger Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln (SSE_S3), serverseitiger Verschlüsselung mit AWS KMS verwalteten Schlüsseln (SSE_KMS) oder clientseitiger Verschlüsselung mit verwalteten Schlüsseln (CSE_KMS) wählen. AWS KMS
- KmsKeyId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn Sie eine AWS KMS Verschlüsselungsoption verwenden, geben Sie den Schlüssel-ARN, die Schlüssel-ID oder den Schlüsselalias des Schlüssels an, den Sie verwenden möchten.
- EnableMinimumEncryptionConfiguration

  Typ: Boolesch

  Standard: True

  Beschreibung: (Optional) Erzwingt eine minimale Verschlüsselungsstufe für die Arbeitsgruppe für Abfrage- und Berechnungsergebnisse, die in Amazon S3 geschrieben werden. Wenn diese Option aktiviert ist, können Arbeitsgruppenbenutzer nur die vom Administrator festgelegte Mindestverschlüsselungsstufe oder eine höhere Verschlüsselungsstufe festlegen, wenn sie Anfragen einreichen. Diese Einstellung gilt nicht für Spark-fähige Arbeitsgruppen.
- EnforceWorkGroupConfiguration

  Typ: Boolesch

  Standard: True

  Beschreibung: (Optional) Wenn auf gesetzt`True`, überschreiben die Einstellungen für die Arbeitsgruppe die clientseitigen Einstellungen. Wenn auf gesetzt`False`, werden clientseitige Einstellungen verwendet.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- aws:branch — Verzweigt auf der im Parameter angegebenen Verschlüsselungsoption. `EncryptionOption`
- aws: executeAwsApi - In diesem Schritt wird die Athena-Arbeitsgruppe mit der angegebenen Verschlüsselungseinstellung aktualisiert.
- aws: executeAwsApi - Aktualisiert die Athena-Arbeitsgruppe mit der angegebenen Verschlüsselungseinstellung.
- aws: assertAwsResource Property — Überprüft, ob die Verschlüsselung für die Arbeitsgruppe aktiviert wurde.

DynamoDB

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon DynamoDB bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-ChangeDDBRWCapacityMode
- AWS-CreateDynamoDBBackup
- AWS-DeleteDynamoDbBackup
- AWSConfigRemediation-DeleteDynamoDbTable
- AWS-DeleteDynamoDbTableBackups
- AWSConfigRemediation-EnableEncryptionOnDynamoDbTable
- AWSConfigRemediation-EnablePITRForDynamoDbTable

- AWS-EnableDynamoDbAutoscaling
- AWS-RestoreDynamoDBTable

AWS-ChangeDDBRWCapacityMode

Beschreibung

Das `AWS-ChangeDDBRWCapacityMode` Runbook ändert den Lese-/Schreibkapazitätsmodus für eine oder mehrere Amazon DynamoDB-Tabellen (DynamoDB) entweder in den On-Demand-Modus oder in den Bereitstellungsmodus.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- CapacityMode

  Typ: Zeichenfolge

  Gültige Werte: PROVISIONED | PAY_PER_REQUEST

Beschreibung: (Erforderlich) Der gewünschte Lese-/Schreibkapazitätsmodus. Beim Wechsel von On-Demand-Kapazität (pay-per-request) zur bereitgestellten Kapazität müssen die anfänglichen Werte für die bereitgestellte Kapazität festgelegt werden. Die anfänglich bereitgestellten Kapazitätswerte werden auf der Grundlage der verbrauchten Lese- und Schreibkapazität Ihrer Tabelle und der globalen sekundären Indizes in den letzten 30 Minuten geschätzt.

- ReadCapacityUnits

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die maximale Anzahl stark konsistenter Lesevorgänge, die pro Sekunde verbraucht werden, bevor DynamoDB eine Drosselungsausnahme zurückgibt.

- TableNames

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Durch Kommas getrennte Liste von DynamoDB-Tabellennamen, für die der Lese-/Schreibkapazitätsmodus geändert werden soll..

- WriteCapacityUnits

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die maximale Anzahl von Schreibvorgängen, die pro Sekunde verbraucht werden, bevor DynamoDB eine Drosselungsausnahme zurückgibt.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Ändert den Lese-/Schreibkapazitätsmodus für die im Parameter angegebenen DynamoDB-Tabellen. `TableNames`

Ausgaben

Modus DDBRWCapacity ändern. SuccessesTables — Liste der DynamoDB-Tabellennamen, bei denen der Kapazitätsmodus erfolgreich geändert wurde

Modus ändernDDBRWCapacity. FailedTables - Zuordnungsliste der DynamoDB-Tabellennamen, bei denen das Ändern des Kapazitätsmodus fehlgeschlagen ist, und der Grund für den Fehler.

AWS-CreateDynamoDBBackup

Beschreibung

Erstellen Sie eine Sicherungskopie einer Amazon DynamoDB-Tabelle.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BackupName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Name der zu erstellenden Sicherung.

- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Name der DynamoDB-Tabelle.

AWS-DeleteDynamoDbBackup

Beschreibung

Löschen Sie die Sicherung einer Amazon DynamoDB-Tabelle.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- BackupArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ARN der zu löschenden DynamoDB-Tabelle-Sicherung.

AWSConfigRemediation-DeleteDynamoDbTable

Beschreibung

Das `AWSConfigRemediation-DeleteDynamoDbTable` Runbook löscht die von Ihnen angegebene Amazon DynamoDB-Tabelle (DynamoDB).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der DynamoDB-Tabelle, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Löscht die im Parameter angegebene DynamoDB-Tabelle. `TableName`
- `aws:executeScript`— Überprüft, ob die DynamoDB-Tabelle gelöscht wurde.

AWS-DeleteDynamoDbTableBackups

Beschreibung

Löschen Sie DynamoDB-Tabellensicherungen auf der Grundlage von Aufbewahrungstagen oder Anzahl.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

- RetentionCount

  Typ: Zeichenfolge

  Standard: 10

  Beschreibung: (Optional) Die Anzahl der Sicherungen, die für die Tabelle aufbewahrt werden sollen. Wenn mehr als die angegebene Anzahl von Sicherungen vorhanden ist, werden die ältesten Sicherungen jenseits dieser Zahl gelöscht. Entweder RetentionCount oder RetentionDays kann verwendet werden, nicht beide.

- RetentionDays

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Tage für die Aufbewahrung von Sicherungen für die Tabelle. Sicherungen, die älter als die angegebene Zahl von Tagen sind, werden gelöscht. Entweder RetentionCount oder RetentionDays kann verwendet werden, nicht beide.

- TableName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Name der DynamoDB-Tabelle.

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

Beschreibung

Das `AWSConfigRemediation-EnableEncryptionOnDynamoDbTable` Runbook verschlüsselt eine Amazon DynamoDB (DynamoDB) -Tabelle mithilfe des kundenverwalteten Schlüssels AWS Key Management Service (AWS KMS), den Sie für den Parameter angeben. `KMSKeyId`

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- KMSKeyID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des vom Kunden verwalteten Schlüssels, den Sie zum Verschlüsseln der DynamoDB-Tabelle verwenden möchten, die Sie im Parameter angeben. `TableName`
- TableName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name der DynamoDB-Tabelle, die Sie verschlüsseln möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Verschlüsselt die DynamoDB-Tabelle, die Sie im Parameter angeben. `TableName`
- `aws:waitForAwsResourceProperty`— Überprüft, ob die `Enabled` Eigenschaft für die DynamoDB-Tabellen auf gesetzt `SSESpecification` ist. `true`
- `aws:assertAwsResourceProperty`— Überprüft, ob die DynamoDB-Tabelle mit dem vom Kunden verwalteten Schlüssel, der im Parameter angegeben ist, verschlüsselt ist. `KMSKeyId`

`AWSConfigRemediation-EnablePITRForDynamoDbTable`

Beschreibung

Das `AWSConfigRemediation-EnablePITRForDynamoDbTable` Runbook aktiviert die point-in-time Wiederherstellung (PITR) für die von Ihnen angegebene Amazon DynamoDB-Tabelle.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der DynamoDB-Tabelle, für die die point-in-time Wiederherstellung aktiviert werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert die point-in-time Wiederherstellung für die DynamoDB-Tabelle, die Sie im `TableName` Parameter angeben.
- `aws:assertAwsResourceProperty`— Bestätigt, dass die point-in-time Wiederherstellung für die DynamoDB-Tabelle aktiviert ist.

AWS-EnableDynamoDbAutoscaling

Beschreibung

Das `AWS-EnableDynamoDbAutoscaling` Runbook aktiviert Application Auto Scaling für die von Ihnen angegebene Amazon DynamoDB-Tabelle mit bereitgestellter Kapazität. Application Auto Scaling passt die bereitgestellte Durchsatzkapazität dynamisch an die Verkehrsmuster an. Weitere Informationen finden Sie unter Automatisches Verwalten der Durchsatzkapazität mit DynamoDB Auto Scaling im Amazon DynamoDB Developer Guide.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- TableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der DynamoDB-Tabelle, für die Sie Application Auto Scaling aktivieren möchten.
- MinReadCapacity

  Typ: Ganzzahl

Beschreibung: (Erforderlich) Die Mindestanzahl von bereitgestellten Durchsatz-Lesekapazitätseinheiten für die DynamoDB-Tabelle.

- MaxReadCapacity

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die maximale Anzahl von bereitgestellten Durchsatz-Lesekapazitätseinheiten für die DynamoDB-Tabelle.

- TargetReadCapacityUtilization

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die gewünschte Zielauslastung der Lesekapazität. Die Zielauslastung ist der Prozentsatz des verbrauchten bereitgestellten Durchsatzes zu einem bestimmten Zeitpunkt. Sie können die Zielnutzungswerte für Auto Scaling zwischen 20 und 90 Prozent festlegen.

- ReadScaleOutCooldown

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Wartezeit in Sekunden, bis eine vorherige Scale-Out-Aktivität für die Lesekapazität wirksam wird.

- ReadScaleInCooldown

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Zeitspanne in Sekunden nach Abschluss einer Scale-In-Aktivität für die Lesekapazität, bevor eine weitere Scale-In-Aktivität gestartet werden kann.

- MinWriteCapacity

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Mindestanzahl von bereitgestellten Durchsatz-Schreibeinheiten für die DynamoDB-Tabelle.

- MaxWriteCapacity

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die maximale Anzahl von bereitgestellten Durchsatz-Schreibeinheiten für die DynamoDB-Tabelle.

- TargetWriteCapacityUtilization

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die gewünschte Zielauslastung der Schreibkapazität. Die Zielauslastung ist der Prozentsatz des verbrauchten bereitgestellten Durchsatzes zu einem bestimmten Zeitpunkt. Sie können die Zielnutzungswerte für Auto Scaling zwischen 20 und 90 Prozent festlegen.
- WriteScaleOutCooldown

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Wartezeit in Sekunden, bis eine vorherige Scale-Out-Aktivität für die Schreibkapazität wirksam wird.
- WriteScaleInCooldown

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Zeitspanne in Sekunden nach Abschluss einer Scale-In-Aktivität für Schreibkapazität, bevor eine weitere Scale-In-Aktivität gestartet werden kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `application-autoscaling:DescribeScalableTargets`
- `application-autoscaling:DescribeScalingPolicies`
- `application-autoscaling:PutScalingPolicy`
- `application-autoscaling:RegisterScalableTarget`

- RegisterAppAutoscalingTargetWrite (`aws:executeAwsApi`) - Konfiguriert Application Auto Scaling für die von Ihnen angegebene DynamoDB-Tabelle.
- RegisterAppAutoscalingTargetWriteDelay (`aws:sleep`) — Schläft, um API-Drosselung zu vermeiden.

- PutScalingPolicyWrite (`aws:executeAwsApi`) - Konfiguriert die Zielauslastung der Schreibkapazität für die DynamoDB-Tabelle.
- PutScalingPolicyWriteDelay (`aws:sleep`) — Schläft, um API-Drosselung zu vermeiden.
- RegisterAppAutoscalingTargetRead (`aws:executeAwsApi`) - Konfiguriert minimale und maximale Lesekapazitätseinheiten für die DynamoDB-Tabelle.
- RegisterAppAutoscalingTargetReadDelay (`aws:sleep`) — Schläft, um API-Drosselung zu vermeiden.
- PutScalingPolicyRead (`aws:executeAwsApi`) - Konfiguriert die Ziel-Lesekapazitätsauslastung für die DynamoDB-Tabelle.
- VerifyDynamoDbAutoscalingEnabled (`aws:executeScript`) — Überprüft, ob Application Auto Scaling für die DynamoDB-Tabelle gemäß den von Ihnen angegebenen Werten aktiviert ist.

Ausgaben

- RegisterAppAutoscalingTargetWrite. Antwort
- PutScalingPolicyWrite. Antwort
- RegisterAppAutoscalingTargetRead. Antwort
- PutScalingPolicyRead. Antwort
- VerifyDynamoDbAutoscalingEnabled.DynamoDbAutoscalingEnabledResponse

`AWS-RestoreDynamoDBTable`

Beschreibung

Das `AWS-RestoreDynamoDBTable` Runbook stellt die von Ihnen angegebene Amazon DynamoDB-Tabelle mithilfe von point-in-time Recovery (PITR) wieder her.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EnablePointInTimeRecoverAsNeeded

  Typ: Boolesch

  Standard: true

  Beschreibung: (Optional) Legt fest, ob die Automatisierung die point-in-time Wiederherstellung aktiviert, wenn dies für die Wiederherstellung der Tabelle erforderlich ist.
- GlobalSecondaryIndexOverride

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die neuen globalen Sekundärindizes sollen die vorhandenen Sekundärindizes für die neue Tabelle ersetzen.
- LocalSecondaryIndexOverride

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die neuen lokalen Sekundärindizes sollen die vorhandenen Sekundärindizes für die neue Tabelle ersetzen.
- RestoreDateTime

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die point-in-time Wiederherstellung, für die Sie Ihre Tabelle in den letzten 35 Tagen wiederherstellen möchten. Geben Sie Datum und Uhrzeit im folgenden Format an: `DD/MM/YYYY HH:MM:SS`

- SourceTableArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der Tabelle, die Sie wiederherstellen möchten.

- SseSpecificationOverride

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die serverseitigen Verschlüsselungseinstellungen, die für die neue Tabelle verwendet werden sollen.

- TargetTableName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der wiederherzustellenden Tabelle.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Stellt die DynamoDB-Tabelle, die Sie im `TargetTableName` Parameter angegeben haben, mithilfe point-in-time der Wiederherstellung wieder her.

AWS Database Migration Service

AWS Systems Manager Die Automatisierung stellt vordefinierte Runbooks für bereit. AWS Database Migration Service Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-TroubleshootDMSTableErrors
- AWSSupport-TroubleshootDMSEndpointConnection

`AWSSupport-TroubleshootDMSTableErrors`

Beschreibung

Das Runbook zur AWS Systems Manager AWSSuport-TroubleshootDMSTableErrorsAutomatisierung unterstützt Sie bei der Automatisierung der Problembehebung bei Aufgaben zur `Table errors` Datenbankmigration oder bei serverloser Replikation von. AWS Database Migration Service Diese Fehler treten auf, wenn Tabellen durch die Datenbankmigrationsaufgabe oder die im Service erstellte serverlose Replikation nicht vom Quellendpunkt (Quelldatenbank) zum Zielendpunkt (Zieldatenbank) migriert werden können. AWS DMS Dieses Runbook analysiert die Signaturfehlermeldungen aus CloudWatch Protokollen und konzentriert sich dabei insbesondere auf Aufgabenprotokolle für herkömmliche Datenbankmigrationsaufgaben und serverlose Protokolle für serverlose Replikation. Es enthält auch gezielte Vorschläge und Schritte zur Behebung häufiger Fehlermeldungen, die bei Migrationen auftreten. `Table error` AWS DMS

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Ruft Informationen über den bereitgestellten AWS DMS ARN ab, bei dem es sich entweder um eine Datenbankmigrationsaufgabe oder um eine serverlose Replikation handeln kann.
- Überprüft, ob die bereitgestellte AWS DMS Ressource mindestens einmal gestartet wurde, indem der `FreshStartDate` Wert in der DescribeReplicationTasks API-Antwort (für Datenbankmigrationsaufgaben) und DescribeReplications API-Antwort (für serverlose Replikation) überprüft wird. Wenn die Ressource nicht gestartet wurde, gibt die Automatisierung einen Fehler aus.

- Wenn die Ressource gestartet wurde, sucht die Automatisierung anhand von `TableStatistics` Informationen nach den Tabellen in den `TableError` Bundesstaaten. Wenn keine Fehler gefunden werden, beendet die Automatisierung den Workflow, nachdem eine Meldung angezeigt wird, in der bestätigt wird, dass bei der angegebenen Datenbankmigrationsaufgabe oder der serverlosen Replikation keine Tabellenfehler gefunden wurden.
- Wenn Tabellen mit `TableError` Status gefunden werden, prüft die Automatisierung, ob die CloudWatch Protokollierung für die angegebene AWS DMS Ressource aktiviert ist. Wenn die Protokollierung nicht aktiviert ist, beendet die Automatisierung den Workflow, nachdem eine Meldung angezeigt wird, dass die Protokollierung nicht aktiviert ist.

  Hinweis: Es wird davon ausgegangen, dass die CloudWatch Protokollierung aktiviert ist, da sich die Automatisierung auf diese Protokolle stützt, um die Probleme mit den Tabellen im `TableError` Status zu analysieren und zu identifizieren.
- Wenn die Protokollierung aktiviert ist, analysiert die Automatisierung die CloudWatch Protokolle und generiert einen Bericht für jede Tabelle, die sich im `TableError` Status befindet. Der Bericht enthält Vorschläge für häufig auftretende Fehlermeldungen und enthält relevante Fehlerprotokolle, um Probleme zu identifizieren und zu lösen, die eine erfolgreiche Tabellenmigration vom AWS DMS Quellendpunkt zum AWS DMS Zielendpunkt verhindern.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DMSArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ARN der Datenbankmigrationsaufgabe oder der serverlosen Replikation

  Zulässiges Muster: `^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

  Typ: Zeichenfolge

  Beschreibung: (Optional) Dieser Parameter definiert den Beginn des Zeitbereichs für die CloudWatch Protokollanalyse der angegebenen Datenbankmigrationsaufgabe oder der serverlosen Replikation. Sofern angegeben, werden nur Protokolle erfasst und analysiert, die ab diesem bestimmten Zeitpunkt generiert wurden. Bitte beachten Sie, dass die Möglichkeit besteht, dass der Workflow zu einem Timeout führt, wenn der Zeitraum zwischen `startDate` und zu lang `endDate` ist. Der Wert sollte im Datums- und Uhrzeitformat nach ISO 6081 angegeben werden.

  Zulässiges Muster: `^$|^(\\d{4})-(\\d{2})-(\\d{2})T(\\d{2}):(\\d{2}):(\\d{2})\\.(\\d{3})Z$`

- EndTimeRange

  Typ: Zeichenfolge

  Beschreibung: (Optional) Dieser Parameter legt das Ende des Zeitbereichs für die CloudWatch Protokollanalyse der angegebenen Datenbankmigrationsaufgabe oder der serverlosen Replikation fest. Sofern angegeben, werden nur Protokolle erfasst und analysiert, die bis zu diesem bestimmten Zeitpunkt generiert wurden. Bitte beachten Sie, dass die Möglichkeit besteht, dass der Workflow zu einem Timeout führt, wenn der Zeitraum zwischen `startDate` und zu lang `endDate` ist. Der Wert sollte im Datums- und Uhrzeitformat nach ISO 6081 angegeben werden.

Zulässiges Muster: `^$|^(\\d{4})-(\\d{2})-(\\d{2})T(\\d{2}):(\\d{2}):(\\d{2})\\.(\\d{3})Z$`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Beispiel für eine IAM-Richtlinie für die Funktion „Automation Assume Role“

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": "*"
```

```
                }
            ]
        }
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-TroubleshootDMSTableErrorsim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - DMSArn

     ARN der Datenbankmigrationsaufgabe oder der serverlosen Replikation, die Tabellenfehler aufweist.
   - StartTimeRange

     (Optional) Das Datums- und Uhrzeitformat nach ISO 6081, das den Beginn des Zeitbereichs für die Analyse der CloudWatch Protokolle der angegebenen Datenbankmigrationsaufgabe oder der serverlosen Replikation definiert.
   - EndTimeRange

     (Optional) Das Datums- und Uhrzeitformat nach ISO 6081, das das Ende des Zeitbereichs für die Analyse der CloudWatch Protokolle der angegebenen Datenbankmigrationsaufgabe oder der serverlosen Replikation definiert.
4. Wählen Sie unten auf der Seite die Schaltfläche Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:

- validieren DMSInput TypeAndGatherDetails

  Überprüft die angegebene AWS DMS ARN-Eingabe und sammelt die grundlegenden Details der Datenbankmigrationsaufgabe oder der serverlosen Replikation, die in den nächsten Schritten erforderlich sind.

- branchOnTableFehler

  Verzweigt den Workflow auf der Grundlage der Anzahl der Tabellenfehler, die im obigen Schritt gefunden wurden. Wenn die Anzahl größer als 0 ist, fahren Sie mit `branchOnCWLoggingStatus` Schritt - fort. Andernfalls fahren Sie mit `outputNoTableErrors` Schritt - fort.

- outputNoTableFehler

  Gibt eine Meldung aus, die besagt, dass die Tabellenfehler bei der angegebenen Datenbankmigrationsaufgabe oder der serverlosen Replikation nicht gefunden wurden.

- Status „BranchOnCWLogging“

  Verzweigt den Workflow auf der Grundlage des im obigen Schritt ermittelten CloudWatch Protokollierungsstatus. Wenn diese Option aktiviert ist, fahren Sie mit `gatherTableDetails` Schritt — fort. Andernfalls fahren Sie mit `outputNoCWLoggingEnabled` Schritt - fort.

- Ausgang: Nein aktiviert CWLogging

  Gibt eine Meldung aus, dass die CloudWatch Protokollierung in der angegebenen Datenbankmigrationsaufgabe oder der serverlosen Replikation nicht aktiviert ist.

- gatherTableDetails

  Sammelt die `FullLoadEndTime` Zeitstempel der fehlgeschlagenen Tabellen und berechnet die Zeitbereichswerte, um die Protokolle zu analysieren. CloudWatch

- analyzeCloudWatchProtokolle

  Analysiert die in der CloudWatch Protokollgruppe gefundenen Protokolle anhand der Signaturfehlermeldungen und sendet den Bericht an den Benutzer zurück.

7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.

   - Fehler in der Ausgabe von Keine Tabelle gefunden

Wenn bei der bereitgestellten Datenbankmigrationsaufgabe oder der serverlosen Replikation keine Tabellenfehler gefunden wurden, zeigt die Automatisierung die entsprechende Ausgabe an.

- Ausgabe von „Keine CloudWatch Anmeldung aktiviert“

  Wenn die CloudWatch Protokollierung in der bereitgestellten Datenbankmigrationsaufgabe oder der serverlosen Replikation nicht aktiviert ist, zeigt die Automatisierung die entsprechende Ausgabe an und enthält die Schritte zum Aktivieren der Protokollierung.

- Bericht zur Protokollanalyse

  Gibt einen Bericht aus, in dem Tabellen identifiziert werden, `Table error` deren Status entweder durch die bereitgestellte Datenbankmigrationsaufgabe oder durch die serverlose Replikation ermittelt wird. Dabei wird zwischen Fehlertypen unterschieden, die aufgetretenen Fehlermeldungen aufgelistet und gezielte Schritte und Vorschläge zur Problembehebung für jede identifizierte Tabelle bereitgestellt.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWSSupport-TroubleshootDMSEndpointConnection

Beschreibung

Das AWSSupport-TroubleshootDMSEndpointConnectionRunbook hilft bei der Diagnose und Behebung von Verbindungsproblemen zwischen AWS Database Migration Service Replikationsinstanzen und Endpunkten. AWS DMS Die Automatisierung verwendet Reachability Analyzer-Prüfungen, um die Netzwerkkonnektivität zu testen, und analysiert die Netzwerkkonfiguration, um potenzielle Verbindungsprobleme zu identifizieren, die erfolgreiche AWS DMS Migrationen verhindern könnten.

Important

Sie müssen die Konnektivität zwischen der AWS DMS Replikationsinstanz und dem Endpunkt mithilfe der AWS DMS Konsole oder API getestet haben, bevor Sie dieses Runbook ausführen. Wenn Sie die Verbindung nicht getestet haben, tun Sie dies bitte zuerst, andernfalls müssen Sie dieses Runbook möglicherweise erneut ausführen. Sowohl die AWS DMS Replikationsinstanz als auch der Endpunkt müssen für genaue Konnektivitätstests verfügbar sein.

Important

Dieses Runbook erstellt und ruft AWS Lambda Funktionen auf, für die Lambda-Gebühren anfallen. Jeder Analyselauf mit dem Reachability Analyzer ist ebenfalls kostenpflichtig. Preisdetails finden Sie auf der Seite mit den Amazon VPC-Preisen unter dem Tab Netzwerkanalyse und unter AWS Lambda Preise.

Wie funktioniert es?

Das Runbook führt eine systematische Analyse der AWS DMS Konnektivität in den folgenden Phasen durch:

Phase 1: Ressourcenvalidierung und Voraussetzungen

- Endpunktvalidierung: Überprüft, ob der AWS DMS Endpunkt existiert, ruft seine Konfiguration ab (Servername, Port, Engine-Typ) und bestätigt, dass die Datenbank-Engine bei der Fehlerbehebung unterstützt wird.
- Status des Verbindungstests: Ruft mithilfe der AWS DMS `DescribeConnections` API den aktuellen Status des Verbindungstests zwischen der Replikationsinstanz und dem Endpunkt ab, einschließlich aller Fehlermeldungen früherer Testversuche.
- Analyse der Replikationsinstanz: Sammelt Netzwerkkonfigurationsdetails, einschließlich Amazon VPC-ID, Subnetz und Sicherheitsgruppe IDs IDs, und identifiziert das zugehörige Elastic Network Interface (ENI) für die Replikationsinstanz.

Phase 2: DNS-Auflösung und Erkennung von Netzwerkpfaden

- Amazon VPC-basierte DNS-Auflösung: Erstellt eine temporäre Lambda-Funktion innerhalb derselben Amazon VPC wie die Replikationsinstanz, um den Endpunkt-Hostnamen innerhalb des Amazon VPC-Kontextes in seine IP-Adresse aufzulösen und so eine genaue private DNS-Auflösung zu gewährleisten.
- Zielidentifikation: Ermittelt das geeignete Ziel für Reachability Analyzer basierend darauf, ob sich der Endpunkt innerhalb derselben Amazon-VPC (verwendet ENI) oder extern (verwendet aufgelöste IP-Adresse) befindet.
- IPv6 Kompatibilitätsprüfung: Überprüft, ob aufgelöste Adressen vorhanden sind IPv4, da Reachability Analyzer keine Adressen unterstützt. IPv6

Phase 3: Umfassende Netzwerkpfadanalyse

- Ausführung des Reachability Analyzer: Erstellt einen Network Insights-Pfad von der Replikationsinstanz ENI zum Ziel (Endpunkt-ENI oder IP-Adresse) und führt eine umfassende Analyse durch, um die TCP-Konnektivität auf dem angegebenen Port zu testen.
- Mehrschichtige Netzwerkanalyse: Untersucht den gesamten Netzwerkpfad, einschließlich Routentabellen, Sicherheitsgruppen, Netzwerk, Internet-Gateways ACLs, NAT-Gateways, Amazon VPC-Peering-Verbindungen und Transit-Gateways, um Konnektivitätsbarrieren zu identifizieren.
- Generierung detaillierter Erläuterungen: Bei fehlgeschlagener Konnektivität werden spezifische Erläuterungen für jede Netzwerkkomponente bereitgestellt, die den Datenverkehr blockiert, einschließlich genauer Regelnummern, CIDR-Blöcke, Portbereiche und Protokolleinschränkungen.

Phase 4: Berichtserstellung und Bereinigung der Ressourcen

- Umfassende Berichterstattung: Generiert einen detaillierten Bericht mit einer Zusammenfassung der Verbindungstests, Ergebnissen der Netzwerkpfadanalyse und spezifischen Fehlererklärungen mit Anleitungen zur Behebung.
- Ressourcenmanagement: Bereinigt automatisch erstellte Ressourcen (Lambda-Funktion, IAM-Rollen, Network Insights Paths), sofern der PersistReachabilityAnalyzerResults Parameter nicht so eingestellt ist, dass Analyseergebnisse für weitere Untersuchungen aufbewahrt werden.
- Fehlerbehandlung: Stellt spezifische Fehlerberichte für verschiedene Fehlerszenarien bereit, darunter nicht unterstützte Datenbank-Engines, fehlende Ressourcen, DNS-Auflösungsfehler und Berechtigungsprobleme.

Das Runbook unterstützt die Fehlerbehebung bei Konnektivität für mehrere Datenbank-Engines, darunter Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon Neptune, Amazon Redshift, Amazon S3, Azure SQL Database, MySQL, Oracle, PostgreSQL DB2, SQL Server und viele andere.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Optionale IAM-Berechtigungen

Die folgenden Berechtigungen sind nur innerhalb von erforderlich, `AutomationAssumeRole` wenn Sie keinen `LambdaRoleArn` Parameter angeben und möchten, dass die Automatisierung die Lambda-Ausführungsrolle für Sie erstellt:

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

> **Important**
>
> Zusätzlich zu den oben genannten Aktionen `AutomationAssumeRole` sollte Amazon VPCReachability AnalyzerFullAccessPolicy als verwaltete Richtlinie beigefügt sein, damit die Reachability Analyzer-Tests erfolgreich durchgeführt werden.

Beispiel für eine Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootDMSEndpointConnection`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es SSM Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet SSM Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - DmsEndpointArn (Erforderlich)
     - Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des AWS Database Migration Service Endpunkts.
     - Typ: `String`

- Zulässiges Muster: `^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 (Erforderlich)
  - Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Database Migration Service Replikationsinstanz.
  - Typ: `String`
  - Zulässiges Muster: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+:\\d{12}:rep:[A-Z0-9]+$`
- PersistReachabilityAnalyzerResults (Fakultativ)
  - Beschreibung: (Optional) Die Markierung, die darüber informiert, ob die Ergebnisse der Ausführung von Network Insights Analysis beibehalten werden sollen oder nicht.
  - Typ: `Boolean`
  - Zulässige Werte: `[true, false]`
  - Standard: `false`
- LambdaRoleArn (Fakultativ)
  - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS AWS Identity and Access Management (IAM) -Rolle, der der AWS Lambda Funktion den Zugriff auf die erforderlichen AWS Dienste und Ressourcen ermöglicht. Wenn keine Rolle angegeben ist, erstellt diese Systems Manager Manager-Automatisierung eine IAM-Rolle für Lambda in Ihrem Konto.
  - Typ: `AWS::IAM::Role::Arn`
  - Standard: `""`
- Bestätigen (erforderlich)
  - Beschreibung: (Erforderlich) Geben Sie ein, `yes` um zu bestätigen, dass dieses Runbook eine Lambda-Funktion in Ihrem Konto erstellt und, falls keine `LambdaRoleArn` angegeben ist, eine IAM-Rolle erstellt.
  - Typ: `String`
  - Zulässiges Muster: `^[Yy][Ee][Ss]$`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - DescribeEndpointAndCheckEngine:

Ruft die AWS DMS Endpunktkonfiguration ab und überprüft, ob der Datenbank-Engine-Typ für die Fehlerbehebung unterstützt wird. Extrahiert Servername, Port und Engine-Typ aus der Endpunktkonfiguration.

- BranchOnEndpointAndCheckEngineErrors:

  Verzweigt die Automatisierung auf der Grundlage von Fehlern bei der Endpunktvalidierung. Wenn Fehler gefunden werden, generiert die Automatisierung weiterhin einen Fehlerbericht. Andernfalls fährt sie mit den Konnektivitätstests fort.

- GetTestConnectionStatus:

  Ruft mithilfe der `DescribeConnections` API den Verbindungsstatus und die Fehlermeldung für den AWS DMS Endpunkt ab. In diesem Schritt wird geprüft, ob ein Verbindungstest durchgeführt wurde, und alle Fehlermeldungen erfasst.

- BranchOnTestConnectionStatusErrors:

  Verzweigt die Automatisierung auf der Grundlage von Statusfehlern beim Verbindungstest. Wenn Fehler erkannt werden, generiert die Automatisierung einen Fehlerbericht. Andernfalls wird mit der Analyse der Replikationsinstanz fortgefahren.

- DescribeReplicationInstance:

  Ruft Netzwerkkonfigurationsdetails für die AWS DMS Replikationsinstanz ab, einschließlich Amazon VPC-ID, Subnetz und Sicherheitsgruppe IDs IDs, und identifiziert das zugehörige Elastic Network Interface (ENI).

- ValidateResourcePermissions:

  Überprüft, ob die Ausführungsrolle über die erforderlichen Berechtigungen verfügt, um Ressourcen zu bereinigen, die während des Automatisierungsprozesses erstellt werden.

- DNSResolverLambda erstellen:

  Erstellt einen AWS CloudFormation Stack, der eine Lambda-Funktion enthält, die in derselben Amazon-VPC wie die Replikationsinstanz bereitgestellt wird. Diese Funktion wird verwendet, um DNS-Namen innerhalb des Amazon VPC-Kontextes in private IP-Adressen aufzulösen.

- DescribeCloudFormationErrorFromStackEvents:

  Wenn die CloudFormation Stack-Erstellung fehlschlägt, werden in diesem Schritt die Fehler anhand der Stack-Ereignisse beschrieben, um detaillierte Fehlerinformationen für die Fehlerbehebung bereitzustellen.

- Holen Sie sich DNSResolverLambdaName:

  Ruft den Namen der Lambda-Funktion des DNS-Resolvers aus den CloudFormation Stack-Ausgaben ab, um ihn in nachfolgenden Schritten zu verwenden.

- ResolveDmsEndpoint:

  Ruft die Lambda-Funktion auf, um den Hostnamen des AWS DMS Endpunkts innerhalb der Amazon VPC in seine IP-Adresse aufzulösen. Dies gewährleistet eine genaue private DNS-Auflösung und bestätigt die Kompatibilität. IPv4

- BranchOnResolveDmsEndpointErrors:

  Verzweigt die Automatisierung auf der Grundlage von DNS-Auflösungsfehlern. Wenn der Endpunkt nicht aufgelöst werden kann oder zu einer IPv6 Adresse aufgelöst werden kann, generiert die Automatisierung einen Fehlerbericht.

- GetReachabilityAnalyzerTarget:

  Identifiziert das geeignete Ziel für Reachability Analyzer auf der Grundlage der Amazon VPC-Konfiguration und des Endpunktstandorts. Legt fest, ob eine ENI (für dieselben Amazon VPC-Endpunkte) oder eine IP-Adresse (für externe Endpunkte) als Ziel verwendet werden soll.

- GenerateErrors:

  Erstellt einen umfassenden Fehlerbericht, wenn in den vorherigen Schritten Fehler aufgetreten sind. Dazu gehören Details zu Fehlern bei der Endpunktvalidierung, fehlgeschlagenen Verbindungstests oder Problemen mit der DNS-Auflösung sowie spezifische Anleitungen zur Problembehebung.

- GenerateReport:

  Erstellt einen umfassenden Bericht zur Problembehandlung, der den Verbindungsstatus, die Ergebnisse der Netzwerkpfadanalyse mithilfe von Reachability Analyzer, detaillierten Erläuterungen zu Konnektivitätsbarrieren und empfohlenen Maßnahmen zur Behebung enthält.

- CheckStackExists:

  Überprüft, ob der CloudFormation Stapel erfolgreich erstellt wurde und während der Bereinigung gelöscht werden muss. Dieser Schritt gewährleistet ein ordnungsgemäßes Ressourcenmanagement unabhängig vom Erfolg oder Misserfolg der Automatisierung.

- DNSResolverLambda löschen:

Löscht den CloudFormation Stack, der die Lambda-Funktion des DNS-Resolvers und die zugehörigen Ressourcen enthält (sofern nicht `PersistReachabilityAnalyzerResults` auf gesetzt`true`), um sicherzustellen, dass nach Abschluss der Automatisierung keine Restressourcen übrig bleiben.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   - GetTestConnectionStatus.status

     Der aktuelle Status des Verbindungstests zwischen der AWS DMS Replikationsinstanz und dem Endpunkt (z. B. erfolgreich, fehlgeschlagen, getestet).

   - DescribeCloudFormationErrorFromStackEvents. Ereignisse

     Falls die CloudFormation Stack-Erstellung fehlschlägt, enthält diese Ausgabe detaillierte Fehlerereignisse aus dem Stack-Erstellungsprozess, um bei der Diagnose von Problemen mit der Infrastrukturbereitstellung zu helfen.

   - GenerateReport.bericht

     Ein umfassender Bericht zur Fehlerbehebung mit Ergebnissen der Verbindungsanalyse, Ergebnissen des Reachability Analyzer, Netzwerkpfadanalysen, identifizierten spezifischen Konnektivitätsbarrieren und detaillierten Empfehlungen zur Behebung von Problemen mit Links zu relevanter Dokumentation. AWS

   - GenerateErrors. Bericht

     Wenn während des Automatisierungsprozesses Fehler auftreten, enthält diese Ausgabe einen detaillierten Fehlerbericht mit spezifischen Fehlergründen, betroffenen Ressourcen und Anleitungen zur Behebung der Probleme, bevor Sie die Automatisierung erneut versuchen.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

Amazon EBS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Elastic Block Store bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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`

Beschreibung

Das `AWSSupport-AnalyzeEBSResourceUsage` Automation Runbook wird verwendet, um die Ressourcennutzung im Amazon Elastic Block Store (Amazon EBS) zu analysieren. Es analysiert die Datenträgernutzung und identifiziert aufgegebene Volumes, Bilder und Snapshots in einer bestimmten Region. AWS

Wie funktioniert es?

Das Runbook führt die folgenden vier Aufgaben aus:

1. Überprüft, ob ein Amazon Simple Storage Service (Amazon S3) -Bucket existiert, oder erstellt einen neuen Amazon S3-Bucket.
2. Sammelt alle Amazon EBS-Volumes im verfügbaren Status.
3. Sammelt alle Amazon EBS-Snapshots, für die das Quellvolume gelöscht wurde.
4. Sammelt alle Amazon Machine Images (AMIs), die nicht von nicht terminierten Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwendet werden.

Das Runbook generiert CSV-Berichte und speichert sie in einem vom Benutzer bereitgestellten Amazon S3 S3-Bucket. Der bereitgestellte Bucket sollte gemäß den am Ende beschriebenen bewährten AWS Sicherheitsmethoden gesichert werden. Wenn der vom Benutzer angegebene Amazon S3 S3-Bucket nicht im Konto vorhanden ist, erstellt das Runbook einen neuen Amazon S3 S3-Bucket im Namensformat`<User-provided-name>-awssupport-YYYY-MM-DD`, verschlüsselt mit einem benutzerdefinierten Schlüssel AWS Key Management Service (AWS KMS), mit aktivierter Objektversionierung, blockiertem öffentlichen Zugriff und erfordert Anfragen zur Verwendung von SSL/TLS.

Wenn Sie Ihren eigenen Amazon S3 S3-Bucket angeben möchten, stellen Sie bitte sicher, dass er gemäß den folgenden bewährten Methoden konfiguriert ist:

- Sperren Sie den öffentlichen Zugriff auf den Bucket (eingestellt `IsPublic` auf`False`).
- Aktivieren Sie die Amazon S3 S3-Zugriffsprotokollierung.
- Erlauben Sie nur SSL-Anfragen an Ihren Bucket.
- Aktivieren Sie die Objektversionierung.
- Verwenden Sie einen Schlüssel AWS Key Management Service (AWS KMS), um Ihren Bucket zu verschlüsseln.

> **Important**
>
> Bei der Verwendung dieses Runbooks können zusätzliche Gebühren für Ihr Konto für die Erstellung von Amazon S3 S3-Buckets und -Objekten anfallen. Weitere Informationen zu den möglicherweise anfallenden Gebühren finden Sie unter Amazon S3 S3-Preise.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- S3 BucketName

  Typ: `AWS::S3::Bucket::Name`

  Beschreibung: (Erforderlich) Der Amazon S3 S3-Bucket in Ihrem Konto, in den der Bericht hochgeladen werden soll. Stellen Sie sicher, dass die Bucket-Richtlinie Parteien, die keinen Zugriff auf die gesammelten Protokolle benötigen, keine unnötigen read/write Berechtigungen gewährt. Wenn der angegebene Bucket nicht im Konto vorhanden ist, erstellt die Automatisierung einen neuen Bucket in der Region, in der die Automatisierung initiiert wird, mit dem Namensformat`<User-provided-name>-awssupport-YYYY-MM-DD`, verschlüsselt mit einem benutzerdefinierten AWS KMS Schlüssel.

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

- CustomerManagedKmsKeyArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der benutzerdefinierte AWS KMS Schlüssel Amazon Resource Name (ARN) zur Verschlüsselung des neuen Amazon S3 S3-Buckets, der erstellt wird, wenn der angegebene Bucket nicht im Konto vorhanden ist. Die Automatisierung schlägt fehl, wenn versucht wird, einen Bucket ohne Angabe eines benutzerdefinierten AWS KMS Schlüssel-ARN zu erstellen.

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

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Beispielrichtlinie mit mindestens erforderlichen IAM-Berechtigungen zum Ausführen dieses Runbooks:

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": "*"
        }]
    }
```

Anweisungen

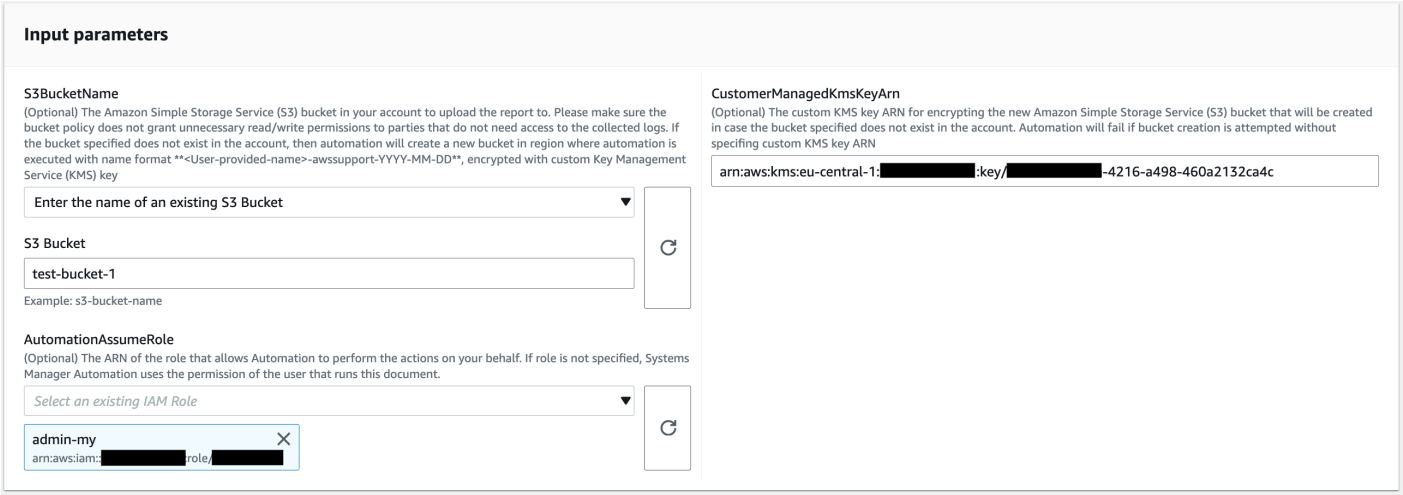
Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-AnalyzeEBSResourceUsagein der AWS Systems Manager Konsole zum.
2. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - S3 BucketName (erforderlich):

     Der Amazon S3 S3-Bucket in Ihrem Konto, in den Sie den Bericht hochladen möchten.
   - CustomerManagedKmsKeyArn(Fakultativ):

     Der benutzerdefinierte AWS KMS Schlüssel Amazon Resource Name (ARN) für die Verschlüsselung des neuen Amazon S3 S3-Buckets, der erstellt wird, wenn der angegebene Bucket nicht im Konto vorhanden ist.



3. Wählen Sie Ausführen aus.
4. Die Automatisierung wird initiiert.
5. Das Automatisierungs-Runbook führt die folgenden Schritte aus:
   - Parallelität prüfen:

     Stellt sicher, dass dieses Runbook in der Region nur einmal initiiert wird. Wenn das Runbook feststellt, dass gerade eine weitere Ausführung ausgeführt wird, gibt es einen Fehler zurück und wird beendet.
   - verifyOrCreateS3-Bucket:

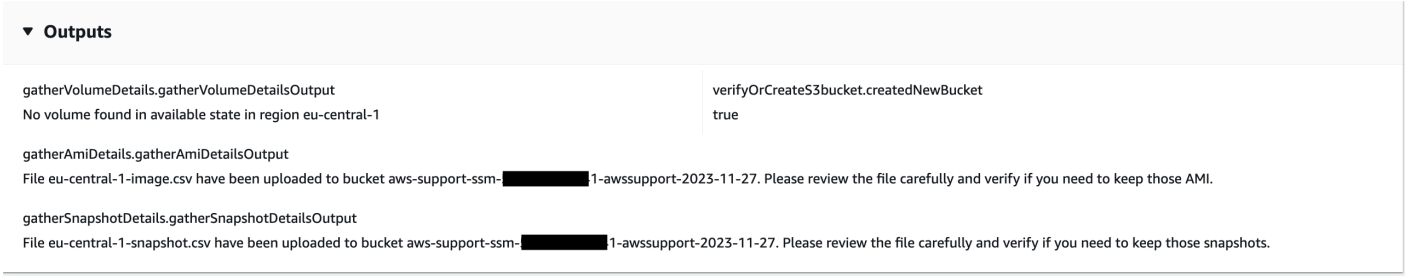
     Überprüft, ob der Amazon S3 S3-Bucket existiert. Wenn nicht, erstellt es einen neuen Amazon S3 S3-Bucket in der Region, in der die Automatisierung initiiert wird, mit dem Namensformat`<User-provided-name>-awssupport-YYYY-MM-DD`, verschlüsselt mit einem benutzerdefinierten AWS KMS Schlüssel.
   - gatherAmiDetails:

     Sucht nach AMIs, die von keiner Amazon EC2 EC2-Instance verwendet werden, generiert den Bericht im Namensformat `<region>-images.csv` und lädt ihn in den Amazon S3 S3-Bucket hoch.
   - gatherVolumeDetails:

     Überprüft Amazon EBS-Volumes im verfügbaren Status, generiert den Bericht im Namensformat `<region>-volume.csv` und lädt ihn in einen Amazon S3 S3-Bucket hoch.
   - gatherSnapshotDetails:

Sucht nach den Amazon EBS-Snapshots der Amazon EBS-Volumes, die bereits gelöscht wurden, generiert den Bericht mit dem Namensformat und lädt ihn in den Amazon `<region>-snapshot.csv` S3 S3-Bucket hoch.

6. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

`AWS-ArchiveEBSSnapshots`

Beschreibung

Das `AWS-ArchiveEBSSnapshots` Runbook hilft Ihnen beim Archivieren von Snapshots für Amazon Elastic Block Store (Amazon EBS) -Volumes, indem es das Tag angibt, das Sie auf Ihre Snapshots angewendet haben. Alternativ können Sie die ID eines Volumes angeben, wenn Ihre Snapshots nicht markiert sind.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Description

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine Beschreibung für den Amazon EBS-Snapshot.

- DryRun

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Beschreibung: (Erforderlich) Überprüft, ob Sie über die erforderlichen Berechtigungen für die Aktion verfügen, ohne die Anfrage tatsächlich zu stellen, und gibt eine Fehlermeldung aus.

- RetentionCount

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Snapshots, die Sie archivieren möchten. Geben Sie keinen Wert für diesen Parameter an, wenn Sie einen Wert für `RetentionDays` angeben.

- RetentionDays

  Typ: Zeichenfolge

Beschreibung: (Optional) Die Anzahl der Snapshots aus früheren Tagen, die Sie archivieren möchten. Geben Sie keinen Wert für diesen Parameter an, wenn Sie einen Wert für `RetentionCount` angeben.

- SnapshotWithTag

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Beschreibung: (Erforderlich) Gibt an, ob die Snapshots, die Sie archivieren möchten, markiert sind.

- TagKey

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Schlüssel des Tags, das den Snapshots zugewiesen ist, die Sie archivieren möchten.

- TagValue

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Wert des Tags, das den Snapshots zugewiesen ist, die Sie archivieren möchten.

- VolumeId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Volumes, dessen Snapshots Sie archivieren möchten. Verwenden Sie diesen Parameter, wenn Ihre Snapshots nicht markiert sind.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

`aws:executeScript`- Archiviert Schnappschüsse mit dem Tag, den Sie mit den `TagValue` Parametern `TagKey` und oder dem `VolumeId` Parameter angeben.

AWS-AttachEBSVolume

Beschreibung

Hängen Sie ein Amazon Elastic Block Store (Amazon EBS) -Volume an eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance an.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Gerät

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Gerätename (z. B. dev/sdh oder xvdh).
- InstanceId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der Instance, der Sie das Volume anfügen möchten.

- VolumeId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Amazon EBS-Volumes. Volume und Instance müssen sich in derselben Availability Zone befinden.

AWSSupport-CalculateEBSPerformanceMetrics

Beschreibung

Das `AWSSupport-CalculateEBSPerformanceMetrics` Runbook hilft bei der Diagnose von Amazon EBS-Leistungsproblemen, indem es Leistungskennzahlen berechnet und in einem CloudWatch Dashboard veröffentlicht. Das Dashboard zeigt die geschätzten durchschnittlichen IOPS und den geschätzten Durchsatz für ein Amazon EBS-Zielvolume oder alle Volumes an, die an die Amazon Elastic Compute Cloud (Amazon EC2) -Zielinstanz angehängt sind. Für Amazon EC2 EC2-Instances werden auch die durchschnittlichen IOPS und der Durchsatz der Instance angezeigt. Das Runbook gibt den Link zum neu erstellten CloudWatch Dashboard aus, in dem die relevanten berechneten Metriken angezeigt werden. CloudWatch Das CloudWatch Dashboard wird in Ihrem Konto mit dem Namen erstellt:`AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>`.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Stellt sicher, dass die angegebenen Zeitstempel gültig sind.
- Überprüft, ob die Ressourcen-ID (Amazon EBS Volume oder Amazon EC2 EC2-Instance) gültig ist.
- Wenn Sie eine Amazon EC2 als ResourceID angeben, wird ein CloudWatch Dashboard mit der tatsächlichen Gesamtsumme IOPS/Throughput für diese Amazon EC2 EC2-Instance und dem Diagramm mit dem geschätzten durchschnittlichen IOPS/Durchsatz für alle Amazon EBS-Volumes erstellt, die an eine Amazon EC2 EC2-Instance angehängt sind.
- Wenn Sie ein Amazon EBS-Volumen als ResourceID angeben, wird ein CloudWatch Dashboard mit dem IOPS/Throughput Diagramm „Geschätzter Durchschnitt“ für dieses Volumen erstellt.
- Wenn nach der Generierung des CloudWatch Dashboards der geschätzte durchschnittliche IOPS oder der geschätzte durchschnittliche Durchsatz höher als der maximale IOPS bzw. der maximale

Durchsatz ist, ist Microbursting für das Volume oder die Volumes möglich, die an eine Amazon EC2 EC2-Instance angehängt sind.

> **Note**
>
> Bei Burst-Volumes (gp2, sc2 und st1) IOPS/throughput sollte das Maximum berücksichtigt werden, bis Sie den Burst-Balance erreicht haben. Wenn das Burst-Balancing vollständig ausgelastet ist, d. h. es Null wird, sollten Sie die Basiskennzahlen berücksichtigen. IOPS/ throughput

> **Important**
>
> Die Erstellung des CloudWatch Dashboards kann zu zusätzlichen Gebühren für Ihr Konto führen. Weitere Informationen finden Sie im CloudWatchAmazon-Preisleitfaden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeVolumes`
- `ec2:DescribeInstances`

- ec2:DescribeInstanceTypes
- cloudwatch:PutDashboard

Beispiel für eine Richtlinie

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": "*"
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-CalculateEBSPerformanceMetricsim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ResourceID (erforderlich):

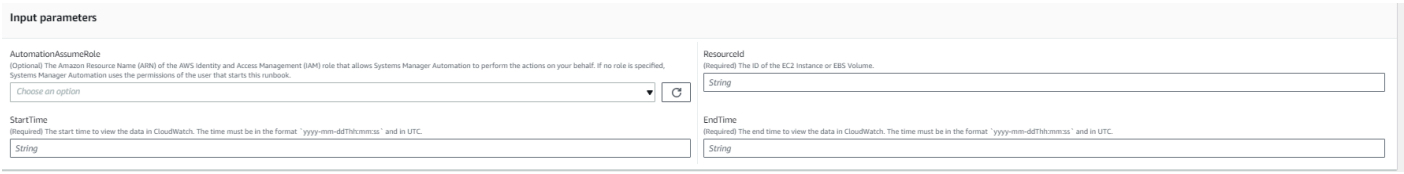
  Die ID der Amazon EC2 EC2-Instance oder des Amazon EBS-Volumes.

- Startzeit (erforderlich):

  Die Startzeit, in der die Daten angezeigt werden sollen CloudWatch. Die Uhrzeit muss im Format `yyyy-mm-ddThh:mm:ss` und in UTC angegeben werden.

- Endzeit (erforderlich):

  Die Endzeit, in der die Daten angezeigt werden sollen CloudWatch. Die Uhrzeit muss im Format `yyyy-mm-ddThh:mm:ss` und in UTC angegeben werden.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:

   - CheckResourceIdAndTimeStamps:

     Überprüft, ob die Endzeit um mindestens eine Minute länger als die Startzeit ist und ob die angegebene Ressource vorhanden ist.

   - CreateCloudWatchDashboard:

     Berechnet die Amazon EBS-Leistung und zeigt ein Diagramm auf der Grundlage Ihrer Ressourcen-ID an. Wenn Sie eine Amazon EBS-Volume-ID für den Parameter Resource ID angeben, erstellt dieses Runbook ein CloudWatch Dashboard mit geschätzten durchschnittlichen IOPS und dem geschätzten durchschnittlichen Durchsatz für das Amazon EBS-Volume. Wenn Sie eine Amazon EC2 EC2-Instance-ID für den Parameter Resource ID angeben, erstellt dieses Runbook ein CloudWatch Dashboard mit den durchschnittlichen Gesamt-IOPS und dem durchschnittlichen Gesamtdurchsatz für die Amazon EC2 EC2-Instance sowie mit den geschätzten durchschnittlichen IOPS und dem geschätzten durchschnittlichen

Durchsatz für alle Amazon EBS-Volumes, die an die Amazon EC2 EC2-Instance angehängt sind.

7. Wenn Sie den Vorgang abgeschlossen haben, finden Sie im Abschnitt Outputs die detaillierten Ergebnisse der Ausführung:

CloudWatch Beispiel-Dashboard für Ressourcen-ID als Amazon EC2 EC2-Instance

CloudWatch > Dashboards >
AWSSupport-i-0[redacted]-EBS-Performance-40121150-f1be-4418-a[redacted]

Autosave: Off

AWSSupport-i-0[redacted]-EBS-Performance-... 2024-01-10T17:44:00 > 2024-01-10T18:07:00 UTC timezone Actions Save

Aggregated Metrics for EC2 Instance i-[redacted]

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

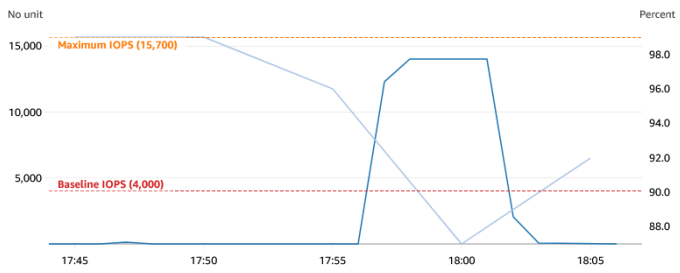
More details on EBS Optimized instances | More details on EBS Volume Types

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

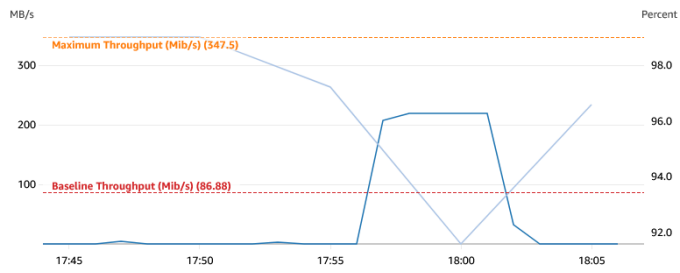
Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	SUM(For All Volumes[(SUM(VolumeReadOps) + SUM(VolumeWriteOps))]) / Period	IOPS
Average Total Throughput	SUM(For All Volumes[(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes))]) / Period / 1024 / 1024	MiB/s

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

Average Total IOPS
2024-01-10 - 2024-01-10



Average Total Throughput
2024-01-10 - 2024-01-10



EBS Volume(s) Metrics

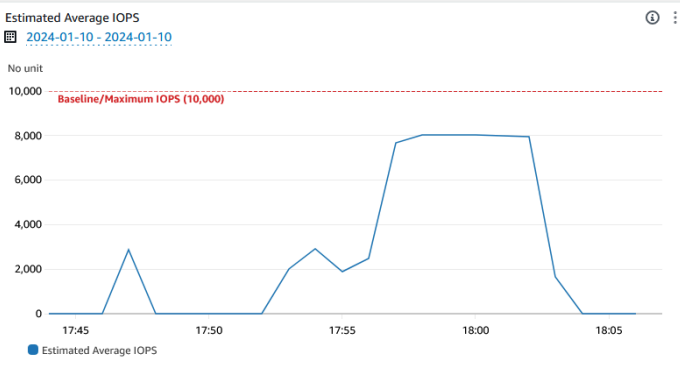
Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	(SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime))	IOPS
Estimated Average Throughput	(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024 / 1024	MiB/s

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

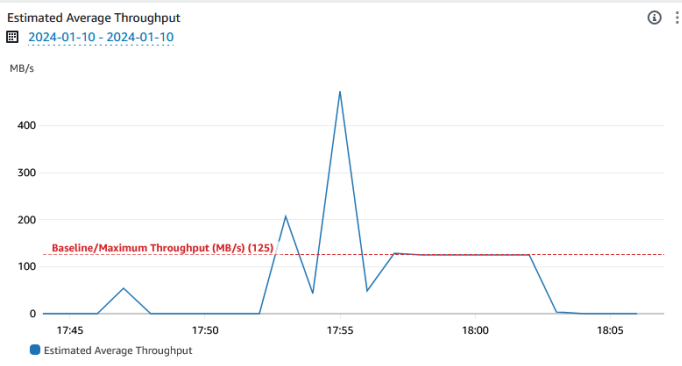
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

Volume: vol[redacted] Type: gp3

Estimated Average IOPS
2024-01-10 - 2024-01-10

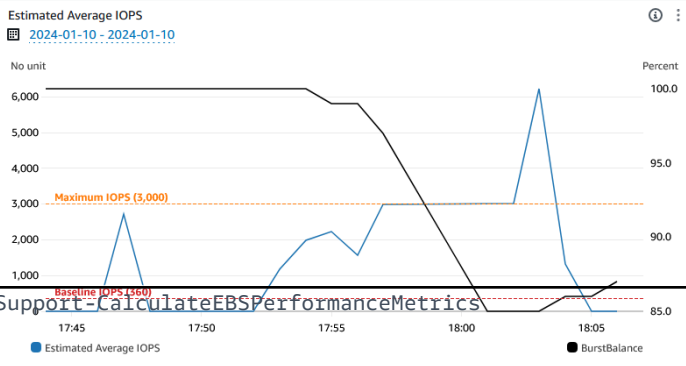


Estimated Average Throughput
2024-01-10 - 2024-01-10

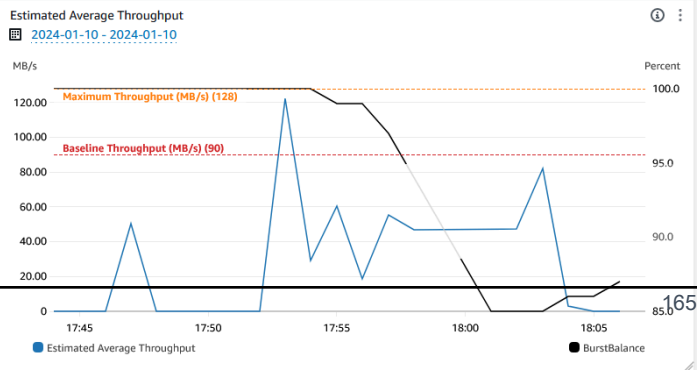


Volume: vol[redacted] | Type: gp2

Estimated Average IOPS
2024-01-10 - 2024-01-10



Estimated Average Throughput
2024-01-10 - 2024-01-10

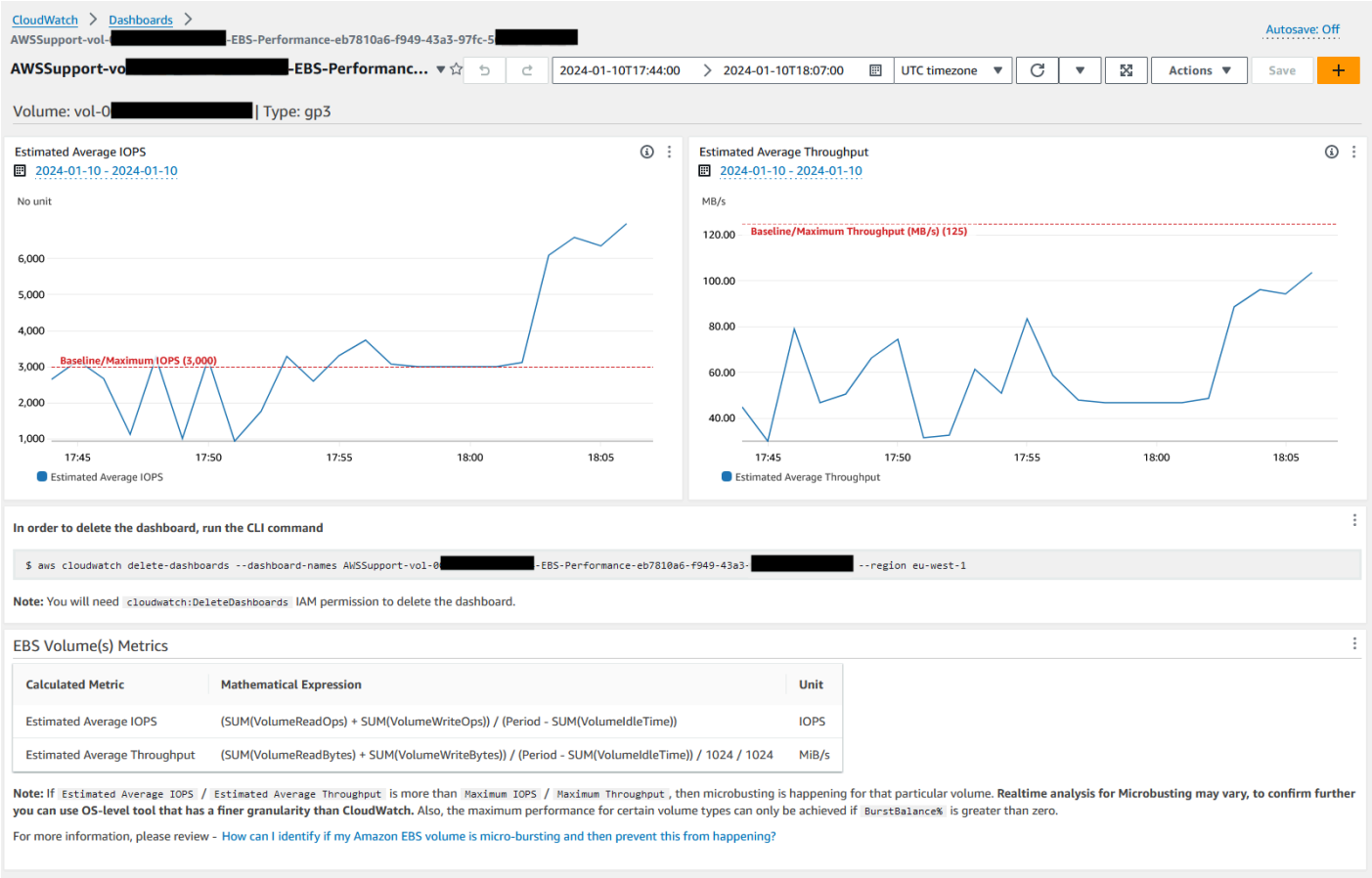


Volume: vol[redacted] | Type: gp3

Estimated Average IOPS

Estimated Average Throughput

CloudWatch Beispiel-Dashboard für Ressourcen-ID als Amazon EBS-Volume-ID



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS Servicedokumentation

- Wie kann ich feststellen, ob mein Amazon EBS-Volume ein Mikro-Bursting ist, und wie kann ich dann verhindern, dass dies passiert?
- Wie verwende ich CloudWatch , um die aggregierten Amazon EBS-Leistungsmetriken für eine EC2-Instance anzuzeigen?

AWS-CopySnapshot

Beschreibung

Kopiert einen point-in-time Snapshot eines Amazon Elastic Block Store (Amazon EBS) -Volumes. Sie können den Snapshot innerhalb derselben Region AWS-Region oder von einer Region in eine andere kopieren. Kopien verschlüsselter Amazon EBS-Snapshots bleiben verschlüsselt. Kopien unverschlüsselter Snapshots bleiben unverschlüsselt. Um einen verschlüsselten Snapshot zu kopieren, der von einem anderen Konto gemeinsam genutzt wurde, benötigen Sie Berechtigungen für den KMS-Schlüssel, der zum Verschlüsseln des Snapshots verwendet wurde. Snapshots, die durch Kopieren eines anderen Snapshot erstellt wurden, haben über eine per Zufallsprinzip ausgewählte Volume-ID, die nicht für andere Zwecke verwendet werden sollte.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Description

  Typ: Zeichenfolge

Beschreibung: (Optional) Eine Beschreibung für den Amazon EBS-Snapshot.

- SnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des zu kopierenden Amazon EBS-Snapshots.

- SourceRegion

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Region, in der sich der Quell-Snapshot zurzeit befindet.

Dokumentschritte

copySnapshot — Kopiert einen Snapshot eines Amazon EBS-Volumes.

Ausgaben

copySnapshot. SnapshotId - Die ID des neuen Snapshots.

AWS-CreateSnapshot

Beschreibung

Erstellen Sie einen Snapshot eines Amazon EBS-Volumes.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Description

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine Beschreibung für den Snapshot.
- VolumeId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Volumes.

AWS-DeleteSnapshot

Beschreibung

Löschen Sie einen Snapshot eines Amazon EBS-Volumes.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- SnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des EBS-Snapshots.

AWSConfigRemediation-DeleteUnusedEBSVolume

Beschreibung

Das `AWSConfigRemediation-DeleteUnusedEBSVolume` Runbook löscht ein unbenutztes Amazon Elastic Block Store (Amazon EBS) -Volume.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- CreateSnapshot

  Typ: Boolescher Wert

  Beschreibung: (Optional) Wenn auf gesetzt`true`, erstellt die Automatisierung einen Snapshot des Amazon EBS-Volumes, bevor es gelöscht wird.

- VolumeId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Amazon EBS-Volumes, das Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`— Überprüft, ob das Amazon EBS-Volume, das Sie im `VolumeId` Parameter angeben, nicht verwendet wird, und erstellt je nach dem Wert, den Sie für den `CreateSnapshot` Parameter wählen, einen Snapshot.
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den `CreateSnapshot` Parameter ausgewählt haben.
- `aws:waitForAwsResourceProperty`- Wartet, bis der Snapshot abgeschlossen ist.

- `aws:executeAwsApi`- Löscht den Snapshot, falls die Snapshot-Erstellung fehlgeschlagen ist.
- `aws:executeAwsApi`- Löscht das Amazon EBS-Volume, das Sie im `VolumeId` Parameter angeben.
- `aws:executeScript`— Überprüft, ob das Amazon EBS-Volume gelöscht wurde.

AWS-DeregisterAMIs

Beschreibung

Das `AWS-DeregisterAMIs` Runbook hilft Ihnen beim Abmelden Amazon Machine Images (AMIs), indem es das Tag angibt, das Sie auf Ihr angewendet haben. AMIs

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DryRun

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

Beschreibung: (Erforderlich) Überprüft, ob Sie über die erforderlichen Berechtigungen für die Aktion verfügen, ohne die Anfrage tatsächlich zu stellen, und gibt eine Fehlermeldung aus.

- RetainNumber

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die NummerAMIs, die Sie behalten möchten. Geben Sie keinen Wert für diesen Parameter an, wenn Sie einen Wert für angeben`Age`.

- Age

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der vorherigen TageAMIs, die Sie behalten möchten. Geben Sie keinen Wert für diesen Parameter an, wenn Sie einen Wert für angeben`RetainNumber`.

- TagKey

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Schlüssel des Tags, das dem Tag zugewiesen istAMIs, dessen Registrierung Sie aufheben möchten.

- TagValue

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Wert des Tags, das dem Tag zugewiesen istAMIs, dessen Registrierung Sie aufheben möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Überprüft die Werte, die Sie für die Runbook-Eingabeparameter angeben.

- `aws:executeAwsApi`- Die Registrierung wird AMIs mit dem Tag aufgehoben, das Sie mit den Parametern und angegeben haben. `TagKey` `TagValue`

`AWS-DetachEBSVolume`

Beschreibung

Trennen Sie ein Amazon EBS-Volume von einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der von Lambda übernommenen Rolle
- VolumeId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID des EBS-Volumes. Volume und Instance müssen sich in derselben Availability Zone befinden.

AWSConfigRemediation-EnableEbsEncryptionByDefault

Beschreibung

Das `AWSConfigRemediation-EnableEbsEncryptionByDefault` Runbook ermöglicht die Verschlüsselung auf allen neuen Amazon Elastic Block Store (Amazon EBS) -Volumes in AWS-Region dem AWS-Konto und auf dem Sie die Automatisierung ausführen. Volumes, die vor der Ausführung der Automatisierung erstellt wurden, sind nicht verschlüsselt.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert die standardmäßige Amazon EBS-Verschlüsselungseinstellung für das aktuelle Konto und die Region.
- `aws:assertAwsResourceProperty`— Überprüft, ob die standardmäßige Amazon EBS-Verschlüsselungseinstellung aktiviert wurde.

AWS-ExtendEbsVolume

Beschreibung

Das `AWS-ExtendEbsVolume` Runbook vergrößert ein Amazon EBS-Volume und erweitert das Dateisystem. Diese Automatisierung unterstützt die `ext4` Dateisysteme `xfs` und.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DriveLetter

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Buchstabe des Laufwerks, dessen Dateisystem Sie erweitern möchten. Dieser Parameter ist für Windows Instanzen erforderlich.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Amazon EC2 EC2-Instance, an die das Amazon EBS-Volume angehängt ist, das Sie erweitern möchten.

- KeepSnapshot

  Typ: Boolescher Wert

  Standard: true

  Beschreibung: (Optional) Legt fest, ob der vor der Erhöhung der Größe Ihres Amazon EBS-Volumes erstellte Snapshot beibehalten werden soll.

- MountPoint

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Bereitstellungspunkt des Laufwerks, dessen Dateisystem Sie erweitern möchten. Dieser Parameter ist für Linux-Instances erforderlich.

- SizeGib

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Größe in GiB, auf die Sie Ihr Amazon EBS-Volume ändern möchten.

- VolumeId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID des EBS-Volumes, das Sie erweitern möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:CreateSnapshot`
- `ec2:CreateTags`
- `ec2:DeleteSnapshot`
- `ec2:DescribeVolumes`
- `ec2:ModifyVolume`
- `ssm:DescribeInstanceInformation`
- `ssm:GetCommandInvocation`
- `ssm:SendCommand`

Dokumentschritte

- `aws:executeScript`- Erhöht die Größe des Volumes auf den Wert, den Sie im `VolumeId` Parameter angeben, und erweitert das Dateisystem.

AWSSupport-ModifyEBSSnapshotPermission

Beschreibung

Das `AWSSupport-ModifyEBSSnapshotPermission` Runbook hilft Ihnen, die Berechtigungen für mehrere Amazon Elastic Block Store (Amazon EBS) -Snapshots zu ändern. Mit diesem Runbook können Sie Schnappschüsse erstellen `Public` oder `Private` diese mit anderen teilen. AWS-Konten Mit einem Standard-KMS-Schlüssel verschlüsselte Snapshots können nicht mit anderen Konten geteilt werden, die dieses Runbook verwenden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AccountIds

  Typ: StringList

  Standard: keiner

  Beschreibung: (Optional) Die IDs Konten, mit denen Sie Snapshots teilen möchten. Dieser Parameter ist erforderlich, wenn Sie `No` den Wert des `Private` Parameters eingeben.
- AccountPermissionOperation

  Typ: Zeichenfolge

  Gültige Werte: hinzufügen | entfernen

  Standard: keiner

  Beschreibung: (Optional) Die Art des auszuführenden Vorgangs.
- Privat

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

Beschreibung: (Erforderlich) Geben Sie No den Wert ein, wenn Sie Snapshots mit bestimmten Konten teilen möchten.

- SnapshotIds

  Typ: StringList

  Beschreibung: (Erforderlich) Die IDs Amazon EBS-Snapshots, deren Berechtigungen Sie ändern möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

1. `aws:executeScript`- Überprüft die im IDs Parameter angegebenen Schnappschüsse. `SnapshotIds` Nach der Überprüfung von sucht das IDs Skript nach verschlüsselten Snapshots und gibt eine Liste aus, falls welche gefunden wurden.
2. `aws:branch`- Verzweigt die Automatisierung auf der Grundlage des Werts, den Sie für den `Private` Parameter eingeben.
3. `aws:executeScript`- Ändert die Berechtigungen der angegebenen Snapshots, um sie für die angegebenen Konten freizugeben.
4. `aws:executeScript`- Ändert die Berechtigungen der Snapshots, um sie von zu zu ändern. `Public` `Private`

Ausgaben

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts. Ergebnis

MakePrivate. Ergebnis

MakePrivate. Befehle

AWSConfigRemediation-ModifyEBSVolumeType

Beschreibung

Das `AWSConfigRemediation-ModifyEBSVolumeType` Runbook ändert den Volumetyp eines Amazon Elastic Block Store (Amazon EBS) -Volumes. Nachdem der Volumetyp geändert wurde, wechselt das Volume in einen Status. `optimizing` Informationen zur Überwachung des Fortschritts von Volumenänderungen finden Sie unter Überwachen des Fortschritts von Volumenänderungen im Amazon EC2 EC2-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- EbsVolumeId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Amazon EBS-Volumes, das Sie ändern möchten.

- EbsVolumeType

  Typ: Zeichenfolge

  Gültige Werte: standard | io1 | io2 | gp2 | gp3 | sc1 | st1

  Beschreibung: Der Volumetyp, auf den Sie das Amazon EBS-Volume ändern möchten. Informationen zu Amazon EBS-Volumetypen finden Sie unter Amazon EBS-Volumetypen im Amazon EC2 EC2-Benutzerhandbuch.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:waitForAwsResourceProperty`- Überprüft, ob der Status des Volumes oder ist`available`. `in-use`
- `aws:executeAwsApi`- Ändert das Amazon EBS-Volume, das Sie im `EbsVolumeId` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Überprüft, ob der Typ des Volumes auf den Wert geändert wurde, den Sie im Parameter angegeben haben. `EbsVolumeType`

Amazon EC2

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Elastic Compute Cloud bereit. Runbooks für Amazon Elastic Block Store befinden sich im Amazon EBS Abschnitt der Runbook-Referenz. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-ASGEnterStandby
- AWS-ASGExitStandby
- AWS-CreateImage
- 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

Beschreibung

Ändern Sie den Standby-Status einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance in einer Auto Scaling Scaling-Gruppe.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID einer EC2 Amazon-Instance, für die Sie den Standby-Status innerhalb einer Auto Scaling Scaling-Gruppe ändern möchten.
- LambdaRoleArn

  Typ: Zeichenfolge

Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

AWS-ASGExitStandby

Beschreibung

Ändern Sie den Standby-Status einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance in einer Auto Scaling Scaling-Gruppe.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID einer EC2 Instance, für die Sie den Standby-Status innerhalb einer Auto Scaling Scaling-Gruppe ändern möchten.

- LambdaRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

AWS-CreateImage

Beschreibung

Erstellen Sie eine neue Amazon Machine Image (AMI) aus einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der EC2-Instance.

- NoReboot

  Typ: Boolescher Wert

  Beschreibung: (Optional) Kein Neustart der Instance vor der Erstellung des Abbilds.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

JSON

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

AWS-DeleteImage

Beschreibung

Löscht einen Amazon Machine Image (AMI) und alle zugehörigen Snapshots.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ImageId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des AMI.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Beschreibung

Patchen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances in einer Auto Scaling Scaling-Gruppe.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instance für das Patching. Geben Sie keine Instanz-ID an, die so konfiguriert ist, dass sie während eines Wartungsfensters ausgeführt wird.

- LambdaRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, der es dem von Automation erstellten Lambda ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

- WaitForInstance

  Typ: Zeichenfolge

  Standard: M PT2

  Beschreibung: (Optional) Dauer, für die die Automatisierung in den Ruhezustand versetzt werden soll, damit die Instanz wieder in Betrieb genommen werden kann.

- WaitForReboot

  Typ: Zeichenfolge

  Standard: PT5 M

  Beschreibung: (Optional) Dauer, für die die Automatisierung in den Ruhezustand versetzt werden soll, damit eine gepatchte Instanz neu gestartet werden kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Beschreibung

Sorgt dafür, dass eine EC2 Instanz mit der entsprechenden Patch-Baseline kompatibel ist. Setzt das Root-Volume bei einem Fehler zurück.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) EC2 InstanceId , auf die wir die Patch-Baseline anwenden.
- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.
- ReportS3Bucket

  Typ: Zeichenfolge

  Beschreibung: (Optional) Amazon S3 S3-Bucket-Ziel für den während des Prozesses generierten Compliance-Bericht.

Dokumentschritte

Schrittnummer	Name des Schritts	Automation-Aktion
1	createDocumentStack	`aws:createStack`

Schrittnummer	Name des Schritts	Automation-Aktion
2	IdentifyRootVolume	`aws:invokeLambdaFunction`
3	PrePatchSnapshot	`aws:executeAutomation`
4	installMissingUpdates	`aws:runCommand`
5	SleepThruInstallation	`aws:invokeLambdaFunction`
6	CheckCompliance	`aws:invokeLambdaFunction`
7	SaveComplianceReportToS3	`aws:invokeLambdaFunction`
8	ReportSuccessOrFailure	`aws:invokeLambdaFunction`
9	RestoreFromSnapshot	`aws:invokeLambdaFunction`
10	DeleteSnapshot	`aws:invokeLambdaFunction`
11	deleteCloudFormationVorlage	`aws:deleteStack`

Ausgaben

IdentifyRootVolume. Nutzlast

PrePatchSnapshot.Leistung

SaveComplianceReportToS3. Nutzlast

RestoreFromSnapshot. Nutzlast

CheckCompliance. Nutzlast

AWS-QuarantineEC2Instance

Beschreibung

Mit dem `AWS-QuarantineEC2Instance` Runbook können Sie einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance eine Sicherheitsgruppe zuweisen, die keinen eingehenden oder ausgehenden Datenverkehr zulässt.

> **Important**
>
> Änderungen an den RDP-Einstellungen sollten sorgfältig geprüft werden, bevor dieses Runbook ausgeführt wird.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der verwalteten Instance, deren RDP-Einstellungen verwaltet werden sollen.

- IsolationSecurityGroup

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Sicherheitsgruppe, die Sie der Instance zuweisen möchten, um eingehenden oder ausgehenden Datenverkehr zu verhindern.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeAwsApi`- Sammelt Details über die Instanz.
- `aws:executeScript`— Überprüft, ob die Instance nicht Teil einer Auto Scaling Scaling-Gruppe ist.
- `aws:executeAwsApi`- Erstellt einen Snapshot des Root-Volumes, das an die Instance angehängt ist.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Snapshot-Status erreicht ist. `completed`

- `aws:executeAwsApi`— Weist Ihrer Instance die im `IsolationSecurityGroup` Parameter angegebene Sicherheitsgruppe zu.

Ausgaben

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

AWS-ResizeInstance

Beschreibung

Ändern Sie den Instanztyp einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der Instance.

- InstanceType

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Typ der Instance.

AWS-RestartEC2Instance

Beschreibung

Starten Sie eine oder mehrere Amazon Elastic Compute Cloud (Amazon EC2) -Instances neu.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: StringList

Beschreibung: (Erforderlich) Die IDs EC2 Amazon-Instances, die neu gestartet werden sollen.

AWS-SetupJupyter

Beschreibung

Das `AWS-SetupJupyter` Runbook hilft Ihnen bei der Einrichtung von Jupyter Notebook auf einer Amazon Elastic Compute Cloud (Amazon) -Instance. EC2 Sie können entweder eine bestehende Instanz angeben oder eine bereitstellen Amazon Machine Image (AMI) ID für die Automatisierung zum Starten und Einrichten einer neuen Instanz. Bevor Sie beginnen, müssen Sie im `SecureString` Parameter Store einen Parameter erstellen, der als Passwort für Jupyter Notebook verwendet werden soll. Parameter Store ist ein Tool in. AWS Systems Manager Informationen zum Erstellen von Parametern finden Sie unter Parameter erstellen im AWS Systems Manager Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AmiId

  Typ: Zeichenfolge

Beschreibung: (Optional) Die ID des AMI die Sie verwenden möchten, um eine neue Instanz zu starten und Jupyter Notebook einzurichten.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instanz, auf der Sie Jupyter Notebook einrichten möchten.

- InstanceType

  Typ: Zeichenfolge

  Standard: t3.medium

  Beschreibung: (Optional) Wenn Sie eine neue Instance starten, um Jupyter Notebook einzurichten, geben Sie den Instance-Typ an, den Sie verwenden möchten.

- JupyterPasswordSSMKey

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des `SecureString` Parameters im Parameter Store, den Sie als Passwort für Jupyter Notebook verwenden möchten.

- KeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das key pair, das Sie der neu gestarteten Instance zuordnen möchten.

- RemoteAccessCidr

  Typ: Zeichenfolge

  Standard: 0.0.0.0/0

  Beschreibung: (Optional) Der CIDR-Bereich, aus dem Sie SSH-Verkehr zulassen möchten.

- RoleName

  Typ: Zeichenfolge

  Standard: SSMManaged InstanceProfileRole

  Beschreibung: (Optional) Der Name des Instanzprofils für die neu gestartete Instance.

- StackName

  Typ: Zeichenfolge

  Standard: CreateManagedInstanceStack {{automation:execution_ID}}

  Beschreibung: (Optional) Der CloudFormation Stack-Name, den die Automatisierung verwenden soll.
- SubnetId

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Optional) Das Subnetz, das Sie starten möchten, um die neue Instance zu verwenden.
- VpcId

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Optional) Die ID der Virtual Private Cloud (VPC), in der Sie die neue Instanz starten möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeScript- Richtet Jupyter Notebook auf der von Ihnen angegebenen Instance oder auf einer neu gestarteten Instance ein und verwendet dabei die Werte, die Sie für die Runbook-Eingabeparameter angeben.

AWS-StartEC2Instance

Beschreibung

Starten Sie eine oder mehrere Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: StringList

  Beschreibung: (Erforderliche) EC2 Instanzen zum Starten.

AWS-StopEC2Instance

Beschreibung

Stoppt eine oder mehrere Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: StringList

  Beschreibung: Zu stoppende (erforderliche) EC2 Instanzen.

AWS-TerminateEC2Instance

Beschreibung

Beenden Sie eine oder mehrere Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: StringList

  Beschreibung: (Erforderlich) IDs , um eine oder mehrere EC2 Instanzen zu beenden.

AWS-UpdateLinuxAmi

Beschreibung

Aktualisieren Sie an Amazon Machine Image (AMI) mit Linux-Distributionspaketen und Amazon-Software.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

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

  - Muss ein gültiger IAM-Rollen-ARN oder eine leere Zeichenfolge sein. Die Systemvariable `{{global:ACCOUNT_ID}}` kann anstelle der AWS Konto-ID im ARN verwendet werden.
- ExcludePackages

  Typ: Zeichenfolge

  Standard: keiner

  Beschreibung: (Optional) Namen der Pakete, die bei Updates unter allen Umständen zurückgehalten werden müssen. Standardmäßig wird kein (\„none\“) Paket ausgeschlossen.

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

  - Muss „none“ ODER eine durch Kommas getrennte Liste von Einträgen sein, die aus Buchstaben, Zahlen, Leerzeichen und den folgenden Zeichen besteht: `, . _ + : = < > ( ) [ ] / * -`
- IamInstanceProfileName

  Typ: Zeichenfolge

  Standard: ManagedInstanceProfile

  Beschreibung: (Erforderlich) Das Instanzprofil, mit dem Systems Manager die Instanz verwalten kann.

  Zulässiges Muster: `^[\w+=,.@-]{1,128}$`

  - Muss zwischen 1 und 128 Zeichen lang sein und nur Buchstaben, Zahlen und die folgenden Zeichen enthalten: `+ = , . @ - _`
- IncludePackages

  Typ: Zeichenfolge

  Standard: alle

  Beschreibung: (Optional) Nur diese benannten Pakete aktualisieren. Standardmäßig werden alle (\„all\“) verfügbaren Updates übernommen.

  Zulässiges Muster: `^(all|[a-zA-Z0-9\s,._+:=<>()\[\]/*-]+)$`

  - Muss „alle“ ODER eine durch Kommas getrennte Liste von Einträgen sein, die aus Buchstaben, Zahlen, Leerzeichen und den folgenden Zeichen besteht: `, . _ + : = < > ( ) [ ] / * -`
- InstanceType

Typ: Zeichenfolge

Standard: t2.micro

Beschreibung (Optional) Der Typ der als Workspace-Host zu startenden Instance. Die Instance-Typen sind je nach Region unterschiedlich.

Zulässiges Muster: `^[a-z0-9]+(-[a-z0-9]+)*\.[a-z0-9]+$`

- Muss das Format Präfix.Suffix haben, wobei beide Teile Kleinbuchstaben und Zahlen enthalten und das Präfix Bindestriche enthalten kann

- MetadataOptions

  Typ: StringMap

  Standard: {“ HttpEndpoint „: „aktiviert“, "„: „optional"} HttpTokens

  Beschreibung: (Optional) Die Metadatenoptionen für die Instanz. Weitere Informationen finden Sie unter InstanceMetadataOptionsRequest.

  Zulässiges Muster: `^\{[^<>\$;|&\\]*\}$`

  - Muss in geschweifte Klammern {} eingeschlossen werden und darf die folgenden Zeichen nicht enthalten: `< > $ ; | & \`

- PostUpdateScript

  Typ: Zeichenfolge

  Standard: keiner

  Beschreibung: (Optional) Die URL eines Skripts, das ausgeführt werden muss, nachdem Paketupdates angewendet werden. Standard („none“) ist die Ausführung keines Skripts.

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

  - Muss „none“ ODER eine gültige HTTP/HTTPS URL sein

- PreUpdateScript

  Typ: Zeichenfolge

  Standard: keiner

Beschreibung: (Optional) Die URL eines Skripts, das ausgeführt werden muss, bevor Updates angewendet werden. Standard („none“) ist die Ausführung keines Skripts.

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

- Muss „none“ ODER eine gültige HTTP/HTTPS URL sein

- SecurityGroupIds

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste IDs der Sicherheitsgruppen, auf die AMI Sie sich beziehen möchten.

  Zulässiges Muster: `^sg-[a-z0-9]{8,17}$`

  - Muss mit „sg-“ beginnen, gefolgt von 8-17 Kleinbuchstaben oder Zahlen

- SourceAmiId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Quell-Amazon Machine Image-ID.

  Zulässiges Muster: `^ami-[a-z0-9]{8,17}$`

  - Muss mit „ami-“ beginnen, gefolgt von 8-17 Kleinbuchstaben oder Zahlen

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Subnetzes, in dem Sie die Instance starten möchten. Wenn Sie Ihre Standard-VPC gelöscht haben, ist dieser Parameter erforderlich.

  Zulässiges Muster: `^$|^subnet-[a-z0-9]{8,17}$`

  - Muss leer sein ODER mit „subnet-“ beginnen, gefolgt von 8-17 Kleinbuchstaben oder Zahlen

- TargetAmiName

  Typ: Zeichenfolge

  Standard: UpdateLinuxAmi _von_ {{}} _am_ {{global:Date_TimeSourceAmiId}}

Beschreibung: (Optional) Der Name des neuen AMIs, das erstellt wird. Der Standard ist eine systemgenerierte Zeichenfolge, die die Quell-AMI-ID sowie Uhrzeit und Datum der Erstellung enthält.

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

- Muss zwischen 3 und 128 Zeichen lang sein und nur Buchstaben, Zahlen, Leerzeichen und die folgenden Zeichen enthalten: `( ) [ ] { } . / ' @ _ : -`

AWS-UpdateWindowsAmi

Beschreibung

Aktualisieren Sie ein Microsoft Windows Amazon Machine Image (AMI). Standardmäßig installiert dieses Runbook alle Windows-Updates, Amazon-Software und Amazon-Treiber. Anschließend wird mit Sysprep ein neues AMI erstellt. Unterstützt Windows Server 2008 R2 bis Windows Server 2022.

> **Important**
>
> Dieses Runbook unterstützt Windows Server 2025 und spätere Versionen nicht, da AWS paravirtuelle Treiber mit diesen Versionen nicht kompatibel sind. Weitere Informationen finden Sie unter Paravirtual-Treiber für Windows-Instances.

> **Important**
>
> Wenn Ihre Instances AWS Systems Manager mithilfe von VPC-Endpunkten eine Verbindung herstellen, schlägt dieses Runbook fehl, sofern es nicht in der Region us-east-1 verwendet wird. Für Instances muss TLS 1.2 aktiviert sein, um dieses Runbook verwenden zu können.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Kategorien

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe von mindestens einer Updatekategorie. Sie können Kategorien anhand kommaseparierter Werte filtern. Optionen: Anwendung, Konnektoren CriticalUpdates DefinitionUpdates, DeveloperKits,, TreiberFeaturePacks, Anleitung, Microsoft, SecurityUpdates ServicePacks,, ToolsUpdateRollups, Updates. Gültige Formate beinhalten einen einzigen Eintrag, zum Beispiel:CriticalUpdates. Oder Sie können eine durch Kommas getrennte Liste angeben:CriticalUpdates,SecurityUpdates. HINWEIS: Um die Kommata herum dürfen keine Leerzeichen stehen.
- ExcludeKbs

  Typ: Zeichenfolge

  Beschreibung: (Optional) Geben Sie einen oder mehrere Microsoft Knowledge Base-Artikel (KB) IDs an, die ausgeschlossen werden sollen. Sie können mehrere ausschließen, indem Sie kommagetrennte Werte IDs verwenden. Gültige Formate: KB9876543 oder 9876543.
- IamInstanceProfileName

  Typ: Zeichenfolge

  Standard: ManagedInstanceProfile

  Beschreibung: (Erforderlich) Der Name der Rolle, mit der Systems Manager die Instanz verwalten kann.

- IncludeKbs

  Typ: Zeichenfolge

  Beschreibung: (Optional) Geben Sie einen oder mehrere Microsoft Knowledge Base-Artikel (KB) IDs an, die aufgenommen werden sollen. Sie können mehrere IDs mithilfe von kommagetrennten Werten installieren. Gültige Formate: KB9876543 oder 9876543.

- InstanceType

  Typ: Zeichenfolge

  Standard: t2.medium

  Beschreibung (Optional) Der Typ der als Workspace-Host zu startenden Instance. Die Instance-Typen sind je nach Region unterschiedlich. Standard ist t2.medium.

- MetadataOptions

  Typ: StringMap

  Standard: {“ HttpEndpoint „: „aktiviert“, "HttpTokens„: „optional"}

  Beschreibung: (Optional) Die Metadatenoptionen für die Instanz. Weitere Informationen finden Sie unter InstanceMetadataOptionsRequest.

- PostUpdateScript

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein als Zeichenfolge bereitgestelltes Skript. Es wird nach der Installation von Betriebssystemaktualisierungen ausgeführt.

- PreUpdateScript

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein als Zeichenfolge bereitgestelltes Skript. Es wird vor der Installation von Betriebssystemaktualisierungen ausgeführt.

- PublishedDateAfter

  Typ: Zeichenfolge

Beschreibung: (Optional) Angabe des Datums, nach dem die Aktualisierungen veröffentlicht werden sollen. Beispiel: Wenn 01.01.2017 angegeben ist, werden alle Aktualisierungen, die während der Windows Update-Suche veröffentlicht wurden, die am oder nach dem 01.01.2017 veröffentlicht wurden, zurückgegeben.

- PublishedDateBefore

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe des Datums, vor dem die Aktualisierungen veröffentlicht werden sollen. Beispiel: Wenn 01.01.2017 angegeben ist, werden alle Aktualisierungen, die während der Windows Update-Suche veröffentlicht wurden, die am oder vor dem 01.01.2017 veröffentlicht wurden, zurückgegeben.

- PublishedDaysOld

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe des erforderlichen Alters der Aktualisierungen in Tagen ab dem Veröffentlichungsdatum. Beispiel: Wenn 10 angegeben ist, werden alle Aktualisierungen, die während der Windows Update-Suche veröffentlicht wurden, die vor 10 oder mehr Tagen veröffentlicht wurden, zurückgegeben.

- SecurityGroupIds

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste IDs der Sicherheitsgruppen, für die AMI Sie gelten möchten.

- SeverityLevels

  Typ: Zeichenfolge

  Beschreibung: (Optional) Angabe mindestens einer MSRC-Ebene, die einem Update zugeordnet ist. Sie können Dringlichkeitsstufen anhand kommaseparierter Werte filtern. Standardmäßig werden Patches für alle Sicherheitsstufen ausgewählt sind. Wenn Werte angegeben sind, wird die Update-Liste nach diesen Werten gefiltert. Optionen: Kritisch, Wichtig, Niedrige, Mittel oder Nicht angegeben. Zu den gültigen Formaten gehört ein einzelner Eintrag. Beispiel: Wichtig. Sie können auch eine kommaseparierte Liste angeben: Kritisch,Wichtig,Niedrig.

- SourceAmiId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die AMI Quell-ID.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Subnetzes, in dem Sie die Instance starten möchten. Wenn Sie Ihre Standard-VPC gelöscht haben, ist dieser Parameter erforderlich.

- TargetAmiName

  Typ: Zeichenfolge

  Standard: UpdateWindowsAmi _from_ {{SourceAmiId}} _am_ {{global:Date_Time}}

  Beschreibung: (Optional) Der Name des neuen AMIs, das erstellt wird. Der Standard ist eine systemgenerierte Zeichenfolge, die die Quell-AMI-ID sowie Uhrzeit und Datum der Erstellung enthält.

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

Beschreibung

Das `AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck` Runbook ermöglicht Integritätsprüfungen für die von Ihnen angegebene Amazon EC2 Auto Scaling (Auto Scaling) -Gruppe.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- AutoScalingGroupARN

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der Auto Scaling-Gruppe, für die Sie Integritätsprüfungen aktivieren möchten.
- HealthCheckGracePeriod

  Typ: Ganzzahl

  Standard: 300

  Beschreibung: (Optional) Die Zeit in Sekunden, die Auto Scaling wartet, bevor der Integritätsstatus einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance überprüft wird, die in Betrieb genommen wurde.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Aktiviert Integritätsprüfungen für die Auto Scaling Scaling-Gruppe, die Sie im `AutoScalingGroupARN` Parameter angeben.

`AWSConfigRemediation-EnforceEC2InstanceIMDSv2`

Beschreibung

Das `AWSConfigRemediation-EnforceEC2InstanceIMDSv2` Runbook benötigt die Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die Sie angeben, um Instance Metadata Service Version 2 (IMDSv2) zu verwenden.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der EC2 Amazon-Instance, die Sie verwenden möchten IMDSv2.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- HttpPutResponseHopLimit

  Typ: Ganzzahl

  Beschreibung: (Optional) Das Hop-Antwortlimit vom IMDS-Service zurück zum Anforderer. Legen Sie den Wert für EC2 Instances, die Container hosten, auf 2 oder höher fest. Auf 0 setzen, um sich nicht zu ändern (Standard).

  Zulässiges Muster: `^([1-5]?\d|6[0-4])$`

  Standard: 0

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`— Setzt die `HttpTokens` Option `required` auf der EC2 Amazon-Instance, die Sie im `InstanceId` Parameter angeben, auf.
- `aws:assertAwsResourceProperty`— Verify IMDSv2 ist für die EC2 Amazon-Instance erforderlich.

AWSEC2-CloneInstanceAndUpgradeSQLServer

Beschreibung

Erstellen Sie ein AMI aus einer EC2 Instanz für Windows Server führen Sie SQL Server 2008 oder höher aus und aktualisieren Sie dann das AMI auf eine neuere Version von SQL Server. Es werden nur englische Versionen von SQL Server unterstützt.

Die folgenden Upgrade-Pfade werden unterstützt:

- SQL Server 2008 auf SQL Server 2017, 2016 oder 2014
- SQL Server 2008 R2 auf SQL Server 2017, 2016 oder 2014
- SQL Server 2012 auf SQL Server 2019, 2017, 2016 oder 2014
- SQL Server 2014 bis SQL Server 2019, 2017 oder 2016
- SQL Server 2016 auf SQL Server 2019 oder 2017

Wenn Sie eine frühere Version von Windows Server verwenden, die nicht mit SQL Server 2019 kompatibel ist, muss das Automatisierungsdokument Ihre Windows Server-Version auf 2016 aktualisieren.

Das Upgrade ist ein aus mehreren Schritten bestehender Prozess, der 2 Stunden in Anspruch nehmen kann. Die Automatisierung erstellt das AMI aus der Instance und startet dann eine temporäre Instance von der neuen AMI in der angegebenen`SubnetID`. Die Sicherheitsgruppen, die Ihrer ursprünglichen Instance zugeordnet sind, werden auf die temporäre Instance angewendet. Die Automatisierung führt dann ein direktes Upgrade `TargetSQLVersion` auf die temporäre Instanz durch. Nach dem Upgrade erstellt die Automatisierung eine neue AMI von der temporären Instanz und beendet dann die temporäre Instanz.

Sie können die Funktionalität der Anwendung testen, indem Sie die neue starten AMI in Ihrer VPC. Nachdem Sie den Test abgeschlossen haben, und bevor Sie eine weitere Aktualisierung durchführen, planen Sie die Anwendungsausfallzeit ein, bevor Sie vollständig zu der aktualisierten Instance wechseln.

> **Note**
>
> Wenn Sie den Computernamen der EC2 Instance ändern möchten, die von der neuen aus gestartet wurde AMI , siehe Umbenennen eines Computers, der eine eigenständige Instanz von SQL Server hostet.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Voraussetzungen

- TLS-Version 1.2.
- Es werden nur englische Versionen von SQL Server unterstützt.
- Die EC2 Instanz muss eine Version von verwenden Windows Server das ist Windows Server 2008 R2 (oder höher) und SQL Server 2008 (oder höher).
- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Installation und Konfiguration des SSM-Agenten auf EC2 Instanzen für Windows Server.
- Konfigurieren Sie die Instanz so, dass sie eine AWS Identity and Access Management (IAM-) Instanzprofilrolle verwendet. Weitere Informationen finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager.
- Stellen Sie sicher, dass die Instance 20 GB freien Speicherplatz auf dem Instance-Boot-Datenträger hat.
- Für Instances, die eine Bring Your Own License (BYOL) SQL Server-Version verwenden, gelten die folgenden zusätzlichen Voraussetzungen:
  - Geben Sie eine EBS-Snapshot-ID an, die das SQL Server-Zielinstallationsmedium enthält. So gehen Sie vor:

    1. Stellen Sie sicher, dass auf der EC2 Instanz Windows Server 2008 R2 oder höher ausgeführt wird.
    2. Erstellen Sie ein 6 GB EBS-Volume in derselben Availability Zone, in der die Instance ausgeführt wird. Fügen Sie das Volume der Instance an. Mounten Sie dies beispielsweise als Laufwerk D.
    3. Klicken Sie mit der rechten Maustaste auf die ISO, und mounten Sie es für eine Instance, beispielsweise als Laufwerk E.
    4. Kopieren Sie den Inhalt der ISO von Laufwerk E:\ zu Laufwerk D:\.
    5. Erstellen Sie einen EBS-Snapshot des 6 GB-Volumes, das Sie in Schritt 2 erstellt haben.

Einschränkungen

- Das Upgrade ist nur auf einem SQL Server mit Windows-Authentifizierung möglich.
- Stellen Sie sicher, dass keine Sicherheits-Patch-Updates auf den Instances ausstehen. Öffnen Sie Control Panel (Systemsteuerung), und wählen Sie dann Check for updates (Auf Aktualisierungen prüfen).
- SQL Server-Bereitstellungen in HA und der Spiegelungsmodus werden nicht unterstützt.

Parameter

- IamInstanceProfile

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Das IAM-Instanzprofil.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die laufende Instanz Windows Server 2008 R2 (oder höher) und SQL Server 2008 (oder höher).
- KeepPreUpgradeImageBackUp

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn auf gesetzt`true`, löscht die Automatisierung das vor dem Upgrade von der Instance erstellte AMI nicht. Wenn auf gesetzt`true`, müssen Sie das AMI löschen. Das AMI wird standardmäßig gelöscht.
- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (erforderlich) Geben Sie ein Subnetz für den Upgrade-Prozess an. Stellen Sie sicher, dass das Subnetz ausgehende Verbindungen zu AWS Services, Amazon S3 und Microsoft hat (um Patches herunterzuladen).
- SQLServerSnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Bedingte) Snapshot-ID für das SQL Server-Zielinstallationsmedium. Dieser Parameter ist für Instances erforderlich, die eine BYOL SQL Server-Version verwenden. Dieser

Parameter ist optional für Instances, die eine SQL Server-Lizenz enthalten (Instances, die mit einem AWS bereitgestellten Amazon Machine Image für Windows Server mit Microsoft SQL Server gestartet wurden).

- RebootInstanceBeforeTakingImage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn auf gesetzt`true`, startet die Automatisierung die Instance neu, bevor ein AMI vor dem Upgrade erstellt wird. Standardmäßig wird die Automatisierung vor dem Upgrade nicht neu gestartet.

- Ziel SQLVersion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wählen Sie die SQL Server-Zielversion aus.

  Mögliche Ziele:

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

  Standardziel: SQL Server 2016

Ausgaben

AMIId: Die ID des AMI, das von der Instanz erstellt wurde, die auf eine neuere Version von SQL Server aktualisiert wurde.

AWSEC2-CloneInstanceAndUpgradeWindows

Beschreibung

Erstelle eine Amazon Machine Image (AMI) aus einem Windows Server 2008 R2-, 2012 R2-, 2016- oder 2019-Instance und aktualisieren Sie dann die AMI to Windows Server 2016, 2019 oder 2022. Die unterstützten Upgrade-Pfade sind wie folgt.

- Windows Server 2008 R2 bis Windows Server 2016.

- Windows Server 2012 R2 bis Windows Server 2016.
- Windows Server 2012 R2 bis Windows Server 2019.
- Windows Server 2012 R2 bis Windows Server 2022.
- Windows Server 2016 bis Windows Server 2019.
- Windows Server 2016 bis Windows Server 2022.
- Windows Server 2019 bis Windows Server 2022.

Die Upgrade-Operation ist ein aus mehreren Schritten bestehender Prozess, der 2 Stunden in Anspruch nehmen kann. Wir empfehlen, ein Betriebssystem-Upgrade auf Instanzen mit mindestens 2 V CPUs und 4 GB RAM durchzuführen. Die Automatisierung erstellt ein AMI aus der Instance und startet dann eine temporäre Instance aus dem neu erstellten AMI in dem`SubnetId`, das Sie angeben. Die Sicherheitsgruppen, die Ihrer ursprünglichen Instance zugeordnet sind, werden auf die temporäre Instance angewendet. Die Automatisierung führt dann ein direktes Upgrade für die `TargetWindowsVersion` temporäre Instance durch. Um Ihr zu aktualisieren Windows Server 2008 R2-Instanz auf Windows Server 2016, 2019 oder 2022 wird ein direktes Upgrade zweimal durchgeführt, da das Upgrade direkt erfolgt Windows Server 2008 R2 auf Windows Server 2016, 2019 oder 2022 werden nicht unterstützt. Die Automatisierung aktualisiert oder installiert auch die AWS Treiber, die für die temporäre Instanz benötigt werden. Nach dem Upgrade erstellt die Automatisierung ein neues AMI aus der temporären Instance und beendet dann die temporäre Instance.

Sie können die Anwendungsfunktionalität testen, indem Sie eine Test-Instance über das aktualisierte AMI in Ihrer Amazon Virtual Private Cloud (Amazon VPC) starten. Nachdem Sie den Test abgeschlossen haben, und bevor Sie eine weitere Aktualisierung durchführen, planen Sie die Anwendungsausfallzeit ein, bevor Sie vollständig zum aktualisierten AMI wechseln.

Führen Sie diese Automatisierung (Konsole) aus

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Windows Server Standard- und Datacenter-Editionen 2008 R2, 2012 R2, 2016 oder 2019

Voraussetzungen

- TLS-Version 1.2.
- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Installation und Konfiguration des SSM-Agenten auf EC2 Instanzen für Windows Server.
- Windows PowerShell 3.0 oder höher muss auf Ihrer Instanz installiert sein.
- Für Instances, die einer Microsoft Active Directory-Domain angehören, empfehlen wir, eine `SubnetId` anzugeben, die keine Verbindung zu Ihren Domain-Cntrollern aufweist, um Hostnamenkonflikte zu vermeiden.
- Das Instance-Subnetz muss über eine ausgehende Verbindung zum Internet verfügen, die Zugriff AWS-Services auf Amazon S3 und den Zugriff auf Download-Patches von Microsoft ermöglicht. Diese Anforderung ist erfüllt, wenn das Subnetz entweder ein öffentliches Subnetz ist und die Instance eine öffentliche IP-Adresse hat, oder wenn es sich bei dem Subnetz um ein privates Subnetz mit einer Route handelt, die Internetverkehr an ein öffentliches NAT-Gerät sendet.
- Diese Automatisierung funktioniert nur mit Windows Server 2008 R2-, 2012 R2-, 2016- und 2019-Instanzen.
- Konfigurieren Sie die Windows Server Instanz mit einem AWS Identity and Access Management (IAM-) Instanzprofil, das die erforderlichen Berechtigungen für Systems Manager bereitstellt. Weitere Informationen finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager.
- Stellen Sie sicher, dass die Instance 20 GB freien Speicherplatz auf dem Boot-Datenträger hat.
- Wenn die Instance keine von AWS Ihnen bereitgestellte Windows-Lizenz verwendet, geben Sie eine Amazon EBS-Snapshot-ID an, die Folgendes umfasst: Windows Server 2012 R2-Installationsmedien. So gehen Sie vor:
  - Stellen Sie sicher, dass die EC2 Instanz läuft Windows Server 2012 oder später.
  - Erstellen Sie ein 6 GB EBS-Volume in derselben Availability Zone, in der die Instance ausgeführt wird. Fügen Sie das Volume der Instance an. Mounten Sie dies beispielsweise als Laufwerk D.
  - Klicken Sie mit der rechten Maustaste auf die ISO, und mounten Sie es für eine Instance, beispielsweise als Laufwerk E.
  - Kopieren Sie den Inhalt der ISO von Laufwerk E:\ zu Laufwerk D:\.
  - Erstellen Sie einen EBS-Snapshot des 6 GB-Volumes, das Sie oben in Schritt 2 erstellt haben.

Einschränkungen

Diese Automatisierung unterstützt keine Upgrades von Windows Domänencontrollern, Clustern oder von Windows-Desktop-Betriebssystemen. Diese Automatisierung unterstützt auch keine EC2 Instanzen für Windows Server mit den folgenden installierten Rollen.

- Remote Desktop Session Host (RDSH)
- Remote Desktop Connection Broker (RDCB)
- Remote Desktop Virtualization Host (RDVH)
- Remote Desktop Web Access (RDWA)

Parameter

- AlternativeKeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name eines alternativen key pair, das während des Upgrade-Vorgangs verwendet werden soll. Dies ist in Situationen nützlich, in denen das der ursprünglichen Instanz zugewiesene key pair nicht verfügbar ist. Wenn der ursprünglichen Instanz kein key pair zugewiesen wurde, müssen Sie einen Wert für diesen Parameter angeben.
- BYOLWindowsMediaSnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des zu kopierenden Amazon EBS-Snapshots, der Windows Server 2012R2-Installationsmedien enthält. Nur erforderlich, wenn Sie eine BYOL-Instance aktualisieren.
- IamInstanceProfile

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des IAM-Instanzprofils, mit dem Systems Manager die Instanz verwalten kann.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die laufende EC2 Instanz Windows Server 2008 R2, 2012 R2, 2016 oder 2019.
- KeepPreUpgradeImageBackUp

Typ: Zeichenfolge

Beschreibung: (Optional) Wenn auf True gesetzt, löscht die Automatisierung das vor dem Upgrade von der EC2 Instance erstellte AMI nicht. Bei „True“ müssen Sie das AMI löschen. Das AMI wird standardmäßig gelöscht.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Dies ist das Subnetz für den Upgrade-Prozess und in dem sich Ihre EC2 Quell-Instance befindet. Stellen Sie sicher, dass das Subnetz ausgehende Verbindungen zu AWS Services, Amazon S3 und Microsoft hat (um Patches herunterzuladen).

- TargetWindowsVersion

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Wählen Sie die Windows-Zielversion aus.

  Standard: 2022

- RebootInstanceBeforeTakingImage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Bei „True“ startet die Automation die Instance vor der Erstellung eines Pre-Upgrade-AMI neu. Standardmäßig startet die Automation vor dem Upgrade nicht neu.

AWSEC2-PatchLoadBalancerInstance

Beschreibung

Aktualisieren und patchen Sie die Nebenversion einer EC2 Amazon-Instance (Windows oder Linux), die an einen beliebigen Load Balancer (Classic, ALB oder NLB) angeschlossen ist. Die Standardzeit für den Verbindungsabbau wird angewendet, bevor die Instance gepatcht wird. Sie können die Wartezeit überschreiben, indem Sie Ihre benutzerdefinierte Entladezeit in Minuten (1-59) für den Parameter eingeben. ConnectionDrainTime

Der Automatisierungs-Workflow sieht wie folgt aus:

1. Der Load Balancer oder die Zielgruppe, an die die Instance angehängt ist, wird bestimmt und die Instance wird als fehlerfrei verifiziert.
2. Die Instance wird aus dem Load Balancer oder der Zielgruppe entfernt.
3. Die Automatisierung wartet auf den Zeitraum, der für den Verbindungsabbau angegeben wurde.
4. Die RunPatchBaselineAWS-Automatisierung wird aufgerufen, um die Instanz zu patchen.
5. Die Instanz wird wieder an den Load Balancer oder die Zielgruppe angehängt.

Führen Sie diese Automatisierung aus (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Voraussetzungen

- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Arbeiten mit dem SSM-Agenten auf EC2 Instanzen für Windows Server.

Parameter

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID der zu patchenden Instanz, die einem Load Balancer (Classic, ALB oder NLB) zugeordnet ist.
- ConnectionDrainTime

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Verbindungsentladungszeit des Load Balancers in Minuten (-). 1 59
- S3BucketLog

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Name des Amazon S3 S3-Buckets, der zum Speichern der Befehlsausgabeantworten verwendet werden soll. Sie können einen Bucket angeben, der Ihnen gehört, oder einen Bucket, der mit Ihnen geteilt wird. Wenn Sie diesen Parameter angeben, müssen Sie auch runCommandAssumeRole angeben.

- runCommandAssumeRolle

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der IAM-Rolle, die verwendet werden soll, um den Befehl auf der Instance auszuführen. Die Rolle muss eine Vertrauensbeziehung mit dem `ssm.amazonaws.com` Service Principal haben, ihr muss die SSMManagedInstanceCoreAmazon-Richtlinie angehängt sein und sie muss über Schreibberechtigungen für den Amazon S3-Bucket verfügen, der für S3 angegeben istBucketLog.

AWSEC2-SQLServerDBRestore

Beschreibung

Das `AWSEC2-SQLServerDBRestore` Runbook stellt in Amazon S3 gespeicherte Microsoft SQL Server-Datenbanksicherungen auf SQL Server 2017 wieder her, der auf einer Amazon Elastic Compute Cloud (EC2) Linux-Instance ausgeführt wird. Sie können Ihre eigene EC2-Instance mit SQL Server 2017 Linux bereitstellen. Wenn keine EC2-Instance bereitgestellt wird, startet und konfiguriert die Automatisierung eine neue Ubuntu 16.04 EC2-Instance mit SQL Server 2017. Die Automatisierung unterstützt die Wiederherstellung vollständiger, differenzierter und transaktionaler Protokollsicherungen. Diese Automatisierung akzeptiert mehrere Datenbank-Sicherungsdateien und stellt die neueste gültige Sicherung der einzelnen Datenbanken in den bereitgestellten Dateien wieder her.

Um sowohl die Sicherung als auch die Wiederherstellung einer lokalen SQL Server-Datenbank auf einer EC2-Instanz zu automatisieren, auf der SQL Server 2017 Linux ausgeführt wird, können Sie das -signierte Skript verwenden. AWS PowerShell `MigrateSQLServerToEC2Linux`

> **Important**
>
> Dieses Runbook setzt das Benutzerkennwort des SQL Server-Administrators (SA) bei jeder Ausführung der Automatisierung zurück. Nach Abschluss der Automatisierung müssen Sie

erneut Ihr eigenes SA-Benutzerkennwort festlegen, bevor Sie eine Verbindung mit der SQL Server-Instanz herstellen.

Führen Sie diese Automatisierung aus (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Voraussetzungen

Um diese Automatisierung auszuführen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Dem IAM-Benutzer oder der IAM-Rolle, die diese Automatisierung ausführt, muss eine Inline-Richtlinie mit den unter beschriebenen Berechtigungen verknüpft sein. Erforderliche IAM-Berechtigungen
- Wenn Sie Ihre eigene EC2-Instance bereitstellen:
  - Die von Ihnen bereitgestellte EC2-Instance muss eine Linux-Instance sein, auf der Microsoft SQL Server 2017 ausgeführt wird.
  - Die von Ihnen bereitgestellte EC2-Instance muss mit einem AWS Identity and Access Management (IAM-) Instanzprofil konfiguriert sein, dem die `AmazonSSMManagedInstanceCore` verwaltete Richtlinie angehängt ist. Weitere Informationen finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager.
  - Der SSM-Agent muss auf Ihrer EC2-Instance installiert sein. Weitere Informationen finden Sie unter Installation und Konfiguration des SSM-Agenten auf EC2-Instances für Linux.
  - Die EC2-Instanz muss über ausreichend freien Speicherplatz verfügen, um die SQL Server-Backups herunterzuladen und wiederherzustellen.

Einschränkungen

Diese Automatisierung unterstützt keine Wiederherstellung auf SQL Server auf EC2-Instances für Windows Server. Diese Automatisierung stellt nur Datenbanksicherungen wieder her, die mit SQL Server Linux 2017 kompatibel sind. Weitere Informationen finden Sie unter Editionen und unterstützte Funktionen von SQL Server 2017 auf Linux.

Parameters

Diese Automatisierung hat die folgenden Parameter:

- DatabaseNames

  Typ: Zeichenfolge

  Beschreibung: (Optional) Durch Komma getrennte Liste der Namen der wiederherzustellenden Datenbanken.
- DataDirectorySize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Gewünschte Volume-Größe (GiB) des SQL Server-Datenverzeichnisses für die neue EC2-Instance.

  Standardwert: 100
- KeyPair

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das beim Erstellen der neuen EC2-Instance zu verwendende Schlüsselpaar.
- IamInstanceProfileName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das IAM-Instanzprofil, das an die neue EC2-Instance angehängt werden soll. Dem IAM-Instanzprofil muss die `AmazonSSMManagedInstanceCore` verwaltete Richtlinie angehängt sein.
- InstanceId

Typ: Zeichenfolge

Beschreibung: (Optional) Die Instance mit SQL Server 2017 auf Linux. Wenn kein Wert angegeben InstanceId wird, startet die Automatisierung eine neue EC2-Instance mit der bereitgestellten InstanceType und SQLServer Edition.

- InstanceType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Instance-Typ der zu startenden EC2-Instance.

- iSS3 PresignedUrl

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn es sich bei S3Input um eine vorsignierte S3-URL handelt, geben Sie dies an. `yes`

  Standardwert: nein

  Gültige Werte: ja | nein

- LogDirectorySize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Gewünschte Volume-Größe (GiB) des SQL Server-Protokollverzeichnisses für die neue EC2-Instance.

  Standardwert: 100

- S3-Eingabe

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) S3-Bucket-Name, kommagetrennte Liste von S3-Objektschlüsseln oder kommagetrennte Liste von vorsignierten S3-Dateien, die die wiederherzustellenden URLs SQL-Backupdateien enthalten.

- SQLServerEdition

  Typ: Zeichenfolge

Beschreibung: (Optional) Die Edition von SQL Server 2017 zur Installation auf der neu erstellten EC2-Instance.

Gültige Werte: Standard | Enterprise | Web | Express

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Subnetz, in dem die neue EC2-Instance gestartet wird. Das Subnetz muss ausgehende Konnektivität zu AWS Diensten haben. Wenn kein Wert für angegeben SubnetId wird, verwendet die Automatisierung das Standardsubnetz.

- TempDbDirectorySize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Gewünschte Volume-Größe (GiB) des SQL Server-TempDB-Verzeichnisses für die neue EC2-Instance.

  Standardwert: 100

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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"
        }
    ]
}
```

Dokumentschritte

Um diese Automatisierung zu verwenden, folgen Sie den Schritten, die für Ihren Instance-Typ gelten:

Für neue EC2-Instances:

1. `aws:executeAwsApi`- Rufen Sie die AMI-ID für SQL Server 2017 auf Ubuntu 16.04 ab.
2. `aws:runInstances`- Starten Sie eine neue EC2-Instance für Linux.
3. `aws:waitForAwsResourceProperty`- Warten Sie, bis die neu erstellte EC2-Instance bereit ist.
4. `aws:executeAwsApi`- Starten Sie die Instance neu, wenn die Instance nicht bereit ist.
5. `aws:assertAwsResourceProperty`- Stellen Sie sicher, dass der SSM-Agent installiert ist.
6. `aws:runCommand`- Führen Sie das SQL Server-Wiederherstellungsskript in PowerShell aus.

Für vorhandene EC2-Instances:

1. `aws:waitForAwsResourceProperty`- Stellen Sie sicher, dass die EC2-Instanz bereit ist.
2. `aws:executeAwsApi`- Starten Sie die Instance neu, wenn die Instance nicht bereit ist.
3. `aws:assertAwsResourceProperty`- Stellen Sie sicher, dass der SSM-Agent installiert ist.
4. `aws:runCommand`- Führen Sie das SQL Server-Wiederherstellungsskript in PowerShell aus.

Ausgaben

getInstance. InstanceId

restoreToNewInstanz.Ausgabe

restoreToExistingInstanz.Ausgabe

AWSSupport-ActivateWindowsWithAmazonLicense

Beschreibung

Das `AWSSupport-ActivateWindowsWithAmazonLicense` Runbook aktiviert eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance für Windows Server mit einer von Amazon bereitgestellten Lizenz. Die Automatisierung überprüft und konfiguriert die erforderlichen Betriebssystemeinstellungen des Schlüsselverwaltungsdienstes und versucht die Aktivierung. Dazu gehören Betriebssystemrouten zu den Schlüsselverwaltungsservern von Amazon und die Betriebssystemeinstellungen des Schlüsselverwaltungsdienstes. Wenn der `AllowOffline` Parameter auf gesetzt wird, `true` kann die Automatisierung erfolgreich auf Instances abzielen, die nicht von der Instance verwaltet werden AWS Systems Manager, sondern die einen Stopp und Start der Instance erfordern.

> **Note**
>
> Dieses Runbook kann nicht für das Modell Bring Your Own License (BYOL) verwendet werden Windows Server Instanzen. Informationen zur Verwendung Ihrer eigenen Lizenz finden Sie unter Microsoft-Lizenzierung in AWS.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AllowOffline

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Legen Sie diese Option fest, `true` wenn Sie eine Wiederherstellung der Windows-Aktivierung im Offlinemodus zulassen, falls die Online-Problembehandlung fehlschlägt oder wenn es sich bei der bereitgestellten Instanz nicht um eine verwaltete Instanz handelt.

  > **Important**
  >
  > Die Offline-Methode erfordert, dass die bereitgestellte EC2 Instanz gestoppt und dann gestartet wird. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP verwenden.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ForceActivation

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Stellen Sie diese Option ein, `true` wenn Sie fortfahren möchten, auch wenn Windows bereits aktiviert ist.

- InstanceId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) ID Ihrer verwalteten EC2 Instanz für Windows Server.

- SubnetId

  Typ: Zeichenfolge

  Standard: CreateNew VPC

  Beschreibung: (Optional) Nur offline — Die Subnetz-ID für die EC2 Rescue-Instanz, die zur Durchführung der Offline-Fehlerbehebung verwendet wurde. Verwenden Sie `SelectedInstanceSubnet` es, um dasselbe Subnetz wie Ihre Instance zu verwenden, oder verwenden Sie es, `CreateNewVPC` um eine neue VPC zu erstellen. WICHTIG: Das Subnetz muss sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Wir empfehlen, dass die EC2 Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, der die von SSMManagedInstanceCoreAmazon verwaltete Richtlinie beigefügt ist. Sie benötigen mindestens ssm: StartAutomationExecution und ssm:, SendCommand um die Automatisierung auszuführen und den Befehl an die Instance zu senden, sowie über ssm:, GetAutomationExecution um die Automatisierungsausgabe lesen zu können. Informationen zur Offline-Behebung finden Sie unter den erforderlichen Berechtigungen von. `AWSSupport-StartEC2RescueWorkflow`

Dokumentschritte

1. `aws:assertAwsResourceProperty`— Vergewissern Sie sich, dass die Plattform der bereitgestellten Instanz Windows ist.
2. `aws:assertAwsResourceProperty`- Vergewissern Sie sich, dass es sich bei der bereitgestellten Instanz um eine verwaltete Instanz handelt:
   a. (Korrektur der Online-Aktivierung) Wenn es sich bei der Eingabeinstanz `aws:runCommand` um eine verwaltete Instanz handelt, führen Sie das PowerShell Skript aus, um zu versuchen, die Windows-Aktivierung zu korrigieren.
   b. (Offline-Aktivierungsreparatur) Wenn die Eingabe-Instance keine verwaltete Instance ist:

i. `aws:assertAwsResourceProperty`— Überprüft, ob die `AllowOffline` Markierung auf `true` gesetzt ist. Wenn ja, wird der Offline-Fix gestartet; andernfalls endet die Automatisierung.

ii. `aws:executeAutomation`- Rufen Sie es `AWSSupport-StartEC2RescueWorkflow` mit dem Offline-Fix-Skript für die Windows-Aktivierung auf. Das Skript verwendet je nach Betriebssystemversion entweder EC2 Config oder EC2 Launch.

iii. `aws:executeAwsApi`- Lesen Sie das Ergebnis von`AWSSupport-StartEC2RescueWorkflow`.

Ausgaben

activateWindows.Output

getActivateWindowsOfflineResult. Ausgabe

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Beschreibung

Das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook analysiert die Konnektivität von einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder einer elastic network interface zu einem AWS-Service Endpunkt. IPv6 wird nicht unterstützt. Das Runbook verwendet den Wert, den Sie für den `ServiceEndpoint` Parameter angeben, um die Konnektivität zu einem Endpunkt zu analysieren. Wenn in Ihrer VPC kein AWS PrivateLink Endpunkt gefunden werden kann, verwendet das Runbook derzeit eine öffentliche IP-Adresse für den Dienst. AWS-Region Diese Automatisierung verwendet Reachability Analyzer von Amazon Virtual Private Cloud. Weitere Informationen finden Sie unter Was ist Reachability Analyzer? , im Reachability Analyzer.

Diese Automatisierung überprüft Folgendes:

- Überprüft, ob Ihre Virtual Private Cloud (VPC) für die Verwendung des von Amazon bereitgestellten DNS-Servers konfiguriert ist.
- Überprüft, ob in der VPC ein AWS PrivateLink Endpunkt für den AWS-Service von Ihnen angegebenen vorhanden ist. Wenn ein Endpunkt gefunden wird, überprüft die Automatisierung, ob das `privateDns` Attribut aktiviert ist.
- Überprüft, ob der AWS PrivateLink Endpunkt die Standard-Endpunktrichtlinie verwendet.

Überlegungen

- Ihnen wird pro Analyselauf zwischen einer Quelle und einem Ziel in Rechnung gestellt. Weitere Informationen dazu finden Sie unter Amazon VPC – Preise.
- Während der Automatisierung werden ein Network Insights-Pfad und eine Network Insights-Analyse erstellt. Wenn die Automatisierung erfolgreich abgeschlossen wurde, löscht das Runbook diese Ressourcen. Wenn der Bereinigungsschritt fehlschlägt, wird der Network Insights-Pfad nicht vom Runbook gelöscht und Sie müssen ihn manuell löschen. Wenn Sie den Network Insights-Pfad nicht manuell löschen, wird er weiterhin auf Ihr Kontingent angerechnet. AWS-KontoWeitere Informationen zu Kontingenten für Reachability Analyzer finden Sie unter Kontingente für Reachability Analyzer in Reachability Analyzer.
- Konfigurationen auf Betriebssystemebene wie die Verwendung eines Proxys, eines lokalen DNS-Resolvers oder einer Hosts-Datei können die Konnektivität beeinträchtigen, selbst wenn der Reachability Analyzer zurückkehrt. `PASS`
- Überprüfen Sie die Auswertung aller vom Reachability Analyzer durchgeführten Prüfungen. Wenn eine der Prüfungen den Status von zurückgibt, kann dies Auswirkungen auf die Konnektivität habenFAIL, selbst wenn die allgemeine Erreichbarkeitsprüfung den Status zurückgibt. `PASS`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Quelle

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance oder der Netzwerkschnittstelle, von der aus Sie die Erreichbarkeit analysieren möchten.

- ServiceEndpoint

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Hostname des Service-Endpunkts, für den Sie die Erreichbarkeit analysieren möchten.

- RetainVpcReachabilityAnalysis

  Typ: Zeichenfolge

  Standard: false

  Beschreibung: (Optional) Legt fest, ob der Network Insight-Pfad und die erstellten zugehörigen Analysen beibehalten werden. Standardmäßig werden die für die Analyse der Erreichbarkeit verwendeten Ressourcen nach erfolgreicher Analyse gelöscht. Wenn Sie sich dafür entscheiden, die Analyse beizubehalten, löscht das Runbook die Analyse nicht und Sie können sie in der Amazon VPC-Konsole visualisieren. In der Automatisierungsausgabe ist ein Konsolenlink verfügbar.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

1. aws:executeScript: Überprüft den Dienstendpunkt, indem versucht wird, den Hostnamen aufzulösen.
2. aws:executeScript: Sammelt Details zur VPC und zum Subnetz.
3. aws:executeScript: Wertet die DNS-Konfiguration der VPC aus.
4. aws:executeScript: Wertet die VPC-Endpunktprüfungen aus.
5. aws:executeScript: Findet ein Internet-Gateway, um eine Verbindung zum Endpunkt des öffentlichen Dienstes herzustellen.
6. aws:executeScript: Bestimmt das Ziel, das für die Erreichbarkeitsanalyse verwendet werden soll.
7. aws:executeScript: Analysiert die Erreichbarkeit von der Quelle bis zum Endpunkt mit Reachability Analyzer und bereinigt die Ressourcen, wenn die Analyse erfolgreich ist.
8. aws:executeScript: Generiert einen Bericht zur Bewertung der Erreichbarkeit.
9. aws:executeScript: Generiert die Ausgabe in JSON.

Ausgaben

- generateReport.EvalReport- Die Ergebnisse der von der Automatisierung durchgeführten Prüfungen im Textformat.

- `generateJsonOutput.Output`- Eine Minimalversion der Ergebnisse im JSON-Format.

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

Beschreibung

Das `AWSPremiumSupport-ChangeInstanceTypeIntelToAMD` Runbook automatisiert Migrationen von von Intel betriebenen Amazon Elastic Compute Cloud (Amazon EC2) -Instances zu den entsprechenden Instance-Typen mit AMD-Unterstützung. Dieses Runbook unterstützt Allzweckinstanzen (M), Burstable-Allzweckinstanzen (T), rechenoptimierte (C) und speicheroptimierte (R) Instances, die auf dem Nitro-System basieren. Dieses Runbook kann auf Instanzen verwendet werden, die nicht von Systems Manager verwaltet werden.

Um das potenzielle Risiko von Datenverlust und Ausfallzeiten zu reduzieren, überprüft das Runbook das Stoppverhalten der Instance, ob sich die Instance in einer Amazon EC2 Auto Scaling Scaling-Gruppe befindet, den Zustand der Instance und ob der entsprechende AMD-betriebene Instance-Typ in derselben Availability Zone verfügbar ist. Standardmäßig ändert dieses Runbook den Instance-Typ nicht, wenn Instance-Speicher-Volumes angehängt sind oder wenn die Instance Teil eines Stacks ist. AWS CloudFormation Wenn Sie dieses Verhalten ändern möchten, geben Sie es `yes` für einen der `AllowCloudFormationInstances` Parameter `AllowInstanceStoreInstances` und an.

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist ein Abonnement für Business + Support, Enterprise Support oder Unified Operations erforderlich. Weitere Informationen finden Sie unter AWS Support Tarife vergleichen.

Überlegungen

- Wir empfehlen, Ihre Instance zu sichern, bevor Sie dieses Runbook verwenden.
- Wenn Sie den Instance-Typ ändern, muss das Runbook Ihre Instance beenden. Wenn eine Instance gestoppt wird, gehen alle im RAM oder auf den Instance-Speicher-Volumes gespeicherten Daten verloren, und die automatische öffentliche IPv4 Adresse wird freigegeben. Weitere Informationen finden Sie unter Anhalten und Starten Ihrer Instance.
- Wenn Sie keinen Wert für den `TargetInstanceType` Parameter angeben, versucht das Runbook, die entsprechende AMD-Instanz in Bezug auf virtuelle Daten CPUs und Arbeitsspeicher

innerhalb derselben Instance-Familie zu identifizieren. Das Runbook endet, wenn es keinen äquivalenten AMD-Instanztyp identifizieren kann.

- Mithilfe dieser `DryRun` Option können Sie den entsprechenden AMD-Instance-Typ erfassen und Anforderungen validieren, ohne den Instance-Typ tatsächlich zu ändern.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Bestätigen

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Geben Sie ein, `yes` um zu bestätigen, dass Ihre Ziel-Instance gestoppt wird, wenn sie läuft.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, deren Typ Sie ändern möchten.

- TargetInstanceType

  Typ: Zeichenfolge

  Standard: automatisch

  Beschreibung: (Optional) Der AMD-Instance-Typ, zu dem Sie Ihre Instance ändern möchten. Der `automatic` Standardwert verwendet den entsprechenden Instance-Typ in Bezug auf virtuelle Instanzen CPUs und Arbeitsspeicher. Beispielsweise würde ein m5.large in m5a.large geändert werden.
- AllowInstanceStoreInstances

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn Sie angeben`yes`, wird das Runbook auf Instances ausgeführt, denen Instance-Speicher-Volumes angehängt sind.
- AllowCloudFormationInstances

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn auf gesetzt`yes`, wird das Runbook auf Instances ausgeführt, die Teil eines CloudFormation Stacks sind.
- AllowCrossGeneration

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`yes`, versucht das Runbook, den neuesten äquivalenten AMD-Instance-Typ innerhalb derselben Instance-Familie zu finden.
- DryRun

Typ: Zeichenfolge

Gültige Werte: nein | ja

Standard: no

Beschreibung: (Optional) Wenn auf gesetzt`yes`, gibt das Runbook den entsprechenden AMD-Instance-Typ zurück und validiert die Migrationsanforderungen, ohne Änderungen am Instance-Typ vorzunehmen.

- SleepWait

  Typ: Zeichenfolge

  Standard: S PT3

  Beschreibung: (Optional) Die Zeit, die das Runbook warten soll, bevor es eine neue Automatisierung startet. Der Wert, den Sie für diesen Parameter angeben, muss dem ISO 8601-Standard entsprechen. Weitere Informationen zum Erstellen von ISO-8601-Zeichenfolgen finden Sie unter Formatieren von Datums- und Uhrzeitzeichenfolgen für Systems Manager.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

1. aws:assertAwsResourceProperty: Bestätigt, dass der Status der Amazon EC2 EC2-Zielinstanzrunning, pendingstopped, oder stopping ist. Andernfalls endet die Automatisierung.
2. aws:executeAwsApi: Sammelt Eigenschaften aus der Amazon EC2 EC2-Zielinstanz.
3. aws:branch: Verzweigt die Automatisierung auf der Grundlage des Status der Amazon EC2 EC2-Instance.
   a. Falls stopped oderstopping, wird die Automatisierung aws:waitForAwsResourceProperty so lange ausgeführt, bis die Amazon EC2 EC2-Instance vollständig gestoppt ist.
   b. Falls running oderpending, wird die Automatisierung aws:waitForAwsResourceProperty so lange ausgeführt, bis die Amazon EC2 EC2-Instance die Statusprüfungen bestanden hat.
4. aws:assertAwsResourceProperty: Bestätigt, dass die Amazon EC2 EC2-Instance nicht Teil einer Auto Scaling Scaling-Gruppe ist, indem geprüft wird, ob das aws:autoscaling:groupName Tag angewendet wurde.
5. aws:executeAwsApi: Sammelt die Eigenschaften des aktuellen Instance-Typs, um den entsprechenden AMD-Instance-Typ zu finden.
6. aws:assertAwsResourceProperty: Bestätigt, dass ein AWS Marketplace Produktcode nicht mit der Amazon EC2 EC2-Instance verknüpft ist. Einige Produkte sind nicht für alle Instance-Typen verfügbar.
7. aws:branch: Verzweigt die Automatisierung, je nachdem, ob die Automatisierung prüfen soll, ob die Amazon EC2 EC2-Instance Teil eines CloudFormation Stacks ist
   a. Wenn das aws:cloudformation:stack-name Tag auf die Instance angewendet wird, wird die Automatisierung ausgeführt, aws:assertAwsResourceProperty um zu bestätigen, dass die Instance nicht Teil eines CloudFormation Stacks ist.
8. aws:branch: Verzweigt die Automatisierung je nachdem, ob der Instance-Root-Volume-Typ Amazon Elastic Block Store (Amazon EBS) ist.
9. aws:assertAwsResourceProperty: Bestätigt, dass das Verhalten beim Herunterfahren der Instance zutrifft stop und nichtterminate.

10. `aws:executeScript`: Bestätigt, dass es nur eine Automatisierung dieses Runbooks gibt, die auf die aktuelle Instanz abzielt. Wenn bereits eine andere Automatisierung ausgeführt wird, die auf dieselbe Instanz abzielt, wird ein Fehler zurückgegeben und beendet.
11. `aws:executeAwsApi`: Gibt eine Liste der AMD-Instanztypen mit derselben Speichermenge und v zurückCPUs.
12. `aws:executeScript`: Prüft, ob der aktuelle Instance-Typ unterstützt wird, und gibt den entsprechenden AMD-Instance-Typ zurück. Wenn es kein Äquivalent gibt, endet die Automatisierung.
13. `aws:executeScript`: Bestätigt, dass der AMD-Instanztyp in derselben Availability Zone verfügbar ist, und überprüft die bereitgestellten IAM-Berechtigungen.
14. `aws:branch`: Verzweigt die Automatisierung je nachdem, ob der `DryRun` Parameterwert `yes`
15. `aws:branch`: Prüft, ob der ursprüngliche Instanztyp und der Zielinstanztyp identisch sind. Wenn sie identisch sind, endet die Automatisierung.
16. `aws:executeAwsApi`: Ruft den aktuellen Instanzstatus ab.
17. `aws:changeInstanceState`: Stoppt die Amazon EC2 EC2-Instance.
18. `aws:changeInstanceState`: Erzwingt die Instance zum Beenden, wenn sie im Stopping-Status feststeckt.
19. `aws:executeAwsApi`: Ändert den Instanztyp in den AMD-Zielinstanztyp.
20. `aws:sleep`: Wartet 3 Sekunden, nachdem der Instanztyp geändert wurde, um die Konsistenz zu gewährleisten.
21. `aws:branch`: Verzweigt die Automatisierung auf der Grundlage des vorherigen Instanzstatus. Wenn ja`running`, wird die Instanz gestartet.
    a. `aws:changeInstanceState`: Startet die Amazon EC2 EC2-Instance, wenn sie vor der Änderung des Instance-Typs ausgeführt wurde.
    b. `aws:waitForAwsResourceProperty`: Wartet darauf, dass die Amazon EC2 EC2-Instance die Statusprüfungen bestanden hat. Wenn die Instance die Statusprüfungen nicht besteht, wird die Instance wieder auf ihren ursprünglichen Instance-Typ zurückgesetzt.
        i. `aws:changeInstanceState`: Stoppt die Amazon EC2 EC2-Instance, bevor sie in ihren ursprünglichen Instance-Typ geändert wird.
        ii. `aws:changeInstanceState`: Erzwingt, dass die Amazon EC2 EC2-Instance beendet wird, bevor sie in ihren ursprünglichen Instance-Typ geändert wird, falls sie in einem Stopp-Zustand hängen bleibt.
        iii. `aws:executeAwsApi`: Ändert die Amazon EC2 EC2-Instance auf ihren ursprünglichen Typ.

iv. `aws:sleep`: Wartet 3 Sekunden nach der Änderung des Instance-Typs, um die Konsistenz zu gewährleisten.

v. `aws:changeInstanceState`: Startet die Amazon EC2 EC2-Instance, wenn sie vor der Änderung des Instance-Typs ausgeführt wurde.

vi. `aws:waitForAwsResourceProperty`: Wartet darauf, dass die Amazon EC2 EC2-Instance die Statusprüfungen bestanden hat.

22`aws:sleep`: Wartet, bevor das Runbook beendet wird.

AWSSupport-CheckXenToNitroMigrationRequirements

Beschreibung

Das `AWSSupport-CheckXenToNitroMigrationRequirements` Runbook überprüft, ob eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance die Voraussetzungen erfüllt, um den Instance-Typ erfolgreich von einer Xen-Instance in einen Nitro-basierten Instance-Typ zu ändern. Diese Automatisierung überprüft Folgendes:

- Das Root-Gerät ist ein Amazon Elastic Block Store (Amazon EBS) -Volume.
- Das `enaSupport` Attribut ist aktiviert.
- Das ENA-Modul ist auf der Instanz installiert.
- Das NVMe Modul ist auf der Instanz installiert. Falls ja, ist das Modul installiert und ein Skript überprüft, ob das Modul in das `initramfs` Image geladen ist.
- Analysiert `/etc/fstab` und sucht anhand von Gerätenamen nach Blockgeräten, die gemountet werden.
- Ermittelt, ob das Betriebssystem (OS) standardmäßig vorhersehbare Netzwerkschnittstellennamen verwendet.

Dieses Runbook unterstützt die folgenden Betriebssysteme:

- 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

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Standard: false

  Beschreibung: (Erforderlich) Die ID der EC2 Amazon-Instance, für die Sie die Voraussetzungen überprüfen möchten, bevor Sie zu einem Nitro-basierten Instance-Typ migrieren.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- 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

Dokumentschritte

- aws:executeAwsApi- Sammelt Details über die Instanz.
- aws:executeAwsApi- Sammelt Informationen über den Hypervisor für die Instanz.
- aws:branch— Verzweigungen basieren darauf, ob auf der Zielinstanz bereits ein Nitro-basierter Instanztyp ausgeführt wird.
- aws:branch— Prüft, ob das Betriebssystem der Instanz von Nitro-basierten Instances unterstützt wird.
- aws:assertAwsResourceProperty— Überprüft, ob die von Ihnen angegebene Instanz von Systems Manager verwaltet wird und ob der Status lautet0nline.
- aws:branch— Verzweigungen basieren darauf, ob es sich bei dem Root-Gerät der Instance um ein Amazon EBS-Volume handelt.
- aws:branch— Verzweigungen basieren darauf, ob das ENA-Attribut für die Instance aktiviert ist.
- aws:runCommand— Sucht nach ENA-Treibern auf der Instance.

- `aws:runCommand`— Sucht nach NVMe Treibern auf der Instanz.
- `aws:runCommand`- Überprüft die `fstab` Datei auf unbekannte Formate.
- `aws:runCommand`- Überprüft, ob die Konfiguration des Schnittstellennamens auf der Instanz vorhersehbar ist.
- `aws:executeScript`- Generiert eine Ausgabe auf der Grundlage der vorherigen Schritte.

Ausgaben

FinalOutput.Output — Die Ergebnisse der von der Automatisierung durchgeführten Prüfungen.

AWSSupport-CloneXenEC2InstanceAndMigrateToNitro

Beschreibung

Die beiden AWSSupport-CloneXenEC InstanceAndMigrateToNitro Runbooks klonen, bereiten die geklonte Amazon Elastic Compute Cloud (Amazon EC2) Linux-Instance, die derzeit auf der Amazon EC2 Xen-Plattform läuft, vor und migrieren sie für die Ausführung auf der Amazon EC2 Nitro-Plattform. Diese Automatisierung ist in drei verschiedene Bereiche unterteilt:

- Vorläufige Prüfungen: Evaluiert alle Voraussetzungen, um mit der Migration fortzufahren, einschließlich der Prüfung, ob die Amazon EC2 EC2-Zielinstanz bereits auf der Nitro-Plattform läuft, ermittelt den Lebenszyklusstatus, validiert das Betriebssystem und überprüft die Systems Manager Manager-Konnektivität.
- Test: Erstellt einen Test AMI aus der Amazon EC2 EC2-Zielinstanz und startet eine Amazon EC2 EC2-Testinstanz, um den Migrationsprozess zu validieren, bevor Sie fortfahren.
- CloneAndMigrate: Erstellt einen Klon der Amazon EC2 EC2-Zielinstanz, installiert die erforderlichen Treiber, konfiguriert das System für die Nitro-Plattform und ändert den Instance-Typ in den gewünschten Nitro-Typ.

> **Important**
>
> Bevor Sie die Genehmigung zum Stoppen der Amazon EC2 EC2-Zielinstanz erteilen, stellen Sie sicher, dass alle Anwendungen, die auf der Instance ausgeführt werden, ordnungsgemäß geschlossen wurden. Wenn der Amazon EC2 EC2-Instance keine Elastic IP-Adresse zugeordnet ist, ändert sich die automatische öffentliche IPv4 Adresse, sobald die Instance gestoppt und gestartet wird.

> **Important**
>
> Haftungsausschluss: Bei der Ausführung dieses Runbooks können zusätzliche Gebühren für Ihr Konto für die Amazon EC2 EC2-Instance, Amazon EBS Volumes & s. anfallen. AMI Weitere Informationen finden Sie in den Amazon EC2 EC2-Preisen und Amazon EBS-Preisen.

> **Important**
>
> Voraussetzungen
> Die Amazon EC2 EC2-Zielinstanz benötigt ausgehenden Zugriff auf die Repositorys, um Treiber und Abhängigkeiten wie`kernel-devel`,,,,,,,`gcc`,,`patch`,`rpm-build`, `wget` `dracut` `makelinux-headers`, zu installieren und bei Bedarf den Paketmanager zu `unzip` verwenden.

Unterstützte Betriebssysteme

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

Wie funktioniert es?

Das Runbook führt die folgenden allgemeinen Schritte aus:

- Validiert die Voraussetzungen und prüft, ob die Instanz für die Migration geeignet ist.
- Erstellt und testet eineAMI, um sicherzustellen, dass die Migration erfolgreich ist.
- Aktiviert das ENA-Attribut (Enhanced Networking) und installiert die neuesten ENA-Treiber.
- Überprüft und konfiguriert das NVMe Modul in initramfs.
- Analysiert und modifiziert /etc/fstab, um Gerätenamen durch zu ersetzen. UUIDs
- Deaktiviert vorhersehbare Schnittstellenbenennungen und entfernt persistente Netzwerkregeln.
- Ändert den Typ der geklonten Instanz in den gewünschten Nitro-Typ.

- Erstellt ein FinalAMI, das als Golden Image für den Start von Nitro-Instanzen verwendet werden kann.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `autoscaling:DescribeAutoScalingInstances`
- `ec2:CreateImage`
- `ec2:CreateTags`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `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

Beispiel für eine IAM-Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-CloneXenEC2InstanceAndMigrateToNitroim Systems Manager unter Dokumente zu.
2. Wählen Sie **`Execute automation`**.
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der ARN der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - TargetInstanceId (Erforderlich):
     - Beschreibung: (Erforderlich) Instance-ID der Amazon EC2 EC2-Zielinstanz, die Sie zur Nitro-Plattform migrieren möchten.
     - Typ: `AWS::EC2::Instance::Id`
   - NitroInstanceType (Optional):
     - Beschreibung: (Optional) Geben Sie den Nitro-Zielinstanztyp ein. Es werden nur Nitro M5-, M6-, C5-, C6-, R5-, R6- und T3-Instances unterstützt (z. B. t3.small). Standard: m5.xlarge.
     - Typ: `String`
     - Zulässiges Muster: `^(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$|^t3a?\\.((x|2x)?large|nano|micro|small|medium)$`
     - Standard: `m5.xlarge`
   - SNSTopicArn (erforderlich):
     - Beschreibung: (Erforderlich) Geben Sie den ARN des Amazon SNS SNS-Themas für die Genehmigungsbenachrichtigung an. Dieses Amazon SNS SNS-Thema wird verwendet, um Genehmigungsbenachrichtigungen während der Ausführung der Automatisierung zu senden.
     - Typ: `String`
     - Zulässiges Muster: `^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 (erforderlich):
  - Beschreibung: (Erforderlich) Geben Sie eine Liste der AWS authentifizierten Principals an, die die Aktion entweder genehmigen oder ablehnen können. Die maximale Anzahl an Genehmigern ist 10.
  - Typ: `StringList`
  - Zulässiges Muster: `^[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 (Fakultativ):
  - Beschreibung: (Optional) Die Mindestanzahl von Genehmigungen, die erforderlich sind, um die Automatisierung wieder aufzunehmen. Standard: 1
  - Typ: Ganzzahl
  - Standard: 1
- DeleteResourcesOnFailure (Fakultativ):
  - Beschreibung: (Optional) Ob die geklonte Amazon EC2 EC2-Instance beendet werden soll und AMI ob die Automatisierung fehlschlägt.
  - Typ: `Boolean`
  - Zulässige Werte: `[true, false]`
  - Standard: `true`
- Bestätigung (erforderlich):
  - Beschreibung: (Erforderlich) Bitte lesen Sie die vollständigen Einzelheiten der Aktionen, die von diesem Automatisierungs-Runbook ausgeführt werden, und schreiben Sie „Ja, ich verstehe und bestätige“, wenn Sie die Schritte bestätigen.
  - Typ: `String`
  - Zulässiges Muster: `^Yes, I understand and acknowledge$`
- AllowInstanceStoreInstances (Fakultativ):
  - Beschreibung: (Optional) Wenn Sie angeben`yes`, wird das Runbook auf Instances ausgeführt, denen Instance-Speicher-Volumes angehängt sind. Warnung: Daten in den Instance-Speicher-Volumes gehen verloren, wenn die Instance gestoppt wird. Dieser Parameter hilft, versehentlichen Datenverlust zu vermeiden.
  - Typ: `Boolean`
  - Zulässige Werte: `[yes, no]`

- Standard: no

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - **`checkConcurrency`**:

     Stellt sicher, dass dieses Runbook nur einmal ausgeführt wird, das auf die aktuelle Amazon EC2 EC2-Instance abzielt.
   - **`getTargetInstanceProperties`**:

     Ruft die Details der Amazon EC2 EC2-Zielinstanz ab.
   - **`checkIfNitroInstanceTypeIsSupportedInAZ`**:

     Ermittelt, ob der Nitro-Zielinstanztyp in derselben Availability Zone wie die Amazon EC2 EC2-Zielinstanz unterstützt wird.
   - **`createTestImage`**:

     Erstellt einen Test anhand AMI der bereitgestellten Instance.
   - **`launchTestInstanceInSameSubnet`**:

     Startet eine Amazon EC2-Testinstanz aus dem Test AMI mit derselben Konfiguration wie die Amazon EC2 EC2-Zielinstanz.
   - **`approvalToStopTargetInstance`**:

     Wartet auf die Genehmigung der zuständigen Principals, die Ziel-Instance zu beenden.
   - **`createBackupImage`**:

     Erstellt eine AMI aus der bereitgestellten Instanz für das Backup.
   - **`launchInstanceInSameSubnet`**:

     Startet eine neue Amazon EC2 EC2-Instance aus dem Backup AMI mit derselben Konfiguration wie die Amazon EC2 EC2-Quell-Instance.
   - **`checkAndInstallENADrivers`**:

     Ermittelt die Verfügbarkeit von ENA-Treibern (Enhanced Networking Adapter) auf der Amazon EC2 EC2-Instance und installiert sie, falls sie fehlen.
   - **`checkAndAddNVMEDrivers`**:

Ermittelt die Verfügbarkeit von NVMe-Treibern auf der geklonten Amazon EC2 EC2-Instance und installiert sie, falls sie fehlen.

- **`checkAndModifyFSTABEntries`**:

  Ermittelt, ob die Gerätenamen in verwendet werden, `/etc/fstab` und ersetzt sie durch ihre eigenen UUIDs, falls sie gefunden werden.

- **`setNitroInstanceTypeForClonedInstance`**:

  Legt den angegebenen Amazon EC2 EC2-Zielinstanztyp für die geklonte Amazon EC2 EC2-Instance fest.

- **`approvalForCreatingImageAfterDriversInstallation`**:

  Wartet auf die Genehmigung durch den Benutzer, wenn die geklonte Amazon EC2 EC2-Instance erfolgreich auf der Nitro-Plattform gestartet wurde.

- **`createImageAfterDriversInstallation`**:

  Erstellt nur dann ein Image aus der neuen Amazon EC2 EC2-Instance, wenn die neue Amazon EC2 EC2-Instance erfolgreich auf der Nitro Platform gestartet wurde.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Outputs die detaillierten Ergebnisse der Ausführung.

Referenzen

AWS Systems Manager -Automatisierung

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

AWSSupport-ConfigureEC2Metadata

Beschreibung

Dieses Runbook hilft Ihnen bei der Konfiguration von IMDS-Optionen (Instance Metadata Service) für Amazon Elastic Compute Cloud (Amazon EC2) -Instances. Mit diesem Runbook können Sie Folgendes konfigurieren:

- Erzwingen Sie IMDSv2 beispielsweise die Verwendung von Metadaten.
- Konfigurieren Sie den `HttpPutResponseHopLimit` Wert.
- Erlauben oder verweigern Sie den Zugriff auf Instanz-Metadaten.

Weitere Informationen zu Instance-Metadaten finden Sie unter Configuring the Instance Metadata Service im EC2 Amazon-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Erzwingen IMDSv2

  Typ: Zeichenfolge

  Gültige Werte: erforderlich | optional

  Standard: optional

  Beschreibung: (Optional) Erzwingen IMDSv2. Wenn Sie möchten`required`, verwendet die EC2 Amazon-Instance nur IMDSv2. Wenn Sie möchten`optional`, können Sie zwischen IMDSv1 und IMDSv2 für den Zugriff auf Metadaten wählen.

> **Important**
>
> Wenn Sie dies erzwingen IMDSv2, funktionieren Anwendungen, die IMDSv1 dies verwenden, möglicherweise nicht richtig. Stellen Sie vor der Durchsetzung sicher IMDSv2, dass Ihre Anwendungen, die IMDS verwenden, auf eine Version aktualisiert wurden, die dies unterstützt. IMDSv2 Informationen zu Instance Metadata Service Version 2 (IMDSv2) finden Sie unter Configuring the Instance Metadata Service im EC2 Amazon-Benutzerhandbuch.

- HttpPutResponseHopLimit

  Typ: Ganzzahl

  Gültige Werte: 0-64

  Standard: 0

  Beschreibung: (Optional) Der gewünschte Grenzwert (1—64) für HTTP-PUT-Antwort-Hop-Anfragen für Instance-Metadaten. Dieser Wert steuert die Anzahl der Hops, die die PUT-Antwort durchlaufen kann. Um zu verhindern, dass die Antwort die Instanz verlässt, geben Sie 1 für den Parameter einen Wert an.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der EC2 Amazon-Instance, deren Metadateneinstellungen Sie konfigurieren möchten.

- MetadataAccess

  Typ: Zeichenfolge

  Gültige Werte: aktiviert | deaktiviert

  Standard: aktiviert

  Beschreibung: (Optional) Erlauben oder verweigern Sie den Zugriff auf Instance-Metadaten in der EC2 Amazon-Instance. Wenn Sie dies angeben`disabled`, werden alle anderen Parameter ignoriert und der Metadatenzugriff für die Instance verweigert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

1. branchOnMetadataZugriff — Verzweigt die Automatisierung auf der Grundlage des `MetadataAccess` Parameterwerts.
2. disableMetadataAccess - Ruft die ModifyInstanceMetadataOptions API-Aktion auf, um den Metadaten-Endpunktzugriff zu deaktivieren.
3. branchOnHttpPutResponseHopLimit - Verzweigt die Automatisierung auf der Grundlage des `HttpPutResponseHopLimit` Parameterwerts.
4. maintainHopLimitAndConfigureImdsVersion - Wenn 0 `HttpPutResponseHopLimit` ist, wird das aktuelle Hop-Limit beibehalten und andere Metadatenoptionen geändert.
5. waitBeforeAssertingIMDSv2Status — Wartet 30 Sekunden, bevor der Status bestätigt wird IMDSv2.
6. setHopLimitAndConfigureImdsVersion - Wenn der `HttpPutResponseHopLimit` Wert größer als 0 ist, werden die Metadatenoptionen mithilfe der angegebenen Eingabeparameter konfiguriert.
7. waitBeforeAssertingHopLimit - Wartet 30 Sekunden, bevor die Metadatenoptionen aktiviert werden.
8. assertHopLimit - Bestätigt, dass die `HttpPutResponseHopLimit` Eigenschaft auf den von Ihnen angegebenen Wert gesetzt ist.
9. branchVerificationOnIMDSv2Option — Überprüfung der Zweige auf der Grundlage des `EnforceIMDSv2` Parameterwerts.
10. assert IMDSv2 IsOptional — Bestätigt den `HttpTokens` Wert, der auf `optional` gesetzt ist.
11. assert IMDSv2 IsEnforced — Bestätigt den `HttpTokens` Wert, der auf gesetzt ist. `required`
12. waitBeforeAssertingMetadataState - Wartet 30 Sekunden, bevor bestätigt wird, dass der Metadatenstatus deaktiviert ist.

13. assertMetadataIsDeaktiviert — Bestätigt, dass Metadaten. `disabled`
14. describeMetadataOptions — Ruft die Metadatenoptionen ab, nachdem die von Ihnen angegebenen Änderungen übernommen wurden.

Ausgaben

describeMetadataOptions. Bundesstaat

describeMetadataOptions.MetadataAccess

describeMetadataOptions.IMDSv2

describeMetadataOptions.HttpPutResponseHopLimit

`AWSSupport-ContainEC2Instance`

Beschreibung

Das `AWSSupport-ContainEC2Instance` Runbook bietet eine automatisierte Lösung für das im Artikel Wie isoliere ich die Amazon EC2 EC2-Instance, wenn ich mit einer potenziell kompromittierten oder verdächtigen Instanz konfrontiert werde? Die Automatisierung verzweigt sich je nach den von Ihnen angegebenen Werten.

Wie funktioniert sie?

Dieses Automation-Runbook `AWSSupport-ContainEC2Instance` führt die Netzwerkeindämmung einer Amazon EC2 EC2-Instance durch eine Reihe koordinierter Schritte durch. Wenn es im `Contain` Modus ausgeführt wird, validiert es zunächst die Eingabeparameter und prüft, ob die Instance nicht beendet wurde. Anschließend wird die aktuelle Sicherheitsgruppenkonfiguration zur späteren Wiederherstellung in einem Amazon S3 S3-Bucket gesichert. Das Runbook erstellt zwei Sicherheitsgruppen: eine temporäre „All-Access-Sicherheitsgruppe“ und eine abschließende Sicherheitsgruppe „Containment“. Dabei werden die Netzwerkschnittstellen der Instance schrittweise von ihren ursprünglichen Sicherheitsgruppen zur Sicherheitsgruppe für alle Zugriffe und schließlich zur Containment-Sicherheitsgruppe umgestellt. Falls angegeben, erstellt es sowohl unverschlüsselte als auch verschlüsselte AMI Backups der Instance. Für Instances in einer Auto Scaling Scaling-Gruppe werden die erforderlichen Änderungen an der Auto Scaling Scaling-Gruppe vorgenommen und die Instance in den Standby-Status versetzt. Wenn es im `Release` Modus ausgeführt wird, stellt es die ursprüngliche Netzwerkkonfiguration der Instance mithilfe der gesicherten Einstellungen von

Amazon S3 wieder her. Das Runbook unterstützt einen `DryRun` Parameter, mit dem eine Vorschau von Aktionen angezeigt werden kann, ohne dass Änderungen vorgenommen werden müssen, und umfasst umfassende Mechanismen zur Fehlerbehandlung und Berichterstattung in den gesamten Containment- und Release-Workflows.

Important

- Dieses Runbook führt verschiedene Operationen aus, für die erhöhte Rechte erforderlich sind, z. B. das Ändern von Sicherheitsgruppen, das Erstellen von AMI s und die Interaktion mit Auto Scaling Scaling-Gruppen. Diese Aktionen können möglicherweise zu einer Eskalation von Rechten führen oder sich auf andere Workloads in Ihrem Konto auswirken. Sie sollten die Berechtigungen überprüfen, die der durch den `AutomationAssumeRole` Parameter angegebenen Rolle gewährt wurden, und sicherstellen, dass sie für den beabsichtigten Anwendungsfall geeignet sind. Weitere Informationen zu IAM-Berechtigungen finden Sie in der folgenden AWS Dokumentation: AWS Identity and Access Management (IAM) PermissionsAWS Systems Manager Automation Permissions.
- Dieses Runbook führt mutative Aktionen durch, die möglicherweise zur Nichtverfügbarkeit oder Unterbrechung Ihrer Workloads führen können. Insbesondere werden die Sicherheitsgruppen geändert, die der Amazon EC2 EC2-Zielinstanz zugeordnet sind, was sich auf die Netzwerkkonnektivität auswirken kann. Wenn die Instance Teil einer Auto Scaling Scaling-Gruppe ist, kann das Runbook außerdem die Konfiguration der Gruppe ändern, was sich möglicherweise auf ihr Skalierungsverhalten auswirkt.
- Während des Containment-Prozesses erstellt dieses Runbook zusätzliche Ressourcen, wie Sicherheitsgruppen und s. AMI Diese Ressourcen werden zwar zur Identifizierung markiert, Sie sollten sich jedoch ihrer Erstellung bewusst sein und sicherstellen, dass sie nach Abschluss des Containment-Prozesses ordnungsgemäß bereinigt oder verwaltet werden.
- Wenn der `Action` Parameter auf gesetzt ist`Release`, versucht dieses Runbook, die Konfiguration der Amazon EC2 EC2-Instance in ihren ursprünglichen Zustand zurückzusetzen. Es besteht jedoch das Risiko, dass der Wiederherstellungsprozess fehlschlägt und die Instance in einem inkonsistenten Zustand zurückbleibt. Das Runbook enthält Anweisungen für die manuelle Wiederherstellung im Falle solcher Fehler. Sie sollten jedoch darauf vorbereitet sein, mögliche Probleme während des Wiederherstellungsprozesses zu lösen.

Es wird empfohlen, das Runbook gründlich zu überprüfen, seine möglichen Auswirkungen zu verstehen und es in einer Nicht-Produktionsumgebung zu testen, bevor Sie es in Ihrer Produktionsumgebung ausführen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- automatische Skalierung: CreateOrUpdateTags
- automatische Skalierung: DeleteTags
- automatische Skalierung: DescribeAutoScalingGroups
- automatische Skalierung: DescribeAutoScalingInstances
- automatische Skalierung: DescribeTags
- automatische Skalierung: EnterStandby
- automatische Skalierung: ExitStandby
- automatische Skalierung: 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

Beispiel für eine Richtlinie:

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": "*"
   }
  ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-ContainEC2Instanceim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:

- AutomationAssumeRole (Fakultativ):
  - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
  - Typ: `AWS::IAM::Role::Arn`
- Aktion (erforderlich):
  - Beschreibung: (Erforderlich) Wählen Sie `Contain` diese Option, um die Amazon EC2 EC2-Instance zu isolieren oder `Restore` zu versuchen, die ursprüngliche Konfiguration der Amazon EC2 EC2-Instance-Konfiguration aus einem früheren Backup wiederherzustellen.
  - Typ: Zeichenfolge
  - Zulässiges Muster: `Contain|Restore`
- DryRun (Fakultativ):
  - Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, führt die Automatisierung keinen der Befehle aus, sondern berichtet stattdessen, was sie versucht hätte, und beschreibt jeden Schritt detailliert. Standardwert: `true`.
  - Typ: Boolescher Wert
  - Zulässige Werte: `true|false`
- Erstellen AMIBackup (optional):
  - Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, wird eine AMI der Amazon EC2 EC2-Instances erstellt, bevor die Containment-Aktionen ausgeführt werden.
  - Typ: Boolescher Wert
  - Zulässige Werte: `true|false`
- KmsKey (Fakultativ):
  - Beschreibung: (Optional) Die ID des AWS KMS Schlüssels, der verwendet wird, um eine verschlüsselte AMI Amazon EC2 EC2-Zielinstanz zu erstellen. Die Standardeinstellung ist auf gesetzt. `alias/aws/ebs`
  - Typ: Zeichenfolge
  - Zulässiges Muster: `^(((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,})$`

- Backups 3 BucketName (bedingt):
  - Beschreibung: (Bedingt) Amazon Amazon S3 S3-Bucket, um die Konfiguration hochzuladen, wenn sie `Action` ist, `Contain` oder um die Konfiguration wiederherzustellen, wenn sie `Action` ist`Release`. Hinweis: Wenn der angegebene Bucket nicht im Konto vorhanden ist, erstellt die Automatisierung in Ihrem Namen einen Amazon S3 S3-Bucket.
  - Typ: `AWS::S3::Bucket::Name`
- TagIdentifier (Optional):
  - Beschreibung: (Optional) Ein Tag in dem Format`Key=BatchId,Value=78925`, das den AWS Ressourcen hinzugefügt wird, die von diesem Runbook während des Containment-Workflows erstellt oder geändert wurden. Dieses Tag kann verwendet werden, um Ressourcen zu identifizieren und zu verwalten, die während des Containment-Prozesses verknüpft wurden. Während des Wiederherstellungs-Workflows wird das durch diesen Parameter angegebene Tag aus den Ressourcen entfernt. Hinweis: Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
  - Typ: Zeichenfolge
  - Zulässiges Muster: `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{0,128}$`
- Backups 3 BucketAccess (bedingt):
  - Beschreibung: (Bedingt) Der ARN der IAM-Benutzer oder -Rollen, denen nach der Ausführung der Containment-Aktionen Zugriff auf den Amazon S3 S3-Backup-Backup gewährt wird. Dieser Parameter ist erforderlich, wenn er `Action` ist. `Contain` Der oder in dessen Abwesenheit der Benutzer`AutomationAssumeRole`, in dessen Kontext die Automatisierung ausgeführt wird, wird automatisch zur Liste hinzugefügt.
  - Typ: Zeichenfolge
  - Zulässiges Muster: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
- IngressTrafficRules (Fakultativ):
  - Beschreibung: (Optional) Eine durch Kommas getrennte Zuordnung von Sicherheitsgruppeneingangsregeln mit Cidr,, FromPort und ToPort in dem Format IpProtocol, das auf die Amazon EC2 EC2-Instance angewendet werden `[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort":"22", "ToPort":"22"}]` soll. Wenn keine Regeln angegeben werden, wird eine Sicherheitsgruppe ohne Eingangsregeln an die Amazon

EC2 EC2-Instance angehängt, wodurch sie effektiv von eingehendem Datenverkehr isoliert wird.

- Typ: MapList
- Zulässiges Muster: `^\\{\\}$|^\\{\"Cidr\":\"[\\x00-\\x7F+]{1,128}\",\"IpProtocol\":\"[\\x00-\\x7F+]{1,128}\",\"FromPort\":\"[\\x00-\\x7F+]{1,128}\",\"ToPort\":\"[\\x00-\\x7F+]{0,255}\"\\}`

- EgressTrafficRules (Fakultativ):
  - Beschreibung: (Optional) Eine durch Kommas getrennte Zuordnung von Sicherheitsgruppenausgangsregeln mit Cidr,, FromPort und ToPort in dem Format IpProtocol, das auf die Amazon Amazon `[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort":"22", "ToPort":"22"}]` EC2 EC2-Instance angewendet werden soll. Wenn keine Regeln angegeben werden, wird eine Sicherheitsgruppe ohne Ausgangsregeln an die Amazon EC2 EC2-Instance angehängt, wodurch der gesamte ausgehende Datenverkehr effektiv verhindert wird.
  - Typ: MapList
  - Zulässiges Muster: `^\\{\\}$|^\\{\"Cidr\":\"[\\x00-\\x7F+]{1,128}\",\"IpProtocol\":\"[\\x00-\\x7F+]{1,128}\",\"FromPort\":\"[\\x00-\\x7F+]{1,128}\",\"ToPort\":\"[\\x00-\\x7F+]{0,255}\"\\}`
- Backups 3 KeyName (optional):
  - Beschreibung: (Optional) Wenn auf gesetzt `Action` ist`Restore`, gibt dies den Amazon S3 S3-Schlüssel an, mit dem die Automatisierung versucht, die Amazon EC2 EC2-Zielinstanzkonfiguration wiederherzustellen. Der Amazon S3 S3-Schlüssel folgt normalerweise diesem Format:`{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json`. Der Schlüssel kann aus der Ausgabe einer früheren Ausführung der Containment-Automatisierung abgerufen werden.
  - Typ: Zeichenfolge
  - Zulässiges Muster: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - ValidateRequiredInputs

     Überprüft, ob alle erforderlichen Eingaben bereitgestellt wurden.
   - AssertInstanceIsNotTerminated

Prüft, ob die Amazon EC2 EC2-Zielinstanz nicht beendet (gelöscht) ist.

- GetAutoScalingInstanceInfo

  Ruft den Amazon EC2 EC2-Instance-Lebenszyklus und den Gruppennamen ab, wenn die Amazon EC2 EC2-Ziel-Instance Teil einer Auto Scaling Scaling-Gruppe ist.

- CheckBackupS3BucketName

  Prüft, ob der Amazon S3 S3-Ziel-Bucket möglicherweise `write` öffentlichen Zugriff auf seine Objekte gewährt`read`. Ein neuer Amazon S3 S3-Bucket wird erstellt, falls der `BackupS3BucketName` Bucket nicht existiert.

- BranchOnActionAndMode

  Verzweigt die Automatisierung auf der Grundlage der Eingabeparameter `Action` und`DryRun`.

- BranchOnAutoScalingGroupMembership

  Verzweigt die Automatisierung auf der Grundlage, ob die Amazon EC2 EC2-Zielinstanz Teil der Auto Scaling Scaling-Gruppe ist und welchen Lebenszyklusstatus sie hat.

- DescribeAutoScalingGroups

  Ruft die zugehörige Amazon EC2 Auto Scaling Scaling-Gruppenkonfiguration ab und speichert sie.

- ModifyAutoScalingGroup

  Ändert die zugehörige Amazon EC2 Auto Scaling Scaling-Gruppenkonfiguration für die Containment-Aktionen, setzt die Amazon EC2 EC2-Instance auf den `Standby` Status und passt die Auto Scaling Scaling-Gruppenkapazität an. `MinSize`

- BackupInstanceSecurityGroups

  Ruft die Konfiguration der Amazon EC2 EC2-Instance-Zielsicherheitsgruppen ab und speichert sie.

- CreateAllAccessSecurityGroup

  Erstellt eine temporäre Sicherheitsgruppe, die den gesamten eingehenden Datenverkehr zulässt und die Sicherheitsgruppen der Amazon EC2 EC2-Zielinstanz ersetzt.

- CreateContainmentSecurityGroup

Erstellt eine restriktive Sicherheitsgruppe mit den angegebenen Eingangs- und Ausgangsregeln und ersetzt die temporäre All-Access-Gruppe durch diese.

- BranchOnCreateAMIBackup

  Verzweigt die Automatisierung auf der Grundlage des Eingabeparameters. `CreateAMIBackup`

- AssertSourceInstanceRootVolumeIsEbs

  Überprüft, ob es sich bei dem Stammvolume der Amazon EC2 EC2-Instance um Amazon EBS handelt.

- CreateImage

  Erstellt eine AMI der Amazon EC2 EC2-Zielinstanzen.

- RestoreInstanceConfiguration

  Stellt die Amazon EC2 EC2-Instance-Zielkonfiguration aus dem Backup wieder her.

- ReportContain

  Gibt Testlaufdetails für die Eindämmungsmaßnahmen aus.

- ReportRestore

  Gibt Details zum Probelauf für die Wiederherstellungsmaßnahmen aus.

- ReportRestoreFailure

  Enthält Anweisungen zum Wiederherstellen der ursprünglichen Konfiguration der Amazon EC2 EC2-Zielinstanz während eines Ausfallszenarios für den Wiederherstellungs-Workflow.

- ReportContainmentFailure

  Enthält Anweisungen zum Wiederherstellen der ursprünglichen Konfiguration der Amazon EC2 EC2-Zielinstanz während eines Ausfallszenarios für den Containment-Workflow.

- FinalOutput

  Gibt die Details der Eindämmungsmaßnahmen aus.

7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   - FinalOutput. Ausgabe

Gibt die Details der von diesem Runbook ausgeführten Containment-Aktionen aus, wenn diese Option auf False gesetzt `DryRun` ist.

- RestoreInstanceConfiguration. Ausgabe

  Gibt die von diesem Runbook ausgeführten Wiederherstellungsaktionen aus, wenn der Wert auf `DryRun` False gesetzt ist.

- ReportContain. Ausgabe

  Gibt die Details der von diesem Runbook ausgeführten Containment-Aktionen aus, wenn diese Option auf True gesetzt `DryRun` ist.

- ReportRestore.Ausgabe

  Gibt die Details der von diesem Runbook ausgeführten Wiederherstellungsaktionen aus, wenn der Wert auf `DryRun` True gesetzt ist.

- ReportContainmentFailure.Ausgabe

  Enthält Anweisungen zum Wiederherstellen der ursprünglichen Konfiguration der Amazon EC2 EC2-Zielinstanz während eines Ausfallszenarios für den Containment-Workflow.

- ReportRestoreFailure. Ausgabe

  Enthält Anweisungen zum Wiederherstellen der ursprünglichen Konfiguration der Amazon EC2 EC2-Zielinstanz während eines Ausfallszenarios für den Wiederherstellungs-Workflow.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Ausführen einer einfachen Automatisierung
- Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

AWSSupport-CopyEC2Instance

Beschreibung

Das `AWSSupport-CopyEC2Instance` Runbook bietet eine automatisierte Lösung für das Verfahren, das im Knowledge Center-Artikel Wie verschiebe ich meine EC2 Instanz in ein anderes Subnetz, in eine Availability Zone oder in eine andere VPC? beschrieben wird. Die Automatisierung verzweigt sich je nach den Werten, die Sie für die `Region` Parameter und angeben. `SubnetId`

Wenn Sie einen Wert für den `SubnetId` Parameter angeben, aber keinen Wert für den `Region` Parameter, erstellt die Automatisierung einen Amazon Machine Image (AMI) der Zielinstanz und startet eine neue Instanz von AMI in dem von Ihnen angegebenen Subnetz.

Wenn Sie einen Wert für den `SubnetId` Parameter und den `Region` Parameter angeben, erstellt die Automatisierung einen AMI der Zielinstanz kopiert die AMI in die von AWS-Region Ihnen angegebene und startet eine neue Instanz von AMI in dem von Ihnen angegebenen Subnetz.

Wenn Sie einen Wert für den `Region` Parameter angeben, aber keinen Wert für den `SubnetId` Parameter, erstellt die Automatisierung einen AMI der Zielinstanz kopiert den AMI in die von Ihnen angegebene Region und startet eine neue Instance von AMI im Standardsubnetz Ihrer Virtual Private Cloud (VPC) in der Zielregion.

Wenn für die `SubnetId` Parameter `Region` oder kein Wert angegeben ist, erstellt die Automatisierung eine AMI der Zielinstanz und startet eine neue Instanz von AMI im Standard-Subnetz Ihrer VPC.

Um ein zu kopieren AMI in eine andere Region müssen Sie einen Wert für den `AutomationAssumeRole` Parameter angeben. Wenn bei der Automatisierung während des `waitForAvailableDestinationAmi` Schritts ein Timeout auftritt, AMI wird möglicherweise immer noch kopiert. In diesem Fall können Sie warten, bis der Kopiervorgang abgeschlossen ist, und die Instance manuell starten.

Bevor Sie diese Automatisierung ausführen, sollten Sie Folgendes beachten:

- AMIs basieren auf Amazon Elastic Block Store (Amazon EBS) -Snapshots. Für große Dateisysteme ohne vorherigen Snapshot AMI Die Erstellung kann mehrere Stunden dauern. Um die zu verringern AMI Erstellungszeit, erstellen Sie einen Amazon EBS-Snapshot, bevor Sie den AMI.
- Erstellen eines AMI erstellt keinen Snapshot, um Volumes auf der Instanz zu speichern. Informationen zum Sichern von Instance-Speicher-Volumes in Amazon EBS finden Sie unter Wie sichere ich ein Instance-Speicher-Volume auf meiner EC2 Amazon-Instance in Amazon EBS?
- Die neue EC2 Amazon-Instance hat eine andere private IPv4 oder öffentliche IPv6 IP-Adresse. Sie müssen alle Verweise auf die alten IP-Adressen (z. B. in DNS-Einträgen) mit den neuen IP-

Adressen aktualisieren, die der neuen Instance zugewiesen sind. Wenn Sie eine Elastic IP-Adresse auf Ihrer Quell-Instance verwenden, achten Sie darauf, diese an die neue Instance anzuhängen.

- Probleme mit dem Domain-Security-Identifier (SID) können auftreten, wenn die Kopie gestartet wird und versucht, die Domain zu kontaktieren. Verwenden Sie Sysprep, bevor Sie das AMI erfassen, oder entfernen Sie die in die Domäne eingebundene Instanz aus der Domäne, um Konfliktprobleme zu vermeiden. Weitere Informationen finden Sie unter Wie kann ich Sysprep verwenden, um benutzerdefinierte wiederverwendbare Windows zu erstellen und zu installieren? AMIs

Führen Sie diese Automatisierung aus (Konsole)

> **Important**
>
> Es wird nicht empfohlen, dieses Runbook zum Kopieren von Microsoft Active Directory-Domänencontroller-Instanzen zu verwenden.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der Instanz, die Sie kopieren möchten.

- KeyPair

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das key pair, das Sie der neuen kopierten Instance zuordnen möchten. Wenn Sie die Instance in eine andere Region kopieren, stellen Sie sicher, dass das key pair in der angegebenen Region existiert.

- Region

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Region, in die Sie die Instance kopieren möchten. Wenn Sie einen Wert für diesen Parameter angeben, aber keine Werte für die `SecurityGroupIds` Parameter `SubnetId` und angeben, versucht die Automatisierung, die Instance in der Standard-VPC mit der Standardsicherheitsgruppe zu starten. Wenn EC2 -Classic in der Zielregion aktiviert ist, schlägt der Start fehl.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Subnetzes, in das Sie die Instance kopieren möchten. Wenn EC2 -Classic in der Zielregion aktiviert ist, müssen Sie einen Wert für diesen Parameter angeben.

- InstanceType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Instance-Typ, als der die kopierte Instance gestartet werden soll. Wenn Sie keinen Wert für diesen Parameter angeben, wird der Quell-Instance-Typ verwendet. Wenn der Quell-Instance-Typ in der Region, in die die Instance kopiert wird, nicht unterstützt wird, schlägt die Automatisierung fehl.

- SecurityGroupIds

  Typ: Zeichenfolge

Beschreibung: (Optional) Eine durch Kommas getrennte Liste von Sicherheitsgruppen, die IDs Sie der kopierten Instance zuordnen möchten. Wenn Sie keinen Wert für diesen Parameter angeben und die Instance nicht in eine andere Region kopiert wird, werden die Sicherheitsgruppen verwendet, die der Quell-Instance zugeordnet sind. Wenn Sie die Instance in eine andere Region kopieren, wird die Standardsicherheitsgruppe für die Standard-VPC in der Zielregion verwendet.

- KeepImageSourceRegion

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: true

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, löscht die Automatisierung nicht AMI der Quellinstanz. Wenn Sie `false` für diesen Parameter angeben, wird durch die Automatisierung die Registrierung aufgehoben AMI und löscht die zugehörigen Snapshots.

- KeepImageDestinationRegion

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: true

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, löscht die Automatisierung nicht AMI das wird in die von Ihnen angegebene Region kopiert. Wenn Sie `false` für diesen Parameter angeben, hebt die Automatisierung die Registrierung des AMI und löscht die zugehörigen Snapshots.

- NoRebootInstanceBeforeTakingImage

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: false

Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, wird die Quellinstanz nicht neu gestartet, bevor die AMI. Wenn diese Option verwendet wird, kann die Integrität des Dateisystems auf dem erstellten Image nicht garantiert werden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

Wenn Sie die Instance in eine andere Region kopieren, benötigen Sie außerdem die folgenden Berechtigungen.

- `ec2:CopyImage`

Dokumentschritte

- describeOriginalInstanceDetails — Sammelt Details aus der Instanz, die kopiert werden soll.
- assertRootVolumeIsEbs - Überprüft, ob es sich um den Gerätetyp des Root-Volumes handelt`ebs`. Ist dies nicht der Fall, wird die Automatisierung beendet.
- evalInputParameters - Wertet die für die Eingabeparameter angegebenen Werte aus.
- createLocalAmi - Erzeugt ein AMI der Quellinstanz.
- tagLocalAmi - Markiert die AMI im vorherigen Schritt erstellt.
- branchAssertRegionIsSame — Verzweigungen basieren darauf, ob die Instanz innerhalb derselben Region oder in eine andere Region kopiert wird.
- branchAssertSameRegionWithKeyPair — Verzweigungen basieren darauf, ob ein Wert für den `KeyPair` Parameter einer Instanz angegeben wurde, die innerhalb derselben Region kopiert wird.

- sameRegionLaunchInstanceWithKeyPair - Startet eine EC2 Amazon-Instance von AMI der Quell-Instance im selben Subnetz oder dem Subnetz, das Sie mit dem von Ihnen angegebenen key pair angeben.
- sameRegionLaunchInstanceWithoutKeyPair - Startet eine EC2 Amazon-Instance von AMI der Quell-Instance im selben Subnetz oder dem von Ihnen angegebenen Subnetz ohne key pair.
- copyAmiToRegion — Kopiert die AMI in die Zielregion.
- waitForAvailableDestinationAmi - Wartet auf das Kopierte AMI Staat, der werden `available` soll.
- destinationRegionLaunchInstance — Startet eine EC2 Amazon-Instance mit der kopierten AMI.
- branchAssertDestinationAmiToDelete — Verzweigt auf der Grundlage des Werts, den Sie für den `KeepImageDestinationRegion` Parameter angegeben haben.
- deregisterDestinationAmiAndDeleteSnapshots - Deregistriert die kopierten AMI und löscht die zugehörigen Schnappschüsse.
- branchAssertSourceAmiTodelete - Verzweigt auf der Grundlage des Werts, den Sie für den `KeepImageSourceRegion` Parameter angegeben haben.
- deregisterSourceAmiAndDeleteSnapshots - Deregistriert den AMI wird von der Quellinstanz erstellt und löscht die zugehörigen Snapshots.
- sleep — Die Automatisierung wird für 2 Sekunden in den Ruhemodus versetzt. Dies ist ein letzter Schritt.

Ausgaben

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchInstanz. DestinationInstanceId

AWSPremiumSupport-DiagnoseDiskUsageOnLinux

Beschreibung

Das AWSPremiumSupport-DiagnoseDiskUsageOnLinuxRunbook analysiert die Amazon Elastic Block Store (Amazon EBS) -Volumes der Amazon Elastic Compute Cloud (Amazon EC2) -Ziel-Instance, um festzustellen, ob sie erweitert werden müssen. Es überprüft die Nutzung, den Dateisystemtyp und den Erweiterungshistorie der einzelnen Volumes anhand der in den Runbook-Eingabeparametern

definierten Schwellenwerte. Das Skript berücksichtigt Faktoren wie kürzlich vorgenommene Änderungen, unterstützte Dateisysteme und AWS Volumenbeschränkungen. Anschließend werden die Volumes, sofern vorhanden, die für eine Erweiterung in Frage kommen, zusammen mit den entsprechenden Details für jedes Volume ausgegeben.

Wie funktioniert es?

Dieses Runbook führt die folgenden Operationen aus:

- Überprüft, ob die Zielinstanz von Systems Manager verwaltet wird und Windows nicht ausgeführt wird
- Ruft Instanzdetails ab, einschließlich Plattform und Root-Gerätetyp
- Ruft die von der Amazon EC2 EC2-Instance verwendeten Volumes ab
- Führt Vorabprüfungen unter Linux durch, um die Festplattennutzung zu analysieren und Erweiterungskandidaten zu ermitteln
- Gibt Volumes, die für eine Erweiterung in Frage kommen, mit entsprechenden Details aus

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist ein Abonnement für Business + Support, Enterprise Support oder Unified Operations erforderlich. Weitere Informationen finden Sie unter AWS Support Tarife vergleichen.

Führen Sie diese Automatisierung aus (Konsole)

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- ssm: DescribeInstanceInformation
- ec2: DescribeInstances
- ec2: DescribeVolumes
- ssm: SendCommand
- ssm: ListCommandInvocations

Beispiel für eine Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSPremiumSupport-DiagnoseDiskUsageOnLinuxim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der IAM-Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - InstanceId (Erforderlich):
     - Beschreibung: (Erforderlich) ID Ihrer Amazon EC2 EC2-Instance.
     - Typ: `String`
     - Muster zulassen: `^i-[0-9a-f]{8,17}$`

- VolumeExpansionUsageTrigger (Erforderlich):
  - Beschreibung: (Erforderlich) Mindestbelegung des Partitionsspeichers, der zum Auslösen der Erweiterung erforderlich ist (in Prozent).
  - Typ: `String`
  - Muster zulassen: `^[0-9]{1,2}$`
- VolumeExpansionCapSize (Erforderlich):
  - Beschreibung: (Erforderlich) Maximale Größe, auf die das Amazon EBS-Volume erhöht wird (in GiB).
  - Typ: `String`
  - Muster zulassen: `^[0-9]{1,4}$`
- VolumeExpansionGibIncrease (Erforderlich):
  - Beschreibung: (Erforderlich) Erhöhung des Volumens in GiB. Der größte Nettozuwachs zwischen `VolumeExpansionGibIncrease` und `VolumeExpansionPercentageIncrease` wird genutzt.
  - Typ: `String`
  - Muster zulassen: `^[0-9]{1,4}$`
- VolumeExpansionPercentageIncrease (Erforderlich):
  - Beschreibung: (Erforderlich) Erhöhung des Prozentsatzes des Volumens. Der größte Nettozuwachs zwischen `VolumeExpansionGibIncrease` und `VolumeExpansionPercentageIncrease` wird genutzt.
  - Typ: `String`
  - Muster zulassen: `^[0-9]{1,2}$`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - AssertInstanceIsManagedInstance:

     Prüft, ob die Zielinstanz von Systems Manager verwaltet wird.
   - DescribeInstance:

     Beschreibt die Amazon EC2 EC2-Zielinstanz und ruft die Instance-Details ab`Platform`, einschließlich, und. `RootDeviceType`
   - BranchOnPlatform:

Verzweigt nach dem Plattformtyp und setzt die Ausführung fort, falls es sich um eine andere Plattform als Windows handelt.

- DescribeVolumes:

  Ruft die von der Amazon EC2 EC2-Instance verwendeten Volumes ab.

- RunPreChecksOnLinux:

  Führt die Prüfungen anhand der im vorherigen Schritt gesammelten Volumes durch.

7. Wenn Sie den Vorgang abgeschlossen haben, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

AWSSupport-EnableWindowsEC2SerialConsole

Beschreibung

Das Runbook `AWSSupport-EnableWindowsEC2SerialConsole` unterstützt Sie bei der Aktivierung der Amazon EC2 Serial Console, der Special Admin Console (SAC) und des Startmenüs auf Ihrer Amazon EC2 EC2-Windows-Instance. Mit der Serial Console-Funktion von Amazon Elastic Compute Cloud (Amazon EC2) haben Sie Zugriff auf die serielle Schnittstelle Ihrer Amazon EC2 EC2-Instance, um Boot-, Netzwerkkonfigurations- und andere Probleme zu beheben. Das Runbook automatisiert die Schritte, die erforderlich sind, um die Funktion für Instances zu aktivieren, die sich im Status Running befinden und von verwaltet werden AWS Systems Manager, sowie für Instances, die sich im Status „Gestoppt“ oder „Nicht verwaltet von“ befinden. AWS Systems Manager

Wie funktioniert es?

Das `AWSSupport-EnableWindowsEC2SerialConsole` Automation Runbook hilft dabei, SAC und das Startmenü auf Amazon EC2 EC2-Instances zu aktivieren, auf denen Microsoft Windows Server ausgeführt wird. Für Instances, die sich im Status Running befinden und von verwaltet werden

AWS Systems Manager, führt das Runbook ein AWS Systems Manager Run PowerShell Command-Skript aus, um SAC und das Startmenü zu aktivieren. Für Instances im Status „Gestoppt“ oder „Nicht verwaltet von“ verwendet das Runbook die AWSSupport-StartEC2 AWS Systems Manager, RescueWorkflow um eine temporäre Amazon EC2 EC2-Instance zu erstellen, um die erforderlichen Änderungen offline durchzuführen.

Weitere Informationen finden Sie unter Amazon EC2 Serial Console für Windows-Instances.

Important

- Wenn Sie SAC auf einer Instance aktivieren, funktionieren die Amazon EC2-Services, die auf den Kennwortabruf angewiesen sind, nicht von der Amazon EC2 EC2-Konsole aus. Weitere Informationen finden Sie unter SAC zur Fehlerbehhebung von Windows-Instances verwenden.
- Um den Zugriff auf die serielle Konsole zu konfigurieren, müssen Sie den Zugriff auf die serielle Konsole auf Kontoebene gewähren und anschließend AWS Identity and Access Management (IAM) -Richtlinien konfigurieren, um Ihren Benutzern Zugriff zu gewähren. Sie müssen auch einen passwortbasierten Benutzer für jede Instance konfigurieren, damit Ihre Benutzer die serielle Konsole zur Fehlerbehebung verwenden können. Weitere Informationen finden Sie unter Zugriff auf die Amazon EC2 Serial Console konfigurieren.
- Informationen darüber, ob die serielle Konsole in Ihrem Konto aktiviert ist, finden Sie unter Kontozugriffsstatus zur seriellen Konsole anzeigen.
- Der serielle Konsolenzugriff wird nur auf virtualisierten Instanzen unterstützt, die auf dem Nitro-System basieren.

Weitere Informationen finden Sie unter Voraussetzungen für die serielle Amazon EC2 EC2-Konsole.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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"
                    ]
                }
            }
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-EnableWindowsEC2SerialConsole` in der AWS Systems Manager Konsole zum.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - InstanceId: (Erforderlich)

     Die ID der Amazon EC2 EC2-Instance, für die Sie die serielle Amazon EC2 EC2-Konsole (SAC) und das Startmenü aktivieren möchten.
   - AutomationAssumeRole: (Optional)

     Der Amazon-Ressourcenname (ARN) der IAM-Rolle, der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - HelperInstanceType: (Bedingt)

     Der Typ der Amazon EC2 EC2-Instance, die das Runbook zur Konfiguration der seriellen Amazon EC2 EC2-Konsole für eine Offline-Instance bereitstellt.
   - HelperInstanceProfileName: (Befriedigend)

     Der Name eines vorhandenen IAM-Instanzprofils für die Helper-Instance. Wenn Sie SAC und das Startmenü für eine Instance aktivieren, die sich im Status Stopped befindet oder nicht von verwaltet wird AWS Systems Manager, ist dies erforderlich. Wenn kein IAM-Instanzprofil angegeben ist, erstellt die Automatisierung eines in Ihrem Namen.
   - SubnetId: (Befriedigend)

     Die Subnetz-ID für eine Hilfsinstanz. Standardmäßig verwendet sie dasselbe Subnetz, in dem sich die bereitgestellte Instanz befindet.

     > **Important**
     >
     > Wenn Sie ein benutzerdefiniertes Subnetz angeben, muss es sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die Systems Manager Manager-Endpunkte ermöglichen. Dies ist nur erforderlich, wenn sich die

Zielinstanz im Status „Gestoppt“ befindet oder nicht von verwaltet wird. AWS Systems Manager

- CreateInstanceBackupBeforeScriptExecution: (Optional)

  Geben Sie True an, um ein Amazon Machine Images (AMI) -Backup der Amazon EC2 EC2-Instance zu erstellen, bevor Sie SAC und das Startmenü aktivieren. Das AMI bleibt nach Abschluss der Automatisierung erhalten. Es liegt in Ihrer Verantwortung, den Zugriff auf das AMI zu sichern oder es zu löschen.

- BackupAmazonMachineImagePrefix: (Befriedigend)

  Ein Präfix für das Amazon Machine Image (AMI), das erstellt wird, wenn der `CreateInstanceBackupBeforeScriptExecution` Parameter auf gesetzt ist`True`.

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - CheckIfEc2SerialConsoleAccessEnabled:

     Prüft, ob der Zugriff auf die Amazon EC2 Serial Console auf Kontoebene aktiviert ist. Hinweis: Der Zugriff auf die serielle Konsole ist standardmäßig nicht verfügbar. Weitere Informationen finden Sie unter Zugriff auf die Amazon EC2 Serial Console konfigurieren.

   - CheckIfEc2: InstanceIsWindows

     Bestätigt, ob es sich bei der Zielinstanzplattform um Windows handelt.

   - GetInstanceType:

     Ruft den Instanztyp der Zielinstanz ab.

   - CheckIfInstanceTypeIsNitro:

     Überprüft, ob der Hypervisor vom Instanztyp Nitro-basiert ist. Der serielle Konsolenzugriff wird nur auf virtualisierten Instanzen unterstützt, die auf dem Nitro-System basieren.

   - CheckIfInstanceIsInAutoScalingGroup:

     Überprüft, ob die Amazon EC2-Instance Teil einer Amazon EC2 Auto Scaling-Gruppe ist, indem die `DescribeAutoScalingInstances` API aufgerufen wird. Wenn die Instance Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe ist, wird sichergestellt, dass sich der Portierungsassistent für .NET-Instance im Standby-Lebenszyklusstatus befindet.

- WaitForEc2: InstanceStateStablized

  Wartet darauf, dass sich die Instanz im Status „Wird ausgeführt“ oder „Gestoppt“ befindet.

- GetEc2: InstanceState

  Ruft den aktuellen Status der Instanz ab.

- BranchOnEc2InstanceState:

  Verzweigt auf der Grundlage des im vorherigen Schritt abgerufenen Instanzstatus. Wenn dieser Instanzstatus ausgeführt wird, geht er zum `CheckIfEc2InstanceIsManagedBySSM` Schritt über, und wenn nicht, geht er zum `CheckIfHelperInstanceProfileIsProvided` Schritt über.

- CheckIfEc2 InstanceIsManagedBy SSM:

  Überprüft, ob die Instanz von AWS Systems Manager verwaltet wird. Wenn das Runbook verwaltet wird, aktiviert es SAC und das Startmenü mithilfe eines PowerShell Run-Befehls.

- BranchOnPreEC2RescueBackup:

  Verzweigt auf der Grundlage des `CreateInstanceBackupBeforeScriptExecution` Eingabeparameters.

- CreateAmazonMachineImageBackup:

  Erstellt ein AMI-Backup der Instance.

- Aktiviert SACAndBootMenu:

  Aktiviert SAC und das Startmenü, indem ein PowerShell Run Command-Skript ausgeführt wird.

- RebootInstance:

  Startet die Amazon EC2 EC2-Instance neu, um die Konfiguration anzuwenden. Dies ist der letzte Schritt, wenn die Instance online ist und von verwaltet wird. AWS Systems Manager

- CheckIfHelperInstanceProfileIsProvided:

  Überprüft, ob der `HelperInstanceProfileName` angegebene Wert existiert, bevor SAC und das Startmenü mithilfe einer temporären Amazon EC2 EC2-Instance offline aktiviert werden.

- RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu:

Führt das`AWSSupport-StartEC2RescueWorkflow`, um SAC und das Startmenü zu aktivieren, aus, wenn sich die Instance im gestoppten Zustand befindet oder nicht von verwaltet wird AWS Systems Manager.

- GetExecutionDetails:

  Ruft die Image-ID der Backup- und Offline-Skriptausgabe ab.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:
   - Aktivieren SACAndBootMenu. Ausgabe:

     Ausgabe der Befehlsausführung im `EnableSACAndBootMenu` Schritt.
   - GetExecutionDetails.OfflineScriptOutput:

     Ausgabe des im `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` Schritt ausgeführten Offline-Skripts.
   - GetExecutionDetails.BackupBeforeScriptExecution:

     Image-ID des AMI-Backups, das erstellt wurde, wenn der `CreateInstanceBackupBeforeScriptExecution` Eingabeparameter True ist.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

`AWSPremiumSupport-ExtendVolumesOnWindows`

Beschreibung

Das `AWSPremiumSupport-ExtendVolumesOnWindows` Runbook erweitert die Amazon Elastic Block Store (Amazon EBS) -Volumes, ihre Partitionen und Dateisysteme auf einer Amazon Elastic Compute Cloud (Amazon EC2) -Zielinstanz.

⚠ Wichtige Überlegungen

- Auswirkungen auf den Betrieb und Volumenstatus: Änderungen des Amazon EBS-Volumens erfolgen in drei Phasen: `modifying`, `optimizing`, und `completed`. Diese Automatisierung wird mit der Dateisystemerweiterung fortgesetzt, wenn das Volume den `optimizing` Status erreicht. Während des `optimizing` Zustands kann es zu vorübergehenden Leistungseinbußen und möglichen Störungen auf Dateisystemebene bei der Größenänderung von Partitionen kommen. Sie können den Fortschritt der Amazon EBS-Volumenänderungen überwachen.
- Kosten und Einschränkungen: Die Erhöhung der Größe eines Amazon EBS-Volumes führt zu höheren monatlichen Speicherkosten. Weitere Informationen finden Sie in der Amazon EBS-Preisübersicht. Für das Backup-AMI und die zugehörigen Snapshots, die von diesem Runbook erstellt werden, fallen zusätzliche Gebühren an, die von ihrer Größe und der Dauer der Aufbewahrung abhängen. Wenn Sie bei einigen Volumetypen nach der Erweiterung das gleiche Verhältnis von IOPS pro GB beibehalten möchten, müssen Sie möglicherweise die bereitgestellten IOPS ändern.
- Backup und Wiederherstellung: Das Runbook erstellt ein Backup-AMI, bevor Änderungen an den Volumes vorgenommen werden. Das AMI und die zugehörigen Snapshots werden nicht automatisch aus Ihrem Konto entfernt. Sie sollten diese Backups manuell entfernen, falls sie nicht mehr benötigt werden. Im Falle eines Fehlers können Volumes aus den Snapshots des zugehörigen AMI wiederhergestellt werden, wie unter Ersetzen eines Amazon EBS-Volumes mithilfe eines Snapshots beschrieben.

Wie funktioniert das?

Dieses Runbook führt die folgenden Operationen aus:

- Überprüft, ob die Zielinstanz von Systems Manager verwaltet wird und Windows Server ausgeführt wird
- Stellt sicher, dass dieses Runbook nur einmal ausgeführt wird, das auf die aktuelle Amazon EC2 EC2-Instance abzielt
- Erstellt ein Backup-Amazon Machine Image (AMI) von der Ziel-Instance
- Erweitert die Amazon EBS-Volumes, die für die Erweiterung spezifiziert wurden
- Erweitert die Dateisysteme auf der Ziel-Instance mithilfe von Befehlen PowerShell

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist ein Abonnement für Business + Support, Enterprise Support oder Unified Operations erforderlich. Weitere Informationen finden Sie unter AWS Support Tarife vergleichen.

Führen Sie diese Automatisierung aus (Konsole)

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Beispiel für eine IAM-Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSPremiumSupport-ExtendVolumesOnWindows`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der IAM-Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - InstanceId (Erforderlich):
     - Beschreibung: (Erforderlich) Die ID der Amazon EC2-Instance.
     - Typ: `String`
     - Muster zulassen: `^i-[0-9a-f]{8,17}$`
   - VolumeExpansionCapSize (Erforderlich):
     - Beschreibung: (Erforderlich) Maximale Größe (in GiB), mit der die Amazon EBS-Volumes erhöht werden.
     - Typ: `String`
     - Muster zulassen: `^[0-9]{1,4}$`
   - DiagnosticResults (Erforderlich):
     - Beschreibung: (Erforderlich) Die Ergebnisse des Prechecks-Skripts aus dem `DiagnoseDiskUsage` Dokument, formatiert als einzeiliges CSV-Format. Die Zeichenfolge

beginnt mit, `EXTEND;` gefolgt von kommagetrennten Volumeninformationen für jeden Datenträger, wobei die Volumen durch Semikolons getrennt sind. Zu den Informationen jedes Volumes gehören: Volume-ID, Laufwerksbuchstabe, Erweiterungskennzeichnung (1 zum Erweitern, 0 zum Überspringen), Neue Größe in GB, AWS Region und Grund/Aktion.

- Typ: `String`
- Muster zulassen: `^EXTEND;[0-9a-zA-Z\\.;_%:\\-\/,\\s]{7,5400}$`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - AssertInstanceIsManagedInstance:

     Überprüft, ob die Zielinstanz von Systems Manager verwaltet wird.
   - DescribeInstance:

     Ruft die Plattforminformationen der Amazon EC2 EC2-Zielinstanz ab.
   - BranchOnPlatform:

     Bestätigt, dass die Amazon EC2 EC2-Instance-Zielplattform Windows Server ist.
   - CheckConcurrency:

     Stellt sicher, dass dieses Runbook nur einmal ausgeführt wird, das auf die aktuelle Amazon EC2 EC2-Instance abzielt.
   - CreateImage:

     Erstellt ein Backup-Amazon Machine Image (AMI) von der Ziel-Instance.
   - WaitUntilImageReady:

     Wartet darauf, dass das Amazon Machine Image (AMI) die Erstellung abgeschlossen hat und den `available` Status erreicht hat.
   - Verlängern EBSVolume:

     Erweitert die Amazon EBS-Volumes der Ziel-Instance, die für die Erweiterung angegeben wurden.
   - DescribeVolumes:

     Beschreibt die Amazon EBS-Volumes der Ziel-Instance, die für die Erweiterung angegeben wurden.

- ExtendFilesystem:

  Erweitert die Dateisysteme der Ziel-Instance mithilfe PowerShell von Befehlen.

7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows
- Amazon EBS-Volumenänderungen anfordern

AWSSupport-ExecuteEC2Rescue

Beschreibung

Dieses Runbook verwendet EC2Rescue Tool zur Behebung und, wenn möglich, Reparatur häufiger Verbindungsprobleme mit der angegebenen Amazon Elastic Compute Cloud (Amazon EC2) - Instance für Linux oder Windows Server. Instanzen mit verschlüsselten Root-Volumes werden nicht unterstützt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- EC2RescueInstanceType

  Typ: Zeichenfolge

  Gültige Werte: t2.small | t2.medium | t2.large

  Standard: t2.small

  Beschreibung: (Erforderlich) Der Instance-Typ für EC2 EC2Rescue sein. Empfohlene Größe: `t2.small`

- LogDestination

  Typ: Zeichenfolge

  Beschreibung: (Optional) Name des Amazon S3 S3-Buckets in Ihrem Konto, in das Sie die Fehlerbehebungsprotokolle hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie keine unnötigen Lese-/Schreibberechtigungen für Parteien gewährt, die keinen Zugriff auf die gesammelten Protokolle benötigen.

- SubnetId

  Typ: Zeichenfolge

  Standard: CreateNew VPC

  Beschreibung: (Optional) Die Subnetz-ID für EC2Rescue sein. Standardmäßig erstellt AWS Systems Manager Automation eine neue VPC. Verwenden Sie `SelectedInstanceSubnet` alternativ dasselbe Subnetz wie Ihre Instance oder geben Sie eine benutzerdefinierte Subnetz-ID an.

> **Important**
>
> Das Subnetz muss sich in derselben Availability Zone befinden wie `UnreachableInstanceId` und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

- UnreachableInstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID Ihrer nicht erreichbaren Instanz. EC2

> **Important**
>
> Systems Manager Automation stoppt diese Instanz und erstellt ein AMI, bevor irgendwelche Operationen ausgeführt werden. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP-Adresse verwenden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Sie benötigen mindestens `ssm:StartAutomationExecution` und`ssm:GetAutomationExecution`, um die Automatisierungsausgabe lesen zu können. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter [AWSSupport-StartEC2RescueWorkflow].

Dokumentschritte

1. `aws:assertAwsResourceProperty`- Bestätigt, ob die angegebene Instanz Windows Server:
   a. (EC2Rescue for Windows Server) Wenn die bereitgestellte Instanz eine ist Windows Server Instanz:
      i. `aws:executeAutomation`- Ruft `AWSSupport-StartEC2RescueWorkflow` mit EC2 Rescue for auf Windows Server Offlineskript.
      ii. `aws:executeAwsApi`- Ruft die Backup-AMI-ID aus der verschachtelten Automatisierung ab.

iii. `aws:executeAwsApi`- Ruft die EC2 Rescue-Zusammenfassung aus der verschachtelten Automatisierung ab.

b. (EC2Rescue für Linux) Wenn es sich bei der bereitgestellten Instanz um eine Linux-Instanz handelt:

i. `aws:executeAutomation`- Wird `AWSSupport-StartEC2RescueWorkflow` mit den Offline-Skripten von EC2 Rescue for Linux aufgerufen

ii. `aws:executeAwsApi`- Ruft die Backup-AMI-ID aus der verschachtelten Automatisierung ab.

iii. `aws:executeAwsApi`- Ruft die EC2 Rescue-Zusammenfassung aus der verschachtelten Automatisierung ab.

Ausgaben

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

Beschreibung

Das `AWSSupport-ListEC2Resources` Runbook gibt Informationen über EC2 Amazon-Instances und zugehörige Ressourcen wie Amazon Elastic Block Store (Amazon EBS) -Volumes, Elastic IP-Adressen und Amazon EC2 Auto Scaling Scaling-Gruppen von den von AWS-Regionen Ihnen angegebenen Daten zurück. Standardmäßig werden die Informationen aus allen Regionen gesammelt und in der Ausgabe der Automatisierung angezeigt. Optional können Sie einen Amazon Simple Storage Service (Amazon S3) -Bucket angeben, in den die Informationen als Datei mit kommagetrennten Werten (.csv) hochgeladen werden sollen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des S3-Buckets, in den die gesammelten Informationen hochgeladen werden.

- DisplayResourceDeletionDocumentation

  Typ: Zeichenfolge

  Standard: true

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, erstellt die Automatisierung in der Ausgabe Links zu Dokumentationen, die sich auf das Löschen Ihrer Ressourcen beziehen.

- RegionsToQuery

  Typ: Zeichenfolge

  Standard: Alle

  Beschreibung: (Optional) Die Regionen, aus denen Sie EC2 Amazon-bezogene Informationen sammeln möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRegions`
- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

Um die gesammelten Informationen erfolgreich in den von Ihnen angegebenen S3-Bucket hochzuladen, sind außerdem die folgenden Aktionen `AutomationAssumeRole` erforderlich:

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

Dokumentschritte

- `aws:executeAwsApi`- Sammelt die Regionen, die für das Konto aktiviert sind.
- `aws:executeScript`- Bestätigt, dass die für das Konto aktivierten Regionen die im `RegionsToQuery` Parameter angegebenen Regionen unterstützen.
- `aws:branch`- Wenn keine Regionen für das Konto aktiviert sind, endet die Automatisierung.
- `aws:executeScript`- Listet alle EC2 Instanzen für das Konto und die Regionen auf, die Sie angeben.
- `aws:executeScript`— Listet alle Amazon Machine Images (AMI) für das Konto und die Regionen auf, die Sie angeben.
- `aws:executeScript`- Listet alle EBS-Volumes für das Konto und die Regionen auf, die Sie angeben.

- `aws:executeScript`— Listet alle Elastic IP-Adressen für das Konto und die Regionen auf, die Sie angeben.
- `aws:executeScript`— Listet alle Elastic Network-Schnittstellen für das Konto und die Regionen auf, die Sie angeben.
- `aws:executeScript`- Listet alle Auto Scaling Scaling-Gruppen für das Konto und die Regionen auf, die Sie angeben.
- `aws:executeScript`- Listet alle Load Balancer für das Konto und die Regionen auf, die Sie angeben.
- `aws:executeScript`- Lädt die gesammelten Informationen in den angegebenen S3-Bucket hoch, wenn Sie einen Wert für den `Bucket` Parameter angeben.

`AWSSupport-ManageRDPSettings`

Beschreibung

Das `AWSSupport-ManageRDPSettings` Runbook ermöglicht es dem Benutzer, allgemeine Remote Desktop Protocol (RDP) -Einstellungen wie den RDP-Port und die Network Layer Authentication (NLA) zu verwalten. Standardmäßig liest das Runbook die Werte der Einstellungen und gibt sie aus.

> **Important**
>
> Änderungen an den RDP-Einstellungen sollten sorgfältig geprüft werden, bevor dieses Runbook ausgeführt wird.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der verwalteten Instance, deren RDP-Einstellungen verwaltet werden sollen.

- NLASettingAktion

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Aktivieren | Deaktivieren

  Standard: Check

  Beschreibung: (Erforderlich) Eine Aktion zur Ausführung auf der NLA-Einstellung: Check, Aktivieren, Deaktivieren.

- RDPPort

  Typ: Zeichenfolge

  Standard: 3389

  Beschreibung: (Optional) Angabe des neuen RDP-Ports. Wird nur verwendet, wenn die Aktion auf „Modify“ gesetzt ist. Die Portnummer muss zwischen 1025 und 65535 liegen. Hinweis: Nachdem der Port geändert wurde, wird der RDP-Service neu gestartet.

- RDPPortAktion

  Typ: Zeichenfolge

Gültige Werte: Prüfen | Ändern

Standard: Check

Beschreibung: (Erforderlich) Eine Aktion, die auf den RDP-Port angewendet werden soll.

- RemoteConnections

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Aktivieren | Deaktivieren

  Standard: Check

  Beschreibung: (Erforderlich) Eine Aktion, die für die TSConnections FDeny-Einstellung ausgeführt werden muss.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Die EC2 Instance, die den Befehl empfängt, muss über eine IAM-Rolle mit der von SSMManagedInstanceCoreAmazon verwalteten Richtlinie verfügen. Der Benutzer muss mindestens über ssm: verfügen, SendCommand um den Befehl an die Instance zu senden, sowie über ssm:, GetCommandInvocation um die Befehlsausgabe lesen zu können.

Dokumentschritte

`aws:runCommand`- Führen Sie das PowerShell Skript aus, um die RDP-Einstellungen auf der Zielinstanz zu ändern oder zu überprüfen.

Ausgaben

.Output verwalten RDPSettings

AWSSupport-ManageWindowsService

Beschreibung

Mit dem `AWSSupport-ManageWindowsService` Runbook können Sie jeden Windows-Dienst auf der Zielinstanz beenden, starten, neu starten, anhalten oder deaktivieren.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der verwalteten Instanz, für die die Dienste verwaltet werden sollen.
- ServiceAction

  Typ: Zeichenfolge

  Gültige Werte: Check | Restart | Force-Restart | Start | Stop | Force-Stop | Pause

  Standard: Check

  Beschreibung: (Erforderlich) Eine Aktion, die auf den Windows-Dienst angewendet werden soll. Beachten Sie, dass `Force-Restart` und verwendet werden `Force-Stop` kann, um einen Dienst, der abhängige Dienste hat, neu zu starten und zu beenden.

- StartupType

  Typ: Zeichenfolge

  Gültige Werte: Check | Auto | Demand | Disabled | DelayedAutoStart

  Standard: Check

  Beschreibung: (Erforderlich) Ein Starttyp, der auf den Windows-Dienst angewendet werden soll.
- WindowsServiceName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Ein gültiger Windows-Service-Name.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass die EC2 Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, der die von SSMManagedInstanceCoreAmazon verwaltete Richtlinie beigefügt ist. Der Benutzer muss mindestens über ssm: StartAutomationExecution und ssm: verfügen, SendCommand um die Automatisierung auszuführen und den Befehl an die Instance zu senden, sowie über ssm:, GetAutomationExecution um die Automatisierungsausgabe lesen zu können.

Dokumentschritte

`aws:runCommand`- Führen Sie das PowerShell Skript aus, um die gewünschte Konfiguration auf den Windows-Dienst auf der Zielinstanz anzuwenden.

Ausgaben

manageWindowsService. Ausgabe

AWSSupport-MigrateEC2ClassicToVPC

Beschreibung

Das `AWSSupport-MigrateEC2ClassicToVPC` Runbook migriert eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance von EC2 -Classic zu einer Virtual Private Cloud (VPC). Dieses

Runbook unterstützt die Migration von EC2 Amazon-Instances des Virtualisierungstyps Hardware Virtual Machine (HVM) mit Amazon Elastic Block Store (Amazon EBS) -Root-Volumes.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- Ich genehmige IAM

  Typ: StringList

  Beschreibung: (Optional) Die Amazon-Ressourcennamen (ARNs) von IAM-Benutzern, die die Aktion genehmigen oder ablehnen können. Dieser Parameter gilt nur, wenn Sie den `CutOver` Wert für den `MigrationType` Parameter angeben.
- DestinationSecurityGroupId

  Typ: StringList

  Beschreibung: (Optional) Die ID der Sicherheitsgruppe, die Sie der EC2 Amazon-Instance zuordnen möchten, die in Ihrer VPC gestartet wird. Wenn Sie keinen Wert für diesen Parameter angeben, erstellt die Automatisierung eine Sicherheitsgruppe in Ihrer VPC und kopiert die Regeln aus der Sicherheitsgruppe in EC2 -Classic. Wenn die Regeln nicht in die neue Sicherheitsgruppe

kopiert werden können, ist die Standardsicherheitsgruppe Ihrer VPC der EC2 Amazon-Instance zugeordnet.

- DestinationSubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Subnetzes, in das Sie Ihre EC2 Amazon-Instance migrieren möchten. Wenn Sie keinen Wert für diesen Parameter angeben, wählt die Automatisierung nach dem Zufallsprinzip ein Subnetz aus Ihrer VPC aus.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der EC2 Amazon-Instance, die Sie migrieren möchten.

- MigrationType

  Typ: Zeichenfolge

  Gültige Werte: CutOver | Test

  Beschreibung: (Erforderlich) Die Art der Migration, die Sie durchführen möchten.

  Für die `CutOver` Option ist eine Genehmigung erforderlich, um Ihre EC2 Amazon-Instance zu beenden, die in EC2 -Classic ausgeführt wird. Nachdem diese Aktion genehmigt wurde, wird die EC2 Amazon-Instance gestoppt und die Automatisierung erstellt eine Amazon Machine Image (AMI). Wenn der AMI Status ist`available`, von hier aus wird eine neue EC2 Amazon-Instance gestartet AMI in der, die `DestinationSubnetId` Sie in Ihrer VPC angeben. Wenn Ihrer EC2 Amazon-Instance, die in EC2 -Classic ausgeführt wird, eine Elastic IP-Adresse zugewiesen ist, wird die Instance auf die neu erstellte EC2 Amazon-Instance in Ihrer VPC verschoben. Wenn die EC2 Amazon-Instance, die in Ihrer VPC gestartet wird, aus irgendeinem Grund nicht erstellt werden kann, wird sie beendet und die Genehmigung für den Start Ihrer EC2 Amazon-Instance in EC2 -Classic angefordert.

  Die `Test` Option erstellt eine AMI Ihrer EC2 Amazon-Instance, die in EC2 -Classic ohne Neustart läuft. Da die EC2 Amazon-Instance nicht neu gestartet wird, können wir die Dateisystemintegrität des erstellten Images nicht garantieren. Wenn der AMI Status ist`available`, von hier aus wird eine neue EC2 Amazon-Instance gestartet AMI in der`DestinationSubnetId`, die Sie in Ihrer VPC angeben. Wenn Ihrer EC2 Amazon-Instance, die in EC2 -Classic ausgeführt wird, eine Elastic IP-Adresse zugewiesen ist, überprüft die Automatisierung, ob die von `DestinationSubnetId`

Ihnen angegebene öffentlich ist. Wenn die EC2 Amazon-Instance, die in Ihrer VPC gestartet wird, aus irgendeinem Grund nicht erstellt werden kann, wird sie beendet und die Automatisierung wird beendet.

- SNSNotificationARNforGenehmigung

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN des Amazon Simple Notification Service (Amazon SNS) - Themas, an das Sie Genehmigungsanfragen senden möchten. Dieser Parameter gilt nur, wenn Sie den `CutOver` Wert für den `MigrationType` Parameter angeben.
- TargetInstanceType

  Typ: Zeichenfolge

  Standard: t2.2xlarge

  Beschreibung: (Optional) Der Typ der EC2 Amazon-Instance, die Sie in Ihrer VPC starten möchten. Es werden nur Xen-basierte Instance-Typen wie T2, M4 oder C4 unterstützt.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeAwsApi- Sammelt Details über die EC2 Amazon-Instance, die Sie im InstanceId Parameter angeben.
- aws:assertAwsResourceProperty— Bestätigt, dass der Instance-Typ, den Sie im TargetInstanceType Parameter angeben, XEN-basiert ist.
- aws:assertAwsResourceProperty— Bestätigt, dass die EC2 Amazon-Instance, die Sie im InstanceId Parameter angeben, vom Virtualisierungstyp HVM ist.
- aws:assertAwsResourceProperty— Bestätigt, dass die EC2 Amazon-Instance, die Sie im InstanceId Parameter angeben, über ein Amazon EBS-Root-Volume verfügt.
- aws:executeScript— Erstellt je nach Bedarf eine Sicherheitsgruppe, abhängig von dem Wert, den Sie für den DestinationSecurityGroupId Parameter angeben.
- aws:branch- Verzweigt auf der Grundlage des Werts, den Sie im DestinationSubnetId Parameter angeben.

- `aws:executeAwsApi`— Identifiziert die Standard-VPC in dem Bereich, in AWS-Region dem Sie diese Automatisierung ausführen.
- `aws:executeAwsApi`- Wählt nach dem Zufallsprinzip die ID eines Subnetzes aus, das sich in der Standard-VPC befindet.
- `aws:createImage`- Erzeugt ein AMI ohne die EC2 Amazon-Instance neu zu starten.
- `aws:branch`— Verzweigt auf der Grundlage des Werts, den Sie für den `MigrationType` Parameter angeben.
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den `DestinationSubnetId` Parameter angeben.
- `aws:runInstances`- Startet eine neue Instanz von AMI erstellt, ohne die EC2 Amazon-Instanz in EC2 -Classic neu zu starten.
- `aws:changeInstanceState`- Beendet die neu gestartete EC2 Amazon-Instance, wenn der vorherige Schritt aus irgendeinem Grund fehlschlägt.
- `aws:runInstances`- Startet eine neue Instance von AMI erstellt, ohne die EC2 Amazon-Instanz in EC2 -Classic neu zu starten, falls angegeben. `DestinationSubnetId`
- `aws:changeInstanceState`- Beendet die neu gestartete EC2 Amazon-Instance, wenn der vorherige Schritt aus irgendeinem Grund fehlschlägt.
- `aws:assertAwsResourceProperty`- Bestätigt das Stoppverhalten für die EC2 Amazon-Instance, die in EC2 -Classic ausgeführt wird.
- `aws:approve`- Wartet auf die Genehmigung zum Stoppen der EC2 Amazon-Instance.
- `aws:changeInstanceState`- Stoppt die Ausführung der EC2 Amazon-Instance in EC2 -Classic.
- `aws:changeInstanceState`- Force stoppt die Ausführung der EC2 Amazon-Instance in EC2 -Classic, falls erforderlich.
- `aws:createImage`- Erzeugt ein AMI der EC2 Amazon-Instance, nachdem sie gestoppt wurde.
- `aws:branch`— Verzweigt auf der Grundlage des für den `DestinationSubnetId` Parameter angegebenen Werts.
- `aws:runInstances`- Startet eine neue Instanz von AMI erstellt aus der gestoppten EC2 Amazon-Instance in EC2 -Classic.
- `aws:approve`- Wartet auf die Genehmigung zum Beenden der neu gestarteten Instance und startet die EC2 Amazon-Instance in EC2 -Classic, falls der vorherige Schritt aus irgendeinem Grund fehlschlägt.
- `aws:changeInstanceState`— Beendet die neu gestartete EC2 Amazon-Instance.

- `aws:runInstances`- Startet eine neue Instance von AMI wurde aus der gestoppten EC2 Amazon-Instance in EC2 -Classic anhand des `DestinationSubnetId` Parameters erstellt.
- `aws:approve`- Wartet auf die Genehmigung zum Beenden der neu gestarteten Instance und startet die EC2 Amazon-Instance in EC2 -Classic, falls der vorherige Schritt aus irgendeinem Grund fehlschlägt.
- `aws:changeInstanceState`— Beendet die neu gestartete EC2 Amazon-Instance.
- `aws:changeInstanceState`- Startet die EC2 Amazon-Instance, die in EC2 -Classic gestoppt wurde.
- `aws:branch`— Verzweigungen basierend darauf, ob die EC2 Amazon-Instance eine öffentliche IP-Adresse hat.
- `aws:executeAwsApi`— Überprüft, ob es sich bei der öffentlichen IP-Adresse um eine Elastic IP-Adresse handelt.
- `aws:branch`— Verzweigt auf der Grundlage des Werts, den Sie im `MigrationType` Parameter angeben.
- `aws:executeAwsApi`- Verschiebt die Elastic IP-Adresse in Ihre VPC.
- `aws:executeAwsApi`- Erfasst die Zuweisungs-ID der Elastic IP-Adresse, die auf Ihre VPC verschoben wurde.
- `aws:branch`— Verzweigungen, die darauf basieren, in welchem Subnetz die EC2 Amazon-Instance, die in Ihrer VPC ausgeführt wird, gestartet wurde.
- `aws:executeAwsApi`- Hängt die Elastic IP-Adresse an die neu gestartete Instance in Ihrer VPC an.
- `aws:executeScript`— Bestätigt, dass das Subnetz, in dem Ihre neu gestartete EC2 Amazon-Instance in Ihrer VPC läuft, öffentlich ist.

Ausgaben

g `etInstanceProperties.virtualizationType` — Der Virtualisierungstyp der EC2 Amazon-Instance, die in EC2 -Classic ausgeführt wird.

`getInstanceProperties.rootDeviceType`— Der Root-Gerätetyp der EC2 Amazon-Instance, die in EC2 -Classic ausgeführt wird.

`createAMIWithoutReboot.ImageId`- Die ID des AMI erstellt, ohne die in -Classic ausgeführte EC2 Amazon-Instance neu zu starten. EC2

`getDefaultVPC.VpcId`— Die ID der Standard-VPC, auf der die neue EC2 Amazon-Instance gestartet wird, wenn kein Wert für den `DestinationSubnetId` Parameter angegeben wird.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`— Die ID des Subnetzes in der Standard-VPC, in dem die neue EC2 Amazon-Instance gestartet wird, wenn kein Wert für den `DestinationSubnetId` Parameter angegeben wird.

`launchTestInstanceDefaultVPC.InstanceIds`— Die ID der neu gestarteten EC2 Amazon-Instance in Ihrer Standard-VPC während des `Test` Migrationstyps.

`launchTestInstanceProvidedSubnet.InstanceIds`— Die ID der neu gestarteten EC2 Amazon-Instance in der`DestinationSubnetId`, die Sie während des `Test` Migrationstyps angegeben haben.

`createAMIAfterStoppingInstance.ImageId`- Die ID der AMI erstellt nach dem Stoppen der EC2 Amazon-Instance, die in EC2 -Classic läuft.

`launchCutOverInstanceProvidedSubnet.InstanceIds`— Die ID der neu gestarteten EC2 Amazon-Instance in der`DestinationSubnetId`, die Sie während des `CutOver` Migrationstyps angegeben haben.

`launchCutOverInstanceDefaultVPC.InstanceIds`— Die ID der neu gestarteten EC2 Amazon-Instance in Ihrer Standard-VPC während des `CutOver` Migrationstyps.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`— Ob das von der Automatisierung in Ihrer Standard-VPC ausgewählte Subnetz öffentlich ist.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`— Ob das von Ihnen angegebene Subnetz öffentlich ist`DestinationSubnetId`.

AWSSupport-MigrateXenToNitroLinux

Beschreibung

Das `AWSSupport-MigrateXenToNitroLinux` Runbook klont, bereitet eine Amazon Elastic Compute Cloud (Amazon EC2) Linux Xen-Instance vor und migriert sie auf eine Nitro Instanztyp. Dieses Runbook bietet zwei Optionen für Operationstypen:

- `Clone&Migrate`— Der Arbeitsablauf dieser Option besteht aus den Vorprüfungen, Tests und Clone&MigratePhasen. Der Workflow wird mit dem `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro` Runbook ausgeführt.

- `FullMigration`— Diese Option führt den `Clone&Migrate` Workflow aus und führt dann den zusätzlichen Schritt „Amazon EBS-Stammvolumes ersetzen“ durch.

> **Important**
>
> Durch die Verwendung dieses Runbooks fallen Ihrem Konto Kosten für die Laufzeit von EC2 Amazon-Instances, die Erstellung von Amazon Elastic Block Store (Amazon EBS) -Volumes und AMIs. Weitere Informationen finden Sie unter EC2 Amazon-Preise und Amazon EBS-Preise.

Vorläufige Prüfungen

Die Automatisierung führt die folgenden vorläufigen Prüfungen durch, bevor sie mit der Migration fortfährt. Wenn eine der Prüfungen fehlschlägt, wird die Automatisierung beendet. Diese Phase ist nur ein Teil des `Clone&Migrate` Workflows.

- Prüft, ob die Zielinstanz bereits eine ist Nitro Instanztyp.
- Prüft, ob die Kaufoption für Spot-Instances für die Ziel-Instance verwendet wurde.
- Prüft, ob Instance-Speicher-Volumes an die Ziel-Instance angehängt sind.
- Überprüft, ob das Betriebssystem (OS) der Zielinstanz Linux ist.
- Prüft, ob die Ziel-Instance Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe ist. Wenn sie Teil einer Auto Scaling Scaling-Gruppe ist, überprüft die Automatisierung, ob sich die Instance im `standby` Status befindet.
- Überprüft, ob die Instanz von verwaltet wird. AWS Systems Manager

Testen

Die Automatisierung erstellt eine Amazon Machine Image (AMI) von der Zielinstanz aus und startet eine Testinstanz von der neu erstellten AMI. Diese Phase ist nur Teil des `Clone&Migrate` Workflows.

Wenn die Test-Instance alle Statusprüfungen besteht, wird die Automatisierung angehalten und die Genehmigung durch die designierten Principals wird per Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung angefordert. Wenn die Genehmigung erteilt wurde, beendet die Automatisierung die Test-Instance, stoppt die Ziel-Instance und setzt die Migration fort, während die neu erstellte AMI wird am Ende des Workflows abgemeldet. `Clone&Migrate`

> **Note**
>
> Wir empfehlen, vor der Genehmigung zu überprüfen, ob alle Anwendungen, die auf der Zielinstanz ausgeführt werden, ordnungsgemäß geschlossen wurden.

Klonen und migrieren

Durch die Automatisierung entsteht ein weiterer AMI von der Zielinstanz aus und startet eine neue Instanz, um zu einer zu wechseln Nitro Instanztyp. Die Automatisierung erfüllt die folgenden Voraussetzungen, bevor mit der Migration fortgefahren werden kann. Wenn eine der Prüfungen fehlschlägt, wird die Automatisierung beendet. Diese Phase ist ebenfalls nur ein Teil des `Clone&Migrate` Workflows.

- Aktiviert das ENA-Attribut (Enhanced Networking).
- Installiert die neueste Version der ENA-Treiber, falls sie noch nicht installiert sind, oder aktualisiert die ENA-Treiberversion auf die neueste Version. Um eine maximale Netzwerkleistung zu gewährleisten, ist eine Aktualisierung auf die neueste ENA-Treiberversion erforderlich, wenn Nitro Der Instanztyp ist die 6. Generation.
- Überprüft, ob das NVMe Modul installiert ist. Wenn das Modul installiert ist, überprüft die Automatisierung, ob das Modul geladen ist. `initramfs`
- Analysiert `/etc/fstab` und ersetzt Einträge mit Blockgerätenamen (`/dev/sd*`oder`/dev/xvd*`) durch die entsprechenden UUIDs. Vor dem Ändern der Konfiguration erstellt die Automatisierung eine Sicherungskopie der Datei im Pfad`/etc/fstab*`.
- Deaktiviert vorhersehbare Schnittstellenbenennungen, indem die `net.ifnames=0` Option zur `GRUB_CMDLINE_LINUX` Zeile in der `/etc/default/grub` Datei hinzugefügt wird, falls sie existiert, oder zum Kernel darin`/boot/grub/menu.lst`.
- Entfernt die `/etc/udev/rules.d/70-persistent-net.rules` Datei, falls sie existiert. Vor dem Entfernen der Datei erstellt die Automatisierung eine Sicherungskopie der Datei im Pfad`/etc/udev/rules.d/`.

Nach der Überprüfung aller Anforderungen wird der Instanztyp auf Folgendes geändert Nitro Instanztyp, den Sie angeben. Die Automatisierung wartet darauf, dass die neu erstellte Instanz alle Statusprüfungen bestanden hat, nachdem sie als Nitro Instanztyp. Die Automatisierung wartet dann auf die Genehmigung der designierten Principals, um eine zu erstellen AMI der erfolgreich

gestarteten Nitro sein. Wenn die Genehmigung verweigert wird, wird die Automatisierung beendet und die neu erstellte Instanz läuft weiter, und die Zielinstanz bleibt gestoppt.

Amazon EBS-Stammvolume ersetzen

Wenn Sie dies wählen `FullMigration0perationType`, migriert die Automatisierung die EC2 Amazon-Zielinstanz auf die Nitro Instanztyp, den Sie angeben. Automation fordert von den zuständigen Principals die Genehmigung an, das Amazon EBS-Root-Volume der EC2 Amazon-Ziel-Instance durch das Root-Volume der geklonten EC2 Amazon-Instance zu ersetzen. Nach erfolgreicher Migration wird die geklonte EC2 Amazon-Instance beendet. Wenn die Automatisierung fehlschlägt, wird das ursprüngliche Amazon EBS-Root-Volume an die EC2 Amazon-Zielinstanz angehängt. Wenn das Amazon EBS-Root-Volume, das an die EC2 Amazon-Zielinstanz angehängt ist, Tags mit `aws:` angewendetem Präfix enthält, wird der `FullMigration` Vorgang nicht unterstützt.

Bevor Sie beginnen

Die Ziel-Instance muss über ausgehenden Internetzugang verfügen. Dies dient dem Zugriff auf Repositorys für Treiber und Abhängigkeiten wie kernel-devel, gcc, patch, rpm-build, wget, dracut, make, linux-headers, und unzip. Bei Bedarf wird der Paketmanager verwendet.

Ein Amazon SNS SNS-Thema ist erforderlich, um Benachrichtigungen über Genehmigungen und Aktualisierungen zu senden. Weitere Informationen zum Erstellen eines Amazon SNS SNS-Themas finden Sie unter Erstellen eines Amazon SNS SNS-Themas im Amazon Simple Notification Service Developer Guide.

Dieses Runbook unterstützt die folgenden Betriebssysteme:

- RHEL 7.x — 8.5
- Amazon Linux (2018.03), Amazon Linux 2
- Debian Server
- Ubuntu Server 18.04 LTS, 20.04 LTS und 20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5, SUSE15SP2)

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Bestätigung

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Lesen Sie die vollständigen Details der Aktionen, die von diesem Automatisierungs-Runbook ausgeführt wurden, und geben Sie sie ein, **`Yes, I understand and acknowledge`** um mit der Verwendung des Runbooks fortzufahren.

- ApproveriAM

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ARNs IAM-Rollen, Benutzer oder Benutzernamen, die Genehmigungen für die Automatisierung erteilen können. Sie können maximal 10 Genehmiger angeben.

- DeleteResourcesOnFailure

  Typ: Boolesch

  Beschreibung: (Optional) Legt fest, ob die neu erstellte Instanz und AMI für die Migration werden gelöscht, wenn die Automatisierung fehlschlägt.

  Gültige Werte: Wahr | Falsch

Standard: True

- MinimumRequiredApprovals

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Mindestanzahl von Genehmigungen, die erforderlich sind, um die Automatisierung weiter auszuführen, wenn Genehmigungen angefordert werden.

  Gültige Werte: 1—10

  Standard: 1

- NitroInstanceType

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Nitro Instanztyp, in den Sie die Instanz ändern möchten. Zu den unterstützten Instance-Typen gehören M5, M6, C5, C6, R5, R6 und T3.

  Standard: m5.xlarge

- OperationType

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Vorgang, den Sie ausführen möchten. Die `FullMigration` Option führt dieselben Aufgaben aus wie das Root-Volume Ihrer Ziel-Instance `Clone&Migrate` und ersetzt zusätzlich das Root-Volume. Das Root-Volume der Ziel-Instance wird nach dem Migrationsprozess durch das Root-Volume der neu erstellten Instance ersetzt. Der `FullMigration` Vorgang unterstützt keine Root-Volumes, die von Logical Volume Manager (LVM) definiert wurden.

  Gültige Werte: Clone&Migrate | FullMigration

- SNSTopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon SNS SNS-Themas für die Genehmigungsbenachrichtigung. Das Amazon SNS SNS-Thema wird verwendet, um während der Automatisierung erforderliche Genehmigungsbenachrichtigungen zu senden.

- TargetInstanceId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der zu migrierenden EC2 Amazon-Instances.

Clone&Migrate Workflow

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- startOfPreliminaryChecksBranch— Wechselt zum Arbeitsablauf für vorläufige Prüfungen.
- getTargetInstanceProperties- Sammelt Details aus der Zielinstanz.
- checkIfNitroInstanceTypeIsSupportedInAZ— Ermittelt, ob der EC2 Amazon-Zielinstanztyp in derselben Availability Zone wie die Ziel-Instance unterstützt wird.
- getXenInstanceTypeDetails— Sammelt Details zum Quell-Instance-Typ.
- checkIfInstanceHypervisorIsNitroAlready— Prüft, ob die Zielinstanz bereits läuft als Nitro Instanztyp.
- checkIfTargetInstanceLifecycleIsSpot— Prüft, ob die Kaufoption der Ziel-Instance Spot ist.
- checkIfOperatingSystemIsLinux— Prüft, ob das Betriebssystem der Zielinstanz Linux ist.
- verifySSMConnectivityForTargetInstance— Überprüft, ob die Zielinstanz von Systems Manager verwaltet wird.
- checkIfEphemeralVolumeAreSupported— Prüft, ob der aktuelle Instance-Typ der Ziel-Instance Instance-Speicher-Volumes unterstützt.
- verifyIfTargetInstanceHasEphemeralVolumesAttached— Prüft, ob an die Zielinstanz Instance-Speicher-Volumes angehängt sind.
- checkIfRootVolumeIsEBS— Prüft, ob der Root-Volume-Typ der Ziel-Instance EBS ist.
- checkIfTargetInstanceIsInASG- Prüft, ob die Zielinstanz Teil einer Auto Scaling Scaling-Gruppe ist.
- endOfPreliminaryChecksBranch— Ende des Zweigs „Preliminary Checks“.
- startOfTestBranch— Verzweigt sich in den Test-Workflow.
- createTestImage- Erstellt einen Test AMI der Zielinstanz.

- `launchTestInstanceInSameSubnet`- Startet eine Testinstanz aus dem Test AMI verwendet dieselbe Konfiguration wie die Zielinstanz.
- `cleanupTestInstance`- Beendet die Testinstanz.
- `endOfTestBranch`- Ende des Testzweigs.
- `checkIfTestingBranchSucceeded`- Überprüft den Status des Testing-Zweigs.
- `approvalToStopTargetInstance`- Wartet auf die Genehmigung der designierten Principals, die Zielinstanz zu beenden.
- `stopTargetEC2Instance`- Stoppt die Zielinstanz.
- `forceStopTargetEC2Instance`- Force stoppt die Zielinstanz nur, wenn der vorherige Schritt die Instanz nicht stoppen konnte.
- `startOfCloneAndMigrateBranch`- Verzweigt zum Clone&Migrate Arbeitsablauf.
- `createBackupImage`- Erzeugt ein AMI der Zielinstanz, die als Backup dienen soll.
- `launchInstanceInSameSubnet`- Startet eine neue Instanz aus dem Backup AMI verwendet dieselbe Konfiguration wie die Quellinstanz.
- `waitForClonedInstanceToPassStatusChecks`- Wartet darauf, dass die neu erstellte Instanz alle Statusprüfungen bestanden hat.
- `verifySSMConnectivityForClonedInstance`— Überprüft, ob die neu erstellte Instanz von Systems Manager verwaltet wird.
- `checkAndInstallENADrivers`- Überprüft, ob ENA-Treiber auf der neu erstellten Instanz installiert sind, und installiert die Treiber bei Bedarf.
- `checkAndAddNVMEDrivers`- Überprüft, ob NVMe Treiber auf der neu erstellten Instanz installiert sind, und installiert die Treiber bei Bedarf.
- `checkAndModifyFSTABEntries`- Überprüft, ob Gerätenamen in verwendet werden, `/etc/fstab` und ersetzt sie bei UUIDs Bedarf durch.
- `stopClonedInstance`- Stoppt die neu erstellte Instanz.
- `forceStopClonedInstance`- Force stoppt die neu erstellte Instanz nur, wenn der vorherige Schritt die Instanz nicht stoppen konnte.
- `checkENAAttributeForClonedInstance`— Prüft, ob das erweiterte Netzwerkattribut für die neu erstellte Instanz aktiviert ist.
- `setNitroInstanceTypeForClonedInstance`- Ändert den Instanztyp für die neu erstellte Instanz in Nitro Instanztyp, den Sie angeben.
- `startClonedInstance`- Startet die neu erstellte Instanz, deren Instanztyp Sie geändert haben.

- `approvalForCreatingImageAfterDriversInstallation`- Wenn die Instanz erfolgreich gestartet wurde als Nitro Instanztyp: Die Automatisierung wartet auf die Genehmigung durch die erforderlichen Principals. Wenn die Genehmigung erteilt wird, ein AMI wurde geschaffen, um als Golden verwendet zu werden AMI.
- `createImageAfterDriversInstallation`- Erzeugt ein AMI um als Golden verwendet zu werden AMI.
- `endOfCloneAndMigrateBranch`- Ende von Clone&Migrate Filiale.
- `cleanupTestImage`- Meldet den ab AMI zum Testen erstellt.
- `failureHandling`- Prüft, ob Sie sich dafür entschieden haben, Ressourcen bei einem Fehler zu beenden.
- `onFailureTerminateClonedInstance`- Beendet die neu erstellte Instanz, wenn die Automatisierung fehlschlägt.
- `onFailurecleanupTestImage`- Deregistriert die AMI zum Testen erstellt.
- `onFailureApprovalToStartTargetInstance`— Wenn die Automatisierung fehlschlägt, wird auf die Genehmigung der designierten Principals gewartet, um die Zielinstanz zu starten.
- `onFailureStartTargetInstance`- Wenn die Automatisierung fehlschlägt, wird die Zielinstanz gestartet.

FullMigration Workflow

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

Der FullMigration Workflow führt dieselben Schritte aus wie der Clone&Migrate Workflow und führt zusätzlich die folgenden Schritte aus:

- checkConcurrency— Überprüft, ob es nur eine Automatisierung dieses Runbooks gibt, die auf die von Ihnen angegebene EC2 Amazon-Instance abzielt. Wenn das Runbook feststellt, dass eine weitere Automatisierung ausgeführt wird, die auf dieselbe Instance abzielt, wird die Automatisierung beendet.

- `getTargetInstanceProperties`- Sammelt Details von der Zielinstanz.
- `checkRootVolumeTags`— Ermittelt, ob das Root-Volume der EC2 Amazon-Zielinstanz irgendwelche AWS reservierten Tags enthält.
- `cloneTargetInstanceAndMigrateToNitro`— Startet eine untergeordnete Automatisierung mithilfe des `AWS-CloneXenInstanceToNitro` Runbooks.
- `branchOnTheOperationType`- Verzweigt nach dem Wert, den Sie für den `OperationType` Parameter angeben.
- `getClonedInstanceId`- Ruft die ID der neu gestarteten Instanz aus der untergeordneten Automatisierung ab.
- `checkIfRootVolumeIsBasedOnLVM`- Stellt fest, ob die Root-Partition von LVM verwaltet wird.
- `branchOnTheRootVolumeLVMStatus`- Wenn die erforderlichen Mindestgenehmigungen von den Principals vorliegen, wird die Automatisierung mit dem Austausch des Root-Volumes fortgesetzt.
- `manualInstructionsInCaseOfLVM`- Wenn das Root-Volume von LVM verwaltet wird, sendet die Automatisierung eine Ausgabe mit Anweisungen zum manuellen Austausch der Root-Volumes.
- `startOfReplaceRootEBSVolumeBranch`- Startet den Workflow zum Ersetzen des Root-EBS-Volume-Zweigs.
- `checkIfTargetInstanceIsManagedByCFN`— Ermittelt, ob die Zielinstanz von einem AWS CloudFormation Stack verwaltet wird.
- `branchOnCFNStackStatus`— Verzweigungen basierend auf dem Status des CloudFormation Stacks.
- `approvalForRootVolumesReplacement(WithCFN)`- Wenn die Ziel-Instance von gestartet wurde CloudFormation, wartet die Automatisierung auf die Genehmigung, nachdem die neu gestartete Instance erfolgreich als Nitro Instanztyp. Wenn Genehmigungen vorliegen, werden die Amazon EBS-Volumes der Ziel-Instance durch die Root-Volumes der neu gestarteten Instance ersetzt.
- `approvalForRootVolumesReplacement`- Wartet auf die Genehmigung, nachdem die neu gestartete Instance erfolgreich als Nitro Instanztyp. Wenn Genehmigungen vorliegen, werden die Amazon EBS-Volumes der Ziel-Instance durch die Root-Volumes der neu gestarteten Instance ersetzt.
- `assertIfTargetEC2InstanceIsStillStopped`— Überprüft, ob sich die Ziel-Instance in einem bestimmten `stopped` Zustand befindet, bevor das Root-Volume ersetzt wird.
- `stopTargetInstanceForRootVolumeReplacement`— Wenn die Ziel-Instance läuft, stoppt die Automatisierung die Instance, bevor das Root-Volume ersetzt wird.

- `forceStopTargetInstanceForRootVolumeReplacement`- Force stoppt die Zielinstanz, wenn der vorherige Schritt fehlschlägt.
- `stopClonedInstanceForRootVolumeReplacement`- Stoppt die neu erstellte Instance, bevor die Amazon EBS-Volumes ersetzt werden.
- `forceStopClonedInstanceForRootVolumeReplacement`— Force stoppt die neu erstellte Instance, falls der vorherige Schritt fehlschlägt.
- `getBlockDeviceMappings`- Ruft die Blockgerätezuordnungen sowohl für die Zielinstanz als auch für die neu erstellten Instanzen ab.
- `replaceRootEbsVolumes`- Ersetzt das Root-Volume der Ziel-Instance durch das Root-Volume der neu erstellten Instanz.
- `EndOfReplaceRootEBSVolumeBranch`— Ende des Workflows „Root EBS Volume Branch ersetzen“.
- `checkENAAttributeForTargetInstance`— Prüft, ob das ENA-Attribut (Enhanced Networking) für die EC2 Amazon-Zielinstanz aktiviert ist.
- `enableENAAttributeForTargetInstance`— Aktiviert bei Bedarf das ENA-Attribut für die EC2 Amazon-Zielinstanz.
- `setNitroInstanceTypeForTargetInstance`- Ändert die Ziel-Instance zu Nitro Instanztyp, den Sie angeben.
- `replicateRootVolumeTags`- Repliziert die Tags auf dem Amazon EBS-Stammvolume von der EC2 Amazon-Zielinstanz.
- `startTargetInstance`— Startet die EC2 Amazon-Zielinstanz, nachdem der Instance-Typ geändert wurde.
- `onFailureStopTargetEC2Instance`- Stoppt die EC2 Amazon-Zielinstanz, wenn sie nicht als Nitro Instanztyp.
- `onFailureForceStopTargetEC2Instance`- Force stoppt die EC2 Amazon-Zielinstanz, wenn der vorherige Schritt fehlschlägt.
- `OnFailureRevertOriginalInstanceType`- Setzt die EC2 Amazon-Zielinstanz auf den ursprünglichen Instance-Typ zurück, wenn die Ziel-Instance nicht als Nitro Instanztyp.
- `onFailureRollbackRootVolumeReplacement`— Macht bei Bedarf alle durch den `replaceRootEbsVolumes` Schritt vorgenommenen Änderungen rückgängig.
- `onFailureApprovalToStartTargetInstance`- Wartet auf die Genehmigung des designierten Principals, die EC2 Amazon-Zielinstanz zu starten, nachdem die vorherigen Änderungen rückgängig gemacht wurden.

- `onFailureStartTargetInstance`- Startet die EC2 Amazon-Zielinstanz.
- `terminateClonedEC2Instance`— Beendet die geklonte EC2 Amazon-Instance, nachdem das Amazon EBS-Stammvolume ersetzt wurde.

AWSSupport-ResetAccess

Beschreibung

Dieses Runbook verwendet das EC2 Rescue-Tool auf der angegebenen EC2 Instanz, um die Kennwortentschlüsselung mithilfe der EC2 Konsole (Windows) erneut zu aktivieren oder ein neues SSH-Schlüsselpaar zu generieren und hinzuzufügen (Linux). Wenn Sie Ihr key pair verloren haben, erstellt diese Automatisierung ein kennwortfähiges AMI, mit dem Sie eine neue EC2 Instance mit einem key pair starten können, das Ihnen gehört (Windows).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EC2RescueInstanceType

  Typ: Zeichenfolge

Gültige Werte: t2.small | t2.medium | t2.large

Standard: t2.small

Beschreibung: (Erforderlich) Der EC2 Instance-Typ für die Rescue-Instance. EC2 Empfohlene Größe: t2.small.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID der EC2 Instanz, für die Sie den Zugriff zurücksetzen möchten.

  > **Important**
  >
  > Systems Manager Automation stoppt diese Instanz und erstellt ein AMI, bevor irgendwelche Operationen ausgeführt werden. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP verwenden.

- SubnetId

  Typ: Zeichenfolge

  Standard: CreateNew VPC

  Beschreibung: (Optional) Die Subnetz-ID für die EC2 Rescue-Instanz. Standardmäßig erstellt Systems Manager Automation eine neue VPC. Verwenden Sie SelectedInstanceSubnet alternativ dasselbe Subnetz wie Ihre Instance, oder geben Sie eine benutzerdefinierte Subnetz-ID an.

  > **Important**
  >
  > Das Subnetz muss sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Sie benötigen mindestens ssm:StartAutomationExecution, ssm: GetParameter (um den Namen des SSH-Schlüsselparameters abzurufen) und ssm:, um die Automatisierungsausgabe lesen GetAutomationExecution zu können. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter AWSSupport-StartEC2RescueWorkflow.

Dokumentschritte

1. `aws:assertAwsResourceProperty`- Bestätigen Sie, ob es sich bei der bereitgestellten Instanz um Windows handelt.
   a. (EC2Rescue für Windows) Wenn es sich bei der bereitgestellten Instanz um Windows handelt:
      i. `aws:executeAutomation`- Rufen Sie `AWSSupport-StartEC2RescueWorkflow` mit dem EC2 Rescue for Windows-Offline-Skript zum Zurücksetzen des Passworts auf
      ii. `aws:executeAwsApi`- Rufen Sie die Backup-AMI-ID aus der verschachtelten Automatisierung ab
      iii. `aws:executeAwsApi`- Rufen Sie die kennwortfähige AMI-ID aus der verschachtelten Automatisierung ab
      iv. `aws:executeAwsApi`— Ruft die EC2 Rescue-Zusammenfassung aus der verschachtelten Automatisierung ab
   b. (EC2Rescue für Linux) Wenn es sich bei der bereitgestellten Instanz um Linux handelt:
      i. `aws:executeAutomation`- Rufen Sie `AWSSupport-StartEC2RescueWorkflow` mit dem Offline-SSH-Schlüsselinjektionsskript von EC2 Rescue for Linux auf
      ii. `aws:executeAwsApi`- Rufen Sie die Backup-AMI-ID aus der verschachtelten Automatisierung ab
      iii. `aws:executeAwsApi`- Ruft den SSM-Parameternamen für den injizierten SSH-Schlüssel ab
      iv. `aws:executeAwsApi`- Ruft die EC2 Rescue-Zusammenfassung aus der verschachtelten Automatisierung ab

Ausgaben

Holen Sie sich .Output EC2 RescueForWindowsResult

getWindowsBackupAmi. ImageId

getWindowsPasswordEnabledAmi.ImageId

EC2RescueForLinuxResult.Output abrufen

getLinuxBackupAmi. ImageId

GetLinux-Parameter.Name SSHKey

AWSSupport-ResetLinuxUserPassword

Beschreibung

Das `AWSSupport-ResetLinuxUserPassword` Runbook hilft Ihnen dabei, das Passwort eines lokalen Betriebssystembenutzers (OS) zurückzusetzen. Dieses Runbook ist besonders hilfreich für Benutzer, die über die serielle Konsole auf ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances zugreifen müssen. Das Runbook erstellt eine temporäre Amazon EC2 EC2-Instance in Ihrem AWS-Konto mit entweder einer automatisch generierten AWS Identity and Access Management (IAM) Rolle oder einem von Ihnen angegebenen benutzerdefinierten IAM-Instance-Profil. Das benutzerdefinierte Instance-Profil (IAM) muss berechtigt sein, den AWS Secrets Manager geheimen Wert, der das Passwort enthält, abzurufen.

Das Runbook stoppt Ihre Amazon EC2 EC2-Ziel-Instance, trennt das Amazon Elastic Block Store (Amazon EBS) -Stammvolume und fügt es der temporären Amazon EC2 EC2-Instance hinzu. Mithilfe von Run Command wird auf der temporären Instance ein Skript ausgeführt, um das Passwort des von Ihnen angegebenen Betriebssystembenutzers festzulegen. Anschließend wird das Amazon EBS-Root-Volume wieder an Ihre Ziel-Instance angehängt. Das Runbook bietet auch die Möglichkeit, zu Beginn der Automatisierung einen Snapshot des Root-Volumes zu erstellen.

Bevor Sie beginnen

Erstellen Sie ein Secrets Manager Manager-Geheimnis mit dem Wert des Passworts, das Sie Ihrem Betriebssystembenutzer zuweisen möchten. Der Wert muss im Klartext sein. Weitere Informationen finden Sie unter Erstellen eines AWS Secrets Manager -Secrets im AWS Secrets Manager - Benutzerhandbuch.

Überlegungen

- Wir empfehlen, Ihre Instance zu sichern, bevor Sie dieses Runbook verwenden. Erwägen Sie, den Wert des `CreateSnapshot` Parameters auf festzulegen. **`Yes`**
- Um das lokale Benutzerkennwort zu ändern, muss das Runbook Ihre Instance beenden. Wenn eine Instance gestoppt wird, gehen alle im Arbeitsspeicher oder auf Instance-Speicher-Volumes gespeicherten Daten verloren. Außerdem werden alle automatisch zugewiesenen öffentlichen IPv4 Adressen freigegeben. Weitere Informationen darüber, was passiert, wenn Sie eine

Instance beenden, finden Sie unter Stoppen und starten Sie Ihre Instance im Amazon EC2 EC2-Benutzerhandbuch.

- Wenn die Amazon EBS-Volumes, die an Ihre Amazon EC2 EC2-Zielinstanz angehängt sind, mit einem vom Kunden verwalteten AWS Key Management Service (AWS KMS) Schlüssel verschlüsselt sind, stellen Sie sicher, dass der AWS KMS Schlüssel nicht verschlüsselt ist, `deleted` da `disabled` sonst Ihre Instance nicht gestartet werden kann.
- Für die Verwendung eines benutzerdefinierten IAM-Instanzprofils ist eine `GetInstanceProfile` IAM-Berechtigung für die `AutomationAssumeRole` Validierung erforderlich, und das benutzerdefinierte Instanzprofil selbst muss die Zugriffsberechtigungen Systems Manager und Secrets Manager enthalten. Das Runbook überprüft das Vorhandensein eines Instanzprofils im Voraus, schlägt jedoch bei Helper-Instance-Vorgängen fehl, wenn für das Instanzprofil kein erforderlicher Zugriff erforderlich ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Linux-Instance, die das Betriebssystembenutzerkennwort enthält, das Sie zurücksetzen möchten.

- LinuxUserName

  Typ: Zeichenfolge

  Standard: ec2-user

  Beschreibung: (Optional) Das Betriebssystem-Benutzerkonto, dessen Passwort Sie zurücksetzen möchten.

- SecretArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN Ihres Secrets Manager Manager-Geheimnisses, das das neue Passwort enthält.

- SecurityGroupId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Sicherheitsgruppe, die an die temporäre Amazon EC2 EC2-Instance angehängt werden soll. Wenn Sie keinen Wert für diesen Parameter angeben, wird die Standardsicherheitsgruppe Amazon Virtual Private Cloud (Amazon VPC) verwendet.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des Subnetzes, in dem Sie die temporäre Amazon EC2 EC2-Instance starten möchten. Standardmäßig wählt die Automatisierung dasselbe Subnetz wie Ihre Ziel-Instance aus. Wenn Sie sich dafür entscheiden, ein anderes Subnetz bereitzustellen, muss es sich in derselben Availability Zone wie die Ziel-Instance befinden und Zugriff auf Systems Manager Manager-Endpunkte haben.

- CreateSnapshot

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Standard: Ja

Beschreibung: (Optional) Legt fest, ob ein Snapshot des Root-Volumes Ihrer Amazon EC2 EC2-Zielinstanz erstellt wird, bevor die Automatisierung ausgeführt wird.

- StopConsent

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Standard: Nein

  Beschreibung: Geben Sie ein, **`Yes`** um zu bestätigen, dass Ihre Amazon EC2 EC2-Zielinstanz während dieser Automatisierung gestoppt wird. Wenn die Amazon EC2 EC2-Instance gestoppt wird, gehen alle im Arbeitsspeicher oder auf Instance-Speicher-Volumes gespeicherten Daten verloren und die automatische öffentliche IPv4 Adresse wird freigegeben. Weitere Informationen finden Sie unter Anhalten und Starten einer Instance im Amazon-EC2-Benutzerhandbuch.

- InstanceProfileName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des IAM-Instance-Profils, das an die Amazon EC2 EC2-Helper-Instance angehängt werden soll. Falls nicht angegeben, wird automatisch ein temporäres Instance-Profil mit den erforderlichen Berechtigungen erstellt. Das benutzerdefinierte Instanzprofil muss über Berechtigungen für den Zugriff auf das angegebene Secrets Manager Manager-Secret und Systems Manager verfügen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

1. aws:branch— Verzweigungen basierend darauf, ob Sie dem Stoppen der Amazon EC2 EC2-Zielinstanz zugestimmt haben.

2. `aws:assertAwsResourceProperty`— Stellt sicher, dass sich der Status der Amazon EC2 EC2-Instance im `stopped` Status `running` oder befindet. Andernfalls endet die Automatisierung.
3. `aws:executeAwsApi`— Ruft die Amazon EC2 EC2-Instance-Eigenschaften ab.
4. `aws:executeAwsApi`— Ruft die Eigenschaften des Root-Volumes ab.
5. `aws:branch`— Verzweigt die Automatisierung in Abhängigkeit davon, ob eine Subnetz-ID für die temporäre Amazon EC2 EC2-Instance bereitgestellt wurde.
6. `aws:assertAwsResourceProperty`— Stellt sicher, dass sich das Subnetz, das Sie im `SubnetId` Parameter angeben, in derselben Availability Zone wie die Amazon EC2 EC2-Ziel-Instance befindet.
7. `aws:assertAwsResourceProperty`— Stellt sicher, dass es sich bei dem Stammvolume der Amazon EC2 EC2-Instance um ein Amazon EBS-Volume handelt.
8. `aws:assertAwsResourceProperty`— Stellt sicher, dass die Amazon EC2 EC2-Instance-Architektur `arm64` oder `x86_64` ist.
9. `aws:assertAwsResourceProperty`— Stellt sicher, dass das Verhalten beim Herunterfahren der Amazon EC2 EC2-Instance stimmt `stop` und nicht`terminate`.
10. `aws:branch`— Stellt sicher, dass es sich bei der Amazon EC2-Instance nicht um eine Spot-Instance handelt. Andernfalls endet die Automatisierung.
11. `aws:executeScript`— Stellt sicher, dass die Amazon EC2 EC2-Instance nicht Teil einer Auto Scaling-Gruppe ist. Wenn die Instance Teil einer Auto Scaling-Gruppe ist, bestätigt die Automatisierung, dass sich die Amazon EC2 EC2-Instance in einem `Standby` Lebenszyklusstatus befindet.
12. `aws:branch`— Verzweigt die Automatisierung je nachdem, ob ein benutzerdefinierter IAM-Instance-Profilname angegeben wurde oder nicht
13. `aws:assertAwsResourceProperty`— Stellt sicher, dass das benutzerdefinierte IAM-Instanzprofil existiert, und überprüft, ob sein Name mit dem Eingabeparameter übereinstimmt.
14. `aws:createStack`— Erstellt eine temporäre Amazon EC2 EC2-Instance, die verwendet wird, um das Passwort für den von Ihnen angegebenen Betriebssystembenutzer zurückzusetzen.
15. `aws:waitForAwsResourceProperty`— Wartet, bis die neu gestartete temporäre Amazon EC2 EC2-Instance läuft.
16. `aws:executeAwsApi`— Ruft die ID der temporären Amazon EC2 EC2-Instance ab.
17. `aws:waitForAwsResourceProperty`— Wartet darauf, dass die temporäre Amazon EC2 EC2-Instance als von Systems Manager verwaltet gemeldet wird.

18. `aws:changeInstanceState` — Stoppt die Amazon EC2 EC2-Zielinstanz.
19. `aws:changeInstanceState` — Zwingt die Amazon EC2 EC2-Zielinstanz zum Beenden, falls sie in einem Stopp-Zustand hängen bleibt.
20. `aws:branch` — Verzweigt die Automatisierung je nachdem, ob ein Snapshot des Root-Volumes der Amazon EC2 EC2-Zielinstanz angefordert wurde.
21. `aws:executeAwsApi` — Erstellt einen Snapshot des Amazon EBS-Stammvolumes der Amazon EC2-Zielinstanz.
22. `aws:waitForAwsResourceProperty` — Wartet darauf, dass sich der Snapshot in einem bestimmten Zustand befindet. `completed`
23. `aws:executeAwsApi` — Trennt das Amazon EBS-Root-Volume von der Amazon EC2 EC2-Zielinstanz.
24. `aws:waitForAwsResourceProperty` — Wartet darauf, dass das Amazon EBS-Root-Volume von der Amazon EC2 EC2-Zielinstanz getrennt wird.
25. `aws:executeAwsApi` — Hängt das Amazon EBS-Stammvolume an die temporäre Amazon EC2 EC2-Instance an.
26. `aws:waitForAwsResourceProperty` — Wartet darauf, dass das Amazon EBS-Root-Volume an die temporäre Amazon EC2 EC2-Instance angehängt wird.
27. `aws:runCommand` — Setzt das Zielbenutzerkennwort zurück, indem ein Shell-Skript mit Run Command auf der temporären Amazon EC2 EC2-Instance ausgeführt wird.
28. `aws:executeAwsApi` — Trennt das Amazon EBS-Root-Volume von der temporären Amazon EC2 EC2-Instance.
29. `aws:waitForAwsResourceProperty` — Wartet darauf, dass das Amazon EBS-Root-Volume von der temporären Amazon EC2 EC2-Instance getrennt wird.
30. `aws:executeAwsApi` — Trennt das Amazon EBS-Root-Volume nach einem Fehler von der temporären Amazon EC2 EC2-Instance.
31. `aws:waitForAwsResourceProperty` — Wartet darauf, dass das Amazon EBS-Root-Volume nach einem Fehler von der temporären Amazon EC2 EC2-Instance getrennt wird.
32. `aws:branch` — Verzweigt die Automatisierung je nachdem, ob ein Snapshot des Root-Volumes angefordert wurde, um den Wiederherstellungspfad für den Fall eines Fehlers zu ermitteln.
33. `aws:executeAwsApi` — Hängt das Amazon EBS-Stammvolume erneut an die Amazon EC2 EC2-Zielinstanz an.
34. `aws:waitForAwsResourceProperty` — Wartet darauf, dass das Amazon EBS-Root-Volume an die Amazon EC2 EC2-Instance angehängt wird.

35. `aws:executeAwsApi`— Erstellt ein neues Amazon EBS-Volume aus dem Root-Volume-Snapshot der Amazon EC2 EC2-Instance der Zielinstanz.
36. `aws:waitForAwsResourceProperty`— Wartet, bis sich das neue Amazon EBS-Volume in einem `available` Zustand befindet.
37. `aws:executeAwsApi`— Hängt das neue Amazon EBS-Volume als Root-Volume an die Ziel-Instance an.
38. `aws:waitForAwsResourceProperty`— Wartet darauf, dass sich das Amazon EBS-Volume in einem `attached` bestimmten Zustand befindet.
39. `aws:executeAwsApi`— Beschreibt die CloudFormation Stack-Ereignisse, wenn die Runbooks den Stack nicht erstellen oder aktualisieren können. CloudFormation
40. `aws:branch`— Verzweigt die Automatisierung in Abhängigkeit vom vorherigen Status der Amazon EC2 EC2-Instanz. Wenn der Status war`running`, wird die Instance gestartet. Wenn sie sich in einem `stopped` Status befand, wird die Automatisierung fortgesetzt.
41. `aws:changeInstanceState`— Startet die Amazon EC2 EC2-Instance bei Bedarf.
42. `aws:waitForAwsResourceProperty`— Wartet, bis sich der CloudFormation Stack im Terminalstatus befindet, bevor er gelöscht wird.
43. `aws:executeAwsApi`— Löscht den CloudFormation Stack einschließlich der temporären Amazon EC2 EC2-Instance.

AWSSupport-RunEC2RescueForWindowsTool

Beschreibung

Das AWSSupport-RunECRescueForWindowsTool2-Runbook führt das Problembehandlungstool Amazon EC2 Rescue for Windows Server auf der von Windows verwalteten Amazon Elastic Compute Cloud (Amazon EC2) -Zielinstanz aus, um allgemeine Probleme zu beheben. Dieses Runbook unterstützt drei Hauptaktionen:

- ResetAccess: Setzt das lokale Administratorkennwort zurück. Das Passwort wird nach dem Zufallsprinzip generiert und sicher im AWS Systems Manager Parameter Store unter gespeichert. `/EC2Rescue/Password/<instance_id>` Wenn Sie keine Parameter angeben, wird das Passwort mit dem Standardschlüssel AWS Key Management Service (AWS KMS) verschlüsselt`alias/aws/ssm`. Optional können Sie eine AWS KMS Schlüssel-ID angeben, um das Passwort mit Ihrem eigenen Schlüssel zu verschlüsseln.

- CollectLogs: Sammelt Protokolle und Konfigurationsdateien vom Betriebssystem und lädt sie in einen Amazon Simple Storage Service (Amazon S3) -Bucket in Ihrem Konto hoch, indem Sie Amazon EC2 Rescue mit der `/collect:all` Option ausführen.
- FixAll: Versucht, Probleme auf einem Offline-Windows-Root-Volume zu erkennen und zu beheben, das mit der aktuellen Instance verbunden ist, indem Amazon EC2 Rescue mit der `/rescue:all` Option ausgeführt wird.

> **Important**
>
> Für dieses Runbook muss es sich bei der Ziel-Instance um eine verwaltete Windows-Instance handeln, auf der die AWS Tools für Windows PowerShell installiert sind. Das Runbook installiert das Amazon EC2 Rescue for Windows Server-Tool mithilfe des Systems Manager Distributor-Pakets. `AWSSupport-EC2Rescue`

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Installiert das Amazon EC2 Rescue for Windows Server-Fehlerbehebungstool mithilfe des Systems Manager Distributor-Pakets.
- Führt die angegebene Aktion (`ResetAccessCollectLogs`, oder`FixAll`) mit den angegebenen Parametern aus.
- Für`ResetAccess`: Generiert ein sicheres Passwort und speichert es im Parameter Store.
- Für`CollectLogs`: Sammelt Systemprotokolle und lädt sie in den angegebenen Amazon S3 S3-Bucket hoch.
- Für`FixAll`: Versuche, Probleme auf dem angegebenen Offline-Volume zu beheben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:DescribeInstanceInformation`
- `ssm:GetCommandInvocation`
- `ssm:PutParameter`(zur ResetAccess Aktion)
- `kms:Encrypt`(für ResetAccess Aktionen mit benutzerdefiniertem AWS KMS Schlüssel)
- `s3:PutObject`(zum CollectLogs Handeln)
- `s3:GetBucketAcl`(zum CollectLogs Handeln)
- `s3:GetBucketPolicy`(zum CollectLogs Handeln)
- `s3:GetBucketPolicyStatus`(zum CollectLogs Handeln)

Beispiel für eine Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-RunEC2RescueForWindowsTool`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - Befehl (erforderlich):
     - Beschreibung: (Erforderlich) Die auszuführende Aktion.
     - Typ: `String`
     - Werte zulassen: `[ResetAccess, CollectLogs, FixAll]`
     - Standard: `ResetAccess`
   - Parameter (erforderlich):
     - Beschreibung: (Erforderlich) Parameter für den Befehl:
       - Für`ResetAccess`: Die AWS AWS KMS Schlüssel-ID oder der Alias (Standard:`alias/aws/ssm`)
       - Für`CollectLogs`: Der Amazon S3 S3-Bucket-Name, in den die Protokolle hochgeladen werden sollen
       - Für`FixAll`: Der Gerätename für die Offline-Behebung (zum Beispiel`xvdf`)
     - Typ: `String`
     - Muster zulassen: `^[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. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.

6. Das Dokument führt die folgenden Schritte aus:
   - Installieren Sie EC2 Rescue:

     Installiert das Amazon EC2 Rescue for Windows Server-Fehlerbehebungstool mithilfe des Systems Manager Distributor-Pakets`AWSSupport-EC2Rescue`.
   - ausführen EC2 RescueForWindows:

     Führt das PowerShell Skript mit der im Command-Parameter angegebenen Aktion aus, um den angeforderten Vorgang auszuführen.
7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows
- Verwenden Sie Amazon EC2 Rescue für Windows Server mit Systems Manager Run Command

`AWSPremiumSupport-ResizeNitroInstance`

Beschreibung

Das `AWSPremiumSupport-ResizeNitroInstance` Runbook bietet eine automatisierte Lösung für die Größenänderung von Amazon Elastic Compute Cloud (Amazon EC2) -Instances, die auf dem Nitro System basieren.

Um das potenzielle Risiko von Datenverlusten und Ausfallzeiten zu verringern, überprüft das Runbook Folgendes:

- Verhalten beim Stoppen der Instanz.
- Wenn die Instance Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe ist und sich im `standby` Modus befindet.
- Instanzstatus und Tenancy.

- Der Instance-Typ, zu dem Sie wechseln möchten, unterstützt die Anzahl der Netzwerkschnittstellen, die derzeit mit Ihrer Instance verbunden sind.
- Die Prozessorarchitektur und der Virtualisierungstyp für den aktuellen Instanztyp und den Zielinstanztyp sind identisch.
- Wenn die Instanz läuft, besteht sie alle Statusprüfungen.
- Der Instance-Typ, zu dem Sie wechseln möchten, ist in derselben Availability Zone verfügbar.

Wenn Amazon EC2 nach der Änderung des Instance-Typs die Statusprüfungen nicht besteht, wird das Runbook automatisch auf den vorherigen Instance-Typ zurückgesetzt.

Standardmäßig ändert dieses Runbook den Instance-Typ nicht, wenn es läuft und Instance-Speicher-Volumes angehängt sind. Das Runbook ändert den Instance-Typ auch nicht, wenn die Instance Teil eines AWS CloudFormation Stacks ist. Wenn Sie eines dieser Verhaltensweisen ändern möchten, geben Sie `yes` für die `AllowCloudFormationInstances` Parameter `AllowInstanceStoreInstances` und an.

Das Runbook bietet zwei verschiedene Möglichkeiten, den Instance-Typ anzugeben, zu dem Sie wechseln möchten:

- Für einfache Automatisierungen, die auf eine einzelne Instanz abzielen, geben Sie mithilfe des Parameters den Instanztyp an, zu dem `TargetInstanceTypeFromParameter` Sie wechseln möchten.
- Um Automatisierungen in großem Umfang auszuführen, um den Instanztyp mehrerer Instanzen zu ändern, geben Sie den Instanztyp mithilfe des `TargetInstanceTypeFromTagValue` Parameters an. Informationen zur skalierten Ausführung von Automatisierungen finden Sie unter Automatisierungen im großen Maßstab ausführen.

Wenn Sie für keinen der Parameter einen Wert angeben, schlägt die Automatisierung fehl.

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist ein Abonnement für Business + Support, Enterprise Support oder Unified Operations erforderlich. Weitere Informationen finden Sie unter AWS Support Tarife vergleichen.

Überlegungen

- Wir empfehlen, Ihre Instance zu sichern, bevor Sie dieses Runbook verwenden.
- Informationen zur Kompatibilität beim Ändern des Instance-Typs finden Sie unter Kompatibilität beim Ändern des Instance-Typs.
- Wenn die Automatisierung fehlschlägt und zum ursprünglichen Instanztyp zurückkehrt, finden Sie weitere Informationen unter Problembehandlung beim Ändern des Instanztyps.
- Um den Instanztyp zu ändern, muss das Runbook Ihre Instance beenden. Wenn eine Instance gestoppt wird, gehen alle im Arbeitsspeicher oder auf Instance-Speicher-Volumes gespeicherten Daten verloren. Außerdem werden alle automatisch zugewiesenen öffentlichen IPv4 Adressen freigegeben. Weitere Informationen darüber, was passiert, wenn Sie eine Instance beenden, finden Sie unter Ihre Instance beenden und starten.
- Mithilfe des `SkipInstancesWithTagKey` Parameters können Sie Instances überspringen, auf die ein bestimmter Amazon EC2-Tagschlüssel angewendet wurde.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Bestätigen

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Geben Sie ein, **`yes`** um zu bestätigen, dass Ihre Instance gestoppt wird, falls sie gerade läuft.

- AllowInstanceStoreInstances

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn Sie dies angeben`yes`, lassen Sie zu, dass das Runbook auf Instances ausgeführt wird, denen Instance-Speicher-Volumes angehängt sind.

- AllowCloudFormationInstances

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn Sie angeben`yes`, wird das Runbook auf Instances ausgeführt, die Teil eines CloudFormation Stacks sind.

- DryRun

  Typ: Zeichenfolge

  Gültige Werte: nein | ja

  Standard: no

  Beschreibung: (Optional) Wenn Sie dies angeben`yes`, überprüft das Runbook die Größenänderungsanforderungen, ohne den Instanztyp zu ändern.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, deren Typ Sie ändern möchten.

- SkipInstancesWithTagKey

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Automatisierung überspringt eine Ziel-Instance, wenn der von Ihnen angegebene Tag-Schlüssel auf die Instance angewendet wird.

- SleepTime

  Typ: Zeichenfolge

  Standard: 3

  Beschreibung: (Optional) Die Anzahl der Sekunden, für die dieses Runbook nach Abschluss in den Ruhezustand versetzt werden soll.

- TagInstance

  Typ: Zeichenfolge

  Beschreibung: (Optional) Taggen Sie die Instances mit dem Schlüssel und Wert Ihrer Wahl und verwenden Sie dabei das folgende Format:*`Key=ChangingType,Value=True`*. Mit dieser Option können Sie Instances verfolgen, auf die dieses Runbook abzielt. Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.

- TargetInstanceTypeFromParameter

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Instance-Typ, auf den Sie Ihre Instance ändern möchten. Lassen Sie diesen Parameter leer, wenn Sie den Wert des im `TargetInstanceTypeFromTagValue` Parameter angegebenen Tag-Schlüssels verwenden möchten.

- TargetInstanceTypeFromTagValue

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der auf Ihre Ziel-Instances angewendete Tag-Schlüssel, dessen Wert den Instance-Typ enthält, zu dem Sie wechseln möchten. Wenn Sie einen Wert für den `TargetInstanceTypeFromParameter` Parameter angeben, überschreibt er jeden Wert, den Sie für diesen Parameter angeben.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

1. `aws:assertAwsResourceProperty`: Stellt sicher, dass die Amazon EC2 EC2-Instance nicht mit dem im `SkipInstancesWithTagKey` Parameter angegebenen Ressourcen-Tag-Schlüssel gekennzeichnet ist. Wenn festgestellt wird, dass der Tag-Schlüssel auf die Instance angewendet wurde, schlägt der Schritt fehl und die Automatisierung wird beendet.
2. `aws:assertAwsResourceProperty`: Bestätigt, dass der Status der Amazon EC2 EC2-Zielinstanz`running`, `pending``stopped`, oder `stopping` ist. Andernfalls endet die Automatisierung.
3. `aws:executeAwsApi`: Sammelt Eigenschaften aus der Amazon EC2 EC2-Instance.
4. `aws:executeAwsApi`: Sammelt Details zum aktuellen Amazon EC2 EC2-Instance-Typ.
5. `aws:branch`: Prüft, ob der aktuelle Instance-Typ und der im `TargetInstanceTypeFromParameter` Parameter angegebene Instance-Typ identisch sind. Wenn dies der Fall ist, endet die Automatisierung.
6. `aws:assertAwsResourceProperty`: Stellt sicher, dass die Instanz auf dem Nitro-System läuft.

7. `aws:branch`: Stellt sicher, dass der Root-Volume-Typ der Amazon EC2 EC2-Instance ein Amazon Elastic Block Store (Amazon EBS) -Volume ist.
8. `aws:assertAwsResourceProperty`: Bestätigt, dass das Verhalten beim Herunterfahren der Instance zutrifft `stop` und nicht. `terminate`
9. `aws:branch`: Stellt sicher, dass die Amazon EC2 EC2-Instance keine Spot-Instance ist.
10. `aws:branch`: Stellt sicher, dass es sich bei der Amazon EC2-Instance-Tenancy um eine Standardinstanz handelt und nicht um einen dedizierten Host oder eine dedizierte Instance.
11. `aws:executeScript`: Bestätigt, dass es nur eine Automatisierung dieses Runbooks gibt, die auf die aktuelle Instance-ID abzielt. Wenn bereits eine andere Automatisierung ausgeführt wird, die auf dieselbe Instanz abzielt, gibt die Automatisierung einen Fehler zurück und wird beendet.
12. `aws:branch`: Verzweigt die Automatisierung auf der Grundlage des Status der Amazon EC2 EC2-Instance.
    a. Falls `stopped` oder`stopping`, wird die Automatisierung `aws:waitForAwsResourceProperty` so lange ausgeführt, bis die Amazon EC2 EC2-Instance vollständig gestoppt ist.
    b. Falls `running` oder`pending`, wird die Automatisierung `aws:waitForAwsResourceProperty` so lange ausgeführt, bis die Amazon EC2 EC2-Instance die Statusprüfungen bestanden hat.
13. `aws:assertAwsResourceProperty`: Bestätigt, dass die Amazon EC2 EC2-Instance nicht Teil einer Auto Scaling Scaling-Gruppe ist, indem der `DescribeAutoScalingInstances` API-Vorgang aufgerufen wird. Wenn die Instance Teil einer Auto Scaling Scaling-Gruppe ist, wird sichergestellt, dass sich die Amazon EC2 EC2-Instance im `standby` Modus befindet.
14. `aws:branch`: Verzweigt die Automatisierung, je nachdem, ob die Automatisierung prüfen soll, ob die Amazon EC2 EC2-Instance Teil eines CloudFormation Stacks ist:
    a. `aws:executeScript`Stellt sicher, dass die Amazon EC2 EC2-Instance nicht Teil eines CloudFormation Stacks ist, indem der `DescribeStackResources` API-Vorgang aufgerufen wird.
15. `aws:executeAwsApi`: Gibt eine Liste von Instance-Typen zurück, die denselben Prozessorarchitekturtyp und denselben Virtualisierungstyp haben und die Anzahl der Netzwerkschnittstellen unterstützen, die derzeit mit der Ziel-Instance verbunden sind.
16. `aws:executeAwsApi`: Ruft den Wert für den Zielinstanztyp aus dem im `TargetInstanceTypeFromTagValue` Parameter angegebenen Tag-Schlüssel ab.
17. `aws:executeScript`: Bestätigt, dass der aktuelle Instanztyp und der Typ der Zielinstanz kompatibel sind. Stellt sicher, dass der Zielinstanztyp im selben Subnetz verfügbar ist. Überprüft,

ob der Principal, der das Runbook gestartet hat, berechtigt ist, den Instanztyp zu ändern und die Instance zu beenden und zu starten, falls sie ausgeführt wurde.

18. `aws:branch`: Verzweigt die Automatisierung je nachdem, ob der `DryRun` Parameterwert auf gesetzt ist. `yes` Wenn`yes`, endet die Automatisierung.
19. `aws:branch`: Prüft, ob der ursprüngliche Instanztyp und der Zielinstanztyp identisch sind. Wenn sie identisch sind, endet die Automatisierung.
20. `aws:executeAwsApi`: Ruft den aktuellen Instanzstatus ab.
21. `aws:changeInstanceState`: Stoppt die Amazon EC2 EC2-Instance.
22. `aws:changeInstanceState`: Erzwingt die Instance zum Beenden, wenn sie im `stopping` Status feststeckt.
23. `aws:executeAwsApi`: Ändert den Instanztyp in den Zielinstanztyp.
24. `aws:sleep`: Wartet 3 Sekunden, nachdem der Instanztyp geändert wurde, um die Konsistenz zu gewährleisten.
25. `aws:branch`: Verzweigt die Automatisierung auf der Grundlage des vorherigen Instanzstatus. Wenn ja`running`, wird die Instanz gestartet.
    a. `aws:changeInstanceState`: Startet die Amazon EC2 EC2-Instance, wenn sie vor der Änderung des Instance-Typs ausgeführt wurde.
    b. `aws:waitForAwsResourceProperty`: Wartet darauf, dass die Amazon EC2 EC2-Instance die Statusprüfungen bestanden hat. Wenn die Instance die Statusprüfungen nicht besteht, wird die Instance wieder auf ihren ursprünglichen Instance-Typ zurückgesetzt.
        i. `aws:changeInstanceState`: Stoppt die Amazon EC2 EC2-Instance, bevor sie in ihren ursprünglichen Instance-Typ geändert wird.
        ii. `aws:changeInstanceState`: Erzwingt, dass die Amazon EC2 EC2-Instance beendet wird, bevor sie in ihren ursprünglichen Instance-Typ geändert wird, falls sie in einem Stopp-Zustand hängen bleibt.
        iii. `aws:executeAwsApi`: Ändert die Amazon EC2 EC2-Instance auf ihren ursprünglichen Typ.
        iv. `aws:sleep`: Wartet 3 Sekunden, nachdem der Instance-Typ geändert wurde, um die Konsistenz zu gewährleisten.
        v. `aws:changeInstanceState`: Startet die Amazon EC2 EC2-Instance, wenn sie vor der Änderung des Instance-Typs ausgeführt wurde.
        vi. `aws:waitForAwsResourceProperty`: Wartet darauf, dass die Amazon EC2 EC2-Instance die Statusprüfungen bestanden hat.
26. `aws:sleep`: Wartet, bevor das Runbook beendet wird.

AWSSupport-ShareEncryptedAMIOrEBSSnapshot

Beschreibung

Dieses Runbook automatisiert das Teilen von verschlüsselten Amazon Machine Image s- oder Amazon Elastic Block Store-Snapshots mit anderen Amazon Web Services Services-Konten. Dieses Runbook behandelt die komplexen Anforderungen für die kontenübergreifende gemeinsame Nutzung verschlüsselter Ressourcen, einschließlich AWS Key Management Service wichtiger Richtlinienänderungen und Aktualisierungen von Ressourcenberechtigungen.

Diese Automatisierung führt die Schritte aus, die im AWS Sicherheits-Blog-Artikel So teilen Sie verschlüsselte AMI s für mehrere Konten beschrieben sind, um verschlüsselte Amazon Elastic Compute Cloud-Instances zu starten.

⚠ Wichtige Überlegungen

- Dieses Runbook ändert Ihre Ressourcen: Das Runbook fügt Ihrer CMK-Richtlinie (AWS KMS Customer Managed Key) kontoübergreifende Berechtigungen hinzu und gewährt dem Zielkonto AMI Startberechtigungen oder Amazon EBS-Snapshot-Berechtigungen zum Erstellen von Volumes.
- Zusätzliche Kosten können anfallen: Beim Kopieren von Ressourcen (andere Region oder AWS verwaltete Schlüsselverschlüsselung) fallen zusätzliche Kosten für den neuen AMI oder Amazon EBS-Snapshot und jede regionsübergreifende Datenübertragung an.
- Bitte überprüfen Sie die Zielkonto-ID: Überprüfen Sie die Zielkonto-ID noch einmal, da dieses Runbook die Existenz eines Kontos nicht überprüfen kann.
- Automatisches Rollback mit manueller Überprüfung: Dieses Runbook versucht, Änderungen automatisch rückgängig zu machen, falls dies fehlschlägt. Schlägt das Rollback selbst jedoch fehl, stellen Sie bitte sicher, dass keine zusätzlichen AMI / Snapshot-Kopien in Ihrem Konto übrig geblieben sind, dass die LaunchPermission/ CreateVolumePermission Ressourcenattribute keine unbeabsichtigten Konten enthalten und dass sich die AWS KMS wichtige Richtlinie im Originalzustand befindet.

Wie funktioniert es?

Das Runbook führt die folgenden allgemeinen Schritte aus:

- Überprüft das Vorhandensein, den Status und die Verschlüsselungskonfiguration der Eingaberessource
- Überprüft die aktuellen Berechtigungen für die gemeinsame Nutzung von Ressourcen mit dem Zielkonto
- Analysiert AWS KMS wichtige Richtlinien und erstellt eine umfassende Vorschau aller erforderlichen Änderungen
- Fordert die Genehmigung der zuständigen Schulleiter an, bevor Änderungen vorgenommen werden
- Führt genehmigte Änderungen aus, darunter das Kopieren von Ressourcen (falls erforderlich), Aktualisierungen von Berechtigungen und AWS KMS wichtige Richtlinienänderungen
- Stellt bei Bedarf einen umfassenden Ausführungsbericht mit Rollback-Informationen bereit

Führen Sie diese Automatisierung aus (Konsole)

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen:

- 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
- Zugriffsanalysator: CheckAccessNotGranted

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-ShareEncryptedAMIOrEBSSnapshotim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname der AWS AWS Identity and Access Management Rolle, die es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - Genehmiger (erforderlich):

     Die Liste der AWS authentifizierten Principals, die die Aktion entweder genehmigen oder ablehnen können. Die maximale Anzahl an Genehmigern ist 10. Sie können Prinzipale angeben, indem Sie eines der folgenden Formate verwenden: Benutzername, Benutzer-ARN, IAM-Rollen-ARN oder IAM Assume Role ARN.
   - ResourceId (Erforderlich):

     AMIoder Amazon EBS Snapshot ID, die geteilt werden soll (z. B. ami-123456789012 oder snap-123456789012).
   - DestinationAccountId (Erforderlich):

     Die 12-stellige AWS Konto-ID, unter der die Ressource gemeinsam genutzt wird.
   - CustomerManagedKeyId (Fakultativ):

AWS KMS CMK-ID zum erneuten Verschlüsseln der Ressource. Erforderlich, wenn die Ressource mit einem AWS verwalteten Schlüssel verschlüsselt ist oder wenn sie für regionsübergreifendes DestinationRegion Kopieren angegeben ist. Für regionsübergreifendes Kopieren muss dieser Schlüssel in der Zielregion vorhanden sein.

- DestinationRegion (Fakultativ):

  Die AWS Region, in die die Ressource kopiert wird. Der Standardwert ist die aktuelle Region. Wenn eine andere Region angegeben wird, wird die Ressource mithilfe des im CustomerManagedKeyId Parameter angegebenen AWS KMS CMK in die Zielregion kopiert.

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - **`ValidateResources`**:

     Überprüft das Vorhandensein, den Status und die Verschlüsselungskonfiguration der Eingaberessourcen und ermittelt, welche Änderungen für die gemeinsame Nutzung erforderlich sind.

   - **`BranchOnResourcePermission`**:

     Verzweigt den Workflow je nachdem, ob die Genehmigung zur gemeinsamen Nutzung von Ressourcen überprüft werden muss.

   - **`CheckResourcePermission`**:

     Prüft, ob für das Zielkonto eine Freigabeberechtigung für die Ressource erforderlich ist.

   - **`AnalyzeChanges`**:

     Analysiert AWS KMS wichtige Richtlinien und erstellt eine umfassende Vorschau aller erforderlichen Änderungen.

   - **`BranchOnChanges`**:

     Verzweigt den Workflow danach, ob Änderungen genehmigt werden müssen.

   - **`GetApproval`**:

     Wartet auf die Genehmigung durch die designierten AWS IAM-Prinzipale, um mit den erforderlichen Änderungen fortzufahren.

   - **`ExecuteChanges`**:

Führt genehmigte Änderungen mit Rollback bei einem Fehler aus.

- **`Results`**:

  Generiert einen umfassenden Ausführungsbericht, in dem alle Aktionen zusammengefasst sind, die während des verschlüsselten Vorgangs AMI oder der gemeinsamen Nutzung von Snapshots ergriffen wurden.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.

Erforderliche AWS AWS Identity and Access Management Richtlinie für das Zielkonto

Die IAM-Rolle oder der Benutzer im Zielkonto muss die folgenden IAM-Berechtigungen konfigurieren, um verschlüsselte Amazon EC2-Instances aus dem gemeinsam genutzten verschlüsselten Amazon EBS-Snapshot zu starten AMI oder Volumes aus dem gemeinsam genutzten verschlüsselten Amazon EBS-Snapshot zu erstellen:

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

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows
- Teilen Sie einen AWS KMS Schlüssel

AWSSupport-RestoreEC2InstanceFromSnapshot

Beschreibung

Das `AWSSupport-RestoreEC2InstanceFromSnapshot` Runbook hilft Ihnen dabei, eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance anhand eines funktionierenden Amazon Elastic Block Store (Amazon EBS) -Snapshots des Root-Volumes zu identifizieren und wiederherzustellen.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EndDate

  Typ: Zeichenfolge

Beschreibung: (Optional) Das letzte Datum, an dem die Automatisierung nach einem Snapshot suchen soll.

- InplaceSwap

  Typ: Boolesch

  Zulässige Werte: true | false

  Beschreibung: (Optional) Wenn der Wert für diesen Parameter auf gesetzt ist`true`, ersetzt das neu erstellte Volume aus dem Snapshot das bestehende Root-Volume, das an Ihre Instance angehängt ist.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instance, die Sie aus einem Snapshot wiederherstellen möchten.

- LookForInstanceStatusCheck

  Typ: Boolesch

  Zulässige Werte: true | false

  Standard: true

  Beschreibung: (Optional) Wenn der Wert für diesen Parameter auf gesetzt ist, prüft die Automatisierung`true`, ob die Instanzstatusprüfungen bei den Testinstanzen, die über die Snapshots gestartet wurden, fehlschlagen.

- SkipSnapshotsBy

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Intervall, in dem Snapshots bei der Suche nach Snapshots zur Wiederherstellung Ihrer Instanz übersprungen werden. Wenn beispielsweise 100 Snapshots verfügbar sind und Sie für diesen Parameter den Wert 2 angeben, wird jeder dritte Snapshot überprüft.

  Standard: 0

- SnapshotId

Typ: Zeichenfolge

Beschreibung: (Optional) Die ID eines Snapshots, aus dem Sie die Instanz wiederherstellen möchten.

- StartDate

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das erste Datum, an dem die Automatisierung nach einem Snapshot suchen soll.

- TotalSnapshotsToLook

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Snapshots, die die Automatisierung überprüft.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

1. `aws:executeAwsApi`- Sammelt Details zur Zielinstanz.
2. `aws:assertAwsResourceProperty`— Überprüft, ob die Zielinstanz existiert.
3. `aws:assertAwsResourceProperty`— Überprüft, ob es sich bei dem Root-Volume um ein Amazon EBS-Volume handelt.
4. `aws:assertAwsResourceProperty`— Überprüft, ob noch keine andere Automatisierung ausgeführt wird, die auf diese Instance abzielt.
5. `aws:executeAwsApi`— Markiert die Zielinstanz.
6. `aws:executeAwsApi`- Erzeugt eine AMI der Instanz.
7. `aws:executeAwsApi`- Sammelt Details über AMI im vorherigen Schritt erstellt.
8. `aws:waitForAwsResourceProperty`- Wartet auf die AMI Zustand, der werden soll, `available` bevor fortgefahren wird.
9. `aws:executeScript`- Startet eine neue Instanz von der neu erstellten AMI.
10. `aws:assertAwsResourceProperty`- Überprüft, ob der Instanzstatus lautet`available`.
11. `aws:executeAwsApi`— Sammelt Details über die neu gestartete Instanz.
12. `aws:branch`— Verzweigt je nachdem, ob Sie einen Wert für den `SnapshotId` Parameter angegeben haben.
13. `aws:executeScript`- Gibt eine Liste von Schnappschüssen innerhalb des angegebenen Zeitraums zurück.
14. `aws:executeAwsApi`- Stoppt die Instanz.
15. `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Lautstärkestatus erreicht ist. `available`
16. `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Instanzstatus erreicht ist. `stopped`

17. `aws:executeAwsApi` - Trennt das Root-Volume.
18. `aws:waitForAwsResourceProperty` - Wartet darauf, dass das Root-Volume getrennt wird.
19. `aws:executeAwsApi` - Hängt das neue Root-Volume an.
20. `aws:waitForAwsResourceProperty` - Wartet darauf, dass das neue Volume angehängt wird.
21. `aws:executeAwsApi` - Startet die Instanz.
22. `aws:waitForAwsResourceProperty` - Wartet darauf, dass der Instanzstatus erreicht ist. `available`
23. `aws:waitForAwsResourceProperty` - Wartet darauf, dass die System- und Instanzstatusprüfungen für die Instanz bestanden sind.
24. `aws:executeScript` - Führt ein Skript aus, um einen Snapshot zu finden, mit dem ein Volume erfolgreich erstellt werden kann.
25. `aws:executeScript` - Führt ein Skript aus, um die Instanz mithilfe des neu erstellten Volumes aus dem durch die Automatisierung identifizierten Snapshot oder mithilfe des Volumes wiederherzustellen, das aus dem Snapshot erstellt wurde, den Sie im `SnapshotId` Parameter angegeben haben.
26. `aws:executeScript` - Löscht Ressourcen, die durch die Automatisierung erstellt wurden.

Ausgaben

launchCloneInstance.InstanceIds

ListSnapshotByDate. Letzte Schnappschüsse

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot. funktionierender Snapshot

InstanceRecovery. Ergebnis

`AWSSupport-SendLogBundleToS3Bucket`

Beschreibung

Das `AWSSupport-SendLogBundleToS3Bucket` Runbook lädt ein vom EC2 Rescue-Tool generiertes Protokollpaket von der Zielinstanz in den angegebenen S3-Bucket hoch. Das Runbook installiert die plattformspezifische Version von EC2 Rescue, die auf der Plattform der Zielinstanz basiert. EC2Rescue wird dann verwendet, um alle verfügbaren Betriebssystemprotokolle (OS) zu sammeln.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der von Windows oder Linux verwalteten Instance, von der Sie Protokolle erfassen möchten.
- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) S3-Bucket, in den die Protokolle hochgeladen werden sollen.
- S3Path

  Typ: Zeichenfolge

  Standard:`AWSSupport-SendLogBundleToS3Bucket/`

  Beschreibung: (Optional) S3-Pfad für die erfassten Protokolle.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass die EC2 Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, der die von SSMManagedInstanceCoreAmazon verwaltete Richtlinie beigefügt ist. Der Benutzer muss mindestens über ssm: StartAutomationExecution und ssm: verfügen, SendCommand um die Automatisierung auszuführen und den Befehl an die Instance zu senden, sowie über ssm:, GetAutomationExecution um die Automatisierungsausgabe lesen zu können.

Dokumentschritte

1. `aws:runCommand`- Installieren Sie EC2 Rescue über. `AWS-ConfigureAWSPackage`
2. `aws:runCommand`- Führen Sie das PowerShell Skript aus, um Windows-Fehlerbehebungsprotokolle mit EC2 Rescue zu sammeln.
3. `aws:runCommand`- Führen Sie das Bash-Skript aus, um Linux-Fehlerbehebungsprotokolle mit EC2 Rescue zu sammeln.

Ausgaben

collectAndUploadWindowsLogBundle. Ausgabe

collectAndUploadLinuxLogBundle. Ausgabe

AWSSupport-StartEC2RescueWorkflow

Beschreibung

Das `AWSSupport-StartEC2RescueWorkflow` Runbook führt das bereitgestellte Base64-kodierte Skript (Bash oder Powershell) auf einer Hilfsinstanz aus, die zur Rettung Ihrer Instanz erstellt wurde. Das Root-Volume Ihrer Instance ist an die Helper-Instance, auch Rescue-Instanz genannt, angehängt und an diese gemountet. EC2 Wenn Ihre Instance unter Windows läuft, geben Sie ein Powershell-Skript an. Verwenden Sie andernfalls Bash. Das Runbook legt einige Umgebungsvariablen fest, die Sie in Ihrem Skript verwenden können. Die Umgebungsvariablen enthalten Informationen über die Eingabe, die Sie bereitgestellt haben, sowie Informationen zu dem Offline-Root-Volume. Das Offline-Volume ist bereits gemountet und kann verwendet werden. Beispiel: Sie können eine Desired State Configuration-Datei zu einem Offline-Windows-Root-Volume oder chroot zu einem Offline-Linux-Root-Volume speichern und eine Offline-Wiederherstellung durchführen.

[Führen Sie diese Automatisierung aus (Konsole)]

> **Important**
>
> Amazon EC2 EC2-Instances, die über Marketplace Amazon Machine Images (AMIs) erstellt wurden, werden von dieser Automatisierung nicht unterstützt.

Zusätzliche Informationen

Um ein Skript mit base64 zu kodieren, können Sie PowerShell oder Bash verwenden. Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

Bash:

```
base64 PATH_TO_FILE
```

Hier sehen Sie eine Liste der Umgebungsvariablen, die Sie in Ihren Offline-Skripts verwenden können, je nach Ziel-Betriebssystem.

Windows:

Variable	Description	Beispielwert
$env: RESCUE_AC COUNT_ID EC2	{{ global:ACCOUNT_ID }}	123456789012
$env: EC2 RESCUE_DATE	{{ global:DATE }}	2018-09-07
$env: EC2 RESCUE_DA TE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
$env: EC2 RESCUE_ RW_DIR EC2	EC2Installationspfad für Rescue für Windows	C:\Program Files\ Amazon\ EC2 Rescue
$env: EC2 RESCUE_ RW_DIR EC2	EC2Installationspfad für Rescue für Windows	C:\Program Files\ Amazon\ EC2 Rescue

Variable	Description	Beispielwert
$env: RESCUE_EXECUTION_ID EC2	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
$env: EC2 RESCUE_OFFLINE_CURRENT_CONTROL_SET	Offline Windows Current Control Set-Pfad	`HKLM:\AWSTempSystem\ControlSet001`
$env: EC2 RESCUE_OFFLINE_DRIVE	Offline-Windows-Laufwerkbuchstabe	D:\
$env: EC2 RESCUE_OFFLINE_EBS_DEVICE	Offline-Root-Volume-EBS-Gerät	xvdf
$env: EC2 RESCUE_OFFLINE_KERNEL_VER	Offline-Windows-Kernel-Version	6.1.7601.24214
$env: EC2 RESCUE_OFFLINE_OS_ARCHITECTURE	Offline-Windows-Architektur	AMD64
$env: EC2 RESCUE_OFFLINE_OS_CAPTION	Offline-Windows-Beschriftung	Windows Server 2008 R2 Datacenter
$env: EC2 RESCUE_OFFLINE_OS_TYPE	Offline-Windows-Betriebssystemtyp	Server
$env: EC2 RESCUE_OFFLINE_PROGRAM_FILES_DIR	Offline-Windows-Programmdateien-Verzeichnispfad	D:\Program Files
$env: EC2 RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	Offline-Windows-Programmdateien-x86-Verzeichnispfad	D:\Program Files (x86)
$env: EC2 RESCUE_OFFLINE_REGISTRY_DIR	Offline-Windows-Registry-Verzeichnispfad	D:\Windows\System32\config

Variable	Description	Beispielwert
$env: EC2 RESCUE_OFFLINE_SYSTEM_ROOT	Offline-Windows-Systemstamm-Verzeichnispfad	D:\Windows
$env: EC2 RESCUE_REGION	{{ global:REGION }}	us-west-1
$env: EC2 RESCUE_S3_BUCKET	{{S3}} BucketName	amzn-s3-Demo-Bucket
$env: RESCUE_S3_PREFIX EC2	{{ S3Prefix }}	myprefix/
$env: EC2 RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
$skript: EC2 RESCUE_OFFLINE_WINDOWS_INSTALL	Offline-Windows-Installations-Metadaten	Customer PowerShell-Objekt

Linux:

Variable	Description	Beispielwert
EC2RESCUE_ACCOUNT-ID	{{ global:ACCOUNT_ID }}	123456789012
EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
EC2RETTUNGSDATUM_UHRZEIT	{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_RL_DIR EC2	EC2Installationspfad von Rescue für Linux	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2RESCUE_OFFLINE-GERÄT	Offline-Gerätename	/dev/xvdf1

Variable	Description	Beispielwert
EC2RESCUE_OFFLINE_EBS_DEVICE	Offline-Root-Volume-EBS-Gerät	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	Offline-Root-Volume-Mounting-Punkt	/mnt/mount
EC2RESCUE_PYTHON	Python-Version	python2.7
EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{S3}} BucketName	amzn-s3-Demo-Bucket
EC2RESCUE_S3_PRÄFIX	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_INSTANZ	{{ InstanceId }}	i-abcdefgh123456789

Typ des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AMIPrefix

  Typ: Zeichenfolge

  Standard: `AWSSupport-EC2Rescue`

  Beschreibung: (Optional) Ein Präfix für den Backup-AMI-Namen.
- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- CreatePostEC2RescueBackup

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Stellen Sie es auf ein, `true` um ein AMI von InstanceId nach der Ausführung des Skripts zu erstellen, bevor Sie es starten. Das AMI bleibt nach Abschluss der Automatisierung erhalten. Es liegt in Ihrer Verantwortung, den Zugriff auf das AMI zu gewährleisten oder es zu löschen.

- CreatePreEC2RescueBackup

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Stellen Sie es auf ein, `true` um InstanceId vor der Ausführung des Skripts ein AMI von zu erstellen. Das AMI bleibt nach Abschluss der Automatisierung erhalten. Es liegt in Ihrer Verantwortung, den Zugriff auf das AMI zu gewährleisten oder es zu löschen.

- EC2RescueInstanceType

  Typ: Zeichenfolge

  Gültige Werte: t2.small | t2.medium | t2.large | t3.small | t3.medium | t3.large | i3.large

  Standard: t3.medium

  Beschreibung: (Optional) Der EC2-Instance-Typ für die Rescue-Instance. EC2

- InstanceId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) ID Ihrer EC2-Instance. WICHTIG: Die AWS Systems Manager Automatisierung stoppt diese Instanz. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP verwenden.

- OfflineScript

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Base64-kodiertes Skript zur Ausführung gegen die Helper-Instance. Verwenden Sie Bash, wenn Ihre Quellinstanz Linux und PowerShell Windows ist.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Name des S3-Buckets in Ihrem Konto, in den Sie die Protokolle zur Fehlerbehebung hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie Parteien, die keinen Zugriff auf die gesammelten Protokolle benötigen, keine unnötigen read/write Berechtigungen gewährt.

- S3Prefix

  Typ: Zeichenfolge

  Standard: `AWSSupport-EC2Rescue`

  Beschreibung: (Optional) Ein Präfix für die S3-Protokolle.

- SubnetId

  Typ: Zeichenfolge

  Standard: SelectedInstanceSubnet

  Beschreibung: (Optional) Die Subnetz-ID für die EC2 Rescue-Instanz. Standardmäßig wird dasselbe Subnetz verwendet, in dem sich die bereitgestellte Instance befindet. WICHTIG: Wenn Sie ein benutzerdefiniertes Subnetz angeben, muss es sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

- UniqueId

  Typ: Zeichenfolge

Standard: {{ automation:EXECUTION_ID }}

Beschreibung: (Optional) Eine eindeutige Kennung für die Automatisierung.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass dem Benutzer, der die Automatisierung ausführt, die von Amazon SSMAutomation Role IAM verwaltete Richtlinie beigefügt ist. Zusätzlich zu dieser Richtlinie benötigt der Benutzer:

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"
        }
    ]
}
```

Dokumentschritte

1. `aws:executeAwsApi`— Beschreiben Sie die bereitgestellte Instanz
2. `aws:executeAwsApi`- Beschreiben Sie das Root-Volume der bereitgestellten Instanz
3. `aws:assertAwsResourceProperty`— Vergewissern Sie sich, dass der Gerätetyp des Root-Volumes EBS ist
4. `aws:assertAwsResourceProperty`- Stellen Sie sicher, dass das Root-Volume nicht verschlüsselt ist
5. `aws:assertAwsResourceProperty`- Überprüfen Sie die angegebene Subnetz-ID
   a. (Verwenden Sie das aktuelle Instanz-Subnetz) — Wenn * SubnetId = SelectedInstanceSubnet *, dann starten Sie, `aws:createStack` um den EC2 Rescue-Stack bereitzustellen CloudFormation
   b. (Neue VPC erstellen) — Wenn * SubnetId = CreateNew VPC*, dann ausführen, `aws:createStack` um den Rescue-Stack bereitzustellen EC2 CloudFormation
   c. (Verwenden eines benutzerdefinierten Subnetzes) – In allen anderen Fällen:

      `aws:assertAwsResourceProperty`- Überprüfen Sie, ob sich das angegebene Subnetz in derselben Availability Zone wie die bereitgestellte Instanz befindet

      `aws:createStack`- Stellen Sie den EC2 Rescue-Stack CloudFormation bereit
6. `aws:invokeLambdaFunction`- Führen Sie eine zusätzliche Eingabevalidierung durch
7. `aws:executeAwsApi`- Aktualisieren Sie den EC2 CloudFormation Rescue-Stack, um die EC2 Rescue-Helper-Instanz zu erstellen
8. `aws:waitForAwsResourceProperty`- Warten Sie, bis das EC2 CloudFormation Rescue-Stack-Update abgeschlossen ist
9. `aws:executeAwsApi`- Beschreiben Sie die EC2 CloudFormation Rescue-Stack-Ausgabe, um die EC2 Rescue-Helper-Instanz-ID zu erhalten
10. `aws:waitForAwsResourceProperty`- Warten Sie, bis die EC2 Rescue-Helper-Instanz zu einer verwalteten Instanz wird

11. `aws:changeInstanceState`- Stoppt die bereitgestellte Instanz
12. `aws:changeInstanceState`- Stoppt die bereitgestellte Instanz
13. `aws:changeInstanceState`- Erzwingt das Stoppen der bereitgestellten Instanz
14. `aws:assertAwsResourceProperty`- Überprüfen Sie den CreatePre EC2 RescueBackup Eingabewert
    a. (EC2Pre-Rescue-Backup erstellen) — Wenn * CreatePre EC2 RescueBackup = true*
    b. `aws:executeAwsApi`- Erstellen Sie ein AMI-Backup der bereitgestellten Instanz
    c. `aws:createTags`- Taggen Sie das AMI-Backup
15. `aws:runCommand`- Installieren Sie EC2 Rescue auf der EC2 Rescue-Helper-Instanz
16. `aws:executeAwsApi`- Trennen Sie das Root-Volume von der bereitgestellten Instanz
17. `aws:assertAwsResourceProperty`- Überprüfen Sie die bereitgestellte Instanzplattform
    a. (Instance ist Windows):

       `aws:executeAwsApi`- Hängen Sie das Root-Volume als *xvdf* an die EC2 Rescue-Helper-Instanz an

       `aws:sleep`- Schlafen Sie 10 Sekunden

       `aws:runCommand`- Führen Sie das bereitgestellte Offline-Skript in Powershell aus
    b. (Instance ist Linux):

       `aws:executeAwsApi`- Hängen Sie das Root-Volume als */dev/sdf* an die EC2 Rescue-Helper-Instanz an

       `aws:sleep`- Schlafen Sie 10 Sekunden

       `aws:runCommand`- Führen Sie das bereitgestellte Offline-Skript in Bash aus
18. `aws:changeInstanceState`- Stoppen Sie die EC2 Rescue-Helper-Instanz
19. `aws:changeInstanceState`- Erzwingt das Stoppen der EC2 Rescue-Helper-Instanz
20. `aws:executeAwsApi`- Trennen Sie das Root-Volume von der EC2 Rescue-Helper-Instanz
21. `aws:executeAwsApi`- Hängen Sie das Root-Volume wieder an die bereitgestellte Instanz an
22. `aws:assertAwsResourceProperty`- Überprüfen Sie den CreatePost EC2 RescueBackup Eingabewert
    a. (Backup nach dem EC2 Rescue erstellen) — Wenn * CreatePost EC2 RescueBackup = true*
    b. `aws:executeAwsApi`- Erstellen Sie ein AMI-Backup der bereitgestellten Instanz

c. `aws:createTags`- Taggen Sie das AMI-Backup

23. `aws:executeAwsApi`— Stellt den ursprünglichen Status „Löschen bei Beendigung“ für das Root-Volume der bereitgestellten Instanz wieder her

24. `aws:changeInstanceState`- Stellt den ursprünglichen Zustand der bereitgestellten Instanz wieder her (laufend/gestoppt)

25. `aws:deleteStack`- Löscht den Rescue-Stack EC2 CloudFormation

Ausgaben

runScriptForLinux.Ausgabe

runScriptForWindows.Ausgabe

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSSupport-TroubleshootActiveDirectoryReplication

Beschreibung

Das AWSSupport-TroubleshootActiveDirectoryReplicationRunbook hilft bei der Behebung von Replikationsfehlern bei der Microsoft Active Directory (AD) -Domänencontroller-Replikation, indem allgemeine Einstellungen auf einer Zieldomänencontroller-Instanz überprüft werden. Dieses Runbook führt eine Reihe von PowerShell Befehlen für die bereitgestellte Domänencontroller-Instanz aus, um den aktuellen Replikationsstatus zu überprüfen und Fehler zu melden, die möglicherweise zu Problemen bei der Domänenreplikation führen können. Das Runbook kann optional replikationskritische Dienste (`Netlogon`,, und`KDC`) starten `RPCSSW32Time`, wenn sie beendet sind, und die Systemzeit synchronisieren, indem sie `w32tm /resync /force` auf der Zielinstanz ausgeführt werden.

> **Important**
>
> AWS Verwaltetes Microsoft AD fällt nicht in den Geltungsbereich dieses Runbooks.

> **Important**
>
> Während die Automatisierung Befehle auf der Zielinstanz ausführt, werden Änderungen am Dateisystem der Zielinstanz vorgenommen. Zu diesen Änderungen gehören die Erstellung des Protokollverzeichnisses (`$env:ProgramData\TroubleshootActiveDirectoryReplication`) und der Berichtsdateien.

Wie funktioniert es?

Das Runbook führt die folgenden Prüfungen und Aktionen durch:

- Überprüft, ob auf der Zielinstanz Windows ausgeführt wird und sie von Systems Manager verwaltet wird.
- Führt PowerShell Skripts aus, um die Konfiguration und den Status der Active Directory-Replikation zu überprüfen.
- Überprüft die Sicherheitsgruppen- und Netzwerk-ACL-Einstellungen auf Konnektivität mit dem Replikationspartner.
- Behebt Fehler bei der Zeitsynchronisierung und beim Status kritischer Dienste.
- Lädt Protokolldateien zur Analyse in den angegebenen Amazon S3 S3-Bucket hoch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeInstances`
- `secretsmanager:GetSecretValue`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicy`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutObject`

Beispiel für eine Richtlinie:

```
{
    "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 einrichten

Das PowerShell Check-Replication-Skript stellt eine Verbindung zum Microsoft Active Directory-Zieldomänencontroller her, indem es den Benutzernamen und das Kennwort mit einem Laufzeitaufruf von abruft. AWS Secrets Manager Folgen Sie den Schritten unter Create an AWS Secrets Manager Secret, um ein neues AWS Secrets Manager Secret zu erstellen. Stellen Sie sicher, dass der Benutzername und das Passwort als key/value Paar im folgenden Format gespeichert sind`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`. Stellen Sie nach der Erstellung des AWS Secrets Manager Geheimnisses sicher, dass Sie der IAM-Instanzprofilrolle Ihres Zieldomänencontrollers die `secretsmanager:GetSecretValue` Berechtigung für den geheimen ARN erteilen.

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootActiveDirectoryReplication`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - InstanceId (Erforderlich):
     - Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Domain-Controller-Instance, für die Sie Probleme mit der Active Directory-Replikation beheben möchten. Beachten Sie, dass es sich bei der bereitgestellten Instance um einen Domain-Controller handeln muss.
     - Typ: `AWS::EC2::Instance::Id`
   - SecretsManagerArn (Erforderlich):
     - Beschreibung: (Erforderlich) Der ARN Ihres AWS Secrets Manager Geheimnisses, der einen Active Directory-Benutzernamen und ein Kennwort mit Enterprise Admin-

oder gleichwertigen Berechtigungen für den Zugriff auf Ihre Active Directory-Domäne und Gesamtstrukturkonfiguration enthält. Stellen Sie sicher, dass der Benutzername und das Passwort als key/value Paar im folgenden Format gespeichert werden`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`. Stellen Sie sicher, dass Sie die `secretsmanager:GetSecretValue` Berechtigung für den geheimen ARN der IAM-Instanzprofilrolle Ihres Zieldomänencontrollers zuordnen.

  - Typ: `String`
  - Zulässiges Muster: `^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 (Fakultativ):
  - Beschreibung: (Optional) Wählen Sie `Check` oder`Sync`. Wenn Sie diese Option auswählen`Check`, druckt das Runbook den aktuellen Status der Systemzeitsynchronisierung aus. Wenn diese Option ausgewählt `Sync` ist, versucht das Runbook, eine erneute Synchronisierung der Zeit zu erzwingen, indem es `w32tm /resync /force` auf der Zielinstanz ausgeführt wird.
  - Typ: `String`
  - Zulässige Werte: `[Check, Sync]`
  - Standard: `Check`
- ServiceAction (Fakultativ):
  - Beschreibung: (Optional) Wählen Sie `Check` oder`Fix`. Wenn Sie diese Option auswählen`Check`, druckt das Runbook den aktuellen Status der `Key Distribution Center (KDC)` Dienste`Netlogon`, `Windows Time service (W32Time)``Remote Procedure Call (RPC) Service`, und aus. Wenn diese Option ausgewählt `Fix` ist, versucht das Runbook, diese Dienste zu starten, falls sie beendet wurden.
  - Typ: `String`
  - Zulässige Werte: `[Check, Fix]`
  - Standard: `Check`
- LogDestination (Erforderlich):
  - Beschreibung: (Erforderlich) Der Amazon Amazon S3 S3-Bucket in Ihrem AWS Konto, um die Befehlsausgaben hochzuladen.
  - Typ: `String`

4. Wählen Sie Ausführen aus.

5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - assertIfOperatingSystemIsWindows:

     Überprüft, ob das Betriebssystem der bereitgestellten Amazon EC2 EC2-Zielinstanz Windows ist.
   - assertifInstanceIsSsmManaged:

     Stellt sicher, dass die Amazon EC2 EC2-Instance von Systems Manager verwaltet wird, andernfalls endet die Automatisierung.
   - Überprüfen Sie die Replikation:

     Führt ein PowerShell Skript auf der angegebenen Domänencontroller-Instanz aus, um die Konfiguration und den Status der Active Directory-Domänenreplikation abzurufen.
   - checkInstanceSgAndNacl:

     Überprüft, ob die Sicherheitsgruppe und die Netzwerk-ACL, die der Ziel-Domänen-Controller-Instanz zugeordnet sind, Datenverkehr zu den Replikationspartnern zulassen.
   - Problembehandlung bei der Replikation:

     Führt ein PowerShell Skript aus, um Fehler bei der Zeitsynchronisierung und beim Status kritischer Dienste zu beheben.
   - Überprüft S3 BucketPublicStatus:

     Prüft, ob der in angegebene Amazon S3 S3-Bucket anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen `LogDestination` zulässt.
   - **`runUploadScript`**:

     Führt ein PowerShell Skript aus, um das Protokollarchiv in den im `LogDestination` Parameter angegebenen AAmazon S3-Bucket hochzuladen, und löscht die archivierte Protokolldatei aus dem Betriebssystem. Die Protokolldateien können zur Fehlerbehebung verwendet oder bei der Behebung von Replikationsproblemen an den AWS Support weitergegeben werden.
7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

AWSPremiumSupport-TroubleshootEC2DiskUsage

Beschreibung

Das `AWSPremiumSupport-TroubleshootEC2DiskUsage` Runbook hilft Ihnen dabei, Probleme mit der Root- und Nicht-Root-Festplattennutzung von Amazon Elastic Compute Cloud (Amazon EC2) -Instances zu untersuchen und möglicherweise zu beheben. Wenn möglich, versucht das Runbook, Probleme zu beheben, indem es das Volume und das zugehörige Dateisystem erweitert. Um diese Aufgaben auszuführen, orchestriert dieses Runbook die Ausführung mehrerer Runbooks, die auf dem Betriebssystem der betroffenen Instanz basieren.

Das erste Runbook (`AWSPremiumSupport-DiagnoseDiskUsageOnWindows`oder) bestimmt`AWSPremiumSupport-DiagnoseDiskUsageOnLinux`, ob Festplattenprobleme durch die Erweiterung des Volumes behoben werden können.

Das zweite Runbook, `AWSPremiumSupport-ExtendVolumesOnWindows` oder`AWSPremiumSupport-ExtendVolumesOnLinux`, verwendet die Ausgabe des ersten Runbooks, um Python-Code auszuführen, der das Volume ändert. Nachdem das Volume geändert wurde, erweitert das Runbook die Partition und das Dateisystem der betroffenen Volumes.

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist ein Abonnement für Business + Support, Enterprise Support oder Unified Operations erforderlich. Weitere Informationen finden Sie unter AWS Support Tarife vergleichen.

Dieses Dokument wurde in Zusammenarbeit mit AWS Managed Services (AMS) erstellt. AMS hilft Ihnen, Ihre AWS Infrastruktur effizienter und sicherer zu verwalten. AMS bietet außerdem betriebliche Flexibilität, verbesserte Sicherheit und Compliance, Kapazitätsoptimierung und Identifizierung von Kosteneinsparungen. Weitere Informationen finden Sie unter AWS Managed Services.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, Windows

Parameter

- InstanceId

  Typ: Zeichenfolge

  Zulässige Werte: ^i- [a-z0-9] {8,17} $

  Beschreibung: (Erforderlich) ID Ihrer Amazon EC2 EC2-Instance.
- VolumeExpansionEnabled

  Typ: Boolescher Wert

  Beschreibung: (Optional) Markierung, mit der gesteuert wird, ob das Dokument die betroffenen Volumes und Partitionen erweitert.

  Standard: true
- VolumeExpansionUsageTrigger

  Typ: Zeichenfolge

  Beschreibung: (Optional) Mindestbelegung des Partitionsspeichers, der zum Auslösen der Erweiterung erforderlich ist (in Prozent).

  Zulässige Werte: ^ [0-9] {1,2} $

  Standard: 85
- VolumeExpansionCapSize

Typ: Zeichenfolge

Beschreibung: (Optional) Maximale Größe, auf die das Amazon Elastic Block Store (Amazon EBS) -Volumen erhöht wird (in GiB).

Zulässige Werte: ^ [0-9] {1,4} $

Standard: 2048

- VolumeExpansionGibIncrease

  Typ: Zeichenfolge

  Beschreibung: (Optional) Erhöhung des Volumens in GiB. Es VolumeExpansionPercentageIncrease wird der größte Nettozuwachs zwischen VolumeExpansionGibIncrease und verwendet.

  Zulässige Werte: ^ [0-9] {1,4} $

  Standard: 20

- VolumeExpansionPercentageIncrease

  Typ: Zeichenfolge

  Beschreibung: (Optional) Erhöhung des Prozentsatzes des Volumens. Es VolumeExpansionPercentageIncrease wird der größte Nettozuwachs zwischen VolumeExpansionGibIncrease und verwendet.

  Zulässige Werte: ^ [0-9] {1,2} $

  Standard: 20

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

1. `aws:assertAwsResourceProperty`- Prüfen Sie, ob die Instanz vom Systems Manager verwaltet wird
2. `aws:executeAwsApi`- Beschreibt die Instanz, von der die Plattform abgerufen werden soll.
3. `aws:branch`— Die Automatisierung von Verzweigungen basiert auf der Plattform der Instanz.
   a. Wenn es sich bei der Instanz um Windows handelt:
      i. `aws:executeAutomation`- Führen Sie das `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` Runbook aus, um Probleme mit der Festplattennutzung auf der Instanz zu diagnostizieren.

ii. `aws:executeAwsApi`- Ruft die Ausgabe der vorherigen Automatisierung ab.

iii. `aws:branch`- Verzweigt anhand der Ergebnisse der Diagnose und ob Volumes vorhanden sind, die erweitert werden können, um die Warnung zu beheben.

A. Es gibt keine Volumen, die erweitert werden müssen: Beenden Sie die Automatisierung.

B. Es gibt Volumen, die erweitert werden müssen:

I. `aws:executeAwsApi`- Erstellen Sie eine Amazon Machine Image (AMI) der Instanz.

II. `aws:waitForAwsResourceProperty`- Wartet darauf, dass der AMI Status erreicht ist. `available`

III. `aws:executeAutomation`- Führen Sie das `AWSPremiumSupport-ExtendVolumesOnWindows` Runbook aus, um die Änderung des Volumes sowie die erforderlichen Schritte im Betriebssystem (OS) durchzuführen, um den neuen Speicherplatz verfügbar zu machen.

b. (Plattform ist nicht Windows) Wenn es sich bei der Eingabeinstanz nicht um Windows handelt:

i. `aws:executeAutomation`- Führen Sie das `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` Runbook aus, um Probleme mit der Festplattennutzung auf der Instanz zu diagnostizieren.

ii. `aws:executeAwsApi`- Ruft die Ausgabe der vorherigen Automatisierung ab.

iii. `aws:branch`- Verzweigt anhand der Ergebnisse der Diagnose und ob Volumes vorhanden sind, die erweitert werden können, um die Warnung zu beheben.

A. Es gibt keine Volumen, die erweitert werden müssen: Beenden Sie die Automatisierung.

B. Es gibt Volumen, die erweitert werden müssen:

I. `aws:executeAwsApi`- Erstellen Sie eine AMI der Instanzen.

II. `aws:waitForAwsResourceProperty`- Wartet darauf, dass AMI der Status erreicht ist. `available`

III. `aws:executeAutomation`- Führen Sie das `AWSPremiumSupport-ExtendVolumesOnLinux` Runbook aus, um die Änderung des Volumes sowie die erforderlichen Schritte im Betriebssystem durchzuführen, um den neuen Speicherplatz verfügbar zu machen.

Ausgaben

diagnoseDiskUsageAlertOnWindows. Ausgabe

extendVolumesOnWindows.Ausgabe

diagnoseDiskUsageAlertOnLinux. Ausgabe

extendVolumesOnLinux.Ausgabe

BackupAMILinux. ImageId

BackupAMIWindows. ImageId

AWSSupport-TroubleshootEC2InstanceConnect

Beschreibung

`AWSSupport-TroubleshootEC2InstanceConnect`Die Automatisierung hilft bei der Analyse und Erkennung von Fehlern und verhindert so die Verbindung zu einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance mithilfe von Amazon EC2 Instance Connect. Es identifiziert Probleme, die durch ein nicht unterstütztes Amazon Machine Image (AMI), eine fehlende Paketinstallation oder -konfiguration auf Betriebssystemebene, fehlende AWS Identity and Access Management (IAM-) Berechtigungen oder Probleme mit der Netzwerkkonfiguration verursacht wurden.

Wie funktioniert es?

Das Runbook verwendet die Amazon EC2-Instance-ID, den Benutzernamen, den Verbindungsmodus, die Quell-IP-CIDR, den SSH-Port und den Amazon-Ressourcennamen (ARN) für die IAM-Rolle oder den Benutzer, bei dem Probleme mit Amazon EC2 Instance Connect auftreten. Anschließend werden die Voraussetzungen für die Verbindung mit einer Amazon EC2-Instance mithilfe von Amazon EC2 Instance Connect geprüft:

- Die Instance läuft und befindet sich in einem fehlerfreien Zustand.
- Die Instance befindet sich in einer AWS Region, die von Amazon EC2 Instance Connect unterstützt wird.
- Das AMI der Instance wird von Amazon EC2 Instance Connect unterstützt.
- Die Instance kann den Instance-Metadaten-Service (IMDSv2) erreichen.
- Das Amazon EC2 Instance Connect-Paket ist auf Betriebssystemebene ordnungsgemäß installiert und konfiguriert.
- Die Netzwerkkonfiguration (Sicherheitsgruppen, Netzwerk-ACL und Routing-Tabellenregeln) ermöglicht die Verbindung mit der Instance über Amazon EC2 Instance Connect.
- Die IAM-Rolle oder der Benutzer, der zur Nutzung von Amazon EC2 Instance Connect verwendet wird, hat Zugriff auf Push-Tasten für die Amazon EC2 EC2-Instance.

Important

- Um das Instance-AMI, die IMDSv2-Erreichbarkeit und die Installation des Amazon EC2 Instance Connect-Pakets zu überprüfen, muss die Instance SSM-verwaltet werden. Andernfalls werden diese Schritte übersprungen. Weitere Informationen finden Sie unter Warum wird meine Amazon EC2 EC2-Instance nicht als verwalteter Knoten angezeigt?
- Bei der Netzwerkprüfung wird nur dann festgestellt, ob Sicherheitsgruppen- und Netzwerk-ACL-Regeln den Datenverkehr blockieren, wenn SourceIp CIDR als Eingabeparameter angegeben wird. Andernfalls werden nur SSH-bezogene Regeln angezeigt.
- Verbindungen, die Amazon EC2 Instance Connect Endpoint verwenden, werden in diesem Runbook nicht validiert.
- Bei privaten Verbindungen überprüft die Automatisierung nicht, ob der SSH-Client auf dem Quellcomputer installiert ist und ob er die private IP-Adresse der Instance erreichen kann.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`

- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootEC2InstanceConnect`in der AWS Systems Manager Konsole zum.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - InstanceId (Erforderlich):

     Die ID der Amazon EC2-Zielinstanz, zu der Sie mit Amazon EC2 Instance Connect keine Verbindung herstellen konnten.
   - AutomationAssumeRole (Optional):

     Der ARN der IAM-Rolle, der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen auszuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - Benutzername (erforderlich):

     Der Benutzername, der für die Verbindung mit der Amazon EC2-Instance mithilfe von Amazon EC2 Instance Connect verwendet wird. Er wird verwendet, um zu bewerten, ob diesem bestimmten Benutzer IAM-Zugriff gewährt wird.
   - EC2InstanceConnectRoleOrUser(Erforderlich):

     Der ARN der IAM-Rolle oder des Benutzers, der Amazon EC2 Instance Connect nutzt, um Schlüssel für die Instance zu übertragen.
   - SSHPort (Optional):

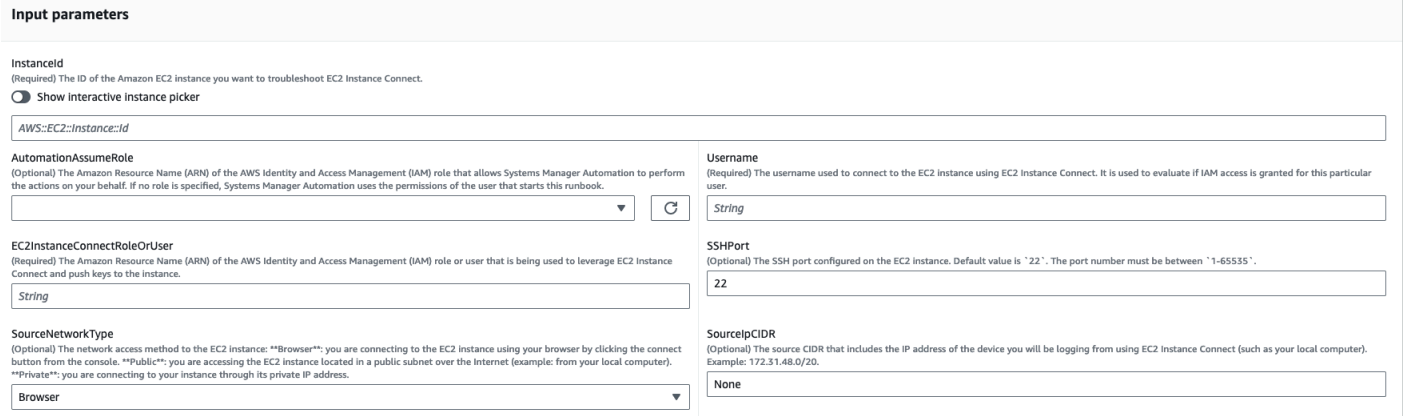
     Der auf der Amazon EC2 EC2-Instance konfigurierte SSH-Port. Der Standardwert ist 22. Die Portnummer muss zwischen liegen. `1-65535`

- SourceNetworkType (Fakultativ):

  Die Netzwerkzugriffsmethode für die Amazon EC2 EC2-Instance:

  - Browser: Sie stellen von der AWS Management Console aus eine Verbindung her.
  - Öffentlich: Sie stellen über das Internet eine Verbindung zu der Instance her, die sich in einem öffentlichen Subnetz befindet (z. B. Ihr lokaler Computer).
  - Privat: Sie stellen eine Verbindung über die private IP-Adresse der Instance her.
- SourceIpCIDR (optional):

  Die Quell-CIDR, die die IP-Adresse des Geräts (z. B. Ihres lokalen Computers) enthält, von dem Sie sich mit Amazon EC2 Instance Connect anmelden. Beispiel: 172.31.48.6/32. Wenn für den öffentlichen oder privaten Zugriffsmodus kein Wert angegeben wird, bewertet das Runbook nicht, ob die Amazon EC2 EC2-Instance-Sicherheitsgruppe und die Netzwerk-ACL-Regeln SSH-Verkehr zulassen. Stattdessen werden SSH-bezogene Regeln angezeigt.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:

   - AssertInitialState:

     Stellt sicher, dass der Amazon EC2 EC2-Instance-Status läuft. Andernfalls endet die Automatisierung.
   - GetInstanceProperties:

     Ruft die aktuellen Amazon EC2 EC2-Instance-Eigenschaften (PlatformDetails, PublicIpAddress VpcId, SubnetId und MetadataHttpEndpoint) ab.
   - GatherInstanceInformationFromSSM:

Ruft den Ping-Status und die Betriebssystemdetails der Systems Manager Manager-Instanz ab, wenn die Instanz SSM-verwaltet wird.

- CheckIfAWSRegionUnterstützt:

  Prüft, ob sich die Amazon EC2-Instance in einer von Amazon EC2 Instance Connect unterstützten AWS Region befindet.

- BranchOnIfAWSRegionUnterstützt:

  Setzt die Ausführung fort, wenn die AWS Region von Amazon EC2 Instance Connect unterstützt wird. Andernfalls erstellt es die Ausgabe und beendet die Automatisierung.

- CheckIfInstanceAMIIsUnterstützt:

  Prüft, ob das der Instance zugeordnete AMI von Amazon EC2 Instance Connect unterstützt wird.

- BranchOnIfInstanceAMIIsUnterstützt:

  Wenn das Instance-AMI unterstützt wird, führt es die Prüfungen auf Betriebssystemebene durch, z. B. die Erreichbarkeit von Metadaten und die Installation und Konfiguration des Amazon EC2 Instance Connect-Pakets. Andernfalls prüft es mithilfe der AWS API, ob HTTP-Metadaten aktiviert sind, und fährt dann mit der Netzwerkprüfung fort.

- Prüfen Sie IMDSReachabilityFromOs:

  Führt ein Bash-Skript auf der Amazon EC2 EC2-Linux-Zielinstanz aus, um zu prüfen, ob sie die erreichen kann. IMDSv2

- Installation überprüfenEICPackage:

  Führt ein Bash-Skript auf der Amazon EC2-Linux-Zielinstanz aus, um zu überprüfen, ob das Amazon EC2 Instance Connect-Paket ordnungsgemäß installiert und konfiguriert ist.

- Prüfen Sie: SSHConfig FromOs

  Führt ein Bash-Skript auf der Amazon EC2 EC2-Linux-Zielinstanz aus, um zu überprüfen, ob der konfigurierte SSH-Port dem Eingabeparameter `entspricht. SSHPort `

- CheckMetadataHTTPEndpointIsEnabled:

  Prüft, ob der HTTP-Endpunkt des Instanz-Metadatendienstes aktiviert ist.

- Überprüfen Sie EICNetwork den Zugriff:

Prüft, ob die Netzwerkkonfiguration (Sicherheitsgruppen, Netzwerk-ACL und Routing-Tabellenregeln) eine Verbindung zur Instance über Amazon EC2 Instance Connect zulässt.

- Prüfen Sie IAMRoleOrUserPermissions:

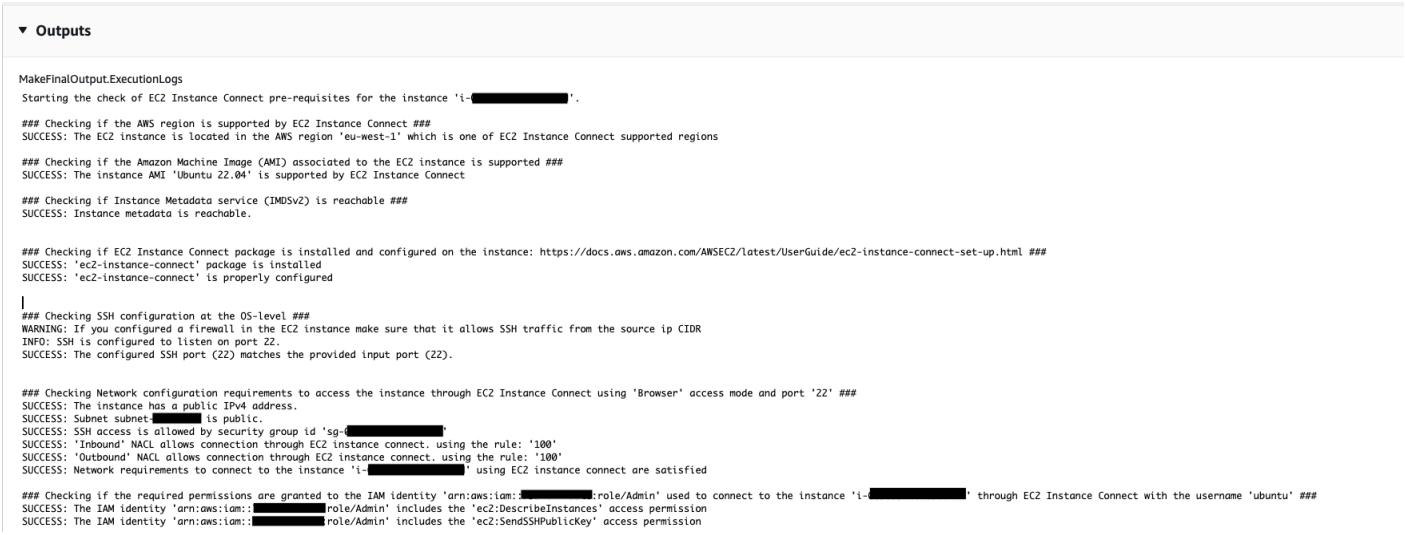
  Überprüft, ob die IAM-Rolle oder der Benutzer, der zur Nutzung von Amazon EC2 Instance Connect verwendet wird, über den angegebenen Benutzernamen Zugriff auf Push-Keys für die Amazon EC2 EC2-Instance hat.

- MakeFinalOutput:

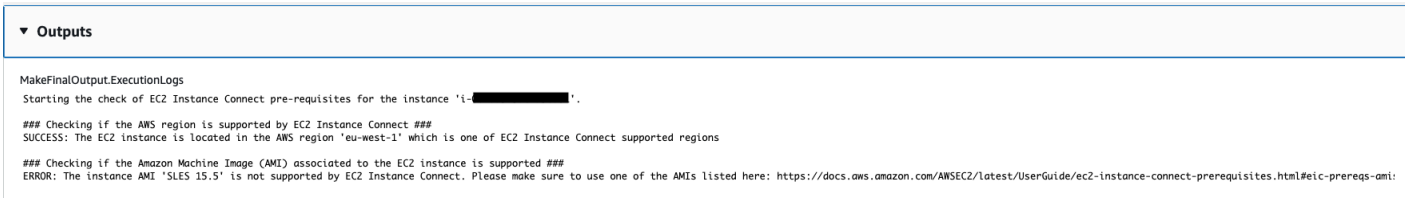
  Konsolidiert die Ergebnisse aller vorherigen Schritte.

7. Wenn Sie den Vorgang abgeschlossen haben, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   Ausführung, bei der die Zielinstanz alle erforderlichen Voraussetzungen erfüllt:



   Ausführung, bei der das AMI der Zielinstanz nicht unterstützt wird:



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage Support Automation Workflows

AWS Servicedokumentation

- Wie behebe ich Probleme beim Herstellen einer Verbindung zu meiner Amazon EC2-Instance mithilfe von Amazon EC2 Instance Connect?

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

Beschreibung

`AWSSupport-TroubleshootLinuxMGNDRSAgentLogs`Automation Runbook wird verwendet, um häufige Fehler bei der Installation der Replikationsagenten AWS Application Migration Service (AWS MGN) und AWS Elastic Disaster Recovery (AWS DRS) auf Linux-Servern zu erkennen, um Quellserver in die Cloud zu migrieren. AWS

Wie funktioniert es?

Das Runbook verwendet `AWSSupport-TroubleshootLinuxMGNDRSAgentLogs` den Amazon Simple Storage Service (Amazon S3) -Pfad, in den das AWS MGN- oder AWS DRS-Installationsprotokoll als `aws_replication_agent_installer.log` Parameter hochgeladen wird. Anschließend führt es die folgenden Aufgaben aus:

- Validierung: Überprüft, ob die bereitgestellte Protokolldatei gültig ist und ob sie mindestens eine Agenteninstallation enthält.
- Analysieren: Analysiert die letzte Agenteninstallation in der Protokolldatei gründlich auf bekannte AWS MGN- oder AWS DRS-Fehler.
- Fehlererkennung und -behebung: Auf der Grundlage der Analyse werden alle Fehler oder Probleme während der Agenteninstallation erkannt und aufgelistet. Für jeden erkannten Fehler bietet das Runbook detaillierte Schritte zur Behebung oder Minderung des Problems.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `s3:GetObject`
- `s3:ListBucket`

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootLinuxMGNDRSAgentLogs`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

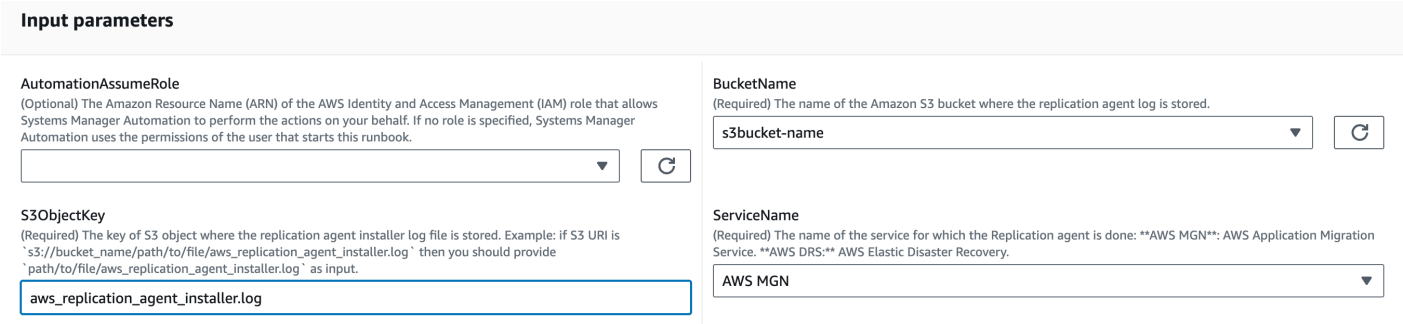
     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - BucketName (Erforderlich):

     Der Name des Amazon S3 S3-Buckets, in dem das Protokoll des Replikationsagenten gespeichert ist.
   - S3 ObjectKey (erforderlich):

Der Schlüssel des Amazon S3 S3-Objekts, in dem die Protokolldatei des Replikationsagenten gespeichert ist. Beispiel: Wenn der Amazon S3 S3-URI lautets3://bucket_name/path/to/file/aws_replication_agent_installer.log, sollten Sie eingebenpath/to/file/aws_replication_agent_installer.log.

- ServiceName (Erforderlich):

  Der Name des Dienstes, für den der Replikationsagent installiert ist. Zulässige Werte: AWS MGN oder AWS DRS



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - **ValidateInput**

     Stellt sicher, dass die Protokolldatei des Replikationsagenten gültig und zugänglich ist, indem der angegebene Amazon S3 S3-Bucket-Name und der Pfad zum Objekt verwendet werden, und gibt dann die Byte-Nummer der letzten Agenteninstallation zurück.

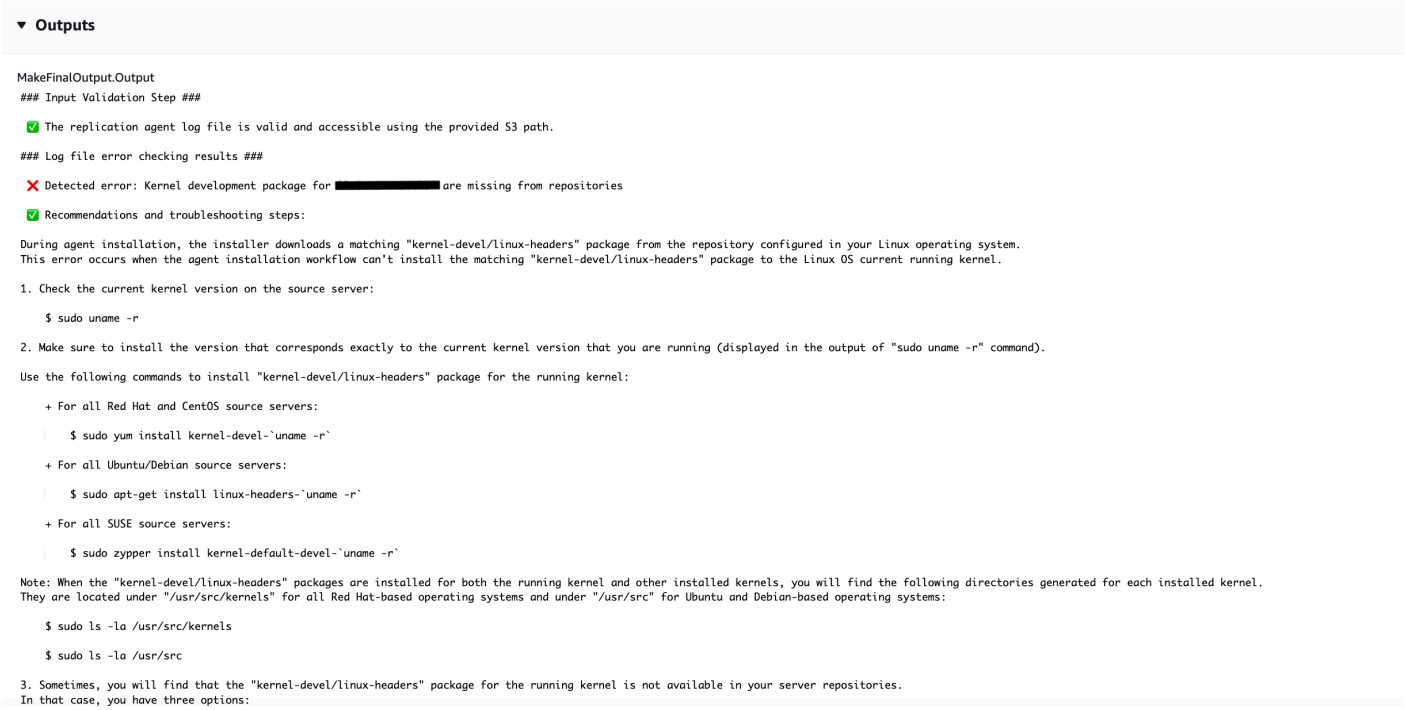
   - **CheckReplicationAgentLogErrors**

     Liest die Protokolldatei des Replikationsagenten ab dem letzten Installationsbyte und sucht nach bekannten AWS MGN- oder AWS DRS-Fehlern.

   - **MakeFinalOutput**

     Erstellt die Ausgabe der vorherigen Prüfungen, einschließlich Informationen zu den gefundenen Fehlern und Empfehlungen zur Problembehandlung.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:



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:
```

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWSSupport-TroubleshootRDP

Beschreibung

Das `AWSSupport-TroubleshootRDP` Runbook ermöglicht es dem Benutzer, allgemeine Einstellungen auf der Zielinstanz zu überprüfen oder zu ändern, die sich auf RDP-Verbindungen (Remote Desktop Protocol) auswirken können, z. B. den RDP-Port, die Network Layer Authentication (NLA) und die Windows-Firewall-Profile. Optional können Sie Änderungen offline anwenden, indem Sie die Instance anhalten und starten, wenn die Offline-Wiederherstellung von Benutzer ausdrücklich zugelassen wurde. Standardmäßig liest das Runbook die Werte der Einstellungen und gibt sie aus.

> **Important**
>
> Änderungen an den RDP-Einstellungen, dem RDP-Dienst und den Windows-Firewallprofilen sollten vor der Verwendung dieses Runbooks sorgfältig geprüft werden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- Aktion

  Typ: Zeichenfolge

  Gültige Werte: CheckAll | FixAll | Benutzerdefiniert

  Standard: Custom

  Beschreibung: (Optional) [Benutzerdefiniert] Verwenden Sie die Werte aus Firewall RDPServiceStartupType, RDPService RDPPort Action, NLASetting Action und RemoteConnections zur Verwaltung der Einstellungen. [CheckAll] Lesen Sie die Werte der Einstellungen, ohne sie zu ändern. [FixAll] Stellen Sie die RDP-Standardeinstellungen wieder her und deaktivieren Sie die Windows-Firewall.
- AllowOffline

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

Beschreibung: (Optional) Fix only - Auf „True“ setzen, um eine Offline-RDP-Wiederherstellung zu erlauben, wenn die Online-Fehlerbehebung fehlschlägt, oder wenn die angegebene Instance keine verwaltete Instance ist. Hinweis: Für die Offline-Wiederherstellung hält SSM Automation die Instance an und erstellt ein AMI, bevor irgendwelche Operationen versucht werden.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Firewall

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Deaktivieren

  Standard: Check

  Beschreibung: (Optional) Prüfen oder deaktivieren der Windows-Firewall (alle Profile).

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instance, deren RDP-Einstellungen einer Fehlerbehebung unterzogen werden sollen.

- NLASettingAktion

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Deaktivieren

  Standard: Check

  Beschreibung: (Optional) Aktivieren oder Deaktivieren von Network Layer Authentication (NLA).

- RDPPortAktion

  Typ: Zeichenfolge

Gültige Werte: Prüfen | Ändern

Standard: Check

Beschreibung: (Optional) Prüfen des aktuell für RDP-Verbindungen verwendeten Ports oder Ändern des Ports zurück zu 3389 und Neustart des Service.

- RDPServiceAktion

  Typ: Zeichenfolge

  Gültige Werte: Check | Start | Restart | Force-Restart

  Standard: Check

  Beschreibung: (Optional) Überprüfen Sie den RDP-Dienst, starten Sie ihn neu oder erzwingen Sie einen Neustart (). TermService

- RDPServiceStartupType

  Typ: Zeichenfolge

  Gültige Werte: Check | Auto

  Standard: Check

  Beschreibung: (Optional) Prüfen oder Einstellen des RDP-Service auf den automatischen Start beim Hochfahren von Windows.

- RemoteConnections

  Typ: Zeichenfolge

  Gültige Werte: Prüfen | Aktivieren

  Standard: Check

  Beschreibung: (Optional) Eine Aktion, die für die TSConnections Einstellung FDeny ausgeführt werden muss: Prüfen, Aktivieren.

- S3 BucketName

  Typ: Zeichenfolge

Beschreibung: (Optional) Nur Offline - Name des S3-Buckets in Ihrem Konto, in den Sie die Protokolle zur Fehlerbehebung hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie keine unnötigen Lese-/Schreibberechtigungen für Parteien gewährt, die keinen Zugriff auf die gesammelten Protokolle benötigen.

- SubnetId

  Typ: Zeichenfolge

  Standard: SelectedInstanceSubnet

  Beschreibung: (Optional) Nur offline — Die Subnetz-ID für die EC2 Rescue-Instanz, die zur Durchführung der Offline-Fehlerbehebung verwendet wurde. Wenn keine Subnetz-ID angegeben ist, erstellt AWS Systems Manager Automation eine neue VPC. WICHTIG: Das Subnetz muss sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass die EC2 Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, der die von SSMManagedInstanceCoreAmazon verwaltete Richtlinie beigefügt ist. Für die Online-Behebung muss der Benutzer mindestens über ssm:, ssm: und ssm: verfügenDescribeInstanceInformation, SendCommand um die Automatisierung auszuführen StartAutomationExecution und den Befehl an die Instance zu senden, sowie über ssm:, um die Automatisierungsausgabe lesen GetAutomationExecution zu können. Für die Offline-Korrektur muss der Benutzer mindestens über ssm:, ssm:DescribeInstanceInformation, ec2: plus ssm: verfügenStartAutomationExecution, um die DescribeInstances Automatisierungsausgabe lesen zu können. GetAutomationExecution `AWSSupport-TroubleshootRDP`AufrufeAWS`Support-ExecuteEC2Rescue`, um die Offline-Korrektur durchzuführen. Bitte überprüfen Sie die Berechtigungen für, `AWSSupport-ExecuteEC2Rescue` um sicherzustellen, dass Sie die Automatisierung erfolgreich ausführen können.

Dokumentschritte

1. `aws:assertAwsResourceProperty`- Prüfen Sie, ob es sich bei der Instanz um eine handelt Windows Server Instance

2. `aws:assertAwsResourceProperty`- Prüfen Sie, ob es sich bei der Instanz um eine verwaltete Instanz handelt
3. (Online-Fehlerbehebung) Wenn die Instance eine verwaltete Instance ist, dann:
   a. `aws:assertAwsResourceProperty`- Überprüfen Sie den angegebenen Aktionswert
   b. (Online-Prüfung) Wenn die Aktion = ist CheckAll, dann:

      `aws:runPowerShellScript`- Führt das PowerShell Skript aus, um den Status der Windows-Firewall-Profile abzurufen.

      `aws:executeAutomation`- Ruft `AWSSupport-ManageWindowsService` auf, um den RDP-Dienststatus abzurufen.

      `aws:executeAutomation`- Ruft `AWSSupport-ManageRDPSettings` auf, um die RDP-Einstellungen abzurufen.
   c. (Online-Fix) Wenn die Aktion = FixAll, dann:

      `aws:runPowerShellScript`- Führt das PowerShell Skript aus, um alle Windows-Firewallprofile zu deaktivieren.

      `aws:executeAutomation`- Ruft `AWSSupport-ManageWindowsService` auf, um den RDP-Dienst zu starten.

      `aws:executeAutomation`- Aufrufe `AWSSupport-ManageRDPSettings` zum Aktivieren von Remoteverbindungen und zum Deaktivieren von NLA.
   d. (Online-Management) Wenn Action = Custom, dann:

      `aws:runPowerShellScript`- Führt das PowerShell Skript zur Verwaltung der Windows-Firewallprofile aus.

      `aws:executeAutomation`- Aufrufe `AWSSupport-ManageWindowsService` zur Verwaltung des RDP-Dienstes.

      `aws:executeAutomation`- Aufrufe `AWSSupport-ManageRDPSettings` zur Verwaltung der RDP-Einstellungen.
4. (Offline-Wiederherstellung) Wenn die Instance keine verwaltete Instance ist:
   a. `aws:assertAwsResourceProperty`- Assert AllowOffline = wahr
   b. `aws:assertAwsResourceProperty`- Aktion bestätigen = FixAll
   c. `aws:assertAwsResourceProperty`- Bestätigt den Wert von SubnetId

(Verwenden Sie das Subnetz der bereitgestellten Instanz) Es ist SubnetId SELECTED_INSTANCE_SUBNET

`aws:executeAwsApi`- Ruft das Subnetz der aktuellen Instanz ab.

`aws:executeAutomation`- Wird `AWSSupport-ExecuteEC2Rescue` mit dem Subnetz der angegebenen Instanz ausgeführt.

d. (Verwenden Sie das bereitgestellte benutzerdefinierte Subnetz) Wenn SubnetId nicht SELECTED_INSTANCE_SUBNET

`aws:executeAutomation`- SubnetId Mit `AWSSupport-ExecuteEC2Rescue` dem angegebenen Wert ausführen.

Ausgaben

manageFirewallProfiles. Ausgabe

Einstellungen verwalten.Ausgabe RDPService

RDPSettings.Output verwalten

checkFirewallProfiles. Ausgabe

überprüfen Sie Einstellungen.Ausgabe RDPService

RDPSettingsüberprüfe .Output

disableFirewallProfiles. Ausgabe

Standardeinstellungen RDPService wiederherstellen. Ausgabe

Standard wiederherstellenRDPSettings. Ausgabe

RDPOffline.Output beheben

.Output beheben RDPOffline WithSubnetId

AWSSupport-TroubleshootSSH

Beschreibung

Das `AWSSupport-TroubleshootSSH` Runbook installiert das Amazon EC2 Rescue-Tool für Linux und verwendet dann das EC2 Rescue-Tool, um häufig auftretende Probleme zu überprüfen oder zu beheben, die eine Remoteverbindung zum Linux-Computer über SSH verhindern. Optional können Sie Änderungen offline anwenden, indem Sie die Instance anhalten und starten, wenn die Offline-Wiederherstellung von Benutzer ausdrücklich zugelassen wurde. Standardmäßig arbeitet das Runbook im schreibgeschützten Modus.

Führen Sie diese Automatisierung aus (Konsole)

Informationen zur Arbeit mit dem `AWSSupport-TroubleshootSSH` Runbook finden Sie in diesem Thema `AWSSupport-TroubleshootSSH` zur Fehlerbehebung von AWS Premium Support.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- Aktion

  Typ: Zeichenfolge

  Gültige Werte: CheckAll | FixAll

  Standard: CheckAll

  Beschreibung: (Erforderlich) Angabe, ob Probleme nur geprüft werden sollen, ohne sie zu beheben, oder ob nach der Prüfung alle erkannten Probleme automatisch behoben werden sollen.

- AllowOffline

  Typ: Zeichenfolge

  Zulässige Werte: true | false

Standard: false

Beschreibung: (Optional) Fix only - Auf „True“ setzen, um eine Offline-SSH-Wiederherstellung zu erlauben, wenn die Online-Fehlerbehebung fehlschlägt, oder wenn die angegebene Instance keine verwaltete Instance ist. Hinweis: Für die Offline-Wiederherstellung hält SSM Automation die Instance an und erstellt ein AMI, bevor irgendwelche Operationen versucht werden.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID Ihrer EC2 Instanz für Linux.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Nur Offline - Name des S3-Buckets in Ihrem Konto, in den Sie die Protokolle zur Fehlerbehebung hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie keine unnötigen Lese-/Schreibberechtigungen für Parteien gewährt, die keinen Zugriff auf die gesammelten Protokolle benötigen.

- SubnetId

  Typ: Zeichenfolge

  Standard: SelectedInstanceSubnet

  Beschreibung: (Optional) Nur offline — Die Subnetz-ID für die EC2 Rescue-Instanz, die zur Durchführung der Offline-Fehlerbehebung verwendet wurde. Wenn keine Subnetz-ID angegeben ist, erstellt AWS Systems Manager Automation eine neue VPC.

> **Important**
>
> Das Subnetz muss sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass die EC2 Instance, die den Befehl empfängt, über eine IAM-Rolle verfügt, der die von SSMManagedInstanceCoreAmazon verwaltete Richtlinie beigefügt ist. Für die Online-Problembehebung muss der Benutzer mindestens über ssm:, ssm: und ssm: verfügenDescribeInstanceInformation, SendCommand um die Automatisierung auszuführen StartAutomationExecution und den Befehl an die Instance zu senden, sowie über ssm:, um die Automatisierungsausgabe GetAutomationExecution lesen zu können. Für die Offline-Korrektur muss der Benutzer mindestens über ssm:, ssm:DescribeInstanceInformation, ec2: plus ssm: verfügenStartAutomationExecution, um die DescribeInstances Automatisierungsausgabe lesen zu können. GetAutomationExecution `AWSSupport-TroubleshootSSH`AufrufeAWS`Support-ExecuteEC2Rescue`, um die Offline-Korrektur durchzuführen. Bitte überprüfen Sie die Berechtigungen für, `AWSSupport-ExecuteEC2Rescue` um sicherzustellen, dass Sie die Automatisierung erfolgreich ausführen können.

Dokumentschritte

1. `aws:assertAwsResourceProperty`— Prüfen Sie, ob es sich bei der Instanz um eine verwaltete Instanz handelt
   a. (Online-Wiederherstellung) Wenn die Instance verwaltete Instance ist:
      i. `aws:configurePackage`- Installieren Sie EC2 Rescue für Linux über`AWS-ConfigureAWSPackage`.
      ii. `aws:runCommand`- Führen Sie das Bash-Skript aus, um EC2 Rescue für Linux auszuführen.
   b. (Offline-Wiederherstellung) Wenn die Instance keine verwaltete Instance ist:
      i. `aws:assertAwsResourceProperty`- Assert AllowOffline = wahr
      ii. `aws:assertAwsResourceProperty`- Aktion bestätigen = FixAll
      iii. `aws:assertAwsResourceProperty`- Bestätigt den Wert von SubnetId

iv. (Verwenden Sie das Subnetz der bereitgestellten Instanz) Wenn SubnetId SelectedInstanceSubnet wir `aws:executeAutomation` `AWSSupport-ExecuteEC2Rescue` mit dem Subnetz der bereitgestellten Instanz arbeiten sollen.

v. (Verwenden Sie das bereitgestellte benutzerdefinierte Subnetz) Wenn nicht für die Ausführung `AWSSupport-ExecuteEC2Rescue` mit dem angegebenen `aws:executeAutomation` Wert SelectedInstanceSubnet verwendet SubnetId wird. SubnetId

Ausgaben

troubleshootSSH.Output

Fehler behebenSSHOffline. Output

Problembehandlung .Output SSHOffline WithSubnetId

AWSSupport-TroubleshootSUSERegistration

Beschreibung

Das `AWSSupport-TroubleshootSUSERegistration` Runbook hilft Ihnen zu erkennen, warum Sie eine Amazon Elastic Compute Cloud (Amazon EC2) registrieren SUSE Linux Enterprise Server Eine Instanz mit SUSE Update Infrastructure ist fehlgeschlagen. Die Automatisierungsausgabe enthält Schritte zur Lösung des Problems oder hilft Ihnen bei der Behebung des Problems. Wenn die Instanz während der Automatisierung alle Prüfungen besteht, wird die Instanz bei SUSE Update Infrastructure registriert.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der EC2 Amazon-Instance, für die Sie eine Fehlerbehebung durchführen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:ListCommands`

Dokumentschritte

- `aws:assertAwsResourceProperty`- Prüft, ob die EC2 Amazon-Instance von verwaltet wird AWS Systems Manager.
- `aws:runCommand`- Prüft, ob die EC2 Amazon-Instance-Plattform SLES.
- `aws:runCommand`— Prüft, ob die `cloud-regionsrv-client` Paketversion größer oder gleich der erforderlichen Version 9.0.10 ist.
- `aws:runCommand`- Überprüft, ob der symbolische Link für das Basisprodukt defekt ist, und repariert den Link, falls er defekt ist.

- `aws:runCommand`- Prüft, ob die Hosts-Datei (`/etc/hosts`) Datensätze für enthält`smt-ec2-suscloud.net`. Die Automatisierung entfernt alle doppelten Einträge.
- `aws:runCommand`- Prüft, ob der `curl` Befehl installiert ist.
- `aws:runCommand`— Prüft, ob die EC2 Amazon-Instance auf die IMDS-Adresse 169.254.169.254 zugreifen kann.
- `aws:runCommand`- Prüft, ob die EC2 Amazon-Instance einen Rechnungscode oder einen AWS Marketplace Produktcode hat.
- `aws:runCommand`- Prüft, ob die EC2 Amazon-Instance mindestens einen regionalen Server über HTTPS erreichen kann.
- `aws:runCommand`- Überprüft, ob die EC2 Amazon-Instance die SMT-Server (Subscription Management Tool) über HTTP erreichen kann.
- `aws:runCommand`- Überprüft, ob die EC2 Amazon-Instance die SMT-Server (Subscription Management Tool) über HTTPS erreichen kann.
- `aws:runCommand`- Prüft, ob die EC2 Amazon-Instance die `smt-ec2.susecloud.net` Adresse über HTTPS erreichen kann.
- `aws:runCommand`- Registriert die EC2 Amazon-Instance bei SUSE Update Infrastructure.
- `aws:executeScript`- Sammelt die Ergebnisse aller vorherigen Schritte und gibt sie aus.

`AWSSupport-TroubleshootWindowsPerformance`

Beschreibung

Das Runbook `AWSSupport-TroubleshootWindowsPerformance` hilft bei der Behebung laufender Leistungsprobleme auf der Windows-Instance Amazon Elastic Compute Cloud (Amazon EC2). Das Runbook erfasst Protokolle von der Ziel-Instance und analysiert CPU-, Arbeitsspeicher-, Festplatten- und Netzwerkleistungskennzahlen. Optional kann die Automatisierung einen Prozess-Dump erfassen, mit dessen Hilfe Sie die mögliche Ursache für Leistungseinbußen ermitteln können. Bei der Automatisierung werden auch die Ereignis- und Systemprotokolle mithilfe des neuesten `EC2Rescue`Tools erfasst, sofern Sie die Installation durch dieses Runbook zulassen.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Überprüft die Amazon EC2 EC2-Instance auf Voraussetzungen.
- Generiert Leistungsprotokolle auf der Root-Festplatte der Amazon EC2 EC2-Windows-Instance

- Speichert die erfassten Protokolle in einem Ordner `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Wenn ein Amazon Simple Storage Service (Amazon S3) -Bucket bereitgestellt wird und die Automation-Annahme-Rolle über die erforderlichen Berechtigungen verfügt, werden die erfassten Protokolle in den Amazon S3 S3-Bucket hochgeladen.
- Installiert das neueste `EC2Rescue` Tool auf der Amazon EC2 EC2-Windows-Instance, um Ereignisse und Systemprotokolle zu erfassen, falls Sie es installieren möchten. Es analysiert jedoch nicht den Prozess-Dump und die von erfassten Protokolle. `EC2Rescue`

Important

- Um dieses Runbook auszuführen, muss die Amazon EC2 EC2-Windows-Instance von verwaltet werden. AWS Systems Manager Weitere Informationen finden Sie unter Warum wird meine Amazon EC2 EC2-Instance nicht als verwalteter Knoten angezeigt?
- Um dieses Runbook auszuführen, muss die Amazon EC2 EC2-Windows-Instance auf den Versionen Windows 8.1/Windows Server 2012 R2 (6.3) oder neuer mit PowerShell 4.0 oder höher ausgeführt werden. Weitere Informationen finden Sie unter Windows-Betriebssystemversion.
- Für die Generierung von Leistungsprotokollen sind mindestens 10 GB freier Speicherplatz auf dem Root-Gerät erforderlich. Wenn die Stammfestplatte größer als 100 GB ist, muss der freie Speicherplatz mehr als 10% der Festplattengröße betragen. Wenn Sie einen Prozess während der Ausführung sichern, muss der freie Speicherplatz größer als 10 GB sein, zuzüglich der gesamten Speichergröße, die der Prozess beansprucht, wenn der Prozess mehr als 10 GB Speicher verbraucht.
- Die auf dem Root-Gerät generierten Protokolle werden nicht automatisch gelöscht.
- Das Runbook deinstalliert das `EC2Rescue` Tool nicht. Weitere Informationen finden Sie unter Verwenden `EC2Rescue` für Windows Server.
- Es hat sich bewährt, diese Automatisierung bei Leistungseinbußen auszuführen. Sie können sie auch regelmäßig mithilfe einer AWS Systems Manager State Manager-Zuordnung oder durch die Planung von AWS Systems Manager Wartungsfenstern ausführen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

(Optional) Die dem Instance-Profil zugeordnete IAM-Rolle oder der auf der Instance konfigurierte IAM-Benutzer erfordert die folgenden Aktionen, um Logs in den für den Parameter angegebenen Amazon S3 S3-Bucket hochzuladen: *`LogUploadBucketName`*

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootWindowsPerformance`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - InstanceId (Erforderlich):

     Die ID der Amazon EC2 EC2-Windows-Zielinstanz, auf der Sie die Automatisierung ausführen möchten. Die Instanz muss von Systems Manager verwaltet werden, um die Automatisierung ausführen zu können.
   - CaptureProcessDump (Optional):

     Der Typ des zu erfassenden Prozess-Dumps. Die Automatisierung kann einen Prozess-Dump für den Prozess erfassen, der zu Beginn der Automatisierung möglicherweise die Leistung beeinträchtigt. Das Instance-Root-Volume benötigt mindestens 10 GB freien Speicherplatz (mehr als 10% der Festplattengröße, wenn das Root-Volume größer als 100 GB ist, und 10 GB zuzüglich der gesamten vom Prozess verbrauchten Speichergröße, wenn der Prozess mehr als 10 GB Speicher verbraucht).
   - LogCaptureDuration (Optional):

     Die Anzahl der Minuten zwischen `1` und`15`, für die diese Automatisierung Protokolle erfasst, solange das Problem noch besteht. Der Standardwert ist `5`.
   - LogUploadBucketName (Fakultativ):

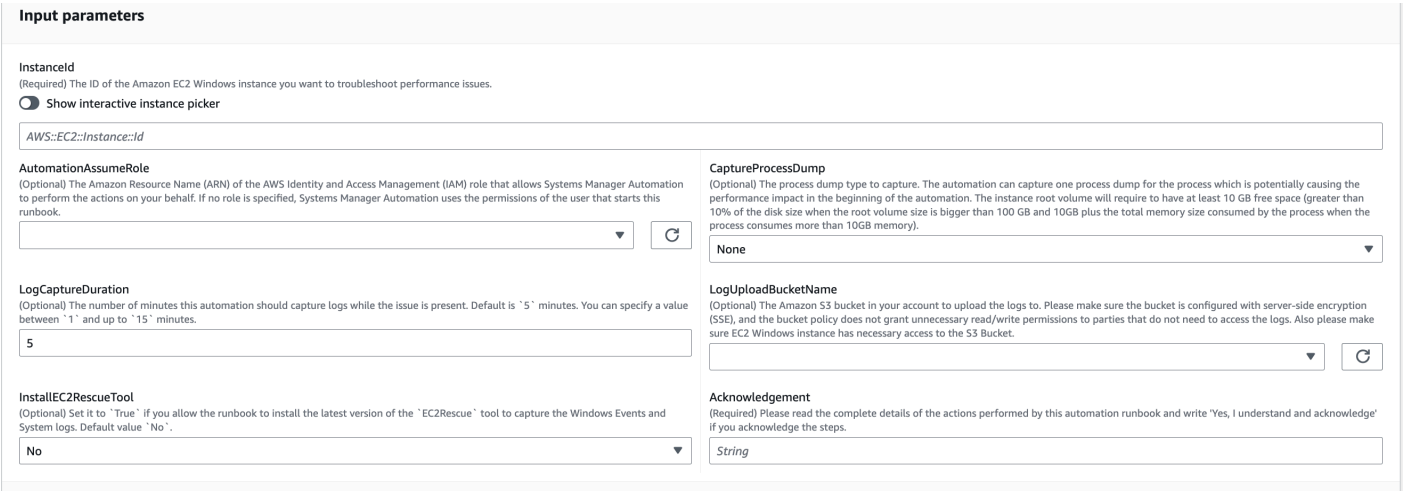
Der Amazon S3 S3-Bucket in Ihrem Konto, in den Sie die Protokolle hochladen möchten. Der Bucket muss mit serverseitiger Verschlüsselung (SSE) konfiguriert sein, und die Bucket-Richtlinie darf Parteien, die keinen Zugriff auf die erfassten Protokolle benötigen, keine unnötigen read/write Berechtigungen gewähren. Die Amazon EC2 EC2-Windows-Instance muss Zugriff auf den Amazon S3 S3-Bucket haben.

- Installation EC2 RescueTool (optional):

  Stellen `Yes` Sie diese Option ein, damit das Runbook die neueste Version des `EC2Rescue` Tools zur Erfassung der Windows-Ereignisse und -Systemprotokolle installieren kann. Der Standardwert ist `No`.

- Bestätigung (erforderlich):

  Lesen Sie die vollständigen Details der Aktionen, die von diesem Automatisierungs-Runbook ausgeführt wurden, und geben Sie Folgendes ein, wenn Sie damit einverstanden sind. `Yes, I understand and acknowledge`



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - **`CheckConcurrency:`**

     Stellt sicher, dass dieses Runbook nur einmal ausgeführt wird, das auf die Instanz abzielt. Wenn das Runbook eine weitere Ausführung findet, die auf dieselbe Instance abzielt, gibt es einen Fehler zurück und wird beendet.

   - **`AssertInstanceIsWindows:`**

Bestätigt, dass die Amazon EC2 EC2-Instance unter einem Windows-Betriebssystem läuft. Andernfalls endet die Automatisierung.

- **`AssertInstanceIsManagedInstance:`**

  Bestätigt, dass die Amazon EC2 EC2-Instance von verwaltet wird. AWS Systems Manager Andernfalls endet die Automatisierung.

- **`VerifyPrerequisites:`**

  Überprüft die PowerShell Version auf dem Instanz-Betriebssystem und stellt sicher, dass die Instanz über Systems Manager verbunden werden kann, um PowerShell Befehle auszuführen. Diese Automatisierung unterstützt die Ausführung PowerShell 4.0 und höher auf den Versionen Windows 8.1/Server 2012 R2 (6.3) oder neuer. Wenn die Version älter ist, schlägt die Automatisierung fehl. Wenn Sie sich dafür entscheiden, Protokolle in den Amazon S3 S3-Bucket hochzuladen, überprüft diese Automatisierung, ob das PowerShell Modul AWS Tools for verfügbar ist. Wenn nicht, endet die Automatisierung.

- **`BranchOnProcessDump:`**

  Verzweigt, je nachdem, ob Sie es so eingestellt haben, dass es den Dump von Prozessen erfasst, die sich auf die Leistung ausgewirkt haben.

- **`CaptureProcessDump:`**

  Prüft, ob die Instanz über genügend Speicherplatz verfügt, um diese Automatisierung auszuführen (wenn Sie „Höchste CPU/Arbeitsspeicher“ wählen).

- **`CapturePerformanceLogs:`**

  Überprüft erneut den Festplattenspeicher und führt das PowerShell Skript auf der Instanz aus, um Leistungsindikatoren zu erstellen und die Protokollierung von Systemmonitor und Windows Performance Recorder zu starten. Das Skript wird beendet, wenn der angegebene Wert erreicht `LogCaptureDuration` ist.

- **`SummarizePerformanceLogs:`**

  Fasst den im vorherigen Schritt generierten XML-Bericht zusammen`CapturePerformanceLogs`, um den verantwortlichen Prozess zu finden, der am meisten WorkingSet 64 (Arbeitsspeicher) und% Prozessorzeit (CPU) verbraucht und in der Ausgabe der Automatisierung angezeigt wird. Es generiert ähnliche Informationen zur Verwendung von LogicalDisk Netzwerkschnittstelle, Speicher TCPv4, IPv4, und UDPv4 und speichert sie `analysis_output.log` im Ausgabeordner.

- **BranchOnInstallEC2Rescue:**

  Verzweigt, wenn Sie es so einstellen, dass das neueste EC2Rescue Tool in der Amazon EC2 EC2-Instance installiert wird.

- **InstallEC2RescueTool:**

  Installiert das EC2Rescue Tool im Instance-Betriebssystem zur Erfassung von EC2Rescue Protokollen mithilfe vonAWS-ConfigureAWSPackage.

- **RunEC2RescueTool:**

  Führt das EC2Rescue Tool im Betriebssystem der Instanz aus, um alle benötigten Protokolle zu erfassen. EC2Rescueerfasst nur die erforderlichen Protokolle, um Speicherplatz zu sparen.

- **BranchOnIfS3BucketProvided:**

  Verzweigt auf der Grundlage von Benutzereingaben vonLogUploadBucketName, um festzustellen, ob ein Bucket-Name zum Hochladen von Logs verfügbar ist.

- **GetS3BucketPublicStatus:**

  Ermittelt, ob ein Amazon S3 S3-Bucket bereitgestellt wird, und wenn ja, bestätigt es, dass der Amazon S3 S3-Bucket nicht öffentlich und mit SSE konfiguriert ist.

- **UploadLogResult:**

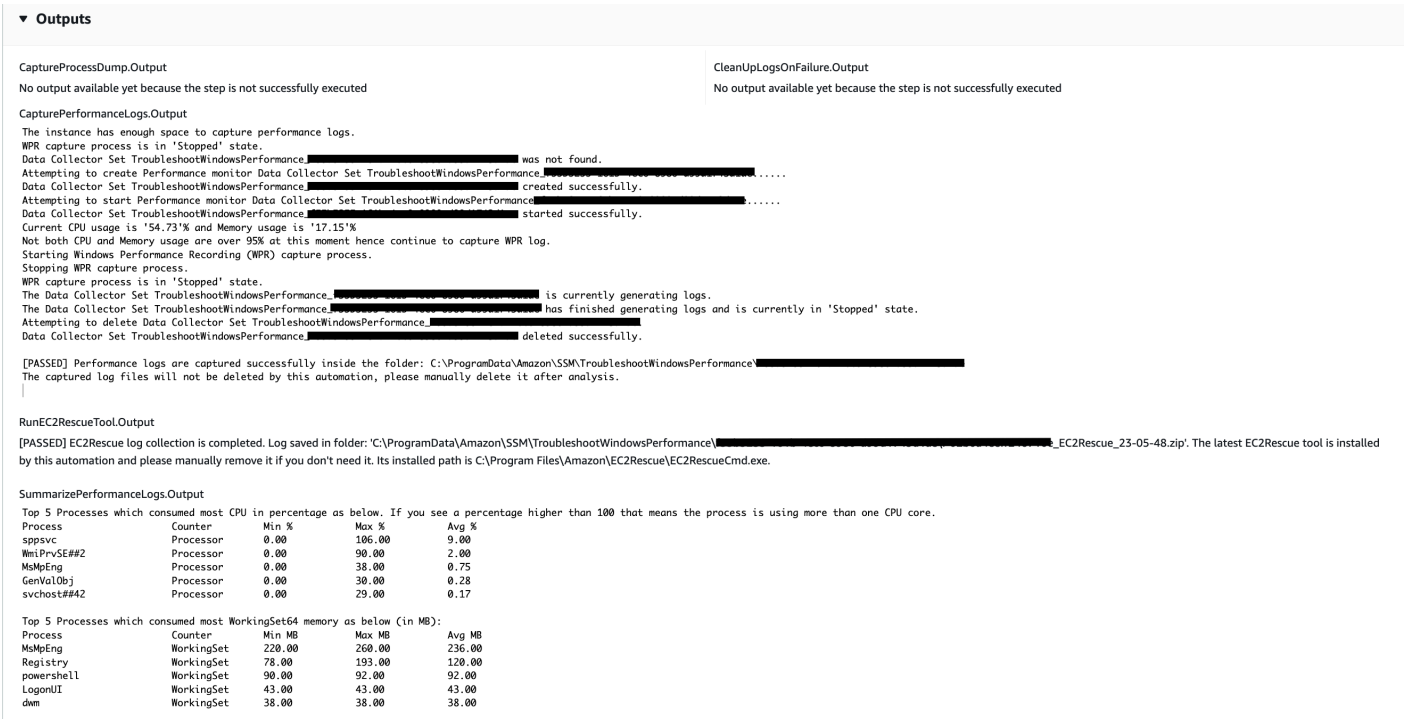
  Lädt die Protokolle in den bereitgestellten Amazon S3 S3-Bucket hoch. Wenn die PowerShell Version 5.0 oder höher ist, werden die Protokolle in ein ZIP-Archiv komprimiert und hochgeladen. Es löscht die ZIP-Datei, nachdem der Upload abgeschlossen ist. Wenn die PowerShell Version unter 5.0 liegt, werden die Dateien direkt in einen Ordner hochgeladen.

- **CleanUpLogsOnFailure:**

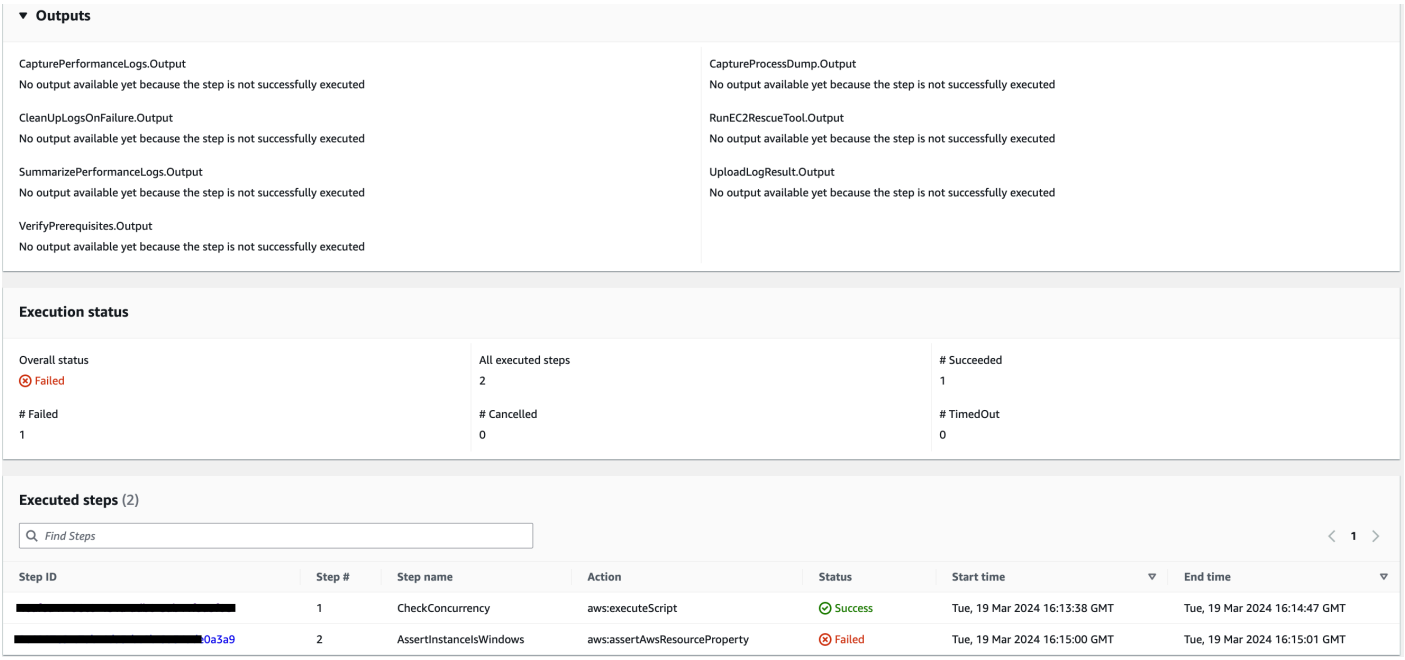
  Löscht alle durch den CapturePerformanceLogs Schritt generierten Protokolle, wenn er fehlschlägt. Der CleanUpLogsOnFailure Schritt schlägt möglicherweise fehl oder es kommt zu einem Timeout, wenn der SSM-Agent nicht ordnungsgemäß funktioniert oder das Windows-System nicht reagiert.

7. Wenn Sie den Vorgang abgeschlossen haben, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

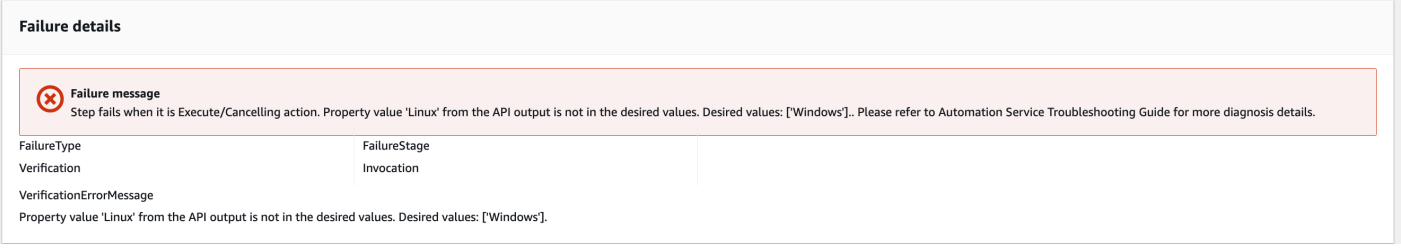
   Ausführung, bei der die Zielinstanz alle erforderlichen Voraussetzungen erfüllt.



Ausführung, bei der sich die Zielinstanz auf der Linux-Plattform befindet und die Ausführung fehlgeschlagen ist. Sie würden die Schritt-ID auswählen, um die Fehlerdetails zu sehen.



Die Fehlerdetails des Schritts`AssertInstanceIsWindows`.



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

`AWSSupport-TroubleshootWindowsUpdate`

Beschreibung

Das `AWSSupport-TroubleshootWindowsUpdate` Runbook wird verwendet, um Probleme zu identifizieren, bei denen die Windows-Updates für Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instances fehlschlagen könnten.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Prüft, ob die Amazon EC2 EC2-Zielinstanz von AWS Systems Manager verwaltet wird.
- Überprüft, ob die Versionen AWS Systems Manager Agent (SSM Agent) und Windows Server für Systems Manager Manager-Patchvorgänge unterstützt werden.
- Prüft den für Windows-Updates empfohlenen verfügbaren Festplattenspeicher und ob ein Neustart aussteht. Ein ausstehender Neustart weist normalerweise darauf hin, dass Updates ausstehen, und ein Neustart ist erforderlich, bevor weitere Updates durchgeführt werden.
- Konfiguriert die Proxyeinstellungen auf Betriebssystemebene, was bei der Behebung von Verbindungsproblemen helfen kann.

- Führt einen Endpunkt-Konnektivitätstest von Amazon Simple Storage Service (Amazon S3) durch und ruft den `GetDeployablePatchSnapshotForInstance`API-Vorgang auf, um den aktuellen Snapshot für die Patch-Baseline abzurufen, die der verwaltete Knoten verwendet.
- Wenn die Verbindung fehlschlägt, bietet es die Möglichkeit, das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook auszuführen, um die Konnektivität der Instance mit Amazon S3 S3-Endpunkten zu analysieren.
- Validiert die Windows-Update-Konfiguration und testet Windows Server Update Services (WSUS) (falls zutreffend).

⚠ Important

- Active Directory-Domänencontroller werden nicht unterstützt.
- Windows Server Version 2008 R2 oder frühere Versionen werden nicht unterstützt.
- SSM Agent 1.2.371 oder frühere Versionen werden nicht unterstützt.
- Das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook wird verwendet `VPC Reachability Analyzer`, um die Netzwerkkonnektivität zwischen einer Quelle und einem Dienstendpunkt zu analysieren. Ihnen wird pro Analyselauf zwischen einer Quelle und einem Ziel berechnet. Weitere Informationen finden Sie unter Amazon VPC-Preise.
- Das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook ist nicht in allen Regionen verfügbar, in denen Systems Manager unterstützt wird.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

> **Note**
>
> Um das untergeordnete Runbook auszuführen`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`, fügen Sie die in diesem Dokument aufgeführten Berechtigungen hinzu.

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootWindowsUpdate`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - InstanceId (Erforderlich):

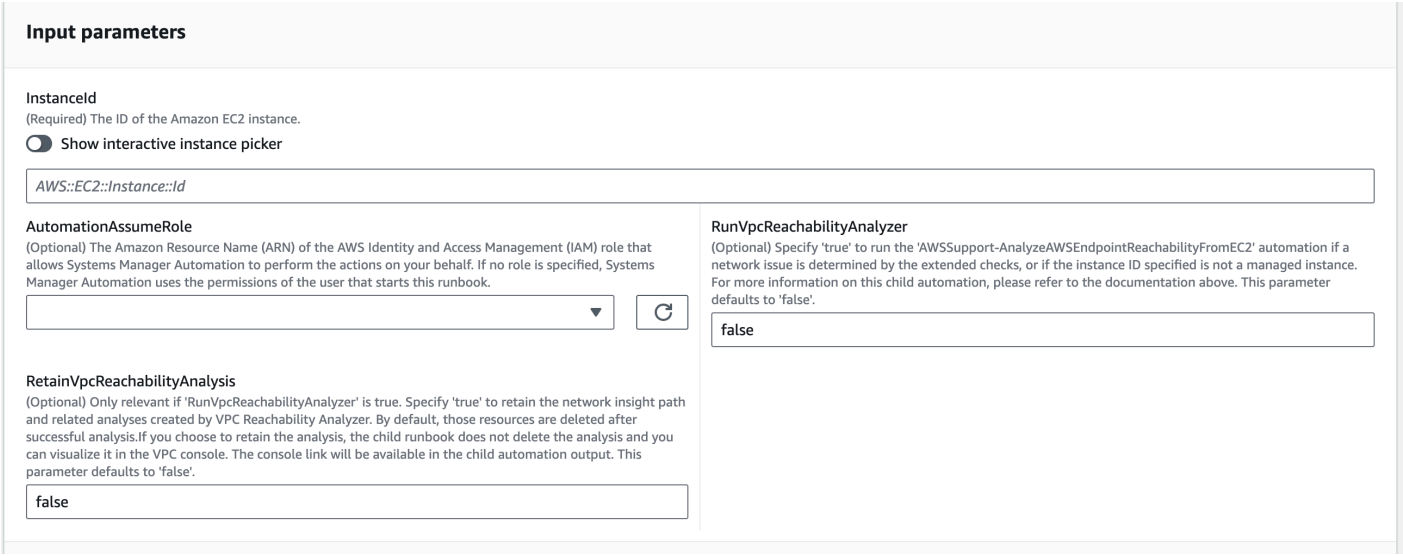
     Geben Sie die ID der Amazon EC2 EC2-Instance ein, bei der das Windows-Update fehlgeschlagen ist.

- RunVpcReachabilityAnalyzer(Optional):

  Geben Sie `true` an, ob die `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Automatisierung ausgeführt werden soll, wenn durch die erweiterten Prüfungen ein Netzwerkproblem festgestellt wurde oder wenn es sich bei der angegebenen Instanz-ID nicht um eine verwaltete Instanz handelt. Weitere Informationen zu dieser untergeordneten Automatisierung finden Sie in der Dokumentation. Der Standardwert ist `false`.

- RetainVpcReachabilityAnalysis(Fakultativ):

  Nur relevant, wenn `RunVpcReachabilityAnalyzer` es ist`true`. Geben Sie `true` an, ob der Netzwerkerkenntpfad und die zugehörigen Analysen, die von erstellt wurden, beibehalten werden sollen`Reachability Analyzer`. Standardmäßig werden diese Ressourcen nach erfolgreicher Analyse gelöscht. Wenn Sie sich dafür entscheiden, die Analyse beizubehalten, löscht das untergeordnete Runbook die Analyse nicht und Sie können sie in der Amazon VPC-Konsole visualisieren. Der Konsolenlink wird in der Ausgabe der untergeordneten Automatisierung verfügbar sein. Der Standardwert`false`.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - **`getWindowsServerAndSSMAgentVersion:`**

     Überprüft, ob die Zielinstanz von der SSM-Agent-Version AWS Systems Manager und der Windows-Version verwaltet wird, und ruft Details dazu ab.

   - **`assertifInstanceIsSsmManaged:`**

Stellt sicher, dass die Amazon EC2 EC2-Instance von AWS Systems Manager (SSM) verwaltet wird, andernfalls endet die Automatisierung.

- **`CheckProxy:`**

  Sucht nach allen Proxytypen für die Windows-Instance.

- **`CheckPrerequisites:`**

  Ruft die SSM-Agent-Version und die Windows-Version ab und ermittelt, ob es sich um einen Active Directory-Domänencontroller (DC) handelt. Wenn es sich bei der Instanz um einen DC handelt oder der SSM-Agent oder die Windows-Version nicht unterstützt wird, wird das Runbook beendet.

- **`CheckDiskSpace:`**

  Ruft den verfügbaren Festplattenspeicher auf der Windows-Instanz ab und überprüft ihn, wenn er für die Durchführung des Windows-Updates ausreicht.

- **`CheckPendingReboot:`**

  Sucht nach ausstehenden Neustarts über die Windows-Instanz.

- **`CheckS3Connectivity:`**

  Prüft, ob die Instance die Amazon S3 S3-Endpunkte für `Patchbaseline` erreichen kann.

- **`branchOnRunVpcReachabilityAnalyzer:`**

  Wenn dies zutrifft, `RunVpcReachabilityAnalyzer` wird die Automatisierung verzweigt, um tiefere Analysen für das Debuggen der Amazon S3 S3-Konnektivität durchzuführen.

- **`GenerateEndpoints:`**

  Generiert einen Endpunkt für eine erweiterte Konnektivitätsprüfung für den Amazon S3 S3-Endpunkt.

- **`analyzeAwsEndpointReachabilityFromEC2:`**

  Ruft das Automatisierungs-Runbook,`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`. auf, um die Erreichbarkeit der ausgewählten Instance für die erforderlichen Endpunkte zu überprüfen.

- **`CheckWindowsUpdateServices:`**

  Überprüft den Status und den Starttyp des Windows Update-Dienstes.

- **CheckWindowsUpdateSettings:**

  Sucht nach Windows Update-Richtlinien, die über die Windows-Instanz konfiguriert wurden.

- **CheckWSUSSettings:**

  Überprüft, ob das Windows-Update mit WSUS oder Microsoft Update Catalog konfiguriert ist, und überprüft die Konnektivität.

- **CheckWUGlobalSettings:**

  Überprüft die globalen Windows Update-Einstellungen, die über die Windows-Instanz konfiguriert wurden.

- **GenerateLogs:**

  Lädt Windows Update-Protokolle und CBS-Protokolle auf den Instanz-Desktop herunter und überprüft die Windows-Ereignisprotokolle auf Fehler.

- **FinalReport:**

  Generiert einen vollständigen Bericht über alle Schritte.

7. Wenn Sie fertig sind, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

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\\Adminisrative 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
"
```

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus

- Eine Automatisierung einrichten
- Landingpage Support Automation Workflows

Dokumentation zum AWS Service

- Weitere Informationen finden Sie im Artikel TroubleShootWindows Update.

AWSSupport-UpgradeWindowsAWSDrivers

Beschreibung

Das `AWSSupport-UpgradeWindowsAWSDrivers` Runbook aktualisiert oder repariert Speicher- und AWS Netzwerktreiber auf der angegebenen EC2-Instance. Das Runbook versucht, die neuesten AWS Treiberversionen online zu installieren, indem es den SSM-Agenten aufruft. Wenn der SSM-Agent nicht erreichbar ist, kann das Runbook auf ausdrücklichen Wunsch eine Offline-Installation der AWS Treiber durchführen.

Dieses Runbook unterstützt die folgenden Betriebssysteme:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

> **Note**
>
> Sowohl beim Online- als auch beim Offline-Upgrade wird vor dem Versuch, irgendwelche Operationen auszuführen, ein AMI erstellt, das auch nach Abschluss der Automatisierung fortbesteht. Es liegt in Ihrer Verantwortung, den Zugriff auf das AMI zu gewährleisten oder es zu löschen. Die Online-Methode startet die Instance als Teil des Upgrade-Prozesses neu, während die Offline-Methode erfordert, dass die bereitgestellte EC2-Instance angehalten und dann gestartet wird.

> **Important**
>
> Wenn Ihre Instances AWS Systems Manager mithilfe von VPC-Endpunkten eine Verbindung herstellen, schlägt dieses Runbook fehl, sofern es nicht in der Region us-east-1 verwendet wird. Dieses Runbook schlägt auch auf einem Domänencontroller fehl. Informationen zum Aktualisieren von AWS PV-Treibern auf einem Domänencontroller finden Sie unter Upgrade eines Domänencontrollers (AWS PV-Upgrade).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AllowOffline

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Auf „true“ setzen, um eine Offline-Treiberaktualisierung zuzulassen, wenn die Online-Installation nicht durchgeführt werden kann. Hinweis: Die Offline-Methode erfordert, die bereitgestellte EC2-Instance anzuhalten und dann neu zu starten. Auf den Instance-Speichervolumes gespeicherte Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP verwenden.
- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ForceUpgrade

  Typ: Zeichenfolge

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Nur Offline - Auf „true“ setzen, um zuzulassen, dass die Offline-Aktualisierung der Treiber fortgesetzt wird, auch wenn auf Ihrer Instance bereits die neuesten Treiber installiert sind.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID Ihrer EC2-Instance für Windows Server.

- SubnetId

  Typ: Zeichenfolge

  Standard: SelectedInstanceSubnet

  Beschreibung: (Optional) Nur offline — Die Subnetz-ID für die EC2 Rescue-Instanz, die für das Offline-Treiber-Upgrade verwendet wurde. Wenn keine Subnetz-ID angegeben ist, erstellt Systems Manager Automation eine neue VPC.

  > **Important**
  >
  > Das Subnetz muss sich in derselben Availability Zone befinden wie InstanceId und es muss den Zugriff auf die SSM-Endpunkte ermöglichen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Die EC2-Instance, die den Befehl empfängt, muss mindestens über eine IAM-Rolle verfügen, die Berechtigungen für ssm: StartAutomationExecution und ssm: umfasst, SendCommand um die Automatisierung auszuführen und den Befehl an die Instance zu senden, sowie ssm:, um die Automatisierungsausgabe GetAutomationExecution lesen zu können. Sie können die von `AmazonSSMManagedInstanceCore` Amazon verwaltete Richtlinie an Ihre IAM-Rolle anhängen, um diese Berechtigungen bereitzustellen. Wir empfehlen jedoch, die Automation-IAM-Rolle `AmazonSSMAutomationRole` zu diesem Zweck zu verwenden. Weitere Informationen finden Sie unter Verwenden von IAM zur Konfiguration von Rollen für die Automatisierung.

Wenn Sie ein Offline-Upgrade durchführen, vgl. die für `AWSSupport-StartEC2RescueWorkflow` erforderlichen Berechtigungen.

Dokumentschritte

1. `aws:assertAwsResourceProperty`— Überprüft, ob es sich bei der Eingabeinstanz um Windows handelt.
2. `aws:assertAwsResourceProperty`— Überprüft, ob es sich bei der Eingabeinstanz um eine verwaltete Instanz handelt. Wenn dies der Fall ist, beginnt das Online-Upgrade, oder das Offline-Upgrade wird evaluiert.
   a. (Online-Upgrade) Wenn die Input-Instance eine verwaltete Instance ist:
      i. `aws:createImage`- Erstellt ein AMI-Backup.
      ii. `aws:createTags`- Markiert das AMI-Backup.
      iii. `aws:runCommand`- Installiert den ENA-Netzwerktreiber.
      iv. `aws:runCommand`- Installiert NVMe den Treiber.
      v. `aws:runCommand`- Installiert den AWS PV-Treiber.
   b. (Offline-Upgrade) Wenn die Input-Instance keine verwaltete Instance ist:
      i. `aws:assertAwsResourceProperty`- Überprüft, ob die AllowOffline Flagge auf `true` gesetzt ist. Wenn ja, wird das Offline-Upgrade gestartet, andernfalls endet die Automatisierung.
      ii. `aws:changeInstanceState`- Stoppen Sie die Quellinstanz.
      iii. `aws:changeInstanceState`- Erzwingen Sie das Stoppen der Quellinstanz.
      iv. `aws:createImage`- Erstellen Sie ein AMI-Backup der Quell-Instance.

v. `aws:createTags`- Kennzeichnen Sie das AMI-Backup der Quell-Instance.

vi. `aws:executeAwsApi`— Aktivieren Sie ENA für die Instanz

vii. `aws:assertAwsResourceProperty`— Bestätigen Sie die ForceUpgrade Flagge.

viii. Offline-Aktualisierung erzwingen) Wenn ForceUpgrade = true, dann ausführen`aws:executeAutomation`, um `AWSSupport-StartEC2RescueWorkflow` mit dem Treiber-Force-Upgrade-Skript aufzurufen. Dadurch werden Treiber unabhängig von der aktuellen Version installiert.

ix. (Offline-Upgrade) Wenn ForceUpgrade = falsch, dann ausführen, `aws:executeAutomation` um es `AWSSupport-StartEC2RescueWorkflow` mit dem Treiber-Upgrade-Skript aufzurufen.

Ausgaben

preUpgradeBackup.ImageId

preOfflineUpgradeBackup. ImageId

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

upgradeDriversOffline. Leistung

forceUpgradeDriversOffline. Ausgabe

Amazon ECS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Elastic Container Service bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-CollectECSInstanceLogs
- AWS-InstallAmazonECSAgent
- AWS-ECSRunTask

- AWSSupport-TroubleshootECSContainerInstance
- AWSSupport-TroubleshootECSTaskFailedToStart
- AWS-UpdateAmazonECSAgent

AWSSupport-CollectECSInstanceLogs

Beschreibung

Das `AWSSupport-CollectECSInstanceLogs` Runbook sammelt Protokolldateien im Zusammenhang mit dem Betriebssystem und dem Amazon Elastic Container Service (Amazon ECS) von einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance, um Sie bei der Behebung häufiger Amazon ECS-Probleme zu unterstützen. Während die Automatisierung die zugehörigen Protokolldateien sammelt, werden Änderungen am Dateisystem vorgenommen. Zu diesen Änderungen gehören die Erstellung temporärer Verzeichnisse und eines Protokollverzeichnisses, das Kopieren von Protokolldateien in diese Verzeichnisse und das Komprimieren der Protokolldateien in ein Archiv.

Wenn Sie einen Wert für den `LogDestination` Parameter angeben, muss auf der Zielinstanz die AWS Befehlszeilenschnittstelle (AWS CLI) für Linux-Instances oder AWS Tools für Windows PowerShell für Windows-Instances installiert sein. Die Automatisierung bewertet den Richtlinienstatus des von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Buckets. Um die Sicherheit der von Ihrer Amazon EC2 EC2-Instance gesammelten Protokolle zu gewährleisten, werden die Protokolle nicht hochgeladen`true`, wenn der Richtlinienstatus auf gesetzt `isPublic` ist oder wenn die Zugriffskontrollliste (ACL) der vordefinierten `All Users` Amazon S3 S3-Gruppe `READ|WRITE` Berechtigungen gewährt. Wenn der bereitgestellte Bucket in Ihrem Konto nicht verfügbar ist, werden die Protokolle außerdem nicht hochgeladen. Weitere Informationen zu vordefinierten Amazon S3 S3-Gruppen finden Sie unter Vordefinierte Amazon S3 S3-Gruppen im Amazon Simple Storage Service-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ECSInstanceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Instanz, von der Sie Protokolle sammeln möchten. Die von Ihnen angegebene Instanz muss von Systems Manager verwaltet werden.
- LogDestination

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon S3 S3-Bucket in Ihrem AWS-Konto , in den Sie die archivierten Protokolle hochladen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`

Wir empfehlen, dass die Amazon EC2 EC2-Instance, die Sie im `ECSInstanceId` Parameter angeben, über eine IAM-Rolle verfügt, an die die von `AmazonSSMManagedInstanceCore` Amazon verwaltete Richtlinie angehängt ist. Um das Protokollarchiv in den Amazon S3 S3-Bucket

hochzuladen, den Sie im `LogDestination` Parameter angeben, müssen Sie die folgenden Berechtigungen hinzufügen:

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

Dokumentschritte

- `assertInstanceIsManaged`- Überprüft, ob die Instanz, die Sie im `ECSInstanceId` Parameter angeben, von Systems Manager verwaltet wird.
- `getInstancePlatform`— Ruft Informationen über die Betriebssystemplattform (OS) der im `ECSInstanceId` Parameter angegebenen Instanz ab.
- `verifyInstancePlatform`— Verzweigt die Automatisierung auf der Grundlage der Betriebssystemplattform.
- `runLogCollectionScriptOnLinux`- Sammelt betriebssystem- und Amazon ECS-bezogene Protokolldateien auf Linux-Instances und erstellt eine Archivdatei im `/var/log/collectECSlogs` Verzeichnis.
- `runLogCollectionScriptOnWindows`- Sammelt betriebssystem- und Amazon ECS-bezogene Protokolldateien auf Windows-Instances und erstellt eine Archivdatei im `C:\ProgramData\collectECSlogs` Verzeichnis.
- `verifyIfS3BucketProvided`— Überprüft, ob ein Wert für den `LogDestination` Parameter angegeben wurde.
- `runUploadScript`- Verzweigt den Automatisierungsschritt auf der Grundlage der Betriebssystemplattform.
- `runUploadScriptOnLinux`- Lädt das Protokollarchiv in den im `LogDestination` Parameter angegebenen Amazon S3 S3-Bucket hoch und löscht die archivierte Protokolldatei aus dem Betriebssystem.
- `runUploadScriptOnWindows`- Lädt das Protokollarchiv in den im `LogDestination` Parameter angegebenen Amazon S3 S3-Bucket hoch und löscht die archivierte Protokolldatei aus dem Betriebssystem.

AWS-InstallAmazonECSAgent

Beschreibung

Das `AWS-InstallAmazonECSAgent` Runbook installiert den Amazon Elastic Container Service (Amazon ECS) -Agenten auf der von Ihnen angegebenen Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Dieses Runbook unterstützt nur Amazon Linux- und Amazon Linux 2-Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceIds

  Typ: StringList

  Beschreibung: (Erforderlich) Die IDs der Amazon EC2 EC2-Instances, auf denen Sie den Amazon ECS-Agenten installieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`

Dokumentschritte

`aws:executeScript`- Installiert den Amazon ECS-Agenten auf den Amazon EC2 EC2-Instances, die Sie im `InstanceIds` Parameter angeben.

Ausgaben

InstallAmazonECSAgent. SuccessfulInstances — Die ID der Instance, bei der die Installation des Amazon ECS-Agenten erfolgreich war.

InstallAmazonECSAgent. FailedInstances — Die ID der Instance, bei der die Installation des Amazon ECS-Agenten fehlgeschlagen ist.

InstallAmazonECSAgent. InProgressInstances — Die ID der Instance, auf der der Amazon ECS-Agent installiert wird.

AWS-ECSRunTask

Beschreibung

Das `AWS-ECSRunTask` Runbook führt die von Ihnen angegebene Amazon Elastic Container Service (Amazon ECS) -Aufgabe aus.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- capacityProviderStrategy

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Kapazitätsanbieter-Strategie, die für die Aufgabe verwendet werden soll.
- Cluster

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Kurzname oder der ARN des Clusters, auf dem Ihre Aufgabe ausgeführt werden soll. Wenn Sie keinen Cluster angeben, wird der Standardcluster verwendet.
- count

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Instanziierungen der angegebenen Aufgabe, die auf Ihrem Cluster platziert werden sollen. Sie können bis zu 10 Aufgaben für jede Anfrage angeben.
- ECSManagedTags aktivieren

  Typ: Boolescher Wert

  Beschreibung: (Optional) Gibt an, ob verwaltete Amazon ECS-Tags für die Aufgabe verwendet werden sollen. Weitere Informationen finden Sie unter Markieren Ihrer Amazon-ECS-Ressourcen im Entwicklerhandbuch für Amazon Elastic Container Service.

- enableExecuteCommand

  Typ: Boolescher Wert

  Beschreibung: (Optional) Legt fest, ob die Funktion zum Ausführen von Befehlen für die Container in dieser Aufgabe aktiviert werden soll. Wenn der Wert wahr ist, aktiviert dies die Funktion zum Ausführen von Befehlen für alle Container in der Aufgabe.

- Gruppe

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der Aufgabengruppe, die der Aufgabe zugeordnet werden soll. Der Standardwert ist der Familienname der Aufgabendefinition. Beispiel, `family:my-family-name`.

- LaunchType

  Typ: Zeichenfolge

  Gültige Werte: EC2 | FARGATE | EXTERNAL

  Beschreibung: (Optional) Die Infrastruktur, auf der Ihre eigenständige Aufgabe ausgeführt werden soll.

- networkConfiguration

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Netzwerkkonfiguration für die Aufgabe. Dieser Parameter ist für Aufgabendefinitionen erforderlich, die den `awsvpc` Netzwerkmodus verwenden, um ihre eigene elastic network interface zu erhalten, und er wird für andere Netzwerkmodi nicht unterstützt.

- überschreibt

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine Liste von Container-Overrides im JSON-Format, die den Namen eines Containers in der angegebenen Aufgabendefinition und die Überschreibungen, die er erhalten soll, spezifiziert. Sie können den Standardbefehl für einen Container, der in der Aufgabendefinition oder im Docker-Image angegeben ist, mit einem Befehl override überschreiben. Sie können auch vorhandene Umgebungsvariablen überschreiben, die in der Aufgabendefinition

oder im Docker-Image eines Containers angegeben sind. Darüber hinaus können Sie neue Umgebungsvariablen mit einer Umgebungsüberschreibung hinzufügen.

- placementConstraints

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine Reihe von Platzierungsbeschränkungsobjekten, die für die Aufgabe verwendet werden sollen. Sie können bis zu 10 Einschränkungen für jede Aufgabe angeben, einschließlich Einschränkungen in der Aufgabendefinition und Einschränkungen, die zur Laufzeit angegeben wurden.

- placementStrategy

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Objekte der Platzierungsstrategie, die für die Aufgabe verwendet werden sollen. Sie können für jede Aufgabe maximal 5 Strategieregeln angeben.

- platformVersion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Plattformversion, die die Aufgabe verwendet. Eine Plattformversion ist nur für Aufgaben spezifiziert, die auf Fargate gehostet werden. Ist keine Plattformversion angegeben, wird die Plattformversion `LATEST` verwendet.

- propagateTags

  Typ: Zeichenfolge

  Beschreibung: (Optional) Legt fest, ob Tags von der Aufgabendefinition an die Aufgabe weitergegeben werden. Wenn kein Wert angegeben wird, werden die Tags nicht weitergegeben. Tags können nur während der Aufgabenerstellung an die Aufgaben übertragen werden.

- Referenz-ID

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Referenz-ID, die für die Aufgabe verwendet werden soll. Die Referenz-ID kann eine maximale Länge von 1024 Zeichen haben.

- Gestartet von

  Typ: Zeichenfolge

Beschreibung: (Optional) Ein optionales Tag, das beim Starten einer Aufgabe angegeben wird. Auf diese Weise können Sie identifizieren, welche Aufgaben zu einem bestimmten Job gehören, indem Sie die Ergebnisse eines `ListTasks` API-Vorgangs filtern. Bis zu 36 Buchstaben (Groß- und Kleinbuchstaben), Zahlen, Bindestriche (-) und Unterstriche (_) sind zulässig.

- tags

  Typ: Zeichenfolge

  Beschreibung: (Optional) Metadaten, die Sie auf die Aufgabe anwenden möchten, um Aufgaben zu kategorisieren und zu organisieren. Jedes Tag besteht aus einem benutzerdefinierten Schlüssel und Wert.

- Aufgabendefinition

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der `family` und `revision` (`family:revision`) oder der vollständige ARN der auszuführenden Aufgabendefinition. Wenn keine Revision angegeben ist, wird die neueste `ACTIVE` Version verwendet.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ecs:RunTask`

Dokumentschritte

`aws:executeScript`— Führt die Amazon ECS-Aufgabe auf der Grundlage der Werte aus, die Sie für die Runbook-Eingabeparameter angeben.

AWSSupport-TroubleshootECSContainerInstance

Beschreibung

Das `AWSSupport-TroubleshootECSContainerInstance` Runbook hilft Ihnen bei der Fehlerbehebung bei einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die sich nicht bei einem Amazon ECS-Cluster registrieren kann. Diese Automatisierung überprüft, ob die

Benutzerdaten für die Instance die richtigen Clusterinformationen enthalten, ob das Instance-Profil die erforderlichen Berechtigungen enthält und ob Probleme mit der Netzwerkkonfiguration auftreten.

> **Important**
>
> Um diese Automatisierung erfolgreich auszuführen, muss der Status Ihrer Amazon EC2 EC2-Instance und der Status des Amazon ECS-Clusters sein`ACTIVE`. `running`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon ECS-Clusters, bei dem sich die Instance nicht registrieren konnte.
- InstanceId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, für die Sie eine Fehlerbehebung durchführen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

aws:ExecuteScript: Prüft, ob die Amazon EC2 EC2-Instance die Voraussetzungen erfüllt, die für die Registrierung bei einem Amazon ECS-Cluster erforderlich sind.

AWSSupport-TroubleshootECSTaskFailedToStart

Beschreibung

Das `AWSSupport-TroubleshootECSTaskFailedToStart` Runbook hilft Ihnen bei der Fehlerbehebung, warum eine Amazon Elastic Container Service (Amazon ECS) -Aufgabe in einem

Amazon ECS-Cluster nicht gestartet werden konnte. Sie müssen dieses Runbook genauso ausführen AWS-Region wie Ihre Aufgabe, die nicht gestartet werden konnte. Das Runbook analysiert die folgenden häufigen Probleme, die das Starten einer Aufgabe verhindern können:

- Netzwerkkonnektivität zur konfigurierten Container-Registry
- Fehlende IAM-Berechtigungen, die für die Aufgabenausführungsrolle erforderlich sind
- Konnektivität des VPC-Endpunkts
- Konfiguration der Sicherheitsgruppenregel
- AWS Secrets Manager geheime Verweise
- Protokollierungskonfiguration

> **Note**
>
> Wenn die Analyse ergibt, dass die Netzwerkkonnektivität getestet werden muss, werden eine Lambda-Funktion und die erforderliche IAM-Rolle in Ihrem Konto erstellt. Diese Ressourcen werden verwendet, um die Netzwerkkonnektivität Ihrer fehlgeschlagenen Aufgabe zu simulieren. Die Automatisierung löscht diese Ressourcen, wenn sie nicht mehr benötigt werden. Wenn die Automatisierung die Ressourcen jedoch nicht löschen kann, müssen Sie dies manuell tun.
> Wenn eine Lambda-IAM-Rolle bereitgestellt wird, verwendet die Automatisierung sie, anstatt eine neue zu erstellen. Die bereitgestellte Lambda-IAM-Rolle muss die AWS verwaltete Richtlinie enthalten `AWSLambdaVPCAccessExecutionRole` und über eine Vertrauensrichtlinie verfügen, die es ermöglicht, dass sie vom Lambda-Serviceprinzipal übernommen wird. `lambda.amazonaws.com`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- LambdaRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der IAM-Rolle, der der AWS Lambda Funktion den Zugriff auf die erforderlichen AWS Dienste und Ressourcen ermöglicht. Wenn keine Rolle angegeben ist, erstellt diese Systems Manager Manager-Automatisierung eine IAM-Rolle für Lambda in Ihrem Konto mit dem Namen`NetworkToolSSMRunbookExecution<ExecutionId>`, der die verwaltete Richtlinie enthält:. `AWSLambdaVPCAccessExecutionRole`

- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon ECS-Clusters, in dem die Aufgabe nicht gestartet werden konnte.

- CloudwatchRetentionPeriod

  Typ: Ganzzahl

  Beschreibung: (Optional) Der Aufbewahrungszeitraum in Tagen, für die Lambda-Funktionsprotokolle, die in Amazon CloudWatch Logs gespeichert werden sollen. Dies ist nur erforderlich, wenn die Analyse ergibt, dass die Netzwerkkonnektivität getestet werden muss.

  Gültige Werte: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

  Standard: 30

- TaskId

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der fehlgeschlagenen Aufgabe. Verwenden Sie die zuletzt fehlgeschlagene Aufgabe.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Wenn LambdaRoleArn angegeben, muss die Automatisierung die Rolle nicht erstellen, und die folgenden Berechtigungen können ausgeschlossen werden:

- iam:CreateRole
- iam:DeleteRole
- iam:AttachRolePolicy

- `iam:DetachRolePolicy`

Dokumentschritte

- `aws:executeScript`- Überprüft, ob der Benutzer oder die Rolle, der die Automatisierung gestartet hat, über die erforderlichen IAM-Berechtigungen verfügt. Wenn Sie nicht über ausreichende Berechtigungen verfügen, um dieses Runbook zu verwenden, sind die fehlenden erforderlichen Berechtigungen in der Ausgabe der Automatisierung enthalten.
- `aws:branch`— Verzweigungen basieren darauf, ob Sie über Berechtigungen für alle erforderlichen Aktionen für das Runbook verfügen.
- `aws:executeScript`- Erstellt eine Lambda-Funktion in Ihrer VPC, wenn die Analyse ergibt, dass die Netzwerkkonnektivität getestet werden muss.
- `aws:branch`— Verzweigungen, die auf den Ergebnissen des vorherigen Schritts basieren.
- `aws:executeScript`- Analysiert mögliche Ursachen dafür, dass Ihre Aufgabe nicht gestartet werden konnte.
- `aws:executeScript`- Löscht Ressourcen, die durch diese Automatisierung erstellt wurden.
- `aws:executeScript`- Formatiert die Ausgabe der Automatisierung so, dass die Ergebnisse der Analyse an die Konsole zurückgegeben werden. Sie können die Analyse nach diesem Schritt überprüfen, bevor die Automatisierung abgeschlossen ist.
- `aws:branch`- Verzweigungen, die darauf basieren, ob die Lambda-Funktion und die zugehörigen Ressourcen erstellt wurden und gelöscht werden müssen.
- `aws:sleep`- Schläft 30 Minuten lang, sodass die elastic network interface für die Lambda-Funktion gelöscht werden kann.
- `aws:executeScript`- Löscht die Netzwerkschnittstelle der Lambda-Funktion.
- `aws:executeScript`— Formatiert die Ausgabe des Schritts zum Löschen der Netzwerkschnittstelle der Lambda-Funktion.

AWS-UpdateAmazonECSAgent

Beschreibung

Das `AWS-UpdateAmazonECSAgent` Runbook aktualisiert den Amazon Elastic Container Service (Amazon ECS) -Agenten auf der von Ihnen angegebenen Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Dieses Runbook unterstützt nur Amazon Linux- und Amazon Linux 2-Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterArn

  Typ: StringList

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Amazon ECS-Clusters, bei dem Ihre Container-Instances registriert sind.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`

- `ec2:DescribeImage`
- `ec2:DescribeInstance`
- `ec2:DescribeInstanceAttribute`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

Dokumentschritte

`aws:executeScript`- Aktualisiert den Amazon ECS-Agenten auf dem Amazon ECS-Cluster, den Sie in den `ClusterARN` Parametern angeben.

Ausgaben

UpdateAmazonECSAgent. UpdatedContainers — Die ID der Instance, bei der das Update des Amazon ECS-Agenten erfolgreich war.

UpdateAmazonECSAgent. FailedContainers - Die ID der Instance, bei der das Update des Amazon ECS-Agenten fehlgeschlagen ist.

UpdateAmazonECSAgent. InProgressContainers — Die ID der Instance, in der das Update des Amazon ECS-Agenten gerade läuft.

Amazon EFS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Elastic File System bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-CheckAndMountEFS

AWSSupport-CheckAndMountEFS

Beschreibung

Das `AWSSupport-CheckAndMountEFS` Runbook überprüft die Voraussetzungen für das Mounten Ihres Amazon Elastic File System (Amazon EFS) -Dateisystems und mountet das Dateisystem auf der von Ihnen angegebenen Amazon Elastic Compute Cloud (Amazon EC2) -Instance. Dieses Runbook unterstützt das Mounten Ihres Amazon EFS-Dateisystems mit dem DNS-Namen oder mithilfe der IP-Adresse des Mount-Ziels.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Action

  Typ: Zeichenfolge

  Gültige Werte: Prüfen Sie | CheckAndMount

  Beschreibung: (Erforderlich) Legt fest, ob das Runbook die Voraussetzungen oder die Voraussetzungen überprüft und das Dateisystem einhängt.
- EfsId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID des Dateisystems, das Sie mounten möchten.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, auf der Sie das Dateisystem mounten möchten.

- MountOptions

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die vom Amazon EFS-Mount-Helper unterstützten Optionen, die Sie beim Mounten des Dateisystems verwenden möchten. Wenn Sie die `tls` Option angeben, stellen Sie sicher, dass Stunnel auf der Ziel-Instance aktualisiert wurde.

- MountPoint

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Verzeichnis, in dem Sie das Dateisystem mounten möchten. Wenn Sie den `Check` Wert für den `Action` Parameter angeben, sollte dieser Parameter nicht angegeben werden.

- MountTargetIP

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die IP-Adresse des Mount-Ziels. Das Mounten nach IP-Adresse funktioniert in Umgebungen, in denen DNS deaktiviert ist, z. B. in virtuellen privaten Clouds (VPCs) mit deaktivierten DNS-Hostnamen. Sie können diese Option auch verwenden, wenn Ihre Umgebung einen anderen DNS-Anbieter als Amazon Route 53 (Route 53) verwendet.

- Region

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der AWS-Region Ort, an dem sich die Amazon EC2 EC2-Instance und das Dateisystem befinden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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:*`

Dokumentschritte

- `aws:executeScript`- Sammelt Details über die Amazon EC2 EC2-Instance, die Sie im `InstanceId` Parameter angeben.
- `aws:executeScript`- Sammelt Details über das Dateisystem, das Sie im Parameter angeben. `EfsId`
- `aws:executeScript`— Überprüft, ob die dem Dateisystem zugeordnete Sicherheitsgruppe Datenverkehr auf Port 2049 von der Amazon EC2 EC2-Instance zulässt, die Sie im Parameter angeben. `InstanceId`

- `aws:assertAwsResourceProperty`— Überprüft, ob die Amazon EC2 EC2-Instance, die Sie im `InstanceId` Parameter angeben, von Systems Manager verwaltet wird und ob der Status lautet. `Online`
- `aws:branch`— Verzweigt auf der Grundlage des Werts, den Sie für den `Action` Parameter angeben.
- `aws:runCommand`- Überprüft die Voraussetzungen für das Mounten des Dateisystems, das Sie im `EfsId` Parameter angeben.
- `aws:runCommand`- Überprüft die Voraussetzungen für das Mounten des Dateisystems, das Sie im `EfsId` Parameter angeben, und mountet das Dateisystem auf der Amazon EC2 EC2-Instance, die Sie im Parameter angeben. `InstanceId`

Amazon EKS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Elastic Kubernetes Service bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-CreateEKSClusterWithFargateProfile
- AWS-CreateEKSClusterWithNodegroup
- AWS-DeleteEKSCluster
- AWS-MigrateToNewEKSSelfManagedNodeGroup
- AWSPremiumSupport-TroubleshootEKSCluster
- AWSSupport-TroubleshootEKSWorkerNode
- AWS-UpdateEKSCluster
- AWS-UpdateEKSManagedNodeGroup
- AWS-UpdateEKSSelfManagedLinuxNodeGroups
- AWSSupport-CollectEKSLinuxNodeStatistics
- AWSSupport-CollectEKSInstanceLogs
- AWSSupport-SetupK8sApiProxyForEKS
- AWSSupport-TroubleshootEbsCsiDriversForEks

- AWSSupport-TroubleshootEKSALBControllerIssues

AWS-CreateEKSClusterWithFargateProfile

Beschreibung

Das `AWS-CreateEKSClusterWithFargateProfile` Runbook erstellt einen Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mithilfe eines. AWS Fargate

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Ein eindeutiger Name für den Cluster.
- ClusterRoleArn

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, der Berechtigungen für die Kubernetes-Steuerebene bereitstellt, um AWS API-Operationen in Ihrem Namen aufzurufen.

- FargateProfileName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Fargate-Profils.

- FargateProfileRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle für die Ausführung von Amazon EKS Pod.

- FargateProfileSelectors

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Selektoren, um Pods dem Fargate-Profil zuzuordnen.

- SubnetIds

  Typ: StringList

  Beschreibung: (Erforderlich) Die IDs Subnetze, die Sie für Ihren Amazon EKS-Cluster verwenden möchten. Amazon EKS erstellt in diesen Subnetzen elastische Netzwerkschnittstellen für die Kommunikation zwischen Ihren Knoten und der Kubernetes-Steuerebene. Sie müssen mindestens zwei Subnetze angeben. IDs

- EKSEndpointPrivateAccess

  Typ: Boolescher Wert

  Standard: True

  Beschreibung: (Optional) Legen Sie diesen Wert auf fest, `True` um privaten Zugriff für den Kubernetes-API-Serverendpunkt Ihres Clusters zu ermöglichen. Wenn Sie den privaten Zugriff aktivieren, verwenden Kubernetes-API-Anfragen aus der VPC Ihres Clusters den privaten VPC-Endpunkt. Wenn Sie den privaten Zugriff deaktivieren und Knoten oder AWS Fargate Pods im Cluster haben, stellen Sie sicher, dass die erforderlichen CIDR-Blöcke für die Kommunikation mit den Knoten oder Fargate-Pods `publicAccessCidrs` enthalten sind.

- EKSEndpointPublicAccess

Typ: Boolescher Wert

Standard: False

Beschreibung: (Optional) Legen Sie diesen Wert auf fest, `False` um den öffentlichen Zugriff auf den Kubernetes-API-Serverendpunkt Ihres Clusters zu deaktivieren. Wenn Sie den öffentlichen Zugriff deaktivieren, kann der Kubernetes-API-Server Ihres Clusters nur Anfragen von der VPC empfangen, in der er gestartet wurde.

- PublicAccessCIDRs

  Typ: StringList

  Beschreibung: (Optional) Die CIDR-Blöcke, denen der Zugriff auf den öffentlichen Kubernetes-API-Serverendpunkt Ihres Clusters gewährt wird. Die Kommunikation mit dem Endpunkt über Adressen außerhalb der von Ihnen angegebenen CIDR-Blöcke wird verweigert. Wenn Sie den privaten Endpunktzugriff deaktiviert haben und Knoten oder Fargate-Pods im Cluster haben, stellen Sie sicher, dass Sie die erforderlichen CIDR-Blöcke angeben.

- SecurityGroupIds

  Typ: StringList

  Beschreibung: (Optional) Geben Sie eine oder mehrere Sicherheitsgruppen an, die den Elastic Network-Schnittstellen zugeordnet werden sollen, die in Ihrem Konto von Amazon EKS erstellt wurden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- Create EKSCluster (aws:executeAwsApi) — Erstellt einen Amazon EKS-Cluster.
- Verify EKSCluster IsActive (aws: waitForAwsResourceProperty) — Überprüft, ob der Cluster-Status lautet`ACTIVE`.
- CreateFargateProfile (aws:executeAwsApi) — Erzeugt ein Fargate für den Cluster.
- VerifyFargateProfileIsActive (aws: waitForAwsResourceProperty) — Überprüft, ob der Status des Fargate-Profils lautet. `ACTIVE`

Ausgaben

`CreateEKSCluster.CreateClusterResponse`

Beschreibung: Die Antwort wurde vom `CreateCluster` API-Aufruf empfangen.

`CreateFargateProfile.CreateFargateProfileResponse`

Beschreibung: Die Antwort wurde vom `CreateFargateProfile` API-Aufruf empfangen.

AWS-CreateEKSClusterWithNodegroup

Beschreibung

Das `AWS-CreateEKSClusterWithNodegroup` Runbook erstellt einen Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster, der eine Knotengruppe für die Kapazität verwendet.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Ein eindeutiger Name für den Cluster.
- ClusterRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, der Berechtigungen für die Kubernetes-Steuerebene bereitstellt, um AWS API-Operationen in Ihrem Namen aufzurufen.
- NodegroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Ein eindeutiger Name für die Knotengruppe.
- NodegroupRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, die Ihrer Knotengruppe zugeordnet werden soll. Der Kubelet-Daemon von Amazon EKS Worker Node ruft in Ihrem Namen AWS APIs auf. Knoten erhalten über ein IAM-Instance-Profil und zugehörige Richtlinien Berechtigungen für diese

API-Aufrufe. Bevor Sie Knoten starten und in einem Cluster registrieren können, müssen Sie eine IAM-Rolle erstellen, die diese Knoten beim Start verwenden können.

- SubnetIds

  Typ: StringList

  Beschreibung: (Erforderlich) Die IDs Subnetze, die Sie für Ihren Amazon EKS-Cluster verwenden möchten. Amazon EKS erstellt in diesen Subnetzen elastische Netzwerkschnittstellen für die Kommunikation zwischen Ihren Knoten und der Kubernetes-Steuerebene. Sie müssen mindestens zwei Subnetze angeben. IDs

- EKSEndpointPrivateAccess

  Typ: Boolescher Wert

  Standard: True

  Beschreibung: (Optional) Legen Sie diesen Wert auf fest, `True` um privaten Zugriff für den Kubernetes-API-Serverendpunkt Ihres Clusters zu ermöglichen. Wenn Sie den privaten Zugriff aktivieren, verwenden Kubernetes-API-Anfragen aus der VPC Ihres Clusters den privaten VPC-Endpunkt. Wenn Sie den privaten Zugriff deaktivieren und Knoten oder AWS Fargate Pods im Cluster haben, stellen Sie sicher, dass die erforderlichen CIDR-Blöcke für die Kommunikation mit den Knoten oder Fargate-Pods `publicAccessCidrs` enthalten sind.

- EKSEndpointPublicAccess

  Typ: Boolescher Wert

  Standard: False

  Beschreibung: (Optional) Legen Sie diesen Wert auf fest, `False` um den öffentlichen Zugriff auf den Kubernetes-API-Serverendpunkt Ihres Clusters zu deaktivieren. Wenn Sie den öffentlichen Zugriff deaktivieren, kann der Kubernetes-API-Server Ihres Clusters nur Anfragen von der VPC empfangen, in der er gestartet wurde.

- PublicAccessCIDRs

  Typ: StringList

  Beschreibung: (Optional) Die CIDR-Blöcke, denen der Zugriff auf den öffentlichen Kubernetes-API-Serverendpunkt Ihres Clusters gewährt wird. Die Kommunikation mit dem Endpunkt über Adressen außerhalb der von Ihnen angegebenen CIDR-Blöcke wird verweigert. Wenn Sie den

privaten Endpunktzugriff deaktiviert haben und Knoten oder Fargate-Pods im Cluster haben, stellen Sie sicher, dass Sie die erforderlichen CIDR-Blöcke angeben.

- SecurityGroupIds

  Typ: StringList

  Beschreibung: (Optional) Geben Sie eine oder mehrere Sicherheitsgruppen an, die den Elastic Network-Schnittstellen zugeordnet werden sollen, die in Ihrem Konto von Amazon EKS erstellt wurden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

Dokumentschritte

- Create EKSCluster (aws:executeAwsApi) — Erstellt einen Amazon EKS-Cluster.
- Verify EKSCluster IsActive (aws: waitForAwsResourceProperty) — Überprüft, ob der Cluster-Status lautet`ACTIVE`.
- CreateNodegroup (aws:executeAwsApi) — Erstellt eine Knotengruppe für den Cluster.
- VerifyNodegroupIsActive (aws: waitForAwsResourceProperty) — Überprüft, ob der Status der Knotengruppe lautet`ACTIVE`.

Ausgaben

- `CreateEKSCluster.CreateClusterResponse`: Die Antwort wurde vom `CreateCluster` API-Aufruf empfangen.
- `CreateNodegroup.CreateNodegroupResponse`: Antwort vom `CreateNodegroup` API-Aufruf erhalten.

AWS-DeleteEKSCluster

Beschreibung

Dieses Runbook löscht die mit einem Amazon EKS-Cluster verknüpften Ressourcen, einschließlich Knotengruppen und Fargate-Profilen. Optional können Sie alle selbstverwalteten Knoten, die CloudFormation Stacks, die zum Erstellen der Knoten verwendet wurden, und den CloudFormation VPC-Stack für Ihren Cluster löschen. Weitere Informationen zum Löschen eines Clusters finden Sie unter Löschen eines Clusters im Amazon EKS-Benutzerhandbuch.

> **Note**
>
> Wenn Sie aktive Dienste in Ihrem Cluster haben, die einem Load Balancer zugeordnet sind, müssen Sie diese Dienste löschen, bevor Sie den Cluster löschen. Wenn Sie dies nicht tun, kann das System die Load Balancer nicht löschen. Gehen Sie wie folgt vor, um Dienste zu suchen und zu löschen, bevor Sie das `AWS-DeleteEKSCluster` Runbook ausführen.

So suchen und löschen Sie Dienste in Ihrem Cluster

1. Installieren Sie das Kubernetes-Befehlszeilenprogramm,. `kubectl` Weitere Informationen finden Sie unter Installation von kubectl im Amazon EKS-Benutzerhandbuch.
2. Führen Sie den folgenden Befehl aus, um alle Dienste aufzulisten, die in Ihrem Cluster ausgeführt werden.

   ```
   kubectl get svc --all-namespaces
   ```

3. Führen Sie den folgenden Befehl aus, um alle Dienste zu löschen, denen ein EXTERNAL-IP-Wert zugeordnet ist. Diese Dienste werden von einem Load Balancer unterstützt, und Sie müssen sie in Kubernetes löschen, damit der Load Balancer und die zugehörigen Ressourcen ordnungsgemäß freigegeben werden können.

```
kubectl delete svc
service-name
```

Sie können das Runbook jetzt ausführen. `AWS-DeleteEKSCluster`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EKSClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon EKS-Clusters, der gelöscht werden soll.
- VPCCloudFormationStack

  Typ: Zeichenfolge

Beschreibung: (Optional) CloudFormation Stack-Name für die VPC für den EKS-Cluster, der gelöscht wird. Dadurch werden der CloudFormation Stack für VPC und alle vom Stack erstellten Ressourcen gelöscht.

- VPCCloudFormationStackRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN einer IAM-Rolle, die CloudFormation davon ausgeht, den CloudFormation VPC-Stack zu löschen. CloudFormation verwendet die Anmeldeinformationen der Rolle, um in Ihrem Namen Anrufe zu tätigen.

- SelfManagedNodeStacks

  Typ: Zeichenfolge

  Beschreibung: (Optional) Durch Kommas getrennte Liste von CloudFormation Stack-Namen für selbstverwaltete Knoten. Dadurch werden die CloudFormation Stacks für selbstverwaltete Knoten gelöscht.

- SelfManagedNodeStacksRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN einer IAM-Rolle, die CloudFormation davon ausgeht, die selbstverwalteten Node Stacks zu löschen. CloudFormation verwendet die Anmeldeinformationen der Rolle, um in Ihrem Namen Anrufe zu tätigen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `sts:AssumeRole`
- `eks:ListNodegroups`
- `eks:DeleteNodegroup`
- `eks:ListFargateProfiles`
- `eks:DeleteFargateProfile`
- `eks:DeleteCluster`

- `cfn:DescribeStacks`
- `cfn:DeleteStack`

Dokumentschritte

- `aws:executeScript`- DeleteNodeGroups: Findet und löscht alle Knotengruppen im EKS-Cluster.
- `aws:executeScript`- DeleteFargateProfiles: Findet und löscht alle Fargate-Profile im EKS-Cluster.
- `aws:executeScript`- DeleteSelfManagedNodes: Löscht alle selbstverwalteten Knoten und die CloudFormation Stacks, die zur Erstellung der Knoten verwendet wurden.
- `aws:executeScript`- LöschenEKSCluster: EKS-Cluster löschen.
- `aws:executeScript`- Löschen VPCCloudFormationStack: Löscht den CloudFormation VPC-Stack.

`AWS-MigrateToNewEKSSelfManagedNodeGroup`

Beschreibung

Das `AWS-MigrateToNewEKSSelfManagedNodeGroup` Runbook hilft Ihnen dabei, eine neue Linux-Knotengruppe von Amazon Elastic Kubernetes Service (Amazon EKS) zu erstellen, zu der Sie Ihre bestehende Anwendung migrieren können. Weitere Informationen finden Sie unter Migration zu einer neuen Knotengruppe im Amazon EKS-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- OldStackName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name oder die Stack-ID Ihres vorhandenen CloudFormation Stacks.

- NewStackName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des neuen CloudFormation Stacks, der für Ihre neue Knotengruppe erstellt wird. Wenn Sie keinen Wert für diesen Parameter angeben, wird der Stack-Name im folgenden Format erstellt:`NewNodeGroup-`*`ClusterName`*`-`*`AutomationExecutionID`*.

- ClusterControlPlaneSecurityGroup

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Sicherheitsgruppe, die Knoten für die Kommunikation mit der Amazon EKS-Steuerebene verwenden sollen. Wenn Sie keinen Wert für diesen Parameter angeben, wird die in Ihrem vorhandenen CloudFormation Stack angegebene Sicherheitsgruppe verwendet.

- NodeInstanceType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Instance-Typ, den Sie für die neue Knotengruppe verwenden möchten. Wenn Sie keinen Wert für diesen Parameter angeben, wird der in Ihrem vorhandenen CloudFormation Stack angegebene Instance-Typ verwendet.

- NodeGroupName

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Name Ihrer neuen Knotengruppe. Wenn Sie keinen Wert für diesen Parameter angeben, wird der in Ihrem vorhandenen CloudFormation Stack angegebene Knotengruppenname verwendet.

- NodeAutoScalingGroupDesiredCapacity

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die gewünschte Anzahl von Knoten, auf die skaliert werden soll, wenn Ihr neuer Stack erstellt wird. Diese Zahl muss größer oder gleich dem `NodeAutoScalingGroupMinSize` Wert und kleiner oder gleich dem Wert sein`NodeAutoScalingGroupMaxSize`. Wenn Sie keinen Wert für diesen Parameter angeben, wird die gewünschte Kapazität der Knotengruppe verwendet, die in Ihrem vorhandenen CloudFormation Stack angegeben ist.

- NodeAutoScalingGroupMaxSize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die maximale Anzahl von Knoten, auf die Ihre Knotengruppe skaliert werden kann. Wenn Sie keinen Wert für diesen Parameter angeben, wird die maximale Größe der Knotengruppe verwendet, die in Ihrem vorhandenen CloudFormation Stack angegeben ist.

- NodeAutoScalingGroupMinSize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Mindestanzahl von Knoten, auf die Ihre Knotengruppe skaliert werden kann. Wenn Sie keinen Wert für diesen Parameter angeben, wird die Mindestgröße der Knotengruppe verwendet, die in Ihrem vorhandenen CloudFormation Stack angegeben ist.

- NodeImageId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID von Amazon Machine Image (AMI), die die Knotengruppe verwenden soll.

- NodeImageIdSSMParam

  Typ: Zeichenfolge

Beschreibung: (Optional) Der öffentliche Systems Manager Manager-Parameter für denAMI, den die Knotengruppe verwenden soll.

- NodeVolumeSize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Größe des Root-Volumes für Ihre Knoten in GiB. Wenn Sie keinen Wert für diesen Parameter angeben, wird die in Ihrem vorhandenen CloudFormation Stack angegebene Knoten-Volume-Größe verwendet.

- NodeVolumeType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Typ des Amazon EBS-Volumes, das Sie für das Root-Volume Ihrer Knoten verwenden möchten. Wenn Sie keinen Wert für diesen Parameter angeben, wird der in Ihrem vorhandenen CloudFormation Stack angegebene Volume-Typ verwendet.

- KeyName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das key pair, das Sie Ihren Knoten zuweisen möchten. Wenn Sie keinen Wert für diesen Parameter angeben, wird das in Ihrem vorhandenen CloudFormation Stack angegebene key pair verwendet.

- Subnets

  Typ: StringList

  Beschreibung: (Optional) Eine durch Kommas getrennte Liste des Subnetzes IDs , das Sie für Ihre neue Knotengruppe verwenden möchten. Wenn Sie keinen Wert für diesen Parameter angeben, werden die in Ihrem vorhandenen CloudFormation Stack angegebenen Subnetze verwendet.

- Deaktivieren IMDSv1

  Typ: Boolescher Wert

  Beschreibung: (Optional) Geben Sie `true` an, ob der Instanz-Metadatendienst Version 1 (IMDSv1) deaktiviert werden soll. Standardmäßig unterstützen Knoten IMDSv1 und IMDSv2.

- BootstrapArguments

Typ: Zeichenfolge

Beschreibung: (Optional) Zusätzliche Argumente, die Sie an das Node-Bootstrap-Skript übergeben möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- DetermineParameterValuesForNewNodeGroup (aws:ExecuteScript) — Sammelt die Parameterwerte, die für die neue Knotengruppe verwendet werden sollen.
- CreateStack (aws:CreateStack) — Erstellt den Stack für die neue Knotengruppe. CloudFormation
- GetNewStackNodeInstanceRole (aws:executeAwsApi) — Ruft die Rolle der Knoteninstanz ab.

- GetNewStackSecurityGroup (aws:executeAwsApi) — Der Schritt ruft die Knotensicherheitsgruppe ab.
- AddIngressRulesToNewNodeSecurityGroup (aws:executeAwsApi) — Fügt der neu erstellten Sicherheitsgruppe Eingangsregeln hinzu, sodass sie Datenverkehr von der Gruppe akzeptieren kann, die Ihrer vorherigen Knotengruppe zugewiesen wurde.
- AddIngressRulesToOldNodeSecurityGroup (aws:executeAwsApi) — Fügt der vorherigen Sicherheitsgruppe Eingangsregeln hinzu, sodass sie Datenverkehr von der Sicherheitsgruppe akzeptieren kann, die Ihrer neu erstellten Knotengruppe zugewiesen ist.
- VerifyStackComplete (aws: assertAwsResource Property) — Überprüft, ob der neue Stack-Status lautet. `CREATE_COMPLETE`

Ausgaben

DetermineParameterValuesForNewNodeGroup. NewStackParameters - Die Parameter, die zur Erstellung des neuen Stacks verwendet wurden.

GetNewStackNodeInstanceRole. NewNodeInstanceRole — Die Knoteninstanzrolle für die neue Knotengruppe.

GetNewStackSecurityGroup. NewNodeSecurityGroup - Die ID der Sicherheitsgruppe für die neue Knotengruppe.

DetermineParameterValuesForNewNodeGroup. NewStackName - Der CloudFormation Stack-Name für die neue Knotengruppe.

CreateStack. StackId - Die CloudFormation Stack-ID für die neue Knotengruppe.

AWSPremiumSupport-TroubleshootEKSCluster

Beschreibung

Das `AWSPremiumSupport-TroubleshootEKSCluster` Runbook diagnostiziert häufig auftretende Probleme mit einem Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster und der zugrunde liegenden Infrastruktur und bietet empfohlene Schritte zur Behebung.

> **Important**
>
> Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist ein Abonnement für Business + Support, Enterprise Support oder Unified Operations erforderlich. Weitere Informationen finden Sie unter AWS Support Tarife vergleichen.

Wenn Sie einen Wert für den `S3BucketName` Parameter angeben, bewertet die Automatisierung den Richtlinienstatus des von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Buckets. Um die Sicherheit der von Ihrer EC2-Instance gesammelten Protokolle zu gewährleisten, werden die Protokolle nicht hochgeladen`true`, wenn der Richtlinienstatus auf gesetzt `isPublic` ist oder wenn die Zugriffskontrollliste (ACL) der vordefinierten `All Users` Amazon S3 S3-Gruppe `READ|WRITE` Berechtigungen gewährt. Weitere Informationen zu vordefinierten Amazon S3 S3-Gruppen finden Sie unter Amazon S3 S3-vordefinierte Gruppen im Amazon Simple Storage Service-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon EKS-Clusters, für den Sie eine Fehlerbehebung durchführen möchten.
- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des privaten Amazon S3 S3-Buckets, in den der vom Runbook generierte Bericht hochgeladen werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Darüber hinaus muss die AWS Identity and Access Management (IAM-) Richtlinie, die dem Benutzer oder der Rolle zugewiesen ist, die die Automatisierung startet, den `ssm:GetParameter` Vorgang mit den folgenden öffentlichen AWS Systems Manager Parametern zulassen, um das neueste empfohlene Amazon EKS Amazon Machine Image (AMI) für die Worker-Knoten abzurufen.

- `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`

Um den vom Runbook generierten Bericht in einen Amazon S3 S3-Bucket hochzuladen, sind die folgenden Berechtigungen für den angegebenen Amazon S3 S3-Bucket erforderlich.

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

Dokumentschritte

- `aws:executeAwsApi`- Sammelt Details für den angegebenen Amazon EKS-Cluster.
- `aws:executeScript`- Sammelt Details zu den Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Auto Scaling Scaling-Gruppen, AMI s und Amazon EC2-GPU-Grafikinstanztypen.
- `aws:executeScript`- Sammelt Details zur Virtual Private Cloud (VPC), Subnetze, Network Address Translation (NAT) -Gateways, Subnetzrouten, Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (ACLs) des Amazon EKS-Clusters.
- `aws:executeScript`— Sammelt Details zu den angehängten IAM-Instance-Profilen und Rollenrichtlinien.
- `aws:executeScript`- Sammelt Details des Amazon S3 S3-Buckets, den Sie im `S3BucketName` Parameter angeben.

- `aws:executeScript`- Klassifiziert die Amazon VPC-Subnetze als öffentlich oder privat.
- `aws:executeScript`- Überprüft die Amazon VPC-Subnetze auf Tags, die als Teil eines Amazon EKS-Clusters erforderlich sind.
- `aws:executeScript`- Überprüft die Amazon VPC-Subnetze auf die Tags, die für Elastic Load Balancing Balancing-Subnetze erforderlich sind.
- `aws:executeScript`- Prüft, ob die Worker-Node-Amazon-EC2-Instances die neuesten für Amazon EKS optimierten AMI s verwenden
- `aws:executeScript`- Überprüft, ob die Amazon VPC-Sicherheitsgruppen den Worker-Knoten die erforderlichen Tags zugewiesen haben.
- `aws:executeScript`- Überprüft die Amazon VPC-Sicherheitsgruppenregeln für Amazon EKS-Cluster und Worker-Nodes auf die empfohlenen Eingangsregeln für den Amazon EKS-Cluster.
- `aws:executeScript`- Überprüft die Amazon VPC-Sicherheitsgruppenregeln für Amazon EKS-Cluster und Worker-Nodes auf die empfohlenen Ausgangsregeln aus dem Amazon EKS-Cluster.
- `aws:executeScript`- Überprüft die Netzwerk-ACL-Konfiguration der Amazon VPC-Subnetze.
- `aws:executeScript`— Prüft, ob die Amazon EC2 EC2-Instances des Worker-Nodes über die erforderlichen verwalteten Richtlinien verfügen.
- `aws:executeScript`- Prüft, ob die Auto Scaling Scaling-Gruppen über die erforderlichen Tags für Cluster-Autoscaling verfügen.
- `aws:executeScript`— Prüft, ob die Amazon EC2 EC2-Instances des Worker-Nodes mit dem Internet verbunden sind.
- `aws:executeScript`- Generiert einen Bericht auf der Grundlage der Ergebnisse der vorherigen Schritte. Wenn ein Wert für den `S3BucketName` Parameter angegeben wird, wird der generierte Bericht in den Amazon S3 S3-Bucket hochgeladen.

AWSSupport-TroubleshootEKSWorkerNode

Beschreibung

Das `AWSSupport-TroubleshootEKSWorkerNode` Runbook analysiert einen Amazon Elastic Compute Cloud (Amazon EC2) -Worker-Knoten und einen Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster, um Sie bei der Identifizierung und Behebung häufiger Ursachen zu unterstützen, die verhindern, dass Worker-Knoten einem Cluster beitreten können. Das Runbook enthält Anleitungen, die Ihnen bei der Lösung aller identifizierten Probleme helfen sollen.

> **Important**
>
> Um diese Automatisierung erfolgreich auszuführen, muss der Status Ihres Amazon EC2 `running` EC2-Worker-Knotens und der Amazon EKS-Cluster-Status sein`ACTIVE`.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon EKS-Clusters.
- Worker-ID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Amazon EC2 EC2-Worker-Knotens, der dem Cluster nicht beitreten konnte.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:assertAwsResourceProperty`— Bestätigt, dass der Amazon EKS-Cluster, den Sie im `ClusterName` Parameter angeben, existiert und sich in einem `ACTIVE` Zustand befindet.

- `aws:assertAwsResourceProperty`— Bestätigt, dass der Amazon EC2 EC2-Worker-Knoten, den Sie im `WorkerID` Parameter angeben, vorhanden ist und sich in einem `running` Status befindet.
- `aws:executeScript`- Führt ein Python-Skript aus, das dabei hilft, mögliche Ursachen dafür zu identifizieren, dass der Worker-Knoten dem Cluster nicht beitreten kann.

AWS-UpdateEKSCluster

Beschreibung

Das `AWS-UpdateEKSCluster` Runbook hilft Ihnen dabei, Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster auf die Kubernetes-Version zu aktualisieren, die Sie verwenden möchten.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name Ihres Amazon EKS-Clusters.

- Version

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Kubernetes-Version, auf die Sie Ihren Cluster aktualisieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `eks:DescribeUpdate`
- `eks:UpdateClusterVersion`

Dokumentschritte

- `aws:executeAwsApi`- Aktualisiert die Kubernetes-Version, die von Ihrem Amazon EKS-Cluster verwendet wird.
- `aws:waitForAwsResourceProperty`- Wartet auf den Aktualisierungsstatus. `Successful`

AWS-UpdateEKSManagedNodeGroup

Beschreibung

Das `AWS-UpdateEKSManagedNodeGroup` Runbook hilft Ihnen bei der Aktualisierung einer von Amazon Elastic Kubernetes Service (Amazon EKS) verwalteten Knotengruppe. Sie können entweder eine oder eine `Version` Aktualisierung auswählen. `Configuration`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Clusters, dessen Knotengruppe Sie aktualisieren möchten.
- NodeGroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Knotengruppe, die aktualisiert werden soll.
- UpdateType

  Typ: Zeichenfolge

  Gültige Werte: Knotengruppenversion aktualisieren | Knotengruppenkonfigurationen aktualisieren

  Standard: Version der Knotengruppe aktualisieren

  Beschreibung: (Erforderlich) Die Art des Updates, das Sie für die Knotengruppe durchführen möchten.

Die folgenden Parameter gelten nur für den `Version` Aktualisierungstyp:

- AMIReleaseVersion

  Typ: Zeichenfolge

Beschreibung: (Optional) Die optimierte Version von Amazon EKSAMI, die Sie verwenden möchten. Standardmäßig wird die neueste Version verwendet.

- ForceUpgrade

  Typ: Boolescher Wert

  Beschreibung: (Optional) Wenn dieser Wert zutrifft, schlägt das Update nicht fehl, wenn das Budget bei einer Pod-Unterbrechung überschritten wurde.

- KubernetesVersion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Kubernetes-Version, auf die die Knotengruppe aktualisiert werden soll.

- LaunchTemplateId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID der Startvorlage.

- LaunchTemplateName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der Startvorlage.

- LaunchTemplateVersion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Version der Startvorlage für Amazon Elastic Compute Cloud (Amazon EC2). Dieser Parameter ist nur gültig, wenn eine Knotengruppe anhand einer Startvorlage erstellt wurde.

Die folgenden Parameter gelten nur für den `Configuration` Aktualisierungstyp:

- AddOrUpdateNodeGroupLabels

  Typ: StringMap

  Beschreibung: (Optional) Kubernetes-Labels, die Sie hinzufügen oder aktualisieren möchten.

- AddOrUpdateKubernetesTaintsEffect

  Typ: StringList

  Beschreibung: (Optional) Die Kubernetes-Taints, die Sie hinzufügen oder aktualisieren möchten.
- MaxUnavailableNodeGroups

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die maximale Anzahl von Knoten, die während eines Versionsupdates gleichzeitig nicht verfügbar sind.
- MaxUnavailablePercentageNodeGroup

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Der Prozentsatz der Knoten, die während eines Versionsupdates nicht verfügbar sind.
- NodeGroupDesiredSize

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die Anzahl der Knoten, die die verwaltete Knotengruppe verwalten soll.
- NodeGroupMaxSize

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die maximale Anzahl von Knoten, auf die die verwaltete Knotengruppe skaliert werden kann.
- NodeGroupMinSize

  Typ: Ganzzahl

  Standard: 0

Beschreibung: (Optional) Die Mindestanzahl von Knoten, auf die die verwaltete Knotengruppe skaliert werden kann.

- RemoveKubernetesTaintsEffect

  Typ: StringList

  Beschreibung: (Optional) Die Kubernetes-Taints, die Sie entfernen möchten.

- RemoveNodeGroupLabels

  Typ: StringList

  Beschreibung: (Optional) Eine durch Kommas getrennte Liste von Labels, die Sie entfernen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

Dokumentschritte

- `aws:executeScript`— Aktualisiert eine Amazon EKS-Cluster-Knotengruppe entsprechend den Werten, die Sie für die Runbook-Eingabeparameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet, bis der Cluster-Aktualisierungsstatus erreicht ist. `Successful`

AWS-UpdateEKSSelfManagedLinuxNodeGroups

Beschreibung

Das `AWS-UpdateEKSSelfManagedLinuxNodeGroups` Runbook aktualisiert selbstverwaltete verwaltete Knotengruppen in Ihrem Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mithilfe eines Stacks. AWS CloudFormation

Wenn Ihr Cluster Auto Scaling verwendet, empfehlen wir, die Bereitstellung auf zwei Replikate herunterzuskalieren, bevor Sie dieses Runbook verwenden.

Um eine Bereitstellung auf zwei Replikate zu skalieren

1. Installieren Sie das Kubernetes-Befehlszeilenprogramm,. `kubectl` Weitere Informationen finden Sie unter Installieren von kubectl im Amazon-EKS-Benutzerhandbuch.
2. Führen Sie den folgenden Befehl aus.

   ```
   kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
   ```
3. Führen Sie das Runbook aus. `AWS-UpdateEKSSelfManagedLinuxNodeGroups`
4. Skalieren Sie die Bereitstellung wieder auf die gewünschte Anzahl von Replikaten, indem Sie den folgenden Befehl ausführen.

   ```
   kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
   ```

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon EKS-Clusters.

- NodeGroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der verwalteten Knotengruppe.

- ClusterControlPlaneSecurityGroup

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe auf der Kontrollebene.

- Deaktivieren IMDSv1

  Typ: Boolescher Wert

  Beschreibung: (Optional) Legt fest, ob Sie Instance Metadata Service Version 1 (IMDSv1) und zulassen möchten IMDSv2.

- KeyName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Schlüsselname für die Instanzen.

- NodeAutoScalingGroupDesiredCapacity

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Knoten, die die Knotengruppe verwalten soll.

- NodeAutoScalingGroupMaxSize

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die maximale Anzahl von Knoten, auf die die Knotengruppe skaliert werden kann.

- NodeAutoScalingGroupMinSize

  Typ: Zeichenfolge

Beschreibung: (Optional) Die Mindestanzahl von Knoten, auf die die Knotengruppe skaliert werden kann.

- NodeInstanceType

  Typ: Zeichenfolge

  Standard: t3.large

  Beschreibung: (Optional) Der Instanztyp, den Sie für die Knotengruppe verwenden möchten.

- NodeImageId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID von Amazon Machine Image (AMI), die die Knotengruppe verwenden soll.

- NodeImageIdSSMParam

  Typ: Zeichenfolge

  Standard:/aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

  Beschreibung: (Optional) Der öffentliche Systems Manager Manager-Parameter für denAMI, den die Knotengruppe verwenden soll.

- StackName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des CloudFormation Stacks, der zur Aktualisierung der Knotengruppe verwendet wird.

- Subnets

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der IDs Subnetze, die Ihr Cluster verwenden soll.

- VpcId

  Typ: Zeichenfolge

Standard: Standard

Beschreibung: (Erforderlich) Die Virtual Private Cloud (VPC), in der Ihr Cluster bereitgestellt wird.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DeleteNodegroup`
- `eks:DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

Dokumentschritte

- `aws:executeScript`— Aktualisiert eine Amazon EKS-Cluster-Knotengruppe entsprechend den Werten, die Sie für die Runbook-Eingabeparameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet auf die Rückgabe des CloudFormation Stack-Aktualisierungsstatus.

AWSSupport-CollectEKSLinuxNodeStatistics

Beschreibung

Das `AWSSupport-CollectEKSLinuxNodeStatistics` Runbook sammelt Linux-Statistiken von einer Amazon EC2 EC2-Instance, die Teil eines Amazon EKS-Clusters ist, und von einem Container, der auf der Instance ausgeführt wird, wenn eine `containerd` Container-ID angegeben ist. Die Amazon EC2 EC2-Instance muss von AWS Systems Manager verwaltet werden.

Zu den gesammelten Linux-Statistiken auf Host-Ebene gehören:

- Betriebssysteminformationen.
- Statistiken zur Netzwerkschnittstelle — von `ethtool` und vom `/sys/class/net/interface/statistics` Verzeichnis.
- Anzahl der Dateideskriptoren.
- Es zählt flüchtige Ports.
- Eine Sammlung von Regeln. `iptables`
- Suchen Sie nach einer vollständigen Conntrack-Tabelle.

Die Linux-Statistiken auf Container-Ebene beinhalten:

- Identifikationsinformationen — Bild-URI und Labels.
- Statistiken zur Netzwerkschnittstelle — von `ethtool` und vom `/sys/class/net/interface/statistics` Verzeichnis.
- Traceroute- und DNS-Ergebnisse, wenn der `NetworkTargets` Parameter gefüllt ist.
- Die Analyse der Paketerfassung zählt — TCP-Neuübertragungen, Pakete, die nicht in der richtigen Reihenfolge sind usw.

Das Runbook sammelt Daten aus verschiedenen Linux-Distributionen, darunter Amazon Linux 2, Amazon Linux 2023 und Debian/Ubuntu. Es verwendet die neuesten Versionen der folgenden Bilder aus der öffentlichen Amazon ECR-Galerie:

- `amazon-ecs-network-sidecar`Bild, um Zugriff auf Tools zur Fehlerbehebung zu erhalten.
- `aws-cli`Bild, um die JSON-Datei und die Paketerfassungsdateien für den Statistikbericht in den angegebenen Amazon S3 S3-Bucket hochzuladen.

> **Important**
>
> Dieses Runbook unterstützt keine Fargate-Instances. Dieses Runbook schlägt möglicherweise fehl, wenn die Instanz während der Ausführung heruntergefahren oder die Verbindung unterbrochen wird.

Wie funktioniert es?

Das Runbook führt die folgenden Aktionen aus:

- Überprüft, ob der Amazon S3 S3-Ziel-Bucket keinen öffentlichen Lese- oder Schreibzugriff gewährt.
- Stellt sicher, dass die Amazon EC2 EC2-Zielinstanz von Systems Manager verwaltet wird und sich im laufenden Zustand befindet.
- Überprüft, ob auf der Instance ein Linux-Betriebssystem ausgeführt wird.
- Sammelt umfassende Linux-Statistiken aus der Amazon EC2 EC2-Instance und optional aus einem angegebenen Container.
- Lädt die gesammelten Statistiken in den angegebenen Amazon S3 S3-Bucket hoch.

Führen Sie diese Automatisierung aus (Konsole)

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen:

- `s3:GetAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketLocation`
- `s3:GetEncryptionConfiguration`
- `s3:PutObject`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `ec2:DescribeInstances`

Beispiel für eine IAM-Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-CollectEKSLinuxNodeStatisticsim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der IAM-Rolle, der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - InstanceId (Erforderlich):

     Die ID der Amazon EC2 EC2-Instance zum Sammeln von Statistiken.
   - S3 BucketName (erforderlich):

     Name des Amazon S3 S3-Buckets, um die JSON-Ausgabe aus der Amazon EC2 EC2-Instance als Datei zu exportieren.
   - S3 KeyPrefix (optional):

Das Amazon S3 S3-Schlüsselpräfix (Unterordner) zum Exportieren der JSON-Ausgabe aus der Amazon EC2 EC2-Instance als Datei. Standard: `AWSSupport-CollectEKSLinuxNodeStatistics`.

- S3 BucketOwnerRoleArn (optional):

  Der ARN der IAM-Rolle mit den Berechtigungen zum Abrufen der Einstellungen für den öffentlichen Zugriff auf den Amazon S3 S3-Bucket und das Konto, zur Konfiguration der Bucket-Verschlüsselung, zum Bucket, zum Bucket ACLs, zum Bucket-Richtlinienstatus und zum Hochladen von Objekten in den Bucket. Wenn dieser Parameter nicht angegeben ist, verwendet das Runbook den `AutomationAssumeRole` (falls angegeben) oder den Benutzer, der dieses Runbook startet (falls nicht `AutomationAssumeRole` angegeben).

- S3 BucketOwnerAccount (optional):

  Das AWS Konto, dem der Amazon S3 S3-Bucket gehört. Wenn Sie diesen Parameter nicht angeben, geht das Runbook davon aus, dass sich der Bucket in diesem Konto befindet.

- ContainerId (Fakultativ):

  Die ID eines Containers, der auf der angegebenen Amazon EC2 EC2-Instance läuft.

- NetworkTargets (Fakultativ):

  Eine durch Kommas getrennte Liste von IPv4 Adressen, and/or DNS-Namen zum Testen der DNS-Auflösung und der Konnektivität mithilfe von Traceroute.

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

   - **`CheckBucketAccess`**:

     Prüft, ob der Amazon S3 S3-Ziel-Bucket möglicherweise öffentlichen Lese- und and/or Schreibzugriff auf seine Objekte gewährt.

   - **`AssertInstanceIsSSMManaged`**:

     Stellt sicher, dass die Amazon EC2 EC2-Zielinstanz von Systems Manager verwaltet wird, andernfalls endet die Automatisierung.

   - **`VerifyInstanceState`**:

Überprüft, ob sich die Amazon EC2 EC2-Instance im laufenden Zustand befindet, bevor versucht wird, Statistiken zu sammeln.

- **`BranchOnVerifyLinuxInstance`**:

  Überprüft, ob es sich bei der Instance um eine Linux-Instance handelt, bevor der Vorgang fortgesetzt wird.

- **`BranchOnVerifyInstanceRunning`**:

  Überprüft, ob sich die Instanz im laufenden Zustand befindet, bevor der Vorgang fortgesetzt wird.

- **`CollectEKSLinuxNodeStatistics`**:

  Sammelt umfassende Linux-Statistiken aus der Amazon EC2 EC2-Instance, einschließlich Betriebssysteminformationen, Netzwerkschnittstellenstatistiken, Dateideskriptoren, kurzlebigen Ports, Firewallregeln und optional Statistiken auf Container-Ebene.

- **`GenerateStatisticsOutputS3Uri`**:

  Generiert den vollständigen Amazon S3 S3-URI für die Linux-Statistikdateien, die als Ausgabe des Automatisierungsdokuments verwendet werden sollen.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

`AWSSupport-CollectEKSInstanceLogs`

Beschreibung

Das `AWSSupport-CollectEKSInstanceLogs` Runbook sammelt Protokolldateien im Zusammenhang mit dem Betriebssystem und Amazon Elastic Kubernetes Service (Amazon

EKS) aus einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance, um Ihnen bei der Behebung häufig auftretender Probleme zu helfen. Während die Automatisierung die zugehörigen Protokolldateien sammelt, werden Änderungen an der Dateisystemstruktur vorgenommen, einschließlich der Erstellung temporärer Verzeichnisse, des Kopierens von Protokolldateien in die temporären Verzeichnisse und der Komprimierung der Protokolldateien in ein Archiv. Diese Aktivität kann zu einer erhöhten Auslastung der `CPUUtilization` Amazon EC2 EC2-Instance führen. Weitere Informationen zu finden Sie `CPUUtilization` unter Instance-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Wenn Sie einen Wert für den `LogDestination` Parameter angeben, bewertet die Automatisierung den Richtlinienstatus des von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Buckets. Um die Sicherheit der von Ihrer Amazon EC2 EC2-Instance gesammelten Protokolle zu gewährleisten, werden die Protokolle nicht hochgeladen`true`, wenn der Richtlinienstatus auf gesetzt `isPublic` ist oder wenn die Zugriffskontrollliste (ACL) der vordefinierten `All Users` Amazon S3 S3-Gruppe `READ|WRITE` Berechtigungen gewährt. Weitere Informationen zu vordefinierten Amazon S3 S3-Gruppen finden Sie unter Amazon S3 S3-vordefinierte Gruppen im Amazon Simple Storage Service-Benutzerhandbuch.

> **Note**
>
> Diese Automatisierung erfordert mindestens 10 Prozent des verfügbaren Festplattenspeichers auf dem Amazon Elastic Block Store (Amazon EBS) -Stammvolume, das an Ihre Amazon EC2 EC2-Instance angehängt ist. Wenn auf dem Root-Volume nicht genügend Festplattenspeicher verfügbar ist, wird die Automatisierung gestoppt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- EKSInstanceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID der Amazon EC2-Instance von Amazon EKS, von der Sie Protokolle sammeln möchten.

- LogDestination

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon Simple Storage Service (Amazon S3) -Bucket in Ihrem Konto, in den die archivierten Protokolle hochgeladen werden sollen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Erforderliche IAM-Berechtigungen für das Amazon EC2 EC2-Instance-Profil

Dem Instance-Profil, das von verwendet wird, `EKSInstanceId` muss die von SSMManagedInstanceCoreAmazon verwaltete Richtlinie zugeordnet sein.

Es muss auch auf den `LogDestination` Amazon S3 S3-Bucket zugreifen können, damit es die gesammelten Protokolle hochladen kann. Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die an dieses Instance-Profil angehängt werden könnte:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::LogDestination/*",
        "arn:aws:s3:::LogDestination"
      ]
    }
  ]
}
```

Wenn AWS KMS Verschlüsselung `LogDestination` verwendet wird, muss der IAM-Richtlinie eine zusätzliche Anweisung hinzugefügt werden, die Zugriff auf den bei der Verschlüsselung verwendeten AWS KMS Schlüssel gewährt:

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

Dokumentschritte

- `aws:assertAwsResourceProperty`- Bestätigt, dass das Betriebssystem, für das der im `EKSInstanceId` Parameter angegebene Wert angegeben ist, Linux ist.
- `aws:runCommand`- Sammelt Protokolldateien zum Betriebssystem und zu Amazon EKS und komprimiert sie in ein Archiv im `/var/log` Verzeichnis.
- `aws:branch`— Bestätigt, ob ein Wert für den `LogDestination` Parameter angegeben wurde.
- `aws:runCommand`- Lädt das Protokollarchiv in den Amazon S3 S3-Bucket hoch, den Sie im `LogDestination` Parameter angeben.

AWSSupport-SetupK8sApiProxyForEKS

Beschreibung

Das AWSSupport-SetupKsApiProxy8-ForeKs-Automatisierungsrunbook bietet eine Möglichkeit, eine AWS Lambda Funktion zu erstellen, die als Proxy für API-Aufrufe der Steuerungsebene an den Cluster-Endpunkt von Amazon Elastic Kubernetes Service fungiert. Es dient als Baustein für Runbooks, die API-Aufrufe der Steuerungsebene zur Automatisierung von Aufgaben und zur Behebung von Problemen mit einem Amazon EKS-Cluster erfordern.

> **Important**
>
> Alle durch diese Automatisierung erstellten Ressourcen sind markiert, sodass sie leicht gefunden werden können. Die verwendeten Tags sind:
>
> - `AWSSupport-SetupK8sApiProxyForEKS`: true

> **Note**
>
> - Die Automatisierung ist ein Hilfs-Runbook und kann nicht als eigenständiges Runbook ausgeführt werden. Es wird als untergeordnete Automatisierung für Runbooks aufgerufen, die API-Aufrufe der Steuerungsebene an den Amazon EKS-Cluster erfordern.
> - Bitte stellen Sie sicher, dass der `Cleanup` Betrieb nach der Nutzung weiterläuft, um unerwünschte Kosten zu vermeiden.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon Elastic Kubernetes Service Service-Clusters.
- Operation

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Durchzuführender Vorgang: stellt die `Setup` Lambda-Funktion im Konto bereit und entfernt die Bereitstellung von Ressourcen, `Cleanup` die im Rahmen der Einrichtungsphase erstellt wurden.

Zulässige Werte: | `Setup` `Cleanup`

Standard: Setup

- LambdaRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der IAM-Rolle, der der AWS Lambda Funktion den Zugriff auf die erforderlichen AWS Dienste und Ressourcen ermöglicht. Wenn keine Rolle angegeben ist, erstellt diese Systems Manager Manager-Automatisierung eine IAM-Rolle für Lambda in Ihrem Konto mit dem Namen`Automation-K8sProxy-Role-<ExecutionId>`, der die verwalteten Richtlinien enthält: `AWSLambdaBasicExecutionRole` und. `AWSLambdaVPCAccessExecutionRole`

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Überprüft, ob die Automatisierung als untergeordnete Ausführung ausgeführt wird. Das Runbook funktioniert nicht, wenn es als eigenständiges Runbook aufgerufen wird, da es selbst keine sinnvollen Aufgaben ausführt.
- Überprüft, ob für die Proxy-Lambda-Funktion für den angegebenen Cluster ein CloudFormation Stack vorhanden ist.
  - Wenn der Stack vorhanden ist, wird die bestehende Infrastruktur wiederverwendet, anstatt sie neu zu erstellen.
  - Ein Referenzzähler wird mithilfe von Tags verwaltet, um sicherzustellen, dass ein Runbook die Infrastruktur nicht löscht, wenn sie von einem anderen Runbook für denselben Cluster wiederverwendet wird.
- Führen Sie den für den Aufruf angegebenen Operationstyp (`Setup`/`Cleanup`) aus:
  - Setup: Erstellt oder beschreibt vorhandene Ressourcen.

    Säuberung: Entfernt bereitgestellte Ressourcen, wenn die Infrastruktur nicht von einem anderen Runbook verwendet wird.

Erforderliche IAM-Berechtigungen

Für den `AutomationAssumeRole` Parameter sind die folgenden Berechtigungen erforderlich, er wurde nicht übergeben `LambdaRoleArn`:

- `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

Wenn LambdaRoleArn angegeben, muss die Automatisierung die Rolle nicht erstellen und die folgenden Berechtigungen können ausgeschlossen werden:

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

Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die zeigt, welche Berechtigungen erforderlich sind AutomationAssumeRole, wenn sie LambdaRoleArn nicht bestanden werden:

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/
AWSLambdaVPCAccessExecutionRole"
                    ]
                }
            },
            "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"
        }
    ]
}
```

Falls die erfüllt `LambdaRoleArn` ist, stellen Sie bitte sicher, dass ihr AWSLambdaBasicExecutionRole Richtlinien für öffentliche Cluster und zusätzlich AWSLambdaVPCAccessExecutionRole für private Cluster beigefügt sind.

Ressourcen erstellt

Die folgenden Ressourcen werden während des `Setup` Betriebs erstellt:

1. AWS Lambda Funktion
2. IAM-Rolle: Lambda-Ausführungsrolle, falls nicht angegeben.
3. CloudWatch Protokollgruppe (Lambda-Protokolle)

Die Lambda-Funktion und die Ausführungsrolle werden beibehalten, bis der *`Cleanup`* Vorgang ausgeführt wird. Die Lambda-Protokollgruppe wird 30 Tage lang aufbewahrt oder bis sie manuell gelöscht wird.

Anweisungen

Das Runbook ist ein Hilfsprogramm, das als untergeordnete Automatisierung innerhalb anderer Runbooks ausgeführt werden kann. Es erleichtert die Erstellung einer Infrastruktur, die es dem übergeordneten Runbook ermöglicht, API-Aufrufe der Amazon EKS K8-Steuerebene durchzuführen. Um das Runbook zu verwenden, können Sie die folgenden Schritte im Kontext der übergeordneten Automatisierung ausführen.

1. Einrichtungsphase: Rufen Sie die Automatisierung mithilfe eines `aws:executeAutomation` Aktionsvorgangs aus dem Runbook auf, das API-Aufrufe der Amazon EKS K8-Steuerungsebene durchführen möchte, wobei der Vorgang auf eingestellt ist. `Setup`

   Beispiel für Eingabeparameter:

   ```
   {
     "AutomationAssumeRole": "<role-arn>",
     "ClusterName": "<eks-cluster-name>",
     "Operation": "Setup"
   }
   ```

   Die Ausgabe des `aws:executeAutomation` Schritts enthält den ARN der Proxy-Lambda-Funktion.

2. Verwenden des Lambda-Proxys: Rufen Sie die Lambda-Funktion innerhalb der `aws:executeScript` Aktion mithilfe von `boto3` s `Lambda.Client.invoke(...)` mit einer Liste von API-Aufrufpfaden und Bearer-Token auf. Die Lambda-Funktion führt `GET` HTTP-Aufrufe an den angegebenen Pfad durch, indem sie das Bearer-Token als Teil des Autorisierungsheaders übergibt.

   Beispiel für ein Lambda-Aufrufereignis:

   ```
   {
       "ApiCalls": ["/api/v1/pods/", ...],
       "BearerToken": "..."
   }
   ```

   > **Note**
   >
   > Das Bearer-Token muss als Teil des übergeordneten Automatisierungsskripts generiert werden. Sie müssen sicherstellen, dass der Principal, der das übergeordnete Runbook ausführt, nur Leseberechtigungen für den angegebenen Amazon EKS-Cluster hat.

3. Bereinigungsphase: Rufen Sie die Automatisierung mithilfe eines `aws:executeAutomation` Aktionsvorgangs aus dem Runbook auf, das API-Aufrufe der Amazon EKS K8-Steuerungsebene durchführen möchte, wobei der Vorgang auf eingestellt ist. `Cleanup`

   Beispiel für Eingabeparameter:

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Cleanup"
}
```

Schritte zur Automatisierung

1. ValidateExecution
   - Überprüft, ob die Automatisierung nicht als eigenständige Ausführung ausgeführt wird.
2. CheckForExistingStack
   - Prüft, ob bereits ein CloudFormation Stack für den angegebenen Clusternamen bereitgestellt wurde.
   - Gibt den Status des Stacks zurück und gibt an, ob er sicher gelöscht werden kann.
3. BranchOnIsStackExists
   - Entscheidungsschritt, der auf der Grundlage der Stack-Existenz verzweigt.
   - Routen, um entweder den vorhandenen Stacknamen zu aktualisieren oder mit der Operationsverzweigung fortzufahren.
4. UpdateStackName
   - Aktualisiert die `StackName` Variable mit dem Namen des vorhandenen Stacks.
   - Wird nur ausgeführt, wenn der Stapel bereits existiert.
5. BranchOnOperation
   - Leitet die Automatisierung auf der Grundlage des `Operation` Parameters (`Setup`/`Cleanup`) weiter.
   - Für`Setup`: Routen, um entweder einen neuen Stack zu erstellen oder bestehende Ressourcen zu beschreiben.
   - Für`Cleanup`: Wird mit dem Löschen des Stapels fortgefahren, sofern das Löschen sicher ist.
6. GetClusterNetworkConfig
   - Beschreibt den Amazon EKS-Cluster zum Abrufen der VPC-Konfiguration.
   - Ruft Endpunkt-, VPC-ID-, Subnetz- IDs, Sicherheitsgruppen-ID- und CA-Daten ab.
7. ProvisionResources
   - Erstellt einen CloudFormation Stack mit den erforderlichen Ressourcen.

- Stellt die Lambda-Funktion mit der erforderlichen Netzwerkkonfiguration bereit.
- Markiert alle Ressourcen zur Nachverfolgung und Verwaltung.

8. DescribeStackResources
   - Ruft Informationen über den created/existing Stack ab.
   - Ruft den ARN der bereitgestellten Lambda-Funktion ab.
9. BranchOnIsLambdaDeploymentRequired
   - Ermittelt, ob die Bereitstellung von Lambda-Code erforderlich ist.
   - Geht nur bei neu erstellten Stacks zur Bereitstellung über.
10. DeployLambdaFunctionCode
    - Stellt den Lambda-Funktionscode mithilfe des Bereitstellungspakets bereit.
    - Aktualisiert die Funktion mit der Proxyimplementierung.
11. AssertLambdaAvailable
    - Überprüft, ob das Update des Lambda-Funktionscodes erfolgreich war.
    - Wartet darauf, dass sich die Funktion im Status befindet. `Successful`
12. PerformStackCleanup
    - Löscht den CloudFormation Stapel und die zugehörigen Ressourcen.
    - Wird während des `Cleanup` Betriebs oder bei Ausfall des `Setup` Vorgangs ausgeführt.

Ausgaben

LambdaFunctionArn: ARN der Proxy-Lambda-Funktion

Referenzen

Systems Manager Automation

- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

AWSSupport-TroubleshootEbsCsiDriversForEks

Beschreibung

Das `AWSSupport-TroubleshootEbsCsiDriversForEks` Runbook hilft bei der Behebung von Problemen mit Amazon Elastic Block Store-Volume-Mounts in Amazon Elastic Kubernetes Service (Amazon EKS) und Amazon EBS Container Storage Interface (CSI) -Treiberproblemen

> **Important**
>
> Derzeit wird der Amazon EBS CSI-Treiber, auf dem ausgeführt AWS Fargate wird, nicht unterstützt.

Wie funktioniert es?

Das Runbook `AWSSupport-TroubleshootEbsCsiDriversForEks` führt die folgenden allgemeinen Schritte aus:

- Überprüft, ob der Amazon EKS-Zielcluster vorhanden ist und sich im aktiven Zustand befindet.
- Stellt die erforderlichen Authentifizierungsressourcen für Kubernetes-API-Aufrufe bereit, je nachdem, ob das Addon von Amazon EKS verwaltet oder selbst verwaltet wird.
- Führt Integritätsprüfungen und Diagnosen für den Amazon EBS CSI-Controller durch.
- Führt IAM-Berechtigungsprüfungen für Knotenrollen und Dienstkontorollen durch.
- Diagnostiziert dauerhafte Probleme bei der Volume-Erstellung für den angegebenen Anwendungs-Pod.
- Überprüft die node-to-pod Planung und untersucht Pod-Ereignisse.
- Sammelt relevante Kubernetes- und Anwendungsprotokolle und lädt sie in den angegebenen Amazon S3 S3-Bucket hoch.
- Führt Knotenzustandsprüfungen durch und verifiziert die Konnektivität mit Amazon EC2 EC2-Endpunkten.
- Überprüft persistente Volume Block-Geräteanhänge und den Montagestatus.
- Bereinigt die Authentifizierungsinfrastruktur, die während der Fehlerbehebung erstellt wurde.
- Generiert einen umfassenden Bericht zur Fehlerbehebung, in dem alle Diagnoseergebnisse zusammengefasst sind.

Note

- Der Authentifizierungsmodus des Amazon EKS-Clusters muss entweder auf `API` oder eingestellt sein`API_AND_CONFIG_MAP`. Wir empfehlen, den Amazon EKS Access-Eintrag zu verwenden. Das Runbook benötigt Kubernetes-Berechtigungen zur rollenbasierten Zugriffskontrolle (RBAC), um die erforderlichen API-Aufrufe durchzuführen.
- Wenn Sie keine IAM-Rolle für die Lambda-Funktion (`LambdaRoleArn`Parameter) angeben, erstellt die Automatisierung eine Rolle, die `Automation-K8sProxy-Role-<ExecutionId>` in Ihrem Konto benannt ist. Diese Rolle umfasst die verwalteten Richtlinien `AWSLambdaBasicExecutionRole` und. `AWSLambdaVPCAccessExecutionRole`
- Für einige Diagnoseschritte müssen die Amazon EKS-Worker-Knoten von Systems Manager verwaltete Instances sein. Wenn es sich bei den Knoten nicht um von Systems Manager verwaltete Instanzen handelt, werden Schritte, für die Systems Manager Manager-Zugriff erforderlich ist, übersprungen, andere Prüfungen werden jedoch fortgesetzt.
- Die Automatisierung umfasst einen Bereinigungsschritt, bei dem die Ressourcen der Authentifizierungsinfrastruktur entfernt werden. Dieser Bereinigungsschritt wird auch dann ausgeführt, wenn die vorherigen Schritte fehlschlagen, wodurch verhindert wird, dass Ressourcen in Ihrem Konto verwaist sind. AWS

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Erstellen Sie eine SSM-Automatisierungsrolle `TroubleshootEbsCsiDriversForEks-SSM-Role` in Ihrem Konto. Überprüfen Sie, dass die Vertrauensstellung die folgende Richtlinie enthält.

   JSON

   ```
   {
       "Version":"2012-10-17",
       "Statement": [
           {
               "Sid": "",
               "Effect": "Allow",
               "Principal": {
                   "Service": "ssm.amazonaws.com"
               },
               "Action": "sts:AssumeRole"
           }
       ]
   }
   ```

2. Fügen Sie der IAM-Rolle die folgende Richtlinie hinzu, um die erforderlichen Berechtigungen für die Ausführung der angegebenen Aktionen auf den angegebenen Ressourcen zu gewähren.

   - Wenn Sie erwarten, Ausführungs- und Ressourcenprotokolle in derselben AWS Region in den Amazon S3 S3-Bucket hochzuladen, ersetzen Sie `arn:{partition}:s3:::BUCKET_NAME/*` diese durch Ihre in`OptionalRestrictPutObjects`.
     - Der Amazon S3 S3-Bucket sollte auf den richtigen Amazon S3 S3-Bucket verweisen, wenn Sie `S3BucketName` in SSM-Ausführung auswählen.
     - Diese Berechtigung ist optional, wenn Sie sie nicht angeben `S3BucketName`
     - Der Amazon S3 S3-Bucket muss privat sein und sich in derselben AWS Region befinden, in der Sie die SSM-Automatisierung ausführen.

   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. Erteilen Sie die erforderlichen Berechtigungen für Amazon EKS-Cluster RBAC (Role-Based Access Control). Der empfohlene Ansatz besteht darin, einen Access-Eintrag in Ihrem Amazon EKS-Cluster zu erstellen.

   Navigieren Sie in der Amazon EKS-Konsole zu Ihrem Cluster. Stellen Sie für Amazon EKS-Zugriffseinträge sicher, dass Ihre Zugriffskonfiguration auf `API_AND_CONFIG_MAP` oder eingestellt ist`API`. Schritte zur Konfiguration des Authentifizierungsmodus für Zugriffseinträge finden Sie unter Zugangseinträge einrichten.

   Wählen Sie Zugriffseintrag erstellen aus.

   - Wählen Sie für den IAM-Prinzipal-ARN die IAM-Rolle aus, die Sie im vorherigen Schritt für die SSM-Automatisierung erstellt haben.
   - Wählen Sie als Typ die Option aus `Standard`.
4. Fügen Sie eine Zugriffsrichtlinie hinzu:
   - Wählen Sie als Zugriffsbereich die Option aus`Cluster`.
   - Wählen Sie als Richtlinienname die Option aus`AmazonEKSAdminViewPolicy`.

Wählen Sie Richtlinie hinzufügen aus.

Wenn Sie keine Zugriffseinträge zur Verwaltung von Kubernetes-API-Berechtigungen verwenden, müssen Sie die aktualisieren `aws-auth` ConfigMap und eine Rollenbindung zwischen Ihrem IAM-Benutzer oder Ihrer IAM-Rolle erstellen. Stellen Sie sicher, dass Ihre IAM-Entität über die folgenden schreibgeschützten Kubernetes-API-Berechtigungen verfügt:

- GET `/apis/apps/v1/namespaces/{namespace}/deployments/{name}`
- GET `/apis/apps/v1/namespaces/{namespace}/replicasets/{name}`
- GET `/apis/apps/v1/namespaces/{namespace}/daemonsets/{name}`
- GET `/api/v1/nodes/{name}`
- GET `/api/v1/namespaces/{namespace}/serviceaccounts/{name}`
- GET `/api/v1/namespaces/{namespace}/persistentvolumeclaims/{name}`
- GET `/api/v1/persistentvolumes/{name}`
- GET `/apis/storage.k8s.io/v1/storageclasses/{name}`
- GET `/api/v1/namespaces/{namespace}/pods/{name}`
- GET `/api/v1/namespaces/{namespace}/pods`
- GET `/api/v1/namespaces/{namespace}/pods/{name}/log`
- GET `/api/v1/events`

5. Führen Sie die Automatisierung aus (Konsole) AWSSupport-TroubleshootEbsCsiDriversForEks
6. Wählen Sie Execute automation (Automatisierung ausführen).
7. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es SSM Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Die Rolle muss Ihrem Amazon EKS-Clusterzugriffseintrag oder Ihrer RBAC-Berechtigung hinzugefügt werden, um Kubernetes-API-Aufrufe zuzulassen.
     - Typ: `AWS::IAM::Role::Arn`
     - Beispiel: `TroubleshootEbsCsiDriversForEks-SSM-Role`
   - EksClusterName:
     - Beschreibung: Der Name des Amazon Elastic Kubernetes Service (Amazon EKS) -Zielclusters.
     - Typ: `String`

- ApplicationPodName:
  - Beschreibung: Der Name des Kubernetes-Anwendungs-Pods, der Probleme mit dem Amazon EBS CSI-Treiber hat.
  - Typ: `String`
- ApplicationNamespace:
  - Beschreibung: Der Kubernetes-Namespace für den Anwendungs-Pod hat Probleme mit dem Amazon EBS CSI-Treiber.
  - Typ: `String`
- EbsCsiControllerDeploymentName(Optional):
  - Beschreibung: (Optional) Der Bereitstellungsname für den Amazon EBS CSI-Controller-Pod.
  - Typ: `String`
  - Standard: `ebs-csi-controller`
- EbsCsiControllerNamespace(Optional):
  - Beschreibung: (Optional) Der Kubernetes-Namespace für den Amazon EBS CSI-Controller-Pod.
  - Typ: `String`
  - Standard: `kube-system`
- S3 (optional)BucketName :
  - Beschreibung: (Optional) Der Name des Amazon S3 S3-Ziel-Buckets, in den die Fehlerbehebungsprotokolle hochgeladen werden.
  - Typ: `AWS::S3::Bucket::Name`
- LambdaRoleArn (Optional):
  - Beschreibung: (Optional) Der ARN der IAM-Rolle, der der AWS Lambda Funktion den Zugriff auf die erforderlichen AWS Dienste und Ressourcen ermöglicht.
  - Typ: `AWS::IAM::Role::Arn`

Wählen Sie Ausführen aus.

8. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Outputs die detaillierten Ergebnisse der Ausführung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

Weitere Informationen zum Amazon EBS CSI-Treiber finden Sie unter Amazon EBS CSI-Treiber.

AWSSupport-TroubleshootEKSALBControllerIssues

Beschreibung

Das `AWSSupport-TroubleshootEKSALBControllerIssues` Automation Runbook hilft bei der Diagnose häufiger Probleme, die verhindern, dass der Load AWS Balancer Controller Application Load Balancer (ALB) und Network Load Balancer (NLB) für Kubernetes-Ingresses und -Services ordnungsgemäß bereitstellt und verwaltet.

Dieses Runbook überprüft wichtige Komponenten wie die Einrichtung end-to-end des OIDC-Identitätsanbieters, die IRSA-Konfiguration, die Netzwerkvoraussetzungen, die Konfiguration und die Ressourcenkontingente. ingress/service Es erfasst auch Controller-Logs und relevante Kubernetes-Ressourcenkonfigurationen, um Fehlkonfigurationen oder Betriebsprobleme zu identifizieren.

> **Important**
>
> Dieses Automatisierungs-Runbook wurde für Amazon EKS-Cluster entwickelt, die Amazon Elastic Compute Cloud (Amazon EC2) -Knotengruppen verwenden, und unterstützt derzeit keine Cluster, auf denen ausgeführt wird. AWS Fargate

Wie funktioniert es?

Das Runbook `AWSSupport-TroubleshootEKSALBControllerIssues` führt die folgenden allgemeinen Schritte aus:

- Überprüft den Amazon EKS-Clusterstatus, die Konfiguration des Zugriffseintrags und die Einrichtung des OIDC-Anbieters.
- Erstellt einen temporären Lambda-Proxy für die Kubernetes-API-Kommunikation.
- Überprüft die Bereitstellung des Load AWS Balancer Controllers und die Konfiguration des Dienstkontos.

- Überprüft die Pod-Identität, den Webhook und die IAM-Rolleninjektion.
- Überprüft die Subnetzkonfiguration und das Tagging für die Bereitstellung von Application Load Balancer und Network Load Balancer.
- Vergleicht die Kontokontingente für Application Load Balancer und Network Load Balancer mit der aktuellen Nutzung.
- Überprüft Anmerkungen zu Eingangs- und Serviceressourcen.
- Überprüft das Tagging von Worker-Knoten-Sicherheitsgruppen auf die Load Balancer-Integration.
- Sammelt Controller-Pod-Protokolle für Diagnosen.
- Bereinigt temporäre Authentifizierungsressourcen.
- Generiert einen Diagnosebericht mit Ergebnissen und Korrekturmaßnahmen.

> **Note**
>
> - Für den Amazon EKS-Cluster muss ein Zugriffseintrag für die IAM-Entität konfiguriert sein, die diese Automatisierung ausführt. Der Authentifizierungsmodus des Clusters muss entweder auf `API` oder `API_AND_CONFIG_MAP` eingestellt sein. Ohne die richtige Konfiguration des Zugriffseintrags wird die Automatisierung bei der ersten Validierung beendet.
> - Der `LambdaRoleArn` Parameter ist erforderlich und muss über die AWS verwalteten Richtlinien verfügen `AWSLambdaBasicExecutionRole` und `AWSLambdaVPCAccessExecutionRole` angehängt sein, damit die Proxyfunktion mit der Kubernetes-API kommunizieren kann.
> - Der AWS Load Balancer Controller muss Version `v2.1.1` oder höher sein.
> - Die Automatisierung umfasst einen Bereinigungsschritt, bei dem temporäre Infrastrukturressourcen für die Authentifizierung entfernt werden. Dieser Bereinigungsschritt wird auch dann ausgeführt, wenn die vorherigen Schritte fehlschlagen, und stellt so sicher, dass keine verwaisten Ressourcen in Ihrem Konto verbleiben. AWS

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren und auszuführen:

> **Note**
>
> Gehen Sie vor dem Ausführen der Automatisierung folgendermaßen vor, um die erforderlichen IAM-Rollen zu konfigurieren: eine für Systems Manager Automation, um das Runbook auszuführen, und eine weitere für Lambda, um mit der Kubernetes-API zu kommunizieren:
>
> 1. Erstellen Sie eine SSM-Automatisierungsrolle in Ihrem Konto. `TroubleshootEKSALBController-SSM-Role` Überprüfen Sie, dass die Vertrauensstellung die folgende Richtlinie enthält.

```
{
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ssm.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
```

2. Fügen Sie die folgende IAM-Richtlinie bei, um die erforderlichen Berechtigungen zu gewähren:

```
{
            "Version": "2012-10-17",
            "Statement": [{
                "Sid": "TroubleshootEKSALBControllerIssuesActions",
                "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. Konfigurieren Sie den Zugriffseintrag für Ihren Amazon EKS-Cluster. Dies ist eine zwingende Voraussetzung für die Automatisierung. Schritte zur Konfiguration des Authentifizierungsmodus für Zugriffseinträge finden Sie unter Zugangseinträge einrichten.

   Navigieren Sie in der Amazon EKS-Konsole zu Ihrem Cluster und gehen Sie wie folgt vor:

   - Stellen Sie im Abschnitt Zugriff sicher, dass Ihre Authentifizierungskonfiguration entweder auf `API` oder eingestellt ist`API_AND_CONFIG_MAP`.
   - Wählen Sie Zugangseintrag erstellen und konfigurieren Sie:
     - Wählen Sie für den IAM-Prinzipal-ARN die IAM-Rolle aus, die Sie erstellt haben ()`TroubleshootEKSALBController-SSM-Role`.
     - Wählen Sie als Typ die Option aus `Standard`.
   - Fügen Sie eine Zugriffsrichtlinie hinzu:
     - Wählen Sie als Richtlinienname die Option aus`AmazonEKSAdminViewPolicy`.
     - Wählen Sie als Zugriffsbereich die Option aus`Cluster`.
   - Wählen Sie Richtlinie hinzufügen aus.
   - Überprüfen Sie die Details und wählen Sie Erstellen aus.

4. Erstellen Sie eine IAM-Rolle für die Lambda-Funktion (referenziert wie `LambdaRoleArn` in den Eingabeparametern):
   - Erstellen Sie eine neue IAM-Rolle mit der folgenden Vertrauensrichtlinie:

```
{
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "lambda.amazonaws.com"
                    },
```

```
                "Action": "sts:AssumeRole"
            }
        ]
    }
```

- Fügen Sie dieser Rolle die folgenden AWS verwalteten Richtlinien hinzu:
  - `AWSLambdaBasicExecutionRole`
  - `AWSLambdaVPCAccessExecutionRole`
- Notieren Sie sich den ARN dieser Rolle, da Sie ihn für den `LambdaRoleArn` Eingabeparameter benötigen.

1. Navigieren Sie AWSSupport-TroubleshootEKSALBControllerIssuesin der AWS Systems Manager Manager-Konsole zu.
2. Wählen Sie Automatisierung ausführen.
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Typ:: AWS::IAM::Role: Arn

     Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

     Zulässiges Muster: ^arn :(? :aws|aws-cn|aws-us-gov) :iam::\ d {12} :role/? [a-zA-Z_0-9+=, .@\ -_/] +$
   - EksClusterName (Erforderlich):

     Typ: Zeichenfolge

     Beschreibung: (Erforderlich) Name des Amazon Elastic Kubernetes Service (Amazon EKS) -Clusters.

     Zulässiges Muster: ^ [0-9A-Za-Z] [A-Za-Z0-9-_] {0,99} $
   - ALBControllerDeploymentName (Fakultativ):

     Typ: Zeichenfolge

Beschreibung: (Optional) Der Name der Load AWS Balancer Controller-Bereitstellung in Ihrem Amazon EKS-Cluster. Dies ist normalerweise 'aws-load-balancer-controller', sofern Sie ihn nicht während der Installation angepasst haben.

Zulässiges Muster: ^ [a-z0-9] ([-.a-z0-9] {0,251} [a-z0-9])? $

Standard: aws-load-balancer-controller

- ALBControllerNamespace (optional):

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Kubernetes-Namespace, in dem der Load AWS Balancer Controller bereitgestellt wird. Standardmäßig ist dies 'kube-system', aber es kann anders sein, wenn Sie den Controller in einem benutzerdefinierten Namespace installiert haben.

  Zulässiges Muster: ^ [a-z0-9] ([-a-z0-9] {0,61} [a-z0-9])? $

  Standard: kube-system

- ServiceAccountName (Fakultativ):

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des Kubernetes-Dienstkontos, das dem AWS Load Balancer Controller zugeordnet ist. Dies ist normalerweise 'aws-load-balancer-controller', sofern er nicht während der Installation angepasst wurde.

  Zulässiges Muster: ^ [a-z0-9] ([-.a-z0-9] {0,251} [a-z0-9])? $

  Standard: aws-load-balancer-controller

- ServiceAccountNamespace (Fakultativ):

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Kubernetes-Namespace, in dem sich das Dienstkonto für den Load AWS Balancer Controller befindet. Dies ist in der Regel „kube-system“, kann sich jedoch unterscheiden, wenn Sie einen benutzerdefinierten Namespace verwendet haben.

  Zulässiges Muster: ^ [a-z0-9] ([-a-z0-9] {0,61} [a-z0-9])? $

  Standard: kube-system

- IngressName (Fakultativ):

  Typ: Zeichenfolge

  Beschreibung: (Optional) Name der zu validierenden Ingress-Ressource (Application Load Balancer). Wenn nicht angegeben, wird die Eingangsvalidierung übersprungen.

  Zulässiges Muster: ^$|^ [a-z0-9] [a-z0-9.-] {0,251} [a-z0-9] $

  Standard: „“ (leere Zeichenfolge)
- IngressNamespace (Fakultativ):

  Typ: Zeichenfolge

  Beschreibung: (Optional) Namespace der Ingress-Ressource. Erforderlich, wenn `IngressName` angegeben.

  Zulässiges Muster: ^$|^ [a-z0-9] [a-z0-9-] {0,61} [a-z0-9] $

  Standard: „“ (leere Zeichenfolge)
- ServiceName (Fakultativ):

  Typ: Zeichenfolge

  Beschreibung: (Optional) Name einer bestimmten Dienstressource zur Überprüfung von Network Load Balancer (Network Load Balancer) -Annotationen. Wenn nicht angegeben, wird die Überprüfung der Dienstressourcen übersprungen.

  Zulässiges Muster: ^$|^ [a-z0-9] [a-z0-9.-] {0,251} [a-z0-9] $

  Standard: „“ (leere Zeichenfolge)
- ServiceNamespace (Fakultativ):

  Typ: Zeichenfolge

  Beschreibung: (Optional) Namespace der Dienstressource. Erforderlich, wenn `ServiceName` angegeben.

  Zulässiges Muster: ^$|^ [a-z0-9] [a-z0-9-] {0,61} [a-z0-9] $

  Standard: „“ (leere Zeichenfolge)

- LambdaRoleArn (Erforderlich):

  Typ:: AWS::IAM::Role: Arn

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, der der AWS Lambda (Lambda-) Funktion den Zugriff auf die erforderlichen AWS Dienste und Ressourcen ermöglicht. Ordnen Sie die AWS verwalteten Richtlinien: `AWSLambdaBasicExecutionRole` und Ihrer `AWSLambdaVPCAccessExecutionRole` IAM-Rolle für die Ausführung der Lambda-Funktion zu.

  Zulässiges Muster: ^arn :(? :aws|aws-cn|aws-us-gov) :iam::\ d {12} :role/? [a-zA-Z_0-9+=, .@\ -_/] +$

4. Wählen Sie Ausführen.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   a. ValidateAccessEntryAndOIDCProvider:

      Validiert das Amazon EKS-Cluster-IAM-Setup, indem die Zugriffsberechtigungen und die OIDC-Anbieterkonfiguration überprüft werden.

   b. sAuthenticationClientK8 einrichten:

      Führen Sie das SAW-Dokument AWSSupport-SetupK 8 sApiProxy für EKS aus, um eine Lambda-Funktion für die Ausführung von Amazon EKS-API-Aufrufen auf dem Cluster einzurichten.

   c. Überprüfen undALBController: IRSASetup

      Überprüft, ob der angegebene Service Account & Application Load Balancer Balancer-Controller in ihren jeweiligen Namespaces vorhanden ist. Überprüft auch die Service Account Role Annotation & Trust-Richtlinie des Application Load Balancer Balancer-Controllers.

   d. VerifyPodIdentityWebhookAndEnv:

      Prüft, ob pod-identity-webhook läuft. Überprüft auch, ob IRSA in die ENV-Variablen des Pods eingefügt wurde.

   e. ValidateSubnetRequirements:

      Prüft mindestens zwei Subnetze in zwei AZs mit 8 verfügbaren IP-Adressen. Für Load Balancer ist die richtige Subnetzkennzeichnung vorhanden. public/private

f. CheckLoadBalancerLimitsAndUsage:

   Vergleichen Sie das Kontolimit mit der Anzahl der Application Load Balancer und Network Load Balancer.

g. CheckIngressOrServiceAnnotations:

   Überprüft die Ingress- und Service-Ressourcen auf korrekte Anmerkungen und Spezifikationen, um sicherzustellen, dass sie für die Verwendung von Application Load Balancer und Network Load Balancer ordnungsgemäß konfiguriert sind.

h. CheckWorkerNodeSecurityGroupTags:

   Stellen Sie sicher, dass genau eine Sicherheitsgruppe, die an die Worker-Knoten angehängt ist, über das erforderliche Cluster-Tag verfügt.

i. ALBControllerProtokolle erfassen:

   Ruft die neuesten Diagnoseprotokolle von den Load AWS Balancer Controller-Pods ab, die im Amazon EKS-Cluster ausgeführt werden.

j. CleanUp K8: sAuthenticationClient

   Führt das SAW-Dokument 'AWSSupport-SetupK8 sApiProxy für Eks' mithilfe der Operation 'Cleanup' aus, um Ressourcen zu bereinigen, die im Rahmen der Automatisierung erstellt wurden.

k. GenerateReport:

   Generiert den Automatisierungsbericht.

7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   a. Bericht:

      Bietet eine umfassende Zusammenfassung aller durchgeführten Prüfungen, einschließlich des Status des Amazon EKS-Clusters, der Einrichtung des Application Load Balancer Controllers, der IRSA-Konfiguration, der Subnetzanforderungen, der Load Balancer-Grenzwerte, ingress/service Anmerkungen, Worker-Node-Sicherheitsgruppen-Tags und der Application Load Balancer Controller-Protokolle. Es enthält auch alle identifizierten Probleme und empfohlene Schritte zur Behebung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

Dokumentation zum AWS Load Balancer Controller

- AWS Load Balancer Balancer-Controller
- Zugangseinträge einrichten

Elastic Beanstalk

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Elastic Beanstalk Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-CollectElasticBeanstalkLogs
- AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming
- AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications
- AWSSupport-TroubleshootElasticBeanstalk

`AWSSupport-CollectElasticBeanstalkLogs`

Beschreibung

Das `AWSSupport-CollectElasticBeanstalkLogs` Runbook sammelt AWS Elastic Beanstalk zugehörige Protokolldateien aus einer Amazon Elastic Compute Cloud (Amazon EC2) Windows Server -Instance, die von Elastic Beanstalk gestartet wurde, um Sie bei der Behebung häufiger Probleme zu unterstützen. Während die Automatisierung die zugehörigen Protokolldateien sammelt, werden Änderungen an der Dateisystemstruktur vorgenommen, einschließlich der Erstellung temporärer Verzeichnisse, des Kopierens von Protokolldateien in die temporären Verzeichnisse

und der Komprimierung der Protokolldateien in ein Archiv. Diese Aktivität kann zu einer erhöhten Auslastung der `CPUUtilization` Amazon EC2 EC2-Instance führen. Weitere Informationen zu finden Sie `CPUUtilization` unter Instance-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Wenn Sie einen Wert für den `S3BucketName` Parameter angeben, bewertet die Automatisierung den Richtlinienstatus des von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Buckets. Um die Sicherheit der von Ihrer Amazon EC2 EC2-Instance gesammelten Protokolle zu gewährleisten, werden die Protokolle nicht hochgeladen`true`, wenn der Richtlinienstatus auf gesetzt `isPublic` ist oder wenn die Zugriffskontrollliste (ACL) der vordefinierten `All Users` Amazon S3 S3-Gruppe `READ|WRITE` Berechtigungen gewährt. Weitere Informationen zu vordefinierten Amazon S3 S3-Gruppen finden Sie unter Amazon S3 S3-vordefinierte Gruppen im Amazon Simple Storage Service-Benutzerhandbuch.

Wenn Sie keinen Wert für den `S3BucketName` Parameter angeben, lädt die Automatisierung das Log-Bundle in den standardmäßigen Elastic Beanstalk Amazon S3 S3-Bucket hoch, in AWS-Region dem Sie die Automatisierung ausführen. Das Verzeichnis ist nach der folgenden Struktur benannt:. `elasticbeanstalk-` *`region`* `-` *`accountID`* Die *`accountID`* Werte *`region`* und unterscheiden sich je nach Region, in der AWS-Konto Sie die Automatisierung ausführen. Das Protokollpaket wird im `resources/environments/logs/bundle/` *`environmentID`* `/` *`instanceID`* Verzeichnis gespeichert. Die *`instanceID`* Werte *`environmentID`* und unterscheiden sich je nach Ihrer Elastic Beanstalk Beanstalk-Umgebung und der Amazon EC2 EC2-Instance, von der Sie Logs sammeln.

Standardmäßig verfügt das AWS Identity and Access Management (IAM-) Instance-Profil, das an die Amazon EC2 EC2-Instances der Elastic Beanstalk-Umgebung angehängt ist, über die erforderlichen Berechtigungen, um das Bundle in den standardmäßigen Elastic Beanstalk Amazon S3 S3-Bucket für Ihre Umgebung hochzuladen. Wenn Sie einen Wert für den `S3BucketName` Parameter angeben, muss das der Amazon EC2 EC2-Instance zugeordnete Instance-Profil die `s3:PutObject` Aktionen`s3:GetBucketAcl`, `s3:GetBucketPolicys3:GetBucketPolicyStatus`, und für den angegebenen Amazon S3 S3-Bucket und -Pfad zulassen.

> **Note**
>
> Für diese Automatisierung sind mindestens 500 MB verfügbarer Festplattenspeicher auf dem Amazon Elastic Block Store (Amazon EBS) -Stammvolume erforderlich, das an Ihre Amazon EC2 EC2-Instance angehängt ist. Wenn auf dem Root-Volume nicht genügend Festplattenspeicher verfügbar ist, wird die Automatisierung gestoppt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EnvironmentId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID Ihrer Elastic Beanstalk Beanstalk-Umgebung, aus der Sie das Log-Bundle sammeln möchten.
- InstanceId

  Typ: Zeichenfolge

  (Erforderlich) Die ID der Amazon EC2 EC2-Instance in Ihrer Elastic Beanstalk Beanstalk-Umgebung, aus der Sie das Protokollpaket abrufen möchten.
- S3 BucketName

  Typ: Zeichenfolge

  (Optional) Der Amazon S3 S3-Bucket, in den Sie die archivierten Protokolle hochladen möchten.
- S3 BucketPath

Typ: Zeichenfolge

(Optional) Der Amazon S3 S3-Bucket-Pfad, in den Sie das Protokollpaket hochladen möchten. Dieser Parameter wird ignoriert, wenn Sie keinen Wert für den `S3BucketName` Parameter angeben.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`

Dokumentschritte

- `aws:assertAwsResourceProperty`— Bestätigt, dass die Amazon EC2 EC2-Instance, die Sie im `InstanceId` Parameter angeben, von AWS Systems Manager verwaltet wird.
- `aws:assertAwsResourceProperty`— Bestätigt, dass es sich bei der Amazon EC2-Instance, die Sie im `InstanceId` Parameter angeben, um eine Windows Server Instance handelt.
- `aws:runCommand`— Prüft, ob die Instance Teil einer Elastic Beanstalk Beanstalk-Umgebung ist, ob ausreichend Speicherplatz vorhanden ist, um die Protokolle zu bündeln, und ob der Amazon S3 S3-Bucket, in den die Logs hochgeladen werden sollen, öffentlich ist.
- `aws:runCommand`- Sammelt die Protokolldateien und lädt das Archiv in den im `S3BucketName` Parameter angegebenen Amazon S3 S3-Bucket oder in den Standard-Bucket für Ihre Elastic Beanstalk Beanstalk-Umgebung hoch, falls kein Wert angegeben ist.

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

Beschreibung

Das `AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming` Runbook ermöglicht die Protokollierung in der von Ihnen angegebenen Umgebung AWS Elastic Beanstalk (Elastic Beanstalk).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- EnvironmentId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Elastic Beanstalk Beanstalk-Umgebung, für die Sie die Anmeldung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert die Protokollierung in der Elastic Beanstalk Beanstalk-Umgebung, die Sie im `EnvironmentId` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich der Status der Umgebung ändert. `Ready`
- `aws:executeScript`— Überprüft, ob die Protokollierung in der Elastic Beanstalk Beanstalk-Umgebung aktiviert wurde.

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

Beschreibung

Das `AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications` Runbook aktiviert Benachrichtigungen für die von Ihnen angegebene AWS Elastic Beanstalk (Elastic Beanstalk-) Umgebung.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- EnvironmentId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Elastic Beanstalk Beanstalk-Umgebung, für die Sie Benachrichtigungen aktivieren möchten.
- TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon Simple Notification Service (Amazon SNS) -Themas, an das Sie Benachrichtigungen senden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert Benachrichtigungen für die Elastic Beanstalk Beanstalk-Umgebung, die Sie im `EnvironmentId` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich der Status der Umgebung ändert. `Ready`

- `aws:executeScript`— Überprüft, ob Benachrichtigungen für die Elastic Beanstalk Beanstalk-Umgebung aktiviert wurden.

AWSSupport-TroubleshootElasticBeanstalk

Beschreibung

Das `AWSSupport-TroubleshootElasticBeanstalk` Runbook hilft Ihnen bei der Behebung der möglichen Gründe, warum sich Ihre AWS Elastic Beanstalk Umgebung im Status „oder“ befindet. `Degraded` `Severe` Diese Automatisierung überprüft die folgenden AWS Ressourcen, die mit Ihrer Elastic Beanstalk Beanstalk-Umgebung verknüpft sind:

- Konfigurationsdetails für einen Load Balancer, einen AWS CloudFormation Stack, eine Amazon EC2 Auto Scaling Scaling-Gruppe, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und eine Virtual Private Cloud (VPC).
- Probleme mit der Netzwerkkonfiguration mit den zugehörigen Sicherheitsgruppenregeln, Routing-Tabellen und Netzwerkzugriffskontrolllisten (ACLs), die Ihren Subnetzen zugeordnet sind.
- Überprüft die Konnektivität zu den Elastic Beanstalk Beanstalk-Endpunkten und zum öffentlichen Internetzugang.
- Überprüft den Status des Load Balancers.
- Überprüft den Status der Amazon EC2 EC2-Instances.
- Ruft ein Log-Bundle aus Ihrer Elastic Beanstalk Beanstalk-Umgebung ab und lädt die Dateien optional in. Support

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- ApplicationName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name Ihrer Elastic Beanstalk Beanstalk-Anwendung.

- EnvironmentName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name Ihrer Elastic Beanstalk Beanstalk-Umgebung.

- AWSS3UploaderLink

  Typ: Zeichenfolge

  Beschreibung: (Optional) Eine URL, die Ihnen zur Verfügung gestellt wurde, Support um das Log-Bundle aus Ihrer Elastic Beanstalk Beanstalk-Umgebung hochzuladen. Diese Option ist nur für Kunden verfügbar, die einen Support Plan erworben und einen Support-Fall eröffnet haben.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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*

Dokumentschritte

- aws:executeScript— Überprüft, ob der AWS Identity and Access Management (IAM-) Principal, der die Automatisierung gestartet hat, über die erforderlichen Berechtigungen verfügt, um alle im Runbook definierten Aktionen auszuführen.
- aws:branch— Verzweigt den Workflow auf der Grundlage der Ergebnisse des vorherigen Schritts.
- aws:executeScript- Sammelt Informationen über die Elastic Beanstalk Beanstalk-Umgebung, einschließlich Load Balancer, CloudFormation Stack, Auto Scaling Scaling-Gruppe, Amazon EC2 EC2-Instances und VPC-Konfiguration.
- aws:executeScript- Überprüft die Routing-Tabellen und die mit den Subnetzen in Ihrer VPC ACLs verknüpften Netzwerkverbindungsprobleme.
- aws:executeScript- Überprüft die mit Ihren Amazon EC2-Instances verknüpften Sicherheitsgruppenregeln auf Probleme mit der Netzwerkkonnektivität.
- aws:executeScript- Überprüft die Statuschecks für die Amazon EC2 EC2-Instances.

- `aws:executeScript`- Generiert einen Link für ein Log-Bundle Ihrer Elastic Beanstalk Beanstalk-Umgebung.
- `aws:executeScript`— Lädt das Protokollpaket hoch auf. Support
- `aws:executeScript`- Gibt einen Bericht mit Aktionspunkten aus, der Sie bei der Behebung von Problemen unterstützt, die sich auf den Status Ihrer Elastic Beanstalk Beanstalk-Umgebung auswirken könnten.

Elastic Load Balancing

AWS Systems Manager Automation bietet vordefinierte Runbooks für Elastic Load Balancing. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-DropInvalidHeadersForALB
- AWS-EnableCLBAccessLogs
- AWS-EnableCLBConnectionDraining
- AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing
- AWSConfigRemediation-EnableELBDeletionProtection
- AWSConfigRemediation-EnableLoggingForALBAndCLB
- AWSSupport-TroubleshootCLBConnectivity
- AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing
- AWS-UpdateALBDesyncMitigationMode
- AWS-UpdateCLBDesyncMitigationMode
- AWSSupport-TroubleshootELBHealthChecks

`AWSConfigRemediation-DropInvalidHeadersForALB`

Beschreibung

Das `AWSConfigRemediation-DropInvalidHeadersForALB` Runbook ermöglicht es dem von Ihnen angegebenen Application Load Balancer, HTTP-Header mit ungültigen Headern zu entfernen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LoadBalancerArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Load Balancers, für den Sie ungültige Header löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert die Einstellung „Ungültige Header löschen“ für den Load Balancer, den Sie im Parameter angeben. `LoadBalancerArn`
- `aws:executeScript`— Überprüft, ob die Einstellung „ungültige Header löschen“ auf dem Load Balancer aktiviert wurde, den Sie im Parameter angeben. `LoadBalancerArn`

`AWS-EnableCLBAccessLogs`

Beschreibung

Das `AWS-EnableCLBAccessLogs` Runbook ermöglicht Zugriffsprotokolle für einen Classic Load Balancer.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EmitInterval

  Typ: Ganzzahl

Gültige Werte: 5 | 60

Standard: 60

Beschreibung: (Optional) Das Intervall für die Veröffentlichung der Zugriffsprotokolle in Minuten.

- LoadBalancerNames

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste von Classic Load Balancers, für die Sie Zugriffsprotokolle aktivieren möchten.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon Simple Storage Service (Amazon S3) -Buckets, in dem die Zugriffsprotokolle gespeichert werden.

- S3 BucketPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die logische Hierarchie, die Sie beispielsweise für Ihren Amazon S3 S3-Bucket erstellt habenmy-bucket-prefix/prod. Wenn das Präfix nicht angegeben wird, wird das Protokoll auf der Bucket-Stammebene platziert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert Zugriffsprotokolle für die Classic Load Balancers, die Sie im `LoadBalancerNames` Parameter angeben.

Ausgaben

Aktiviert CLBAccess Protokolle. SuccessesLoadBalancers — Liste der Load Balancer-Namen, für die die Zugriffsprotokolle erfolgreich aktiviert wurden.

Aktivieren Sie CLBAccess Protokolle. FailedLoadBalancers — MapList der Namen der Load Balancer, bei denen die Aktivierung der Zugriffsprotokolle fehlgeschlagen ist, und der Grund für den Fehler.

AWS-EnableCLBConnectionDraining

Beschreibung

Das AWS-EnableCLBConnectionDraining Runbook ermöglicht den Verbindungsabbau auf einem Classic Load Balancer (CLB) bis zum angegebenen Timeout-Wert. Connection Drainings ermöglichen es der CLB, Anfragen während der Übertragung zu bearbeiten, die an Instances gestellt werden, deren Registrierung aufgehoben wird oder deren Status nicht korrekt ist. Der angegebene Timeout ist die Zeit, in der Verbindungen aufrechterhalten werden, bevor die Instance als deregistriert gemeldet wird. Weitere Informationen zum Verbindungsabbau finden Sie unter Connection Draining für Ihren Classic Load Balancer konfigurieren im Benutzerhandbuch für Classic Load Balancer. CLBs

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- LoadBalancerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Load Balancers, für den Sie den Verbindungsabbau aktivieren möchten.

- ConnectionTimeout

  Typ: Ganzzahl

  Gültige Werte: 1—3600

  Standard: 300

  Beschreibung: (Erforderlich) Der Wert für das Verbindungs-Timeout für den Load Balancer. Der Timeout-Wert kann zwischen 1 und 3600 Sekunden festgelegt werden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- ModifyLoadBalancerConnectionDraining (aws:executeAwsApi): Aktiviert den Verbindungsabbau und legt den angegebenen Timeout-Wert für den von Ihnen angegebenen Load Balancer fest.
- VerifyLoadBalancerConnectionDrainingEnabled(aws: assertAwsResource Eigenschaft): Überprüft, ob der Verbindungsabbau für den Load Balancer aktiviert ist.
- VerifyLoadBalancerConnectionDrainingTimeout(aws: assertAwsResource Property): Überprüft, ob der Wert für das Verbindungs-Timeout für den Load Balancer dem von Ihnen angegebenen Wert entspricht.

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

Beschreibung

Das `AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` Runbook ermöglicht zonenübergreifendes Load Balancing für den von Ihnen angegebenen Classic Load Balancer (CLB).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LoadBalancerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des CLB, für den Sie den zonenübergreifenden Load Balancing aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert den zonenübergreifenden Lastenausgleich für den CLB, den Sie im Parameter angeben. `LoadBalancerName`
- `aws:assertAwsResourceProperty`- Überprüft, ob der zonenübergreifende Load Balancing auf dem CLB aktiviert wurde.

`AWSConfigRemediation-EnableELBDeletionProtection`

Beschreibung

Das `AWSConfigRemediation-EnableELBDeletionProtection` Runbook aktiviert den Löschschutz für den von Ihnen angegebenen Elastic Load Balancer (ELB).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- LoadBalancerArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des ELB, für den Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeScript`- Aktiviert den Löschschutz auf dem ELB, den Sie im `LoadBalancerArn` Parameter angeben.

AWSConfigRemediation-EnableLoggingForALBAndCLB

Beschreibung

Das `AWSConfigRemediation-EnableLoggingForALBAndCLB` Runbook ermöglicht die Protokollierung für den angegebenen AWS Application Load Balancer oder einen Classic Load Balancer (CLB).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LoadBalancerId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Classic Load Balancer Balancer-Name oder der Application Load Balancer Balancer-ARN.
- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon S3 S3-Bucket-Name.
- S3 BucketPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die logische Hierarchie, die Sie beispielsweise für Ihren Amazon Simple Storage Service (Amazon S3) -Bucket erstellt haben`my-bucket-prefix/prod`. Wenn das Präfix nicht angegeben wird, wird das Protokoll auf der Bucket-Stammebene platziert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeScript`- Aktiviert und überprüft die Protokollierung für den Classic Load Balancer oder den Application Load Balancer.

`AWSSupport-TroubleshootCLBConnectivity`

Beschreibung

Das `AWSSupport-TroubleshootCLBConnectivity` Runbook hilft Ihnen bei der Behebung von Verbindungsproblemen zwischen Classic Load Balancer (CLB) und Amazon Elastic Compute Cloud (Amazon EC2) -Instances. Außerdem werden Verbindungsprobleme zwischen einem Client und der CLB überprüft. In diesem Runbook werden auch die Integritätsprüfungen für das CLB überprüft, es wird überprüft, ob die bewährten Methoden befolgt werden, und es wird ein Dashboard zur Problembehebung für Sie erstellt. Optional können Sie die Automatisierungsausgabe in einen Amazon Simple Storage Service (Amazon S3) -Bucket hochladen. Dieses Runbook unterstützt jedoch nicht das Hochladen von Ausgaben in öffentlich zugängliche S3-Buckets. Wir empfehlen, für diese Automatisierung einen temporären S3-Bucket zu erstellen.

> **Important**
>
> Bei der Verwendung dieses Runbooks können Gebühren für das erstellte Dashboard anfallen. Weitere Informationen finden Sie unter CloudWatchAmazon-Preise

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InvestigationType

  Typ: Zeichenfolge

  Gültige Werte: Bewährte Methoden | Verbindungsprobleme | Dashboard zur Fehlerbehebung

  Beschreibung: (Erforderlich) Die Operationen, die das Runbook ausführen soll.
- LoadBalancerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des CLB.
- S3Location

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des S3-Buckets, an den Sie die Automatisierungsergebnisse senden möchten. Öffentlich zugängliche Buckets werden nicht unterstützt. Wenn Ihr S3-Bucket serverseitige Verschlüsselung verwendet, muss der Benutzer oder die Rolle, die diese Automatisierung ausführt, über `kms:GenerateDataKey` Berechtigungen für den AWS KMS Schlüssel verfügen.
- S3 LocationPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Amazon S3 S3-Schlüsselpräfix (Unterordner), in das Sie die Automatisierungsausgabe hochladen möchten. Die Formatausgabe wird im

folgenden Format gespeichert: amzn-s3-demo-bucket/*S3LocationPrefix*/{{}} _ {{automation:*InvestigationType*}} .txt. *EXECUTION_ID*

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:executeScript`- Überprüft, ob der CLB, den Sie im Parameter angeben, existiert. `LoadBalancerName`
- `aws:branch`- Verzweigt auf der Grundlage des für den Parameter angegebenen Werts. `InvestigationType`
- `aws:executeScript`- Führt Konnektivitätsprüfungen mit dem CLB durch.
- `aws:executeScript`— Überprüft, ob die CLB-Konfiguration den Best Practices von Elastic Load Balancing entspricht.
- `aws:executeScript`- Erstellt ein CloudWatch Amazon-Dashboard für Ihr CLB.
- `aws:executeScript`- Erstellt eine Textdatei mit den Ergebnissen der Automatisierung und lädt sie in den Amazon S3 S3-Bucket hoch, den Sie im `S3Location` Parameter angeben.

Ausgaben

RunBestPractices. Zusammenfassung

RunConnectivityChecks.Zusammenfassung

CreateTroubleshootingDashboard. Ausgabe

UploadOutputToS3. Ausgabe

`AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing`

Beschreibung

Das `AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` Runbook aktiviert den zonenübergreifenden Load Balancing für den von Ihnen angegebenen Network Load Balancer (NLB).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LoadBalancerArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des NLB, für den Sie zonenübergreifendes Load Balancing aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert zonenübergreifendes Load Balancing für den NLB, den `LoadBalancerArn` Sie im Parameter angeben.
- `aws:executeScript`- Überprüft, ob der zonenübergreifende Load Balancing auf dem NLB aktiviert wurde.

AWS-UpdateALBDesyncMitigationMode

Beschreibung

Das `AWS-UpdateALBDesyncMitigationMode` Runbook aktualisiert den Desync-Minimierungsmodus auf einem Application Load Balancer (ALB) auf den angegebenen Mitigationsmodus. Der Desync-Minimationsmodus bestimmt, wie der Load Balancer Anfragen verarbeitet, die ein Sicherheitsrisiko für Ihre Anwendung darstellen könnten.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LoadBalancerArn

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des ALB, dessen Desync-Minderungsmodus Sie ändern möchten.

- DesyncMitigationMode

  Typ: Zeichenfolge

  Gültige Werte: überwachen | defensiv | strictest

  Beschreibung: (Erforderlich) Der Schadensbegrenzungsmodus, den die ALB verwenden soll. Informationen zu Desync-Minimationsmodi finden Sie unter Desync-Minimationsmodus im Benutzerhandbuch für Application Load Balancers.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- VerifyLoadBalancerType (aws: assertAwsResource Property) — Überprüft, ob der für den `LoadBalancerArn` Eingabeparameter angegebene Wert für einen Application Load Balancer bestimmt ist, bevor mit dem nächsten Schritt fortgefahren wird.
- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) — Aktualisiert den ALB, sodass er den angegebenen Wert verwendet. `DesyncMitigationMode`
- VerifyLoadBalancerDesyncMitigationMode (aws:ExecuteScript) — Überprüft, ob der Desync-Minderungsmodus für das Ziel-ALB aktualisiert wurde.

Ausgaben

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Nutzdaten der Nachricht des Skripts, das die Änderung an Ihrem ALB verifiziert.

AWS-UpdateCLBDesyncMitigationMode

Beschreibung

Das `AWS-UpdateCLBDesyncMitigationMode` Runbook aktualisiert den Desync-Minimierungsmodus auf einem Classic Load Balancer (CLB) auf den angegebenen Mitigationsmodus. Der Desync-Minimationsmodus bestimmt, wie der Load Balancer Anfragen verarbeitet, die ein Sicherheitsrisiko für Ihre Anwendung darstellen könnten.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LoadBalancerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des CLB, für den Sie den Modus zur Vermeidung der Desynchronisierung ändern möchten.

- DesyncMitigationMode

  Typ: Zeichenfolge

  Gültige Werte: monitor | defensive | strictest

  Beschreibung: (Erforderlich) Der Schadensbegrenzungsmodus, den die CLB verwenden soll. Informationen zu Desync-Minimationsmodi finden Sie unter Desync-Minimationsmodus im Benutzerhandbuch für Application Load Balancers.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Dokumentschritte

- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) — Aktualisiert den CLB so, dass er den angegebenen Wert verwendet. `DesyncMitigationMode`
- VerifyLoadBalancerDesyncMitigationMode (aws:ExecuteScript) — Überprüft, ob der Desync-Minderungsmodus für die Ziel-CLB aktualisiert wurde.

Ausgaben

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Payload der Nachricht des Skripts, das die Änderung an Ihrem CLB verifiziert.

AWSSupport-TroubleshootELBHealthChecks

Beschreibung

Das AWSSupport-TroubleshootELBHealthChecksRunbook hilft bei der Behebung von Problemen mit der AWS Elastic Load Balancing (Elastic Load Balancing) -Zustandsprüfung, indem es die

zugehörigen Amazon CloudWatch (CloudWatch) -Metriken analysiert, die Netzwerkkonnektivität überprüft und Diagnosebefehle auf den Ziel-Instances ausführt.

Dieses Runbook befasst sich mit den folgenden Anwendungsfällen:

- Es gibt fehlerhafte Instanzen innerhalb der Zielinstanzen eines Load Balancers oder einer Zielgruppe.
- Es gibt zwar keine fehlerhaften Instanzen, aber CloudWatch Metriken deuten auf Datenpunkte für `UnHealthyHostCounts`

> **Important**
>
> Wichtige Überlegungen:
>
> - Die Automatisierung konzentriert sich auf die Fehlerbehebung bei Zielen vom Typ Instance.
> - Die maximale Anzahl von Instanzen, die für die Fehlerbehebung zulässig sind, beträgt 50.
> - Die Zielinstanzen müssen von Systems Manager verwaltet werden, um die Ausführung von Diagnosebefehlen auf Instanzebene zu ermöglichen.
> - Der `S3BucketName` Parameter ist optional, aber bestimmte Diagnoseergebnisse werden direkt in den angegebenen Amazon S3 S3-Bucket hochgeladen und nicht in der Automatisierungsausgabe angezeigt.
> - IPv6 Die Fehlerbehebung bei der Netzwerkkonnektivität wird nicht unterstützt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Beispiel für eine Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootELBHealthChecks`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es SSM Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet SSM Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - LoadBalancerOrTargetGroupName (Erforderlich):
     - Beschreibung: (Erforderlich) Der Name eines Classic Load Balancer oder der Name der Zielgruppe, die einem Application Load Balancer oder Network Load Balancer zugeordnet ist.
     - Typ: `String`
     - Zulässiges Muster: `^[a-zA-Z0-9-]+$`
   - ExecutionMode (Erforderlich):
     - Beschreibung: (Erforderlich) Steuert den Ausführungsmodus der Automatisierung. `Complete`führt alle Schritte einschließlich RunCommands auf Amazon EC2 EC2-Instances

aus. `SkipRunCommands`führt alle Schritte aus, mit Ausnahme der Ausführung von Befehlen auf Instances.

- Typ: `String`
- Zulässige Werte: `[Complete, SkipRunCommands]`

- S3 BucketName (fakultativ):
  - Beschreibung: (Optional) Der Name des Amazon S3 S3-Buckets in Ihrem Konto, in das Sie die Fehlerbehebungsprotokolle hochladen möchten.
  - Typ: `String`
  - Standard: `""`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - getBucketPublicStatus:

     Prüft, ob der Amazon S3 S3-Ziel-Bucket möglicherweise öffentlichen Lese- oder Schreibzugriff auf seine Objekte gewährt.
   - getLoadBalancerEinzelheiten:

     Identifiziert den Load Balancer-Typ und gibt ein einheitliches Load Balancer-Detailobjekt zurück.
   - checkLoadBalancerType:

     Prüft, ob der Load Balancer existiert.
   - Ziele abrufen:

     Auf der Grundlage der verschiedenen Typen von Load Balancern beschreiben Abfragen, wie eine Übersicht mit fehlerfreien und fehlerhaften Zielen zurückgegeben werden APIs soll.
   - checkCloudWatchMetriken:

     Überprüft die CloudWatch Metriken `HealthyHostCounts` `UnHealthyHostCounts` und generiert die CloudWatch Links.
   - checkUnhealthyReasons:

     Prüft nach schädlichen Gründen und filtert Ziele.
   - Überprüfen Sie die Konnektivität:

     Überprüft die Konnektivität zwischen dem Load Balancer und seinen Instances.

- Befehle ausführen:

  Führt Befehle zur Fehlerbehebung auf Instances aus und lädt die Ausgabe hoch, wenn der Bucket-Name angegeben wird.
- Bericht generieren:

  Generiert den Abschlussbericht auf der Grundlage der Ergebnisse der vorherigen Schritte und lädt den Bericht, falls angegeben, in den Amazon S3 S3-Bucket hoch.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Outputs die detaillierten Ergebnisse der Ausführung.

Diagnosebefehle

Das Runbook führt die folgenden Diagnosebefehle auf Instanzen aus:

- Linux-Shell: top, free, ss, curl, iptables, tcpdump
- Windows PowerShell: Get-CimInstance, Get-, Get-NetFirewallProfile, Invoke-NetFirewallRuleWebRequest, Netstat, Netsh, Pktmon

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

Amazon EMR

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon EMR bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-AnalyzeEMRLogs

- AWSSupport-DiagnoseEMRLogsWithAthena

AWSSupport-AnalyzeEMRLogs

Beschreibung

Dieses Runbook hilft bei der Identifizierung von Fehlern bei der Ausführung eines Jobs auf einem Amazon EMR-Cluster. Das Runbook analysiert eine Liste definierter Protokolle im Dateisystem und sucht nach einer Liste mit vordefinierten Schlüsselwörtern. Diese Protokolleinträge werden verwendet, um Amazon CloudWatch Events-Ereignisse zu erstellen, sodass Sie auf der Grundlage der Ereignisse alle erforderlichen Maßnahmen ergreifen können. Optional veröffentlicht das Runbook Protokolleinträge in der Amazon CloudWatch Logs-Protokollgruppe Ihrer Wahl. Dieses Runbook sucht derzeit in Protokolldateien nach den folgenden Fehlern und Mustern:

- container_out_of_memory — Der YARN-Container hat nicht mehr genügend Speicher, die Ausführung des Jobs kann fehlschlagen.
- yarn_nodemanager_health: Der CORE- oder TASK-Knoten hat nur noch wenig Speicherplatz zur Verfügung und er kann keine Aufgaben ausführen.
- node_state_change: Der CORE- oder TASK-Knoten ist vom MASTER-Knoten nicht erreichbar.
- step_failure: Ein EMR-Schritt ist fehlgeschlagen.
- no_core_nodes_running: Derzeit laufen keine CORE-Knoten, der Cluster ist fehlerhaft.
- hdfs_missing_blocks: Es fehlen HDFS-Blöcke, was zu Datenverlust führen könnte.
- hdfs_high_util: Die HDFS-Auslastung ist hoch, was sich auf Jobs und die Clusterintegrität auswirken kann.
- instance_controller_restart: Der Instance-Controller-Prozess wurde neu gestartet. Dieser Prozess ist für die Clusterintegrität unerlässlich.
- instance_controller_restart_legacy: Der Instance-Controller-Prozess wurde neu gestartet. Dieser Prozess ist für die Clusterintegrität unerlässlich.
- high_load: Es wurde ein hoher Lastdurchschnitt erkannt. Dies kann sich auf die Berichterstattung über den Knotenstatus auswirken oder zu Timeouts oder Verlangsamungen führen.
- yarn_node_blacklisted: Der CORE- oder TASK-Knoten wurde von YARN für die Ausführung von Aufgaben gesperrt.
- yarn_node_lost: Der CORE- oder TASK-Knoten wurde von YARN als LOST markiert, mögliche Verbindungsprobleme.

Instanzen, die mit dem von Ihnen angegebenen verknüpft sind`ClusterID`, müssen von verwaltet werden. AWS Systems Manager Sie können diese Automatisierung einmal ausführen, die Automatisierung so planen, dass sie in einem bestimmten Zeitintervall ausgeführt wird, oder einen zuvor durch eine Automatisierung erstellten Zeitplan entfernen. Dieses Runbook unterstützt die Amazon EMR-Release-Versionen 5.20 bis 6.30.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Clusters, dessen Knotenprotokolle Sie analysieren möchten.
- Operation

  Typ: Zeichenfolge

  Gültige Werte: Einmal ausführen | Zeitplan | Zeitplan entfernen

Beschreibung: (Erforderlich) Der Vorgang, der auf dem Cluster ausgeführt werden soll.

- IntervalTime

  Typ: Zeichenfolge

  Gültige Werte: 5 Minuten | 10 Minuten | 15 Minuten

  Beschreibung: (Optional) Die Zeitspanne zwischen der Ausführung der Automatisierung. Dieser Parameter ist nur anwendbar, wenn Sie ihn `Schedule` für den `Operation` Parameter angeben.

- LogToCloudWatchLogs

  Typ: Zeichenfolge

  Gültige Werte: ja | nein

  Beschreibung: (Optional) Wenn Sie `yes` für den Wert dieses Parameters einen Wert angeben, erstellt die Automatisierung eine CloudWatch Logs-Protokollgruppe mit dem im `CloudWatchLogGroup` Parameter angegebenen Namen, in der alle übereinstimmenden Protokolleinträge gespeichert werden.

- CloudWatchLogGroup

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der CloudWatch Logs-Log-Gruppe, in der Sie alle passenden Logeinträge speichern möchten. Dieser Parameter ist nur anwendbar, wenn Sie ihn `yes` für den `LogToCloudWatchLogs` Parameter angeben.

- CreateLogInsightsDashboard

  Typ: Zeichenfolge

  Gültige Werte: ja | nein

  Beschreibung: (Optional) Wenn Sie dies angeben`yes`, wird das CloudWatch Dashboard erstellt, sofern es noch nicht vorhanden ist. Dieser Parameter ist nur anwendbar, wenn Sie ihn `yes` für den `LogToCloudWatchLogs` Parameter angeben.

- CreateMetricFilters

  Typ: Zeichenfolge

Gültige Werte: ja | nein

Beschreibung: (Optional) Geben Sie an, `yes` ob Sie Metrikfilter für die Protokollgruppe CloudWatch Logs erstellen möchten. Dieser Parameter ist nur anwendbar, wenn Sie ihn `yes` für den `LogToCloudWatchLogs` Parameter angeben.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:executeAwsApi`- Sammelt Informationen über den im Parameter angegebenen Amazon EMR-Cluster. `ClusterID`
- `aws:branch`— Verzweigungen auf der Grundlage von Eingaben.
  - Wenn die angegebene Operation `Run Once` oder ist`Schedule`:
    - `aws:assertAwsResourceProperty`- Überprüft, ob der Cluster verfügbar ist.
    - `aws:executeAwsApi`- Sammelt alle Instanzen, IDs die im Cluster ausgeführt werden.
    - `aws:assertAwsResourceProperty`- Überprüft, ob der SSM-Agent auf allen Instanzen im Cluster ausgeführt wird.
    - `aws:branch`- Verzweigt je nachdem, ob Sie angegeben haben, dass die Automatisierung einmal oder nach einem Zeitplan ausgeführt werden soll.
      - Wenn der bereitgestellte Vorgang wie folgt lautet`Run Once`:
        - `aws:branch`- Verzweigt auf der Grundlage des im `LogToCloudWatchLogs` Parameter angegebenen Werts.
          - Wenn `LogToCloudWatchLogs` der Wert ist`yes`:
            - `aws:executeScript`- Prüft, ob eine CloudWatch Logs-Log-Gruppe mit dem im Parameter angegebenen Namen `CloudWatchLogGroup` bereits existiert. Wenn nicht, wird die Gruppe mit dem angegebenen Namen erstellt.
            - `aws:branch`- Verzweigt auf der Grundlage des im `CreateMetricFilters` Parameter angegebenen Werts.
              - Wenn `CreateMetricFilters` der Wert ist`yes`:

- `aws:executeAwsApi`- Für jeden metrischen Filter werden 12 Schritte ausgeführt
- `aws:branch`- Verzweigungen, die auf dem im `CreateLogInsightsDashboard` Parameter angegebenen Wert basieren.
  - Wenn `CreateLogInsightsDashboard` der Wert ist`yes`:
    - `aws:executeAwsApi`- Erstellt ein CloudWatch Dashboard mit demselben Namen, der im `CloudWatchLogGroup` Parameter angegeben ist, falls es noch nicht existiert.
  - Wenn `CreateLogInsightsDashboard` der Wert ist`no`:
    - `aws:runCommand`- Führt ein Shell-Skript aus, um Protokollmuster auf jeder Instanz im Cluster zu finden.
- Wenn `CreateMetricFilters` der Wert ist`no`:
  - `aws:branch`- Verzweigt auf der Grundlage des im `CreateLogInsightsDashboard` Parameter angegebenen Werts.
    - Wenn `CreateLogInsightsDashboard` der Wert ist`yes`:
      - `aws:executeAwsApi`- Erstellt ein CloudWatch Dashboard mit demselben Namen, der im `CloudWatchLogGroup` Parameter angegeben ist, falls es noch nicht existiert.
    - Wenn `CreateLogInsightsDashboard` der Wert ist`no`:
      - `aws:runCommand`- Führt ein Shell-Skript aus, um Protokollmuster auf jeder Instanz im Cluster zu finden.
- Wenn `LogToCloudWatchLogs` der Wert ist`no`:
  - `aws:executeAwsApi`- Führt ein Shell-Skript aus, um Protokollmuster auf jeder Instanz im Cluster zu finden.
- Wenn die bereitgestellte Operation wie folgt lautet`Schedule`:
  - `aws:createStack`— Erstellt ein EventBridge Amazon-Ereignis, das auf dieses Runbook abzielt.
- Wenn die angegebene Operation wie folgt lautet`Remove Schedule`:
  - `aws:executeAwsApi`- Überprüft, ob ein Zeitplan für den Cluster existiert.
  - `aws:deleteStack`- Löscht den Zeitplan.

Ausgaben

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstances. Instanz IDs

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists. Ausgabe

FindLogPatternOnEMRNode.CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

Beschreibung

Das `AWSSupport-DiagnoseEMRLogsWithAthena` Runbook hilft bei der Diagnose von Amazon EMR-Protokollen mithilfe von Amazon Athena in Integration mit AWS Glue Data Catalog. Amazon Athena wird verwendet, um die Amazon EMR-Protokolldateien nach Containern, Knotenprotokollen oder beidem abzufragen, mit optionalen Parametern für bestimmte Datumsbereiche oder schlüsselwortbasierte Suchen.

Das Runbook kann automatisch den Amazon EMR-Protokollspeicherort für einen vorhandenen Cluster abrufen, oder Sie können den Amazon S3 S3-Protokollspeicherort angeben. Um die Protokolle zu analysieren, geht das Runbook wie folgt vor:

- Erstellt eine AWS Glue Datenbank und führt Amazon Athena Data Definition Language (DDL) - Abfragen am Amazon S3-Protokollspeicherort von Amazon EMR aus, um Tabellen für Cluster-Protokolle und eine Liste bekannter Probleme zu erstellen.
- Führt DML-Abfragen (Data Manipulation Language) aus, um in den Amazon EMR-Protokollen nach bekannten Problemmustern zu suchen. Die Abfragen geben eine Liste der erkannten Probleme, deren Anzahl und die Anzahl der übereinstimmenden Keywords pro Amazon S3 S3-Dateipfad zurück.
- Die Ergebnisse werden in einen Amazon S3 S3-Bucket hochgeladen, den Sie unter dem Präfix angeben`saw_diagnose_EMR_known_issues`.
- Das Runbook gibt die Amazon Athena Athena-Abfrageergebnisse zurück und hebt Ergebnisse, Empfehlungen und Verweise auf Artikel aus dem Amazon Knowledge Center (KC) hervor, die aus einer vordefinierten Untergruppe stammen.

- Nach Abschluss oder Fehlschlag werden die AWS Glue Datenbank und die Dateien mit bekannten Problemen, die in den Amazon S3 S3-Bucket hochgeladen wurden, gelöscht.

Wie funktioniert das?

`AWSSupport-DiagnoseEMRLogsWithAthena`Sie führen mithilfe von Amazon Athena Analysen von Amazon EMR-Protokollen durch, um Fehler zu erkennen und Ergebnisse, Empfehlungen und relevante Knowledge Center-Artikel hervorzuheben.

Das Runbook führt die folgenden Schritte aus:

- Rufen Sie den Amazon EMR-Cluster-Protokollstandort mithilfe der Cluster-ID ab oder geben Sie den Amazon S3 S3-Standort ein, um den Speicherort und die Größe des Protokolls abzurufen.
- Geben Sie eine Schätzung der Athena-Kosten auf der Grundlage der Größe des Protokollstandorts an.
- Holen Sie sich die Genehmigung zum Fortfahren, indem Sie die Genehmigung von den zuständigen IAM-Prinzipalen einholen, bevor Sie Athena-Abfragen ausführen und mit den nächsten Schritten fortfahren.
- Laden Sie bekannte Probleme in den angegebenen Amazon S3 S3-Bucket hoch, erstellt eine AWS Glue Datenbank und Tabellen.
- Führen Sie Athena-Abfragen an den Amazon EMR-Protokolldaten aus. Abfragen können nach Datumsbereich, Schlüsselwörtern oder beiden Kriterien suchen oder auf der Grundlage der bereitgestellten Eingaben ohne Filter ausgeführt werden.
- Analysieren Sie die Ergebnisse, um Ergebnisse, Empfehlungen und relevante KC-Artikel hervorzuheben.
- Ausgabelinks für Amazon Athena DML-Abfrageergebnisse.
- Bereinigen Sie die Umgebung, indem Sie erstellte Datenbanken, Tabellen und hochgeladene bekannte Probleme entfernen.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden:

- Athene: GetQueryExecution
- Athene: StartQueryExecution
- Athene: GetPreparedStatement
- Athene: CreatePreparedStatement
- kleben: GetDatabase
- kleben: CreateDatabase
- kleben: DeleteDatabase
- kleben: CreateTable
- kleben: GetTable
- kleben: DeleteTable
- elastisches MapReduce: DescribeCluster
- s3: ListBucket
- s3: GetBucketVersioning
- s3: ListBucketVersions
- s3: GetBucketPublicAccessBlock
- s3: GetBucketPolicyStatus
- s3: GetObject
- s3: GetBucketLocation
- Preisgestaltung: GetProducts
- Preisgestaltung: GetAttributeValues
- Preisgestaltung: DescribeServices
- Preisgestaltung: ListPriceLists

Important

Um den Zugriff nur auf die Ressourcen zu beschränken, die für diese Automatisierung benötigt werden, fügen Sie der IAM-Rolle, die dem SSM-Dienst vertraut, die folgende

Richtlinie hinzu. Ersetzen Sie Partition, Region und Konto durch die entsprechenden Werte für die Partition, Region und Kontonummer, auf der das Runbook ausgeführt wird.

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"
            ]
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-DiagnoseEMRLogsWithAthenaim AWS Systems Manager Bereich Dokumente.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - ClusterID (erforderlich):

     Die Amazon EMR-Cluster-ID.
   - S3 LogLocation (optional):

     Der Amazon S3 S3-Speicherort für Amazon EMR-Protokolle. Geben Sie die URL des Amazon S3 S3-Speicherorts im Path-Stil ein, zum Beispiel:. `s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/` Geben Sie diesen Parameter an, wenn der Amazon EMR-Cluster für mehr als `30` Tage beendet wurde.
   - S3 BucketName (erforderlich):

     Der Amazon S3 S3-Bucket-Name zum Hochladen einer Liste bekannter Probleme und der Ausgabe von Amazon Athena Athena-Abfragen. Für den Bucket sollte Block Public Access aktiviert sein und sich in derselben AWS Region und demselben Konto wie der Amazon EMR-Cluster befinden.
   - Genehmiger (erforderlich):

Die Liste der AWS authentifizierten Principals, die die Aktion entweder genehmigen oder ablehnen können. Sie können Prinzipale angeben, indem Sie eines der folgenden Formate verwenden: Benutzername, Benutzer-ARN, IAM-Rollen-ARN oder IAM Assume Role ARN. Die maximale Anzahl an Genehmigern ist 10.

- FetchNodeLogsOnly (Optional):

  Wenn auf gesetzt`true`, diagnostiziert die Automatisierung die Protokolle des Amazon EMR-Anwendungscontainers. Der Standardwert ist `false`.

- FetchContainersLogsOnly(Fakultativ):

  Wenn auf gesetzt`true`, diagnostiziert die Automatisierung die Amazon EMR-Container-Protokolle. Der Standardwert ist `false`.

- EndSearchDate (Fakultativ):

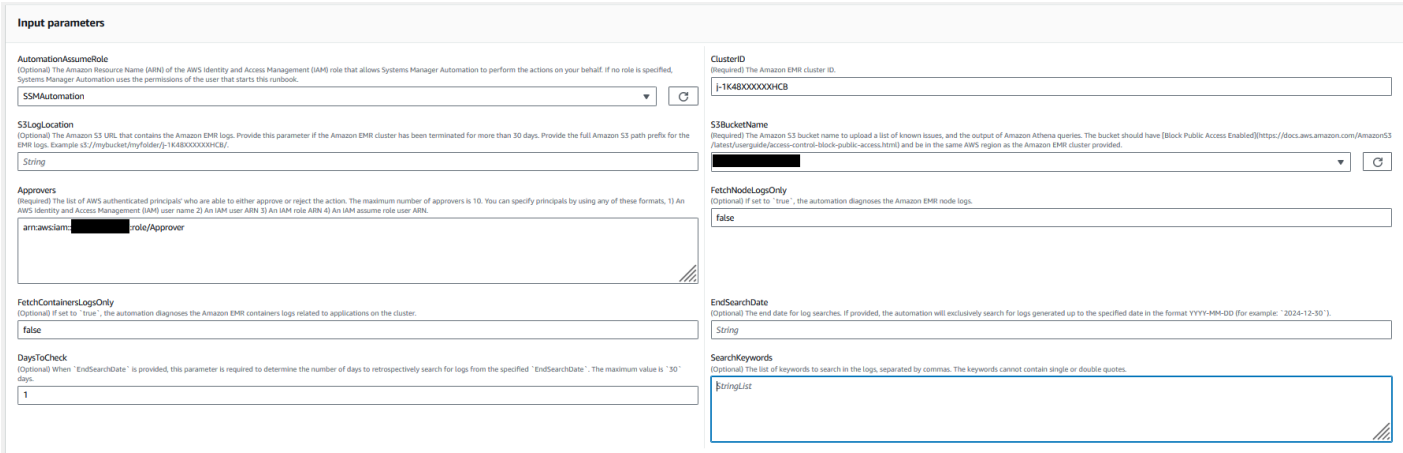
  Das Enddatum für Protokollsuchen. Falls angegeben, sucht die Automatisierung ausschließlich nach Protokollen, die bis zum angegebenen Datum im Format generiert wurden YYYY-MM-DD (zum Beispiel:`2024-12-30`).

- DaysToCheck (Fakultativ):

  Wenn angegeben, `EndSearchDate` ist dieser Parameter erforderlich, um die Anzahl der Tage zu bestimmen, für die rückwirkend nach Protokollen aus den angegebenen Daten gesucht werden soll. `EndSearchDate` Der Höchstwert beträgt `30` Tage. Der Standardwert ist `1`.

- SearchKeywords (Fakultativ):

  Die Liste der Schlüsselwörter, nach denen in den Protokollen gesucht werden soll, getrennt durch Kommas. Die Schlüsselwörter dürfen keine einfachen oder doppelten Anführungszeichen enthalten.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - getLogLocation:

     Ruft den Amazon S3 S3-Protokollspeicherort ab, indem die angegebene Amazon EMR-Cluster-ID abgefragt wird. Wenn die Automatisierung den Protokollspeicherort nicht anhand der Amazon EMR-Cluster-ID abfragen kann, verwendet das Runbook den `S3LogLocation` Eingabeparameter.
   - branchOnValidProtokoll:

     Überprüft den Speicherort der Amazon EMR-Protokolle. Wenn der Standort gültig ist, fahren Sie mit der Schätzung der potenziellen Kosten von Amazon Athena bei der Ausführung von Abfragen in den Amazon EMR-Protokollen fort.
   - estimateAthenaCosts:

     Ermittelt die Größe der Amazon EMR-Protokolle und bietet eine Kostenschätzung für die Ausführung von Athena-Scans für den Protokolldatensatz. Für nicht kommerzielle Regionen (keine AWS Partitionen) wird in diesem Schritt lediglich die Protokollgröße angegeben, ohne die Kosten zu schätzen. Die Kosten können anhand der Athena-Preisdokumentation in der angegebenen Region berechnet werden.
   - Automatisierung genehmigen:

     Wartet auf die Genehmigung durch die designierten IAM-Prinzipale, um mit den nächsten Schritten der Automatisierung fortzufahren. Die Genehmigungsbenachrichtigung enthält die geschätzten Kosten für den Amazon Athena Athena-Scan in den Amazon EMR-Protokollen sowie Einzelheiten zu den Ressourcen, die durch die Automatisierung bereitgestellt werden.
   - uploadKnownIssuesExecuteAthenaQueries:

     Lädt die vordefinierten bekannten Probleme in den im `S3BucketName` Parameter angegebenen Amazon S3 S3-Bucket hoch. Erstellt eine AWS Glue Datenbank und Tabellen. Führt Amazon Athena Athena-Abfragen in der AWS Glue Datenbank auf der Grundlage der Eingabeparameter aus.
   - getQueryExecutionStatus:

Wartet, bis die Ausführung der Amazon Athena Athena-Abfrage im SUCCEEDED Status ist. Die Amazon Athena DML-Abfrage sucht nach Fehlern und Ausnahmen in Amazon EMR-Clusterprotokollen.

- analyzeAthenaResults:

  Analysiert die Amazon Athena Athena-Ergebnisse, um Ergebnisse, Empfehlungen und Knowledge Center-Artikel (KC) bereitzustellen, die aus einem vordefinierten Satz von Zuordnungen stammen.

- getAnalyzeResultsAbfrage 1: ExecutionStatus

  Wartet, bis die Abfrageausführung im Status ist. SUCCEEDED Die Amazon Athena DML-Abfrage analysiert die Ergebnisse der vorherigen DML-Abfrage. Diese Analyseabfrage gibt übereinstimmende Ausnahmen mit Lösungen und KC-Artikeln zurück

- getAnalyzeResultsAbfrage 2ExecutionStatus:

  Wartet, bis die Abfrageausführung im Status ist. SUCCEEDED Die Amazon Athena DML-Abfrage analysiert die Ergebnisse der vorherigen DML-Abfrage. Diese Analyseabfrage gibt eine Liste der in jedem Amazon S3 S3-Protokollpfad exceptions/errors erkannten Daten zurück.

- printAthenaQueriesNachricht:

  Druckt Links für die Ergebnisse der Amazon Athena DML-Abfragen.

- Ressourcen bereinigen:

  Bereinigt Ressourcen, indem die erstellte AWS Glue Datenbank und Dateien mit bekannten Problemen gelöscht werden, die im Amazon EMR-Protokoll-Bucket erstellt wurden.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt „Ausgaben“ die detaillierten Ergebnisse der Ausführung:

   Output bietet drei Links für Athena-Abfrageergebnisse:

   - Liste aller Fehler und häufig aufgetretenen Ausnahmen, die in den Amazon EMR-Clusterprotokollen gefunden wurden, zusammen mit den entsprechenden Protokollspeicherorten (Amazon S3 S3-Präfix).
   - Zusammenfassung der eindeutigen bekannten Ausnahmen, die in den Amazon EMR-Protokollen gefunden wurden, zusammen mit empfohlenen Lösungen und KC-Artikeln zur Unterstützung bei der Fehlerbehebung.

- Details darüber, wo bestimmte Fehler und Ausnahmen in den Amazon S3 S3-Protokollpfaden auftreten, um weitere Diagnosen zu unterstützen.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS Servicedokumentation

- Weitere Informationen finden Sie unter Problembehandlung bei Amazon EMR-Clustern

OpenSearch Amazon-Dienst

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon OpenSearch Service bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-DeleteOpenSearchDomain
- AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain
- AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups
- AWSSupport-TroubleshootOpenSearchRedYellowCluster
- AWSSupport-TroubleshootOpenSearchHighCPU

AWSConfigRemediation-DeleteOpenSearchDomain

Beschreibung

Das `AWSConfigRemediation-DeleteOpenSearchDomain` Runbook löscht die angegebene Amazon OpenSearch Service-Domain mithilfe der DeleteDomainAPI.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- DomainName

  Typ: Zeichenfolge

  Zulässige Werte: (\ d {12}/)? [a-z] {1} [a-z0-9-] {2,28}

  Beschreibung: (Erforderlich) Der Name der Amazon OpenSearch Service-Domain, die Sie löschen möchten.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DeleteDomain`
- `es:DescribeDomain`

Dokumentschritte

- `aws:executeScript`- Akzeptiert den Amazon OpenSearch Service-Domainnamen als Eingabe, löscht ihn und verifiziert den Löschvorgang.

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

Beschreibung

Das `AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain` Runbook wird `EnforceHTTPS` auf einer bestimmten Amazon OpenSearch Service-Domain mithilfe der UpdateDomainConfigAPI aktiviert.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- DomainName

Typ: Zeichenfolge

Zulässige Werte: (\ d {12}/)? [a-z] {1} [a-z0-9-] {2,28}

Beschreibung: (Erforderlich) Der Name der Amazon OpenSearch Service-Domain, die Sie verwenden möchten, um HTTPS durchzusetzen.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Dokumentschritte

- `aws:executeScript`— Aktiviert die `EnforceHTTPS` Endpunktoption auf der Amazon OpenSearch Service-Domain, die Sie im `DomainName` Parameter angeben.

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

Beschreibung

Das `AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups` Runbook aktualisiert die Sicherheitsgruppenkonfiguration auf einer bestimmten Amazon OpenSearch Service-Domain mithilfe der UpdateDomainConfigAPI.

> **Note**
>
> AWS Sicherheitsgruppen können nur auf Amazon OpenSearch Service-Domains angewendet werden, die für Amazon Virtual Private Cloud (VPC) Access konfiguriert sind, und nicht auf Amazon OpenSearch Service-Domains, die für Public Access konfiguriert sind.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- DomainName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Amazon OpenSearch Service-Domain, die Sie zur Aktualisierung von Sicherheitsgruppen verwenden möchten.
- SecurityGroupList

  Typ: StringList

  Beschreibung: (Erforderlich) Die Sicherheitsgruppe IDs , die Sie der Amazon OpenSearch Service-Domain zuweisen möchten.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Dokumentschritte

- `aws:executeScript`- Aktualisiert die Sicherheitsgruppenkonfiguration auf der Amazon OpenSearch Service-Domain, die Sie im `DomainName` Parameter angeben.

`AWSSupport-TroubleshootOpenSearchRedYellowCluster`

Beschreibung

`AWSSupport-TroubleshootOpenSearchRedYellowCluster`Das Automation-Runbook wird verwendet, um die Ursache für den roten oder gelben Cluster-Status zu ermitteln und Sie bei der Umstellung des Clusters auf Grün zu unterstützen.

Wie funktioniert es?

Das Runbook `AWSSupport-TroubleshootOpenSearchRedYellowCluster` hilft Ihnen bei der Behebung der Ursache eines roten oder gelben Clusters und enthält die nächsten Schritte zur Behebung dieses Problems, indem die Clusterkonfiguration und die Ressourcennutzung analysiert werden.

Das Runbook führt die folgenden Schritte aus:

- Ruft die DescribeDomainAPI für die Zieldomäne auf, um die Clusterkonfiguration abzurufen.
- Überprüft, ob die OpenSearch Service-Domain internetbasiert (öffentlich) oder Amazon Virtual Private Cloud (VPC) basiert.
- Erzeugt je nach Cluster-Konfiguration eine öffentliche oder Amazon VPC-basierte AWS Lambda Funktion. Hinweis: Die Lambda-Funktion enthält den Code zur Fehlerbehebung, mit dem der

OpenSearch Dienst für den APIs Cluster ausgeführt wird, um festzustellen, warum sich der Cluster im roten oder gelben Zustand befindet.

- Löscht die Lambda-Funktion.
- Zeigt die durchgeführten Prüfungen und die nächsten empfohlenen Schritte an, um das rote oder gelbe Cluster-Problem zu lösen.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Der LambdaExecutionRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden:

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface

Überblick über die LambdaExecutionRole Richtlinie:

Im Folgenden finden Sie ein Beispiel für die Ausführungsrolle (AWS Identity and Access Management (IAM)) einer Lambda-Funktion, die der Funktion die Berechtigung erteilt, auf AWS Dienste und Ressourcen zuzugreifen, die für dieses Runbook erforderlich sind. Weitere Informationen finden Sie unter Lambda-Ausführungsrolle.

> **Note**
>
> Die ec2:DescribeNetworkInterfacesec2:CreateNetworkInterface, und ec2:DeleteNetworkInterface sind nur erforderlich, wenn Ihr OpenSearch Service-Cluster auf Amazon VPC basiert, damit die Lambda-Funktion die Amazon VPC-Netzwerkschnittstellen erstellen und verwalten kann. Weitere Informationen finden Sie unter Outbound-Netzwerke mit Ressourcen in einer Amazon VPC- und Lambda-Ausführungsrolle verbinden.

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"
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

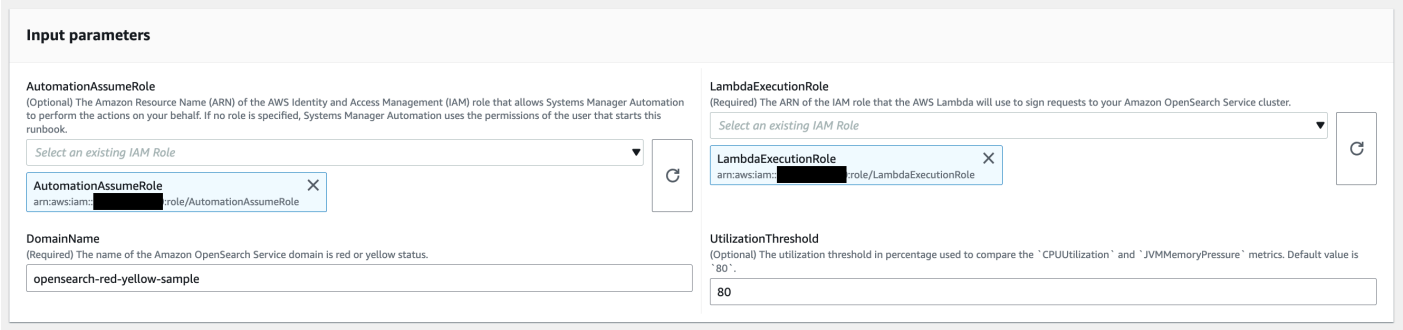
1. Navigieren Sie AWSSupport-TroubleshootOpenSearchRedYellowClusterin der AWS Systems Manager Konsole zum.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - LambdaExecutionRole (Erforderlich):

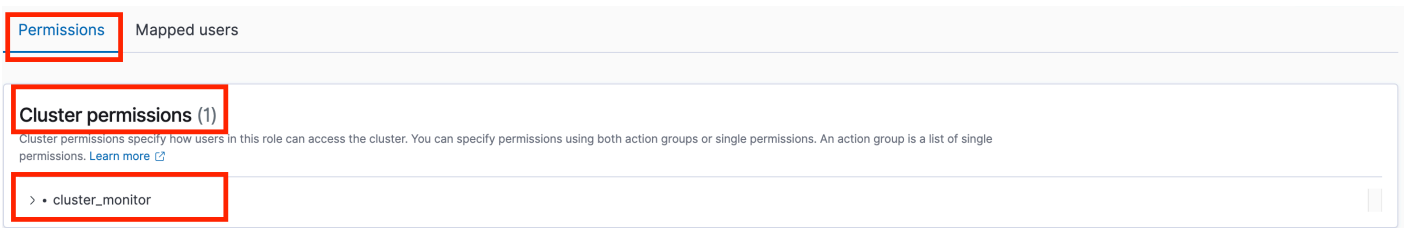
     Der ARN der IAM-Rolle, die Lambda verwendet, um Anfragen an Ihren Amazon OpenSearch Service-Cluster zu signieren.
   - DomainName (Erforderlich):

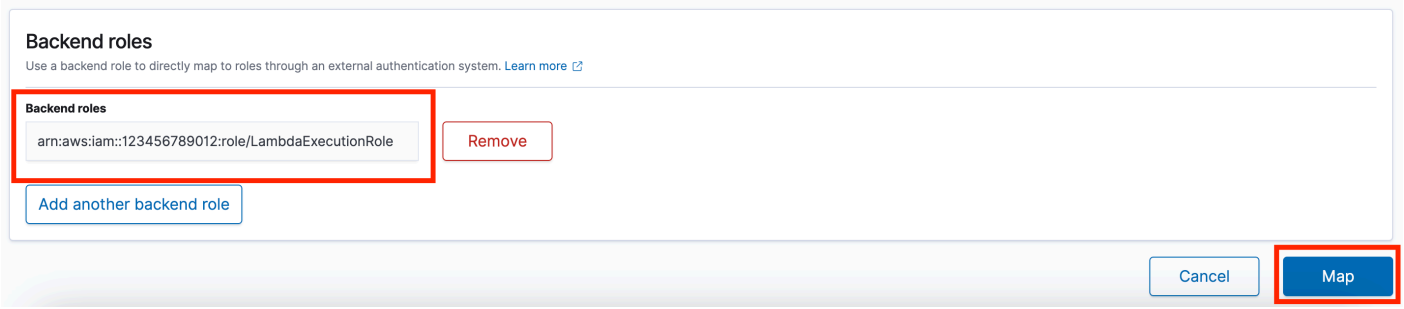
     Der Name der OpenSearch Dienstdomäne mit rotem oder gelbem Cluster-Integritätsstatus.
   - UtilizationThreshold (Fakultativ):

     Der Auslastungsschwellenwert in Prozent, der für den Vergleich der Messwerte CPUUtilization und JVMMemory Pressure verwendet wird. Der Standardwert ist 80.



4. Wenn Sie die differenzierte Zugriffskontrolle auf einem OpenSearch Service-Cluster aktiviert haben, stellen Sie sicher, dass die `LambdaExecutionRole` Rolle arn einer Rolle zugeordnet ist, die mindestens über die erforderlichen Berechtigungen verfügt. `cluster_monitor`





5. Wählen Sie Ausführen aus.
6. Die Automatisierung wird initiiert.
7. Das Automatisierungs-Runbook führt die folgenden Schritte aus:
   - GetClusterConfiguration:

     Ruft die OpenSearch Service-Cluster-Konfiguration ab.
   - Erstellen Sie AWSLambdaFunctionStack:

     Erstellt eine temporäre Lambda-Funktion in Ihrem Konto mit CloudFormation. Die Lambda-Funktion wird verwendet, um den OpenSearch Service APIs auszuführen.
   - WaitForAWSLambdaFunctionStack:

     Wartet, bis der CloudFormation Stack abgeschlossen ist.
   - GetClusterMetricsFromCloudWatch:

     Ruft die Cluster-bezogenen Kennzahlen zu Amazon CloudWatch ClusterStatus CPUUtilization, und JVMMemory Pressure OpenSearch Service sowie das Erstellungsdatum ab.
   - RunOpenSearchAPIs:

     Verwendet die Lambda-Funktion, um den OpenSearch Service aufzurufen APIs und die Cluster-Metrikdaten zu analysieren, um die Ursache für den roten oder gelben Clusterstatus zu diagnostizieren.
   - Löschen AWSLambdaFunctionStack:

     Löscht die durch diese Automatisierung erstellte Lambda-Funktion in Ihrem Konto.
8. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.
   - RootCause:

Bietet einen Überblick über die identifizierte Ursache dafür, dass der Status des Clusters rot oder gelb angezeigt wird.

- IssueDescription:

  Enthält Informationen darüber, warum sich der Cluster im roten oder gelben Zustand befindet, sowie mögliche Schritte, um den Cluster wieder in den grünen Zustand zu versetzen.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage Support Automation Workflows

AWS Servicedokumentation

- Weitere Informationen finden Sie unter Problembehandlung bei Amazon OpenSearch Service.

AWSSupport-TroubleshootOpenSearchHighCPU

Beschreibung

Das `AWSSupport-TroubleshootOpenSearchHighCPU` Runbook bietet eine automatisierte Lösung zum Sammeln von Diagnosedaten aus einer Amazon OpenSearch Service-Domain, um Probleme mit hoher CPU-Auslastung zu beheben.

Wie funktioniert es?

Das `AWSSupport-TroubleshootOpenSearchHighCPU` Runbook hilft bei der Behebung von Problemen mit hoher CPU-Auslastung in der Amazon OpenSearch Service-Domain.

Das Runbook führt die folgenden Schritte aus:

- Führt die DescribeDomainAPI für die angegebene Amazon OpenSearch Service-Domain aus, um die Cluster-Metadaten abzurufen.

- Überprüft, ob die Amazon OpenSearch Service-Domain öffentlich oder Amazon VPC-basiert ist und erstellt mit Hilfe von CloudFormation eine öffentliche oder Amazon AWS Lambda VPC-basierte Funktion.
- Die Lambda-Funktion ruft Diagnosedaten aus den Amazon OpenSearch Service-Domains ab.
- Verwendet eine AWS Step Functions Zustandsmaschine, um mehrere Lambda-Funktionsausführungen zu orchestrieren, um umfassendere Daten zu sammeln.
- Speichert die gesammelten Daten standardmäßig für 24 Stunden in einer CloudWatch Amazon-Protokollgruppe.
- Löscht die erstellten Ressourcen mit Ausnahme der CloudWatch Protokollgruppe.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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**
>
> Die `iam:CreateRole` Parameter`iam:DeleteRole`, `iam:GetRole` `iam:PutRolePolicy`iam:PutRolePolicy, und `iam:DeleteRolePolicy` sind nur erforderlich, wenn Sie keine vorhandene IAM-Rolle für den Parameter verwenden LambdaInvocationRoleForStepFunctions

Der `LambdaExecutionRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden:

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DeleteNetworkInterface`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Die Lambda-Ausführungsrolle gewährt der Funktion die Berechtigung, auf AWS Dienste und Ressourcen zuzugreifen, die für dieses Runbook erforderlich sind. Weitere Informationen finden Sie unter Lambda-Ausführungsrolle.

> **Note**
>
> Die `ec2:DescribeNetworkInterfacesec2:CreateNetworkInterface`, und `ec2:DeleteNetworkInterface` sind nur erforderlich, wenn Ihr OpenSearch Service-Cluster auf Amazon VPC basiert, damit die Lambda-Funktion die Amazon VPC-Netzwerkschnittstellen erstellen und verwalten kann. Weitere Informationen finden Sie unter Outbound-Netzwerke mit Ressourcen in einer Amazon VPC- und Lambda-Ausführungsrolle verbinden.

Der `LambdaInvocationRoleForStepFunctions` Parameter gewährt der AWS Step Functions Zustandsmaschine die Berechtigungen zum Aufrufen der Lambda-Funktion. Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die Step Functions die Erlaubnis erteilt, die Lambda-Funktion aufzurufen, die Diagnosedaten aus der Service-Domäne abruft. OpenSearch Weitere Informationen

finden Sie unter Erstellen einer IAM-Rolle für Zustandsmaschinen im Entwicklerhandbuch. AWS Step Functions

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource": [
                "arn:aws:lambda:us-east-1:111122223333:function:AWSSupport-
HighCPU-*"
            ]
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-TroubleshootOpenSearchHighCPUin der AWS Systems Manager Konsole zum.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - DomainName (Erforderlich):

     Der Name der Amazon OpenSearch Service-Domain, die Sie bei CPU-Problemen beheben möchten.
   - LambdaExecutionRoleForOpenSearch(Erforderlich):

Der ARN der IAM-Rolle, die an die Lambda-Funktion angehängt werden soll. Die Lambda-Funktion verwendet die Anmeldeinformationen aus dieser Rolle, um Anfragen an die Amazon OpenSearch Service-Domain zu signieren. Wenn für die Amazon OpenSearch Service-Domain eine differenzierte Zugriffskontrolle aktiviert ist, müssen Sie diese Rolle einer OpenSearch Service Dashboards-Backend-Rolle mit mindestens der „cluster_monitor“ -Berechtigung zuordnen.

- LambdaInvocationRoleForStepFunctions(Optional):

  (Optional) Der ARN der IAM-Rolle, die an den Step Functions Functions-Workflow angehängt werden soll. Die Zustandsmaschine verwendet die Anmeldeinformationen dieser Rolle, um die Lambda-Funktion aufzurufen, die Diagnosedaten aus der OpenSearch Service-Domäne abruft. Wenn keine Rolle angegeben ist, erstellt diese Automatisierung eine IAM-Rolle für Step Functions in Ihrem Konto.

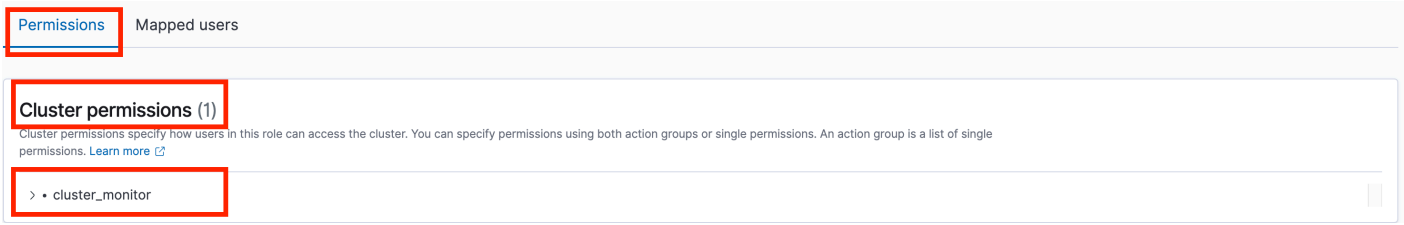
- DataRetentionDays (Fakultativ):

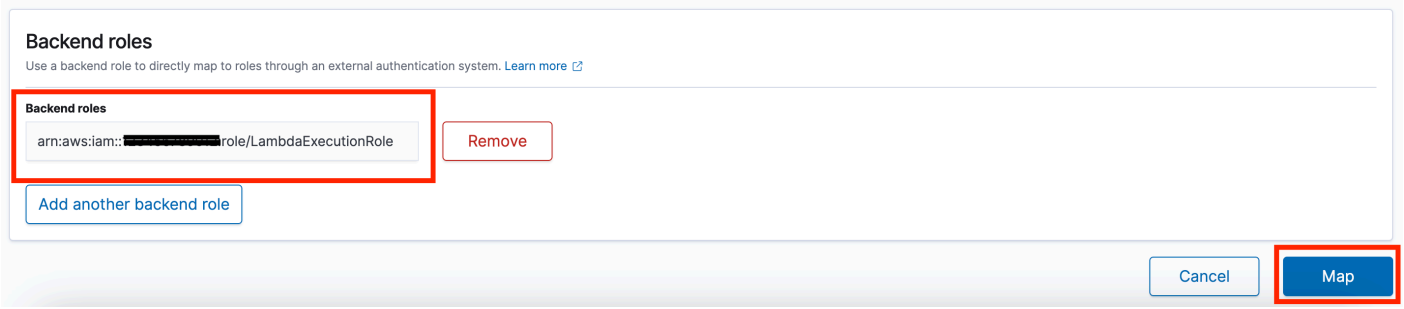
  Die Anzahl der Tage, für die die von der Amazon OpenSearch Service-Domain gesammelten Diagnosedaten aufbewahrt werden sollen. Standardmäßig werden die Daten für 24 Stunden (einen Tag) aufbewahrt. Sie können wählen, ob die Daten maximal bis zu 30 Tage aufbewahrt werden sollen.

- NumberOfDataSamples (Fakultativ):

  Die Anzahl der Datenproben, die aus der Amazon OpenSearch Service-Domain gesammelt werden sollen. Standardmäßig werden 5 Datenproben gesammelt. Sie können bis zu 10 Proben sammeln und die Lambda-Funktion wird für jede Probensammlung aufgerufen.

4. Wenn Sie die differenzierte Zugriffskontrolle auf einem OpenSearch Service-Cluster aktiviert haben, stellen Sie sicher, dass die `LambdaExecutionRole` Rolle arn einer Rolle mit mindestens Berechtigungen zugeordnet ist. `cluster_monitor`





5. Wählen Sie Ausführen aus.
6. Die Automatisierung wird initiiert.
7. Das Automatisierungs-Runbook führt die folgenden Schritte aus:
   - Parallelität prüfen:

     Stellt sicher, dass dieses Runbook nur einmal ausgeführt wird, das auf die angegebene Amazon OpenSearch Service-Domain abzielt. Wenn das Runbook eine weitere Ausführung findet, die auf denselben Domainnamen abzielt, gibt es einen Fehler zurück und wird beendet.
   - getDomainConfig:

     Ruft die Konfigurationsdetails für die OpenSearch Zieldienstdomäne ab.
   - Ressourcen bereitstellen:

     Stellt die Ressourcen für die Datenerfassung bereit mithilfe von. CloudFormation
   - waitForStackSchöpfung:

     Wartet, bis der CloudFormation Stapel abgeschlossen ist.
   - describeStackResources:

     Beschreibt den CloudFormation Stack und ruft den ARN der Zustandsmaschine ab.
   - runStateMachine:

     Ruft die Lambda-Funktion des Datensammlers ein- oder mehrmals auf, indem eine Step Functions Functions-Zustandsmaschine ausgeführt wird.
   - describeErrorsFromStackEvents:

     Beschreibt Fehler aus dem CloudFormation Stack für Fehler.
   - unstageOpenSearchHochCPUAutomation:

     Löscht den `AWSSupport-TroubleshootOpenSearchHighCPU` CloudFormation Stapel.

- describeErrorsFromStackDeletion:

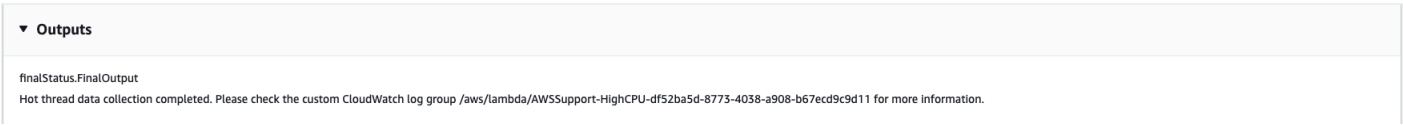
  Beschreibt Fehler, die beim Löschen des CloudFormation Stacks aufgetreten sind.

- Endgültiger Status:

  Gibt die endgültige Ausgabe des Runbooks zurück. `AWSSupport-TroubleshootOpenSearchHighCPU`

8. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.
   - Endgültiger Status. FinalOutput:

     Stellt die CloudWatch Protokollgruppe bereit, in der die Diagnosedaten gespeichert sind.



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS Servicedokumentation

- Weitere Informationen finden Sie unter Problembehandlung bei Amazon OpenSearch Service

EventBridge

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon EventBridge bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-AddOpsItemDedupStringToEventBridgeRule
- AWS-DisableEventBridgeRule

AWS-AddOpsItemDedupStringToEventBridgeRule

Beschreibung

Das `AWS-AddOpsItemDedupStringToEventBridgeRule` Runbook fügt eine Deduplizierungszeichenfolge für alle hinzu, die mit einer AWS Systems Manager OpsItems Amazon-Regel verknüpft sind. EventBridge Das Runbook fügt der Regel keine Deduplizierungszeichenfolge hinzu, wenn bereits eine angewendet wurde. Weitere Informationen zu Deduplizierungszeichenfolgen und OpsItems finden Sie unter Reduzieren von Duplikaten OpsItems im Benutzerhandbuch.AWS Systems Manager

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DedupString

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die Deduplizierungszeichenfolge, die Sie der Regel hinzufügen möchten.

- RuleName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Regel, zu der Sie die Deduplizierungszeichenfolge hinzufügen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

Dokumentschritte

- `aws:executeScript`- Fügt der EventBridge Regel, die Sie im Parameter angeben, eine Deduplizierungszeichenfolge hinzu. `RuleName`

AWS-DisableEventBridgeRule

Beschreibung

Das *AWS-DisableEventBridgeRule* Runbook deaktiviert die von Ihnen angegebene EventBridge Amazon-Regel. Weitere Informationen zu Regeln finden Sie unter EventBridge EventBridge Amazon-Regeln im Amazon-Benutzerhandbuch. EventBridge

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EventBusName

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Optional) Der Event-Bus, der der Regel zugeordnet ist, die Sie deaktivieren möchten.
- RuleName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Regel, die Sie deaktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

Dokumentschritte

- `aws:executeAwsApi`- Deaktiviert die EventBridge Regel, die Sie im `RuleName` Parameter angeben.

AWS Glue

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS Glue Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-TroubleshootGlueConnection

`AWSSupport-TroubleshootGlueConnection`

Beschreibung

Das AWSSupport-TroubleshootGlueConnectionsRunbook hilft bei der Behebung von AWS Glue Verbindungsproblemen. Das Ziel der getesteten Verbindung muss über eine JDBC-Verbindung erreicht werden und kann entweder ein Amazon Relational Database Service (Amazon RDS) - Cluster/Instance, ein Amazon Redshift Redshift-Cluster oder ein anderes Ziel sein, auf das über JDBC zugegriffen werden kann. In den ersten beiden Fällen wird das Reachability Analyzer-Tool verwendet, um festzustellen, ob die Konnektivität zwischen der Quelle (AWS Glue) und dem Ziel (Amazon RDS oder Amazon Redshift) gewährt ist.

Wenn das Ziel der Verbindung weder Amazon RDS noch Amazon Redshift ist, wird die Konnektivität trotzdem getestet, indem eine AWS Lambda Funktion im selben Subnetz wie die AWS Glue Verbindung (ein Netzwerkpoint of Presence) erstellt und geprüft wird, ob der Zielname auflösbar ist und ob er im Zielport erreichbar ist.

> **Important**
>
> Um die Reachability Analyzer-Prüfungen durchzuführen, werden Elastic Network Interfaces in jedem der Datenquellen-Subnetze der Verbindung erstellt. Bitte stellen Sie sicher, dass in diesen Subnetzen genügend Speicherplatz IPs zur Verfügung steht und dass sich der

Verbrauch einer IP nicht auf Ihre Arbeitslast auswirkt, bevor Sie diese Automatisierung ausführen.

Important

Alle durch diese Automatisierung erstellten Ressourcen sind markiert, sodass sie leicht gefunden werden können. Die verwendeten Tags sind:

- `AWSSupport-TroubleshootGlueConnection`: true
- `AutomationExecutionId`: *`Amazon EC2 Systems Manager Execution Id`*

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Beschreibt die AWS Glue Verbindung zum Abrufen der Quellinformationen (Subnetz und Sicherheitsgruppen) für die Konnektivitätsprüfungen.
- Ruft die Zielinformationen (Subnetz und Sicherheitsgruppen) aus der Datenquelle ab, auf die in der JDBC-URL verwiesen wird, oder aus den `DatasourceSecurityGroups` Parametern und, falls sie vorhanden sind. `DatasourceSubnets`
- Wenn die in der JDBC-URL vorhandene Datenquelle eine Amazon RDS-Instance oder ein Amazon RDS-Cluster oder ein Amazon Redshift Redshift-Cluster ist, erstellt ENIs diese Automatisierung sowohl die Quell- als auch die Zielinformationen, die in den vorherigen Schritten gesammelt wurden, und verwendet Reachability Analyzer, um eine Konnektivitätsprüfung zwischen ihnen durchzuführen.
- Eine Lambda-Funktion (Network Point of Presence, im Rahmen dieser Automatisierung) wird verwendet, um L4-Konnektivität und Namensauflösungsprüfungen durchzuführen.
- Dieselbe Lambda-Funktion wird verwendet, um die Prüfungen gegen den Amazon S3 S3-Endpunkt durchzuführen.
- Der Policy Simulator wird verwendet, um festzustellen, ob die in der Verbindung verwendete IAM-Rolle über die erforderlichen Berechtigungen verfügt.
- Die Automatisierung prüft, ob die von der Verbindung verwendete Sicherheitsgruppe die erwartete Konfiguration hat.

- Es wird ein Bericht generiert, der die möglichen Ursachen für den Fehler beim Testen der Verbindung and/or sowie die erfolgreich durchgeführten Tests enthält.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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**
>
> Zusätzlich zu den oben genannten Aktionen `AutomationAssumeRole` sollten die Amazon VPCReachability AnalyzerFullAccessPolicy als verwaltete Richtlinie beigefügt sein, damit die Reachability Analyzer-Tests erfolgreich durchgeführt werden.

Hier ist ein Beispiel für eine Richtlinie, die gewährt werden könnte für: `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"
                }
            }
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-TroubleshootGlueConnectionim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - TestConnectionRole (Erforderlich)

     Der Amazon-Ressourcenname (ARN) der IAM-Rolle, die während des Verbindungstests verwendet wird.
   - ConnectionName (Erforderlich)

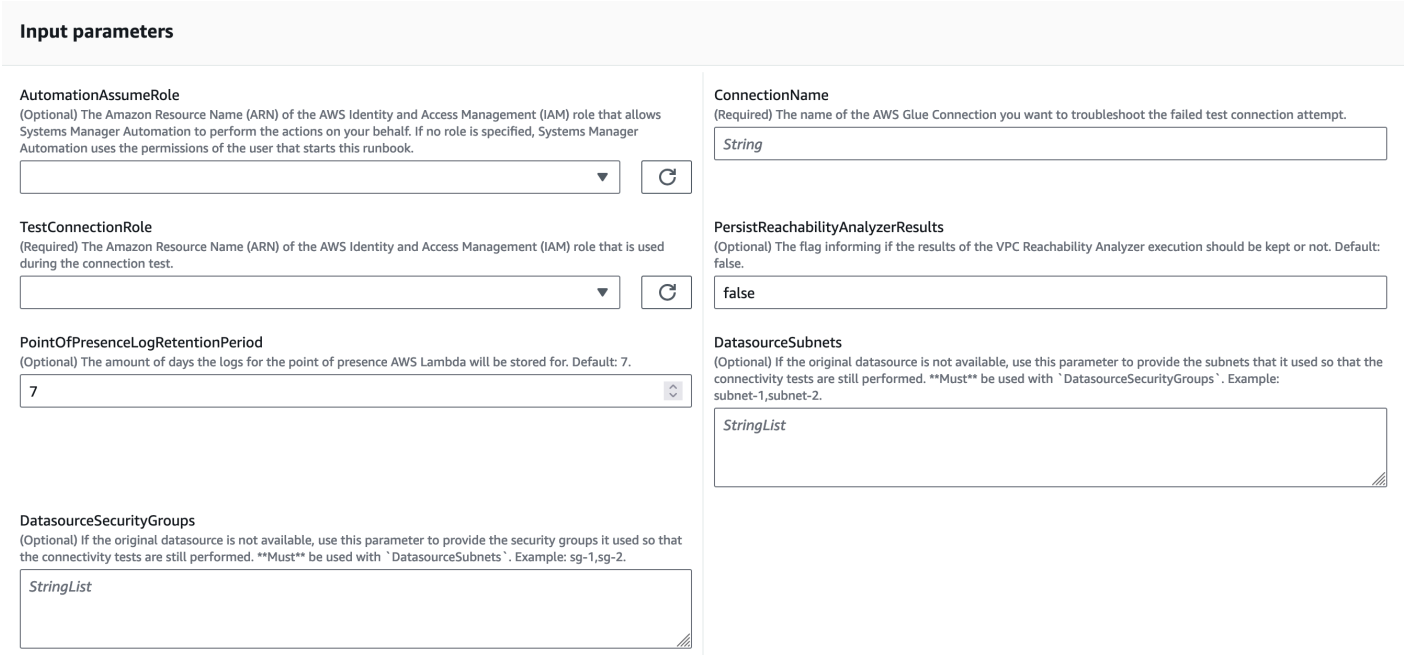
     AWS Glue Name der fehlgeschlagenen Testverbindung, für die Sie eine Fehlerbehebung durchführen möchten.
   - PersistReachabilityAnalyzerResults(Fakultativ)

     Die Markierung, die darüber informiert, ob die Ergebnisse der Ausführung von Reachability Analyzer beibehalten werden sollen oder nicht. Standard: `false.`
   - PointOfPresenceLogRetentionPeriod(Fakultativ)

     Die Anzahl der Tage, für die die Protokolle für den Point of Presence Lambda gespeichert werden. Standard: 7.
   - DatasourceSubnets (Fakultativ)

     Wenn die ursprüngliche Datenquelle nicht verfügbar ist, geben Sie mit diesem Parameter die von ihr verwendeten Subnetze an, sodass die Konnektivitätstests weiterhin durchgeführt werden. Muss mit verwendet werden. `DatasourceSecurityGroups` Beispiel: `subnet-1,subnet-2`.
   - DatasourceSecurityGroups (Fakultativ)

     Wenn die ursprüngliche Datenquelle nicht verfügbar ist, geben Sie mit diesem Parameter die verwendeten Sicherheitsgruppen an, sodass die Konnektivitätstests weiterhin durchgeführt werden. Muss mit verwendet werden. `DatasourceSubnets` Beispiel: `sg-1,sg-2`.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Automatisierungs-Runbook führt die folgenden Schritte aus:
   - ParseInputs:

     In diesem Schritt wird die Kombination der Eingaben validiert. Wenn `DatasourceSecurityGroups` sowohl als auch angegeben `DatasourceSubnets` werden, sind sie gültig und werden unverändert zurückgegeben. Wenn keine angegeben werden, werden zwei leere Listen zurückgegeben. Wenn nur eine von ihnen angegeben wird, löst der Schritt eine aus`ValueException`.
   - GetConnectionDetails:

     Dieser Schritt gibt die Details der bereitgestellten AWS Glue Verbindung zurück.
   - ParseSecurityGroupList:

     Dieser Schritt wird verwendet, um die Daten `String` für die future Verwendung `SecurityGroupIdList` in dieser Automatisierung zu verketten.
   - GetConnectionData:

     Ermittelt anhand der JDBC-URL, welche Art von Verbindung zwischen:, und. `RedShift` `RdsInstance` `RdsCluster` `Other` Gibt außerdem die in der JDBC-Verbindung verwendete Domain und den Port, die Amazon VPC der Verbindung und ihre Domain-Namenserver zurück.

- GetNetworkDetails:

  Ruft die Subnetz- und Sicherheitsgruppeninformationen vom Amazon RDS- oder Amazon Redshift Redshift-Ziel ab.

- Erstellen Sie: ENITemplate

  Generiert die AWS CloudFormation Vorlage, die zum Erstellen der Netzwerkschnittstellen verwendet wird, die zum Testen der Konnektivität verwendet werden. Dies ist erforderlich, um das Reachability Analyzer-Tool auszuführen.

- Erstellen Sie: ENIStack

  Erstellt den CloudFormation Stapel aus der Vorlage, die im vorherigen Schritt erstellt wurde.

- GetStackDetails:

  Beschreibt den CloudFormation Stapel, der im vorherigen Stapel erstellt wurde, und ruft die `SourceNetworkInterface` `TargetNetworkInterfaces` AN-Informationen ab.

- RunSourceToTargetCheck:

  Führt mithilfe des Tools Reachability Analyzer Prüfungen zwischen der Quelle und dem Ziel durch, die im vorherigen Schritt ENIs erstellt wurden.

- Löschen: ENIStack

  Löscht den CloudFormation Stapel, der Netzwerkschnittstellen erstellt

- CreateNetworkPointOfPresence:

  CloudFormation erstellt die Lambda-Funktion, die als Netzwerk-Präsenzpunkt verwendet wird.

- GetFunctionName:

  Führt einen CloudFormation Describe-Stack-API-Aufruf durch, um den Namen der Lambda-Funktion abzurufen, die im vorherigen Schritt erstellt wurde.

- RunEndpointChecks:

  Verwendet den Netzwerk-Präsenzpunkt, um festzustellen, ob der in der JDBC-Verbindung vorhandene Endpunkt im deklarierten Port auflösbar und erreichbar ist.

- Überprüft die Konnektivität von KS3:

  Überprüft die Netzwerkkonnektivität von der AWS Glue Verbindung zum Amazon S3 S3-Service.

- DeletePointOfPresence:

Löscht den CloudFormation Stack, der den Network Point of Presence Lambda erstellt.

- TestberechtigungenIAMRole:

  Prüft, ob die für den Test verwendete IAM-Rolle über die erforderlichen Berechtigungen verfügt, um ihn auszuführen.

- CheckConnectionSecurityGroupReferencingRule:

  Überprüft, ob die in der AWS Glue Verbindung verwendete Sicherheitsgruppe den gesamten eingehenden Datenverkehr von sich selbst zulässt. Es wird eine Liste der Sicherheitsgruppen ohne diese Regel zurückgegeben, falls vorhanden.

- GenerateReport:

  Generiert einen Bericht mit einer Liste der Ergebnisse (mögliche Gründe für den Fehler beim Verbindungstest) und den nächsten Schritten (Versuche, den fehlgeschlagenen Verbindungstest zu beheben).

7. Wenn Sie den Vorgang abgeschlossen haben, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   - Ergebnisse der Automatisierung

     In diesem Abschnitt finden Sie Szenarien, in denen mögliche Ursachen für das Fehlschlagen des Verbindungsversuchs beschrieben werden (Ergebnisse) und wie diese behoben werden können (nächste Schritte). Wenn die Automatisierung die Ursache für den Testfehler nicht finden kann, wird dies ebenfalls in diesem Abschnitt beschrieben.

   - Erfolgreiche Tests

     In diesem Abschnitt finden Sie Szenarien, die darüber informieren, was mit dieser Automatisierung erfolgreich getestet wurde. Erfolgreiche Tests sind nützlich, falls die Automatisierung nicht in der Lage ist, die Ursache für den Ausfall der Testverbindung zu ermitteln, da sie den Umfang der Untersuchung einschränken, indem sie darüber informieren, was nicht zu dem Problem beigetragen hat.

   - Fehler bei der Automatisierung

     In diesem Abschnitt finden Sie Szenarien, in denen Probleme beschrieben werden, die während der Automatisierung aufgetreten sind und die Anzahl der Tests, die die Automatisierung durchführen konnte, möglicherweise eingeschränkt haben. Die Beschreibung des Szenarios gibt Aufschluss darüber, welcher Schritt fehlgeschlagen ist.

```
TroubleshootGlueConnection
_____________________________________________________________________________________________________________________
Automation Results
Bellow 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 dumy-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-[redacted]) 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::[redacted]: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::[redacted]: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::[redacted]: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::[redacted]:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-lLu7FYAp9bfi.


_____________________________________________________________________________________________________________________
✓ Successful Tests
Below are the successful tests performed by the automation, for further troublehsooting.

-------------------------------------------------------------

# 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.
```

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

Amazon FSx

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon FSx bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-ValidateFSxWindowsADConfig

AWSSupport-ValidateFSxWindowsADConfig

Beschreibung

Das `AWSSupport-ValidateFSxWindowsADConfig` Runbook wird verwendet, um die selbstverwaltete Active Directory-Konfiguration (AD) eines Amazon FSx for Windows-Dateiservers zu validieren

Wie funktioniert es?

Das Runbook `AWSSupport-ValidateFSxWindowsADConfig` führt das Amazon FSx-Validierungsskript auf der temporären Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instance aus, die vom Runbook im Amazon-Subnetz gestartet wurde. FSx Das Skript führt mehrere Prüfungen durch, um die Netzwerkkonnektivität zu selbstverwalteten AD/DNS Servern und die Berechtigungen des FSx Amazon-Servicekontos zu überprüfen. Das Runbook kann einen ausgefallenen oder falsch konfigurierten Amazon FSx for Windows File Server validieren oder einen neuen Amazon FSx for Windows File Server mit selbstverwaltetem AD erstellen.

Standardmäßig erstellt das Runbook die Amazon EC2 EC2-Windows-Instance, die Sicherheitsgruppe für den AWS Systems Manager (SSM) -Zugriff, die AWS Identity and Access Management (IAM) -Rolle und die Richtlinie, die im Amazon FSx-Subnetz verwendet CloudFormation wird. Wenn Sie das Skript auf einer vorhandenen Amazon EC2 EC2-Instance ausführen möchten, geben Sie die ID im Parameter `InstanceId` an. Bei erfolgreicher Ausführung werden die CloudFormation Ressourcen gelöscht. Um die Ressourcen beizubehalten, setzen Sie den `RetainCloudFormationStack` Parameter jedoch auf`true`.

Die CloudFormation Vorlage erstellt in Ihrem Namen eine IAM-Rolle mit den erforderlichen Berechtigungen, um sie an die Amazon EC2 EC2-Instance anzuhängen, um das FSx Amazon-Validierungsskript auszuführen. Verwenden Sie den Parameter, um ein vorhandenes IAM-Instance-Profil für die temporäre Instance anzugeben. `InstanceProfileName` Die zugehörige IAM-Rolle muss die folgenden Berechtigungen enthalten:

- `ec2:DescribeSubnets`und `ec2:DescribeVpcs` Berechtigungen und die Amazon Managed Policy`AmazonSSMManagedInstanceCore`.
- Berechtigungen zum Abrufen des Benutzernamens und des Kennworts des FSx Amazon-Servicekontos vom Systems Manager durch Aufrufen der `GetSecretValue` API.

- Berechtigungen zum Platzieren eines Objekts in den Amazon Simple Storage Service (Amazon S3) -Bucket für die Skriptausgabe.

Voraussetzungen

Das Subnetz, in dem die temporäre Amazon EC2 EC2-Instance erstellt wird (oder die im `InstanceId` Parameter angegebene vorhandene Instance), muss den Zugriff auf die Endpunkte AWS Systems Manager AWS Secrets Manager, und Amazon S3 ermöglichen, um das `AmazonFSxADValidation` Skript mit SSM Run Command auszuführen.

AWS Secrets Manager einrichten

Das Validierungsskript stellt eine Verbindung zur Microsoft AD-Domain her, indem es den Benutzernamen und das Passwort des FSx Amazon-Servicekontos mit einem Runtime-Aufruf von Secrets Manager abruft. Folgen Sie den Schritten unter Ein AWS Secrets Manager Geheimnis erstellen, um ein neues Secrets Manager-Geheimnis zu erstellen. Stellen Sie sicher, dass der Benutzername und das Passwort als key/value Paar im folgenden Format gespeichert sind`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`". Informationen zur Sicherung des Zugriffs auf geheime AWS Secrets Manager Daten finden Sie unter Authentifizierung und Zugriffskontrolle.

Weitere Informationen zu dem Tool finden Sie in den `README.md` Dateien `TROUBLESHOOTING.md` und in der FSxADValidationAmazon-Datei.

Ausführung des Runbooks

Führen Sie das Runbook mit Amazon FSx ID- oder AD-Parametern aus. Im Folgenden finden Sie den Runbook-Workflow:

- Ruft die Parameter von der FSx Amazon-ID ab oder verwendet die AD-Eingabeparameter.
- Erstellt die temporäre Validierungs-Amazon-EC2-Windows-Instance im FSx Amazon-Subnetz, Sicherheitsgruppe für SSM-Zugriff, IAM-Rolle und Richtlinie (bedingt) mithilfe. CloudFormation Wenn der `InstanceId` Parameter angegeben ist, wird er verwendet.
- Lädt das Validierungsskript auf die Amazon EC2 EC2-Zielinstanz im FSx primären Amazon-Subnetz herunter und führt es aus.
- Stellt den Ergebniscode der AD-Validierung in der Automatisierungsausgabe bereit. Darüber hinaus wird die vollständige Skriptausgabe in den Amazon S3 S3-Bucket hochgeladen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Beispiel für eine IAM-Richtlinie für die Funktion „Automation Assume Role“

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": "*"
                    }
                ]
            }
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-ValidateFSxWindowsADConfigim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie die folgenden Parameter ein, um das selbstverwaltete AD mit einem vorhandenen ausgefallenen oder falsch konfigurierten Amazon FSx zu validieren:
   - AutomationAssumeRole (Optional):

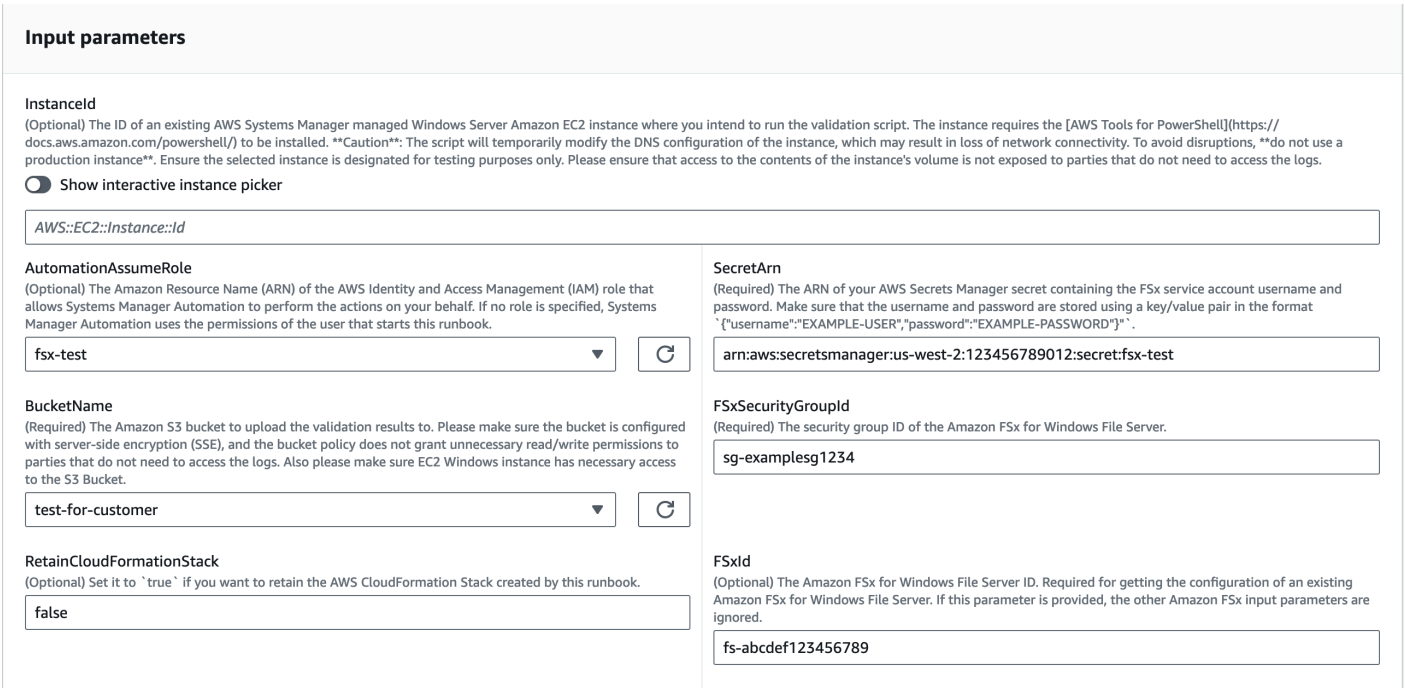
     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - FSxID (Bedingt):

     Die Dateiserver-ID von Amazon FSx für Windows. Dies ist erforderlich, um zu überprüfen, ob Amazon FSx bereits ausgefallen oder falsch konfiguriert ist.
   - SecretArn (Erforderlich):

     Der ARN Ihres Secrets Manager Manager-Geheimnisses, der den Benutzernamen und das Passwort des FSx Amazon-Servicekontos enthält. Stellen Sie sicher, dass der Benutzername und das Passwort als key/value Paar im folgenden Format gespeichert sind`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`. Der CloudFormation Stack erstellt die Validierungsinstanz mit Berechtigungen `GetSecretValue` zur Ausführung dieses ARN.
   - FSxSecurityGroupId (Erforderlich):

     Die Sicherheitsgruppen-ID für den Amazon FSx for Windows File Server.
   - BucketName (Erforderlich):

     Der Amazon S3 S3-Bucket, in den die Validierungsergebnisse hochgeladen werden sollen. Stellen Sie sicher, dass der Bucket mit serverseitiger Verschlüsselung (SSE) konfiguriert ist und dass die Bucket-Richtlinie Parteien, die nicht auf die Protokolle zugreifen müssen, keine unnötigen read/write Berechtigungen gewährt. Stellen Sie außerdem sicher, dass die Amazon EC2 EC2-Windows-Instance über den erforderlichen Zugriff auf den Amazon S3 S3-Bucket verfügt.



4. Um die selbstverwaltete AD-Konfiguration für eine neue FSx Amazon-Kreation zu validieren, geben Sie die folgenden Parameter ein:

   - AutomationAssumeRole (Optional):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

   - SecretArn (Erforderlich):

     Der ARN Ihres Secrets Manager Manager-Geheimnisses, der den Benutzernamen und das Passwort des FSx Amazon-Servicekontos enthält. Stellen Sie sicher, dass der Benutzername und das Passwort als key/value Paar im folgenden Format gespeichert sind`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`. Der CloudFormation Stack erstellt die Validierungsinstanz mit Berechtigungen `GetSecretValue` zur Ausführung dieses ARN.

   - FSxSecurityGroupId (Erforderlich):

     Die Sicherheitsgruppen-ID für den Amazon FSx for Windows File Server.

   - BucketName (Erforderlich):

Der Amazon S3 S3-Bucket, in den die Validierungsergebnisse hochgeladen werden sollen. Stellen Sie sicher, dass der Bucket mit serverseitiger Verschlüsselung (SSE) konfiguriert ist und dass die Bucket-Richtlinie Parteien, die nicht auf die Protokolle zugreifen müssen, keine unnötigen read/write Berechtigungen gewährt. Stellen Sie außerdem sicher, dass die Amazon EC2 EC2-Windows-Instance über den erforderlichen Zugriff auf den Amazon S3 S3-Bucket verfügt.

- FSxPreferredSubnetId(Befristet):

  Das bevorzugte Subnetz von Amazon FSx für Windows File Server.

- DomainName (Befristet):

  Der vollqualifizierte Domainname Ihrer selbstverwalteten Microsoft AD-Domain.

- DnsIpAddresses (Befristet):

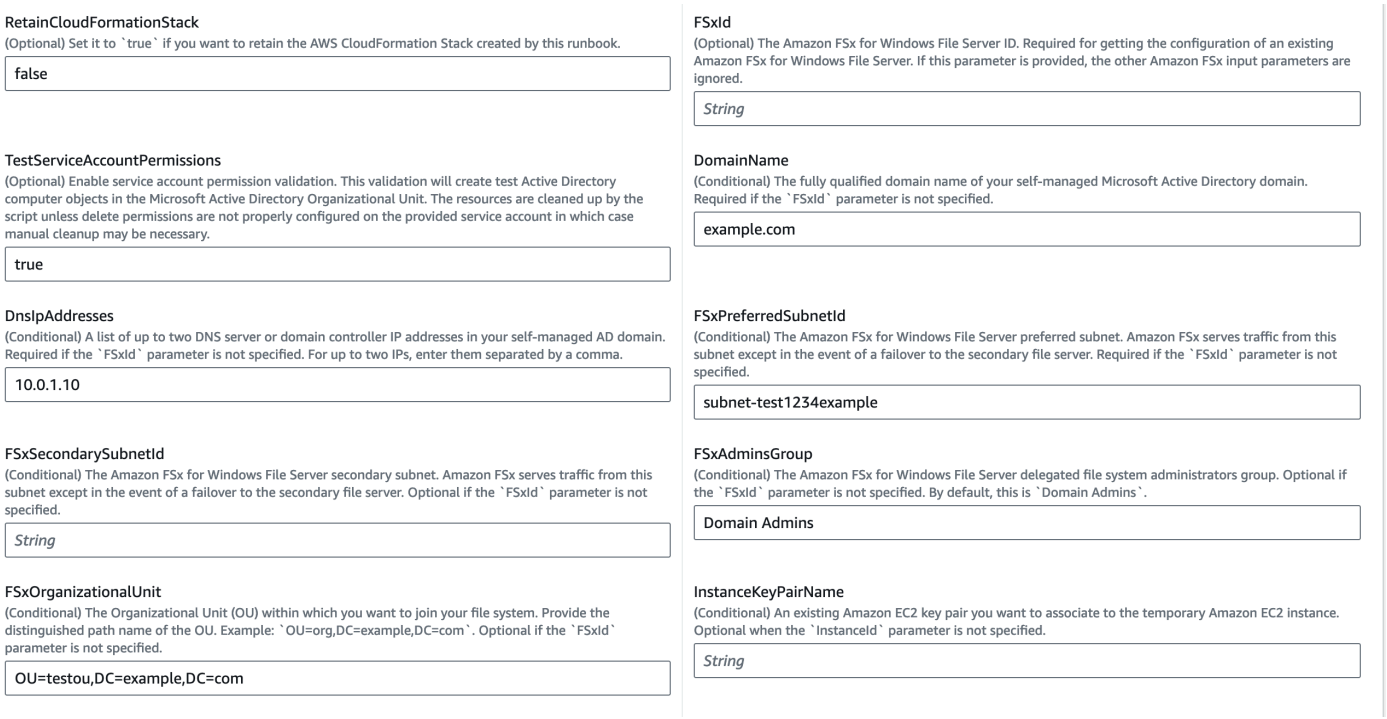
  Eine Liste mit bis zu zwei DNS-Server- oder Domänencontroller-IP-Adressen in Ihrer selbstverwalteten AD-Domäne. Geben Sie für bis zu zwei IPs Werte diese durch ein Komma getrennt ein.

- FSxAdminsGroup (Befristet):

  Die Gruppe der delegierten Dateisystemadministratoren von Amazon FSx für Windows File Server. Standardmäßig ist dies `Domain Admins`.

- FSxOrganizationalUnit(Befristet):

  Die Organisationseinheit (OU), innerhalb der Sie Ihr Dateisystem verbinden möchten. Geben Sie den definierten Pfadnamen der Organisationseinheit an. Beispiel: `OU=org,DC=example,DC=com`.



5. Wählen Sie Ausführen aus.
6. Die Automatisierung wird initiiert.
7. Das Dokument führt die folgenden Schritte aus:
   - CheckBucketPublicStatus(aws:ExecuteScript):

     Prüft, ob der Amazon S3 S3-Ziel-Bucket möglicherweise öffentlichen Lese- und and/or Schreibzugriff auf seine Objekte gewährt.
   - BranchOnInputParameters(aws:branch):

     Verzweigt nach den angegebenen Eingabeparametern wie FSx Amazon-ID oder FSx Amazon-Parametern.
   - AssertFileSystemTypeIsWindows(aws: assertAwsResource Eigentum):

     Wenn die FSx Amazon-ID angegeben ist, wird überprüft, ob der Dateisystemtyp Amazon FSx for Windows File Server ist.
   - GetValidationInputs(aws:ExecuteScript):

     Gibt die selbstverwaltete Microsoft AD-Konfiguration zurück, die für die CloudFormation Vorlage zum Erstellen der Amazon EC2 EC2-Instance erforderlich ist.
   - BranchOnInstanceId (aws:branch):

Verzweigt auf der angegebenen Eingabe. `InstanceId` Falls angegeben, `InstanceId` wird das Validierungsskript automatisch auf der Amazon EC2 EC2-Zielinstanz ausgeführt. `step:RunValidationScript`

- Erstellen EC2 InstanceStack (aws:CreateStack):

  Erstellt die Amazon EC2 EC2-Instance im bevorzugten Subnetz und verwendet den CloudFormation Ort, an dem das `AmazonFSxADValidation` Tool ausgeführt wird

- DescribeStackResources(aws:): executeAwsApi

  Beschreibt den CloudFormation Stack zum Abrufen der temporären Amazon EC2 EC2-Instance-ID.

- WaitForEC2InstanceToBeManaged(aws waitForAwsResourceProperty):

  Wartet, bis die Amazon EC2 EC2-Instance von Systems Manager verwaltet wird, um das Validierungsskript mit SSM Run Command auszuführen.

- GetAmazonFSxADValidationAnhang (aws): executeAwsApi

  Ruft die `AmazonFSxADValidation` Tool-URL aus den Runbook-Anhängen ab.

- RunValidationScript(aws:RunCommand):

  Führt das `AmazonFSxADValidation` Tool auf der temporären Amazon EC2 EC2-Instance aus und speichert das Ergebnis in dem im `BucketName` Parameter angegebenen Amazon S3 S3-Bucket.

- DescribeErrorsFromStackEvents(aws:ExecuteScript):

  Beschreibt die CloudFormation Stack-Ereignisse, falls die Runbooks den Stack nicht erstellen können.

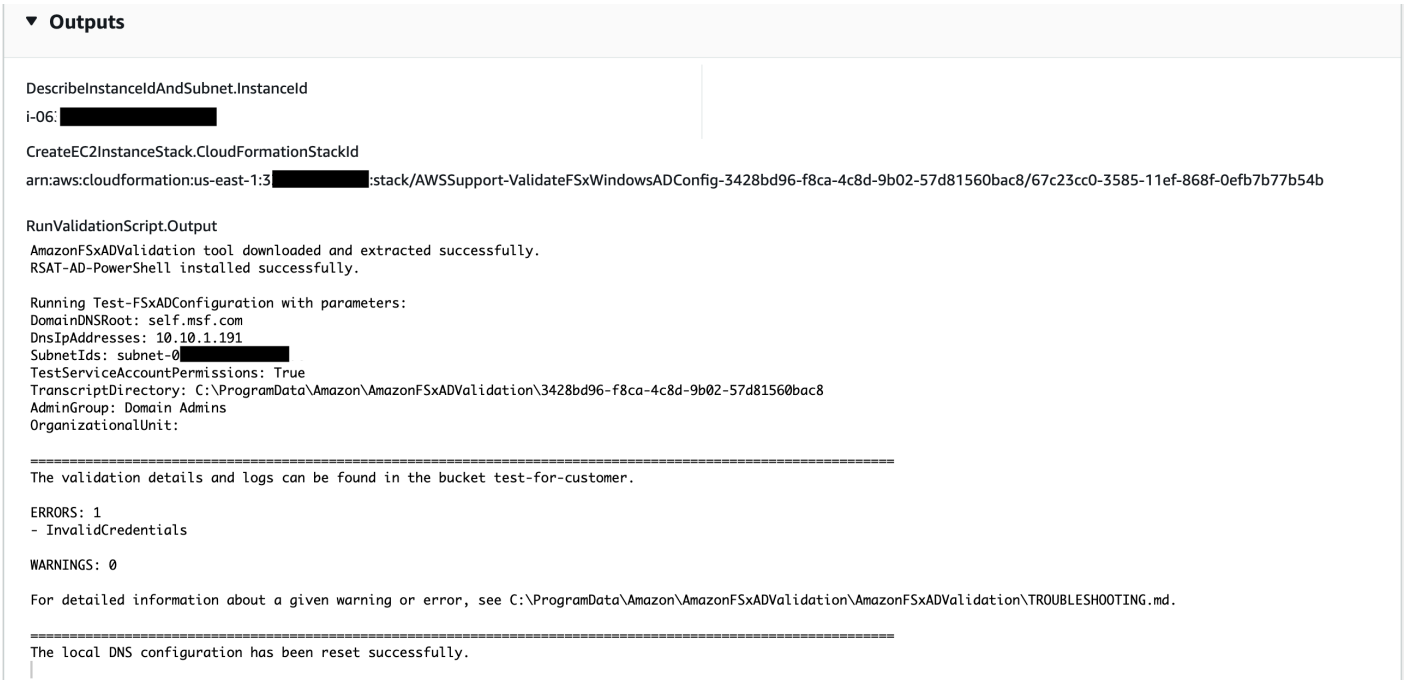
- BranchOnRetainCloudFormationStack(aws:branch):

  Verzweigt nach den `InstanceId` Parametern `RetainCloudFormationStack` und, um zu bestimmen, ob der CloudFormation Stack gelöscht werden soll.

- DeleteCloudFormationStack(aws:deleteStack):

  Löscht den CloudFormation Stapel.

8. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die Ergebnisse der Ausführung:



Das Runbook lädt die Ergebnisse der Ausführung des Überprüfungsskripts in den Amazon S3 S3-Bucket hoch.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS Servicedokumentation

- Was ist Amazon FSx for Windows File Server?
- Validierung der selbstverwalteten AD-Konfiguration für Amazon FSx for Windows File Server

GuardDuty

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon GuardDuty bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with

runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-CreateGuardDutyDetector

AWSConfigRemediation-CreateGuardDutyDetector

Beschreibung

Das `AWSConfigRemediation-CreateGuardDutyDetector` Runbook erstellt einen Amazon GuardDuty (GuardDuty) -Detektor in dem Bereich, in AWS-Region dem Sie die Automatisierung ausführen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `guardduty:CreateDetector`
- `guardduty:GetDetector`

Dokumentschritte

- `aws:executeAwsApi`- Erzeugt einen GuardDuty Detektor.
- `aws:assertAwsResourceProperty`- Überprüft, ob `Status` der Detektor aktiviert ist`ENABLED`.

IAM

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Identity and Access Management Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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-TroubleshootIAMAccessDeniedEvents

Beschreibung

Das AWSSupport-TroubleshootIAMAccessDeniedEvents Automation-Runbook hilft bei der Behebung von Problemen mit AWS Identity and Access Management verweigertem Zugriff (IAM). Das Runbook fragt CloudTrail nach aktuellen Ereignissen mit verweigertem Zugriff ab, die sich auf die angegebene IAM-Entität und AWS die Dienstereignisquelle beziehen. Es analysiert Ereignisse innerhalb eines konfigurierbaren Zeitfensters von bis zu 24 Stunden und verarbeitet bis zu 10 Ereignisse pro Ausführung. Jedes identifizierte Ereignis, bei dem der Zugriff verweigert wurde, wird untersucht, um den Kontext der Ablehnung und der versuchten Aktionen besser zu verstehen. Die Automatisierung analysiert sowohl identitäts- als auch ressourcenbasierte IAM-Richtlinien. Bei identitätsbasierten Richtlinien werden Inline- und verwaltete Richtlinien untersucht, die der IAM-Entität zugeordnet sind. Bei ressourcenbasierten Richtlinien werden Richtlinien für mehrere AWS Dienste bewertet, darunter Amazon Simple Storage Service (Amazon S3), AWS Key Management Service (AWS KMS) AWS Lambda, Amazon Simple Notification Service (Amazon SNS), Amazon Elastic Container Registry (Amazon ECR), Amazon API Gateway CodeArtifact, Amazon Elastic File System (Amazon EFS), Amazon Simple Queue Service (Amazon SQS), Amazon OpenSearch Service AWS Cloud9, Signer und. AWS AWS Serverless Application Repository AWS Secrets Manager

Das Runbook nutzt Funktionen zur Simulation von IAM-Richtlinien, um diese Richtlinien anhand der in den CloudTrail Ereignissen festgestellten abgelehnten Aktionen zu bewerten. Das Runbook nutzt die IAM-Funktionen zur Richtliniensimulation sowohl SimulatePrincipalPolicyfür IAM-Benutzer als auch für IAM-Rollen, um diese Richtlinien anhand der in den Ereignissen festgestellten abgelehnten Aktionen zu bewerten. SimulateCustomPolicy CloudTrail Die Automatisierung gibt einen Bericht aus, der dabei hilft, die spezifischen Aktionen zu identifizieren, die verweigert wurden. Dabei wird zwischen impliziten und expliziten Verweigerungen unterschieden, die für Zugriffsverweigerungen verantwortlichen Richtlinien aufgeführt und Erklärungen für jede Verweigerung bereitgestellt. Der Bericht schlägt auch mögliche Lösungen vor, z. B. die Identifizierung fehlender Genehmigungserklärungen oder widersprüchlicher Verweigerungserklärungen

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Beschreibt und validiert `RequesterARN` (Rolle oder Benutzer), um Informationen wie den IAM-Entitätstyp und die IAM-ID abzurufen.
- Ruft CloudTrail Ereignisse ab, die mit, und verknüpft sind `RequesterARNEventSource`, falls angegeben. `ResourceARN`
- Analysiert die CloudTrail Ereignisse, um die Aktion zu ermitteln, die ausgeführt wurde, als der Fehler „Zugriff verweigert“ zurückgegeben wurde. Anschließend werden alle IAM-Richtlinien untersucht, z. B. Inline-Richtlinien und verwaltete Richtlinien, die der IAM-Entität zugeordnet sind, sowie ressourcenbasierte Richtlinien. Anschließend werden diese Richtlinien anhand der Aktionen simuliert, die in den Fehlern „Zugriff verweigert“ bei den betreffenden CloudTrail Ereignissen gefunden wurden, um die Ursache des Fehlers zu ermitteln.
- Gibt einen Bericht aus, in dem die Art des Fehlers „Zugriff verweigert“ und die für die Fehler verantwortlichen Richtlinien ermittelt werden, und es werden Vorschläge für eine mögliche Lösung des Fehlers gemacht.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Beispiel für eine Richtlinie:

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"
            }
        ]
    }
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootIAMAccessDeniedEvents`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es SSM Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Die Rolle muss Ihrem Amazon EKS-Clusterzugriffseintrag oder Ihrer RBAC-Berechtigung hinzugefügt werden, um Kubernetes-API-Aufrufe zuzulassen.
     - Typ: `AWS::IAM::Role::Arn`
   - RequestErn (erforderlich):
     - Beschreibung: (Erforderlich) Der ARN des IAM-Benutzers oder der IAM-Rolle, für den Sie die Zugriffsberechtigungen für eine bestimmte AWS Ressource untersuchen möchten.
     - Typ: `String`
     - Muster zulassen: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
   - ResourceARN (optional):
     - Beschreibung: (Optional) Der ARN AWS der Ressource, für die der verweigerte Zugriff ausgewertet wird. Die AWS Zielressource sollte sich in derselben Region befinden, in der das Automatisierungs-Runbook ausgeführt wird.
     - Typ: `String`
     - Muster zulassen: `^$|^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 (Erforderlich):
     - Beschreibung: (Erforderlich) Der Amazon-API-Endpunkt, von dem das CloudTrail Ereignis ausgelöst wurde. Beispiel: `s3.amazonaws.com`.

- Typ: `String`
- Muster zulassen: `^([a-zA-Z0-9.-]+)\\.amazonaws\\.com$`

- EventName (Fakultativ):
  - Beschreibung: (Optional) Der Amazon-API-Aktionsname, der dem CloudTrail Ereignis zugeordnet ist. Beispiel: `s3:CreateBucket`.
  - Typ: `String`
  - Muster zulassen: `^$|^[a-z0-9]+:[A-Za-z0-9]+$`
- LookBackHours (Fakultativ):
  - Beschreibung: (Optional) Die Anzahl der Stunden, für die bei der Suche `Access Denied` nach Ereignissen in den CloudTrail Ereignissen zurückgegriffen werden soll. Gültiger Bereich: `1` bis `24` Stunden.
  - Typ: Ganzzahl
  - Muster zulassen: `^([1-9]|1[0-9]|2[0-4])$`
  - Standard: 12
- MaxEvents (Fakultativ):
  - Beschreibung: (Optional) Die maximale Anzahl von CloudTrail `Access Denied` Ereignissen, die bei der Suche nach Ereignissen zurückgegeben werden. Gültiger Bereich: `1` bis zu `5` Ereignissen.
  - Typ: Ganzzahl
  - Muster zulassen: `^([1-9]|1[0-9]|2[0-4])$`
  - Standard: 3
- UseContextEntries (Fakultativ):
  - Beschreibung: (Optional) Wenn Sie dies angeben`true`, extrahiert die Automatisierung Details zum Kontext der API-Anfrage aus dem CloudTrail Ereignis und bezieht sie in die IAM-Richtliniensimulation ein.
  - Typ: Boolescher Wert
  - Muster zulassen: `^([1-9]|1[0-9]|2[0-4])$`
  - Standard: 3

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

- ValidateRequesterArn

  Validiert und dekonstruiert den `RequesterArn` ARN und ruft Informationen über den IAM-Zielbenutzer oder die Zielrolle ab.

- GetCloudTrailEventsWithAccessDeniedError

  Fragt die CloudTrail Ereignisse nach aktuellen `Access Denied` Ereignissen ab, die sich auf die angegebene IAM-Entität und den angegebenen IAM-Dienst beziehen. AWS `EventSource`

- Evaluieren Sie die Richtlinien IAMRequester

  Vergleicht die IAM-Berechtigungen der IAM-Entität, die die Anfrage gestellt hat, anhand der Aktionen aus Ereignissen. CloudTrail Diese Bewertung umfasst die Analyse sowohl identitäts- als auch ressourcenbasierter Richtlinien im Zusammenhang mit dem Antragsteller. Die Automatisierung nutzt die Funktionen von IAM zur Richtliniensimulation, um diese Richtlinien im Kontext der bei den Ereignissen festgestellten abgelehnten Aktionen zu bewerten. CloudTrail

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt „Ergebnisse“ die detaillierten Ergebnisse der Ausführung:

   - PermissionEvaluationResults

     Gibt einen Bericht aus, der dabei hilft, die spezifischen Aktionen zu identifizieren, die verweigert wurden, wobei zwischen impliziten und expliziten Ablehnungen unterschieden wird. Außerdem werden die Richtlinien aufgeführt, die für Zugriffsverweigerungen verantwortlich sind, und es werden Erklärungen für jede Verweigerung bereitgestellt. Der Bericht schlägt auch mögliche Lösungen vor, z. B. die Identifizierung fehlender Genehmigungserklärungen oder widersprüchlicher Verweigerungserklärungen

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS-AttachIAMToInstance

Beschreibung

Ordnen Sie einer verwalteten Instanz eine AWS Identity and Access Management (IAM-) Rolle zu.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ForceReplace

  Typ: Boolescher Wert

  Beschreibung: (Optional) Markierung, um anzugeben, ob das vorhandene IAM-Profil ersetzt werden soll oder nicht.

  Standard: true
- InstanceId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der Instance, der Sie eine IAM-Rolle zuweisen möchten.

- RoleName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der IAM-Rolle, die der verwalteten Instanz hinzugefügt werden soll.

Dokumentschritte

1. `aws:executeAwsApi`- DescribeInstanceProfile - Suchen Sie das IAM-Instanzprofil, das der EC2-Instance zugeordnet ist.
2. `aws:branch`- CheckInstanceProfileAssociations - Überprüfen Sie das mit der EC2-Instance verknüpfte IAM-Instanzprofil.
   a. Wenn ein IAM-Instanzprofil angehängt und auf Folgendes eingestellt `ForceReplace` ist: `true`
      i. `aws:executeAwsApi`- DisassociateIamInstanceProfile - Trennen Sie das IAM-Instanzprofil von der EC2-Instance.
   b. `aws:executeAwsApi`- ListInstanceProfilesForRole - Listet die Instanzprofile für die angegebene IAM-Rolle auf.
   c. `aws:branch`- CheckInstanceProfileCreated - Prüfen Sie, ob der angegebenen IAM-Rolle ein zugeordnetes Instanzprofil zugeordnet ist.
      i. Wenn der IAM-Rolle ein Instanzprofil zugeordnet ist:
         A. `aws:executeAwsApi`- AttachIAM ProfileToInstance — Hängen Sie die IAM-Instance-Profilrolle an die EC2-Instance an.
      i. Wenn der IAM-Rolle kein Instanzprofil zugeordnet ist:
         A. `aws:executeAwsApi`- CreateInstanceProfileForRole - Erstellen Sie eine Instanzprofilrolle für die angegebene IAM-Rolle.
         B. `aws:executeAwsApi`- AddRoleToInstanceProfile - Ordnen Sie die Instanzprofilrolle der angegebenen IAM-Rolle zu.
         C. `aws:executeAwsApi`- GetInstanceProfile - Ruft die Instanzprofildaten für die angegebene IAM-Rolle ab.
         D. `aws:executeAwsApi`- AttachIAM ProfileToInstanceWithRetry — Hängt die IAM-Instanzprofilrolle an die EC2-Instance an.

Ausgaben

IAMProfileToInstanceWithRetryAnhängen. AssociationId

GetInstanceProfile.InstanceProfileName

GetInstanceProfile.InstanceProfileArn

Anhängen IAMProfileToInstance. AssociationId

ListInstanceProfilesForRole.InstanceProfileName

ListInstanceProfilesForRole.InstanceProfileArn

AWS-DeleteIAMInlinePolicy

Beschreibung

Das `AWS-DeleteIAMInlinePolicy` Runbook löscht alle AWS Identity and Access Management (IAM-) Inline-Richtlinien, die mit den von Ihnen angegebenen IAM-Identitäten verknüpft sind.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- IamArns

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der ARNs IAM-Identitäten, aus denen Sie Inline-Richtlinien löschen möchten. Diese Liste kann IAM-Benutzer, -Gruppen oder -Rollen enthalten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

Dokumentschritte

- `aws:executeScript`— Löscht die IAM-Inline-Richtlinien, die mit den Ziel-IAM-Identitäten verknüpft sind.

AWSConfigRemediation-DeleteIAMRole

Beschreibung

Das `AWSConfigRemediation-DeleteIAMRole` Runbook löscht die von Ihnen angegebene AWS Identity and Access Management (IAM-) Rolle. Durch diese Automatisierung werden keine Instanzprofile gelöscht, die der IAM-Rolle zugeordnet sind, oder dienstverknüpfte Rollen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- IAMRoleID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der IAM-Rolle, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfilesForRole`
- `iam:ListRolePolicies`
- `iam:ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

Dokumentschritte

- `aws:executeScript`- Erfasst den Namen der IAM-Rolle, die Sie im Parameter angeben. `IAMRoleID`
- `aws:executeScript`- Sammelt Richtlinien und Instanzprofile, die der IAM-Rolle zugeordnet sind.
- `aws:executeScript`- Löscht die angehängten Richtlinien.
- `aws:executeScript`— Löscht die IAM-Rolle und überprüft, ob die Rolle gelöscht wurde.

`AWSConfigRemediation-DeleteIAMUser`

Beschreibung

Das `AWSConfigRemediation-DeleteIAMUser` Runbook löscht den von Ihnen angegebenen AWS Identity and Access Management (IAM-) Benutzer. Durch diese Automatisierung werden die folgenden Ressourcen, die dem IAM-Benutzer zugeordnet sind, gelöscht oder getrennt:

- Access keys (Zugriffsschlüssel)
- Angehängte verwaltete Richtlinien
- Git-Anmeldeinformationen
- Mitgliedschaften in IAM-Gruppen
- IAM-Benutzerpasswort
- Eingebundene Richtlinien
- Geräte mit Multi-Faktor-Authentifizierung (MFA)
- Zertifikate signieren
- Öffentliche SSH-Schlüssel

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- IAMUserID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des IAM-Benutzers, den Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeScript- Erfasst den Benutzernamen des IAM-Benutzers, den Sie im Parameter angeben. IAMUserId
- aws:executeScript- Sammelt Zugriffsschlüssel, Zertifikate, Anmeldeinformationen, MFA-Geräte und SSH-Schlüssel, die dem IAM-Benutzer zugeordnet sind.
- aws:executeScript— Sammelt Gruppenmitgliedschaften und Richtlinien für den IAM-Benutzer.
- aws:executeScript- Löscht Zugriffsschlüssel, Zertifikate, Anmeldeinformationen, MFA-Geräte und SSH-Schlüssel, die dem IAM-Benutzer zugeordnet sind.
- aws:executeScript— Löscht Gruppenmitgliedschaften und Richtlinien für den IAM-Benutzer.
- aws:executeScript- Löscht den IAM-Benutzer und überprüft, ob der Benutzer gelöscht wurde.

AWSConfigRemediation-DeleteUnusedIAMGroup

Beschreibung

Das AWSConfigRemediation-DeleteUnusedIAMGroup Runbook löscht eine IAM-Gruppe, die keine Benutzer enthält.

Das AWSConfigRemediation-DeleteUnusedIAMGroup Runbook löscht eine IAM-Gruppe, die keine Benutzer enthält.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- GroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der IAM-Gruppe, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteGroup`
- `iam:DeleteGroupPolicy`
- `iam:DetachGroupPolicy`

Dokumentschritte

- `aws:executeScript`— Entfernt verwaltete IAM-Richtlinien und Inline-IAM-Richtlinien, die der IAM-Zielgruppe zugeordnet sind, und löscht dann die IAM-Gruppe.

AWSConfigRemediation-DeleteUnusedIAMPolicy

Beschreibung

Das AWSConfigRemediation-DeleteUnusedIAMPolicy Runbook löscht eine AWS Identity and Access Management (IAM-) Richtlinie, die keinen Benutzern, Gruppen oder Rollen zugeordnet ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- IAMResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID der IAM-Richtlinie, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- ssm:StartAutomationExecution

- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DeletePolicy
- iam:DeletePolicyVersion
- iam:GetPolicy
- iam:ListEntitiesForPolicy
- iam:ListPolicyVersions

Dokumentschritte

- aws:executeScript- Löscht die Richtlinie, die Sie im IAMResourceId Parameter angeben, und überprüft, ob die Richtlinie gelöscht wurde.

AWSConfigRemediation-DetachIAMPolicy

Beschreibung

Das AWSConfigRemediation-DetachIAMPolicy Runbook trennt die von Ihnen angegebene AWS Identity and Access Management (IAM-) Richtlinie.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- IAMResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der IAM-Richtlinie, die Sie trennen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DetachGroupPolicy`
- `iam:DetachRolePolicy`
- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`

Dokumentschritte

- `aws:executeScript`— Trennt die IAM-Richtlinie von allen Ressourcen.

AWSConfigRemediation-EnableAccountAccessAnalyzer

Beschreibung

Das `AWSConfigRemediation-EnableAccountAccessAnalyzer` Runbook erstellt einen AWS Identity and Access Management (IAM) Access Analyzer in Ihrem. AWS-Konto Informationen zu Access Analyzer finden Sie unter Using AWS IAM Access Analyzer im IAM-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AnalyzerName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des zu erstellenden Analyzers.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

Dokumentschritte

- `aws:executeAwsApi`- Erstellt einen Access Analyzer für Ihr Konto.
- `aws:waitForAwsResourceProperty`- Wartet auf den Status des Access Analyzers. `ACTIVE`
- `aws:assertAwsResourceProperty`- Bestätigt, dass der Status des Access Analyzers lautet`ACTIVE`.

`AWSSupport-GrantPermissionsToIAMUser`

Beschreibung

Dieses Runbook gewährt einer IAM-Gruppe (neu oder bereits vorhanden) die angegebenen Berechtigungen und fügt der Gruppe den vorhandenen IAM-Benutzer hinzu. Zur Auswahl stehende Richtlinien: Fakturierung oder Support. Denken Sie zur Aktivierung des Fakturierungszugriffs für IAM auch an die Aktivierung des Zugriffs von IAM-Benutzern und verbundenen Benutzern auf die Fakturierungs- und Kostenmanagement-Seiten.

> **Important**
>
> Wenn Sie eine vorhandene IAM-Gruppe bereitstellen, erhalten alle aktuellen IAM-Benutzer in der Gruppe die neuen Berechtigungen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- IAMGroupName

  Typ: Zeichenfolge

  Standard: ExampleSupportAndBillingGroup

  Beschreibung: (Erforderlich). Dabei kann es sich um eine neue oder vorhandene Gruppe handeln. Muss mit Einschränkungen für IAM-Entitätsnamen übereinstimmen.

- IAMUserName

  Typ: Zeichenfolge

  Standard: ExampleUser

  Beschreibung: (Erforderlich) Es muss sich um einen vorhandenen Benutzer handeln.

- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die Lambda annimmt.

- Berechtigungen

  Typ: Zeichenfolge

  Gültige Werte: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

  Standard: SupportAndBillingFullAccess

  Beschreibung: (Erforderlich) Wählen Sie eine der folgenden Optionen: `SupportFullAccess` Gewährt vollen Zugriff auf das Support Center. `BillingFullAccess`gewährt vollen Zugriff auf das Abrechnungs-Dashboard. `SupportAndBillingFullAccess`gewährt vollen Zugriff auf das Support Center und das Abrechnungs-Dashboard. Weitere Informationen zu den Richtlinien finden Sie unter „Dokumentdetails“.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Die erforderlichen Berechtigungen hängen davon ab, wie `AWSSupport-GrantPermissionsToIAMUser` das Programm ausgeführt wird.

Wird als der aktuell angemeldete Benutzer oder die aktuell angemeldete Rolle ausgeführt

Es wird empfohlen, die von `AmazonSSMAutomationRole` Amazon verwaltete Richtlinie und die folgenden zusätzlichen Berechtigungen beizufügen, um die Lambda-Funktion und die IAM-Rolle für die Übergabe an Lambda erstellen zu können:

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": "*"
        }
    ]
}
```

Verwenden von und AutomationAssumeRole LambdaAssumeRole

Der Benutzer muss über die StartAutomationExecution Berechtigungen ssm: für das Runbook und über PassRoleiam: für die IAM-Rollen verfügen, die als und übergeben wurden. AutomationAssumeRoleLambdaAssumeRole Hier finden Sie die Berechtigungen, die die einzelnen IAM-Rollen benötigen:

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

Dokumentschritte

1. `aws:createStack`- Führen Sie CloudFormation Template aus, um eine Lambda-Funktion zu erstellen.
2. `aws:invokeLambdaFunction`- Führen Sie Lambda aus, um IAM-Berechtigungen festzulegen.
3. `aws:deleteStack`- Vorlage löschen CloudFormation .

Ausgaben

configureIAM.Payload

AWSConfigRemediation-RemoveUserPolicies

Beschreibung

Das `AWSConfigRemediation-RemoveUserPolicies` Runbook löscht die AWS Identity and Access Management (IAM-) Inline-Richtlinien und trennt alle verwalteten Richtlinien, die dem von Ihnen angegebenen Benutzer zugewiesen sind.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- IAMUserID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Benutzers, für den Sie Richtlinien entfernen möchten.
- PolicyType

  Typ: Zeichenfolge

  Gültige Werte: Alle | Inline | Verwaltet

  Standard: Alle

  Beschreibung: (Erforderlich) Der Typ der IAM-Richtlinien, die Sie aus dem Benutzer entfernen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam:ListAttachedUserPolicies`

- `iam:ListUserPolicies`
- `iam:ListUsers`

Dokumentschritte

- `aws:executeScript`- Löscht und trennt IAM-Richtlinien von dem Benutzer, den Sie im Parameter angeben. `IAMUserID`

AWSConfigRemediation-ReplaceIAMInlinePolicy

Beschreibung

Das `AWSConfigRemediation-ReplaceIAMInlinePolicy` Runbook ersetzt eine Inline-Richtlinie AWS Identity and Access Management (IAM) durch eine replizierte verwaltete IAM-Richtlinie. Bei einer Inline-Richtlinie, die einem Benutzer, einer Gruppe oder einer Rolle zugewiesen ist, werden die Inline-Richtlinienberechtigungen in eine verwaltete IAM-Richtlinie geklont. Die verwaltete IAM-Richtlinie wird der Ressource hinzugefügt und die Inline-Richtlinie wird entfernt. AWS Config muss an dem Ort aktiviert sein AWS-Region , an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- InlinePolicyName

  Typ: StringList

  Beschreibung: (Erforderlich) Die Inline-IAM-Richtlinie, die Sie ersetzen möchten.

- ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des IAM-Benutzers, der Gruppe oder der Rolle, deren Inline-Richtlinie Sie ersetzen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:executeScript`- Ersetzen Sie die Inline-IAM-Richtlinie durch eine AWS replizierte Richtlinie für die von Ihnen angegebene Ressource.

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

Beschreibung

Das `AWSConfigRemediation-RevokeUnusedIAMUserCredentials` Runbook widerruft unbenutzte AWS Identity and Access Management (IAM-) Passwörter und aktive Zugriffsschlüssel. Dieses Runbook deaktiviert auch abgelaufene Zugriffsschlüssel und löscht abgelaufene Anmeldeprofile. AWS Config muss an dem Ort aktiviert sein, AWS-Region an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- IAMResourceID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der IAM-Ressource, für die Sie ungenutzte Anmeldeinformationen sperren möchten.

- MaxCredentialUsageAge

  Typ: Zeichenfolge

  Standard: 90

  Beschreibung: (Erforderlich) Die Anzahl der Tage, innerhalb derer die Anmeldeinformationen verwendet worden sein müssen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:ListDiscoveredResources`
- `iam:DeleteAccessKey`
- `iam:DeleteLoginProfile`
- `iam:GetAccessKeyLastUsed`
- `iam:GetLoginProfile`
- `iam:GetUser`
- `iam:ListAccessKeys`
- `iam:UpdateAccessKey`

Dokumentschritte

- `aws:executeScript`- Widerruft die IAM-Anmeldeinformationen für den im Parameter angegebenen Benutzer. `IAMResourceId` Abgelaufene Zugriffsschlüssel werden deaktiviert und abgelaufene Anmeldeprofile werden gelöscht.

> **Note**
>
> Stellen Sie sicher, dass der `MaxCredentialUsageAge` Parameter dieser Behebungsaktion so konfiguriert ist, dass er dem `maxAccessKeyAge` Parameter der AWS Config Regel entspricht, die Sie zum Auslösen dieser Aktion verwenden:. access-keys-rotated

`AWSConfigRemediation-SetIAMPasswordPolicy`

Beschreibung

Das `AWSConfigRemediation-SetIAMPasswordPolicy` Runbook legt die AWS Identity and Access Management (IAM-) Benutzerkennwortrichtlinie für Ihre fest. AWS-Konto

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- AllowUsersToChangePassword

  Typ: Boolescher Wert

  Standard: false

Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, AWS-Konto können alle IAM-Benutzer in Ihrem Konto den verwenden, um ihre AWS-Managementkonsole Passwörter zu ändern.

- HardExpiry

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, können IAM-Benutzer ihre Passwörter nach Ablauf des Kennworts nicht zurücksetzen.

- MaxPasswordAge

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die Anzahl der Tage, an denen das Passwort eines IAM-Benutzers gültig ist.

- MinimumPasswordLength

  Typ: Ganzzahl

  Standard: 6

  Beschreibung: (Optional) Die Mindestanzahl von Zeichen, die ein IAM-Benutzerkennwort haben darf.

- PasswordReusePrevention

  Typ: Ganzzahl

  Standard: 0

  Beschreibung: (Optional) Die Anzahl der vorherigen Passwörter, die ein IAM-Benutzer nicht wiederverwenden darf.

- RequireLowercaseCharacters

  Typ: Boolescher Wert

Standard: false

Beschreibung: (Optional) Wenn auf gesetzt`true`, muss das Passwort eines IAM-Benutzers einen Kleinbuchstaben aus dem lateinischen ISO-Alphabet (a bis z) enthalten.

- RequireNumbers

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt`true`, muss das Passwort eines IAM-Benutzers ein numerisches Zeichen (0-9) enthalten.

- RequireSymbols

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt`true`, muss das Passwort eines IAM-Benutzers ein nicht-alphanumerisches Zeichen enthalten (! @ # $% ^ * () _ + - = [] {} | ').

- RequireUppercaseCharacters

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt`true`, muss das Passwort eines IAM-Benutzers einen Großbuchstaben des lateinischen ISO-Grundalphabets (A bis Z) enthalten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

Dokumentschritte

- `aws:executeScript`- Legt die IAM-Benutzerkennwortrichtlinie auf der Grundlage der Werte fest, die Sie für die Runbook-Parameter für Ihren angeben. AWS-Konto

AWSSupport-ContainIAMPrincipal

Beschreibung

Im Falle eines Sicherheitsvorfalls oder einer vermuteten Kompromittierung eines AWS Identity and Access Management (IAM-) Benutzers/einer Rolle oder eines AWS Identity Center (IDC) - Benutzers ist eine schnelle Isolierung der betroffenen Identität von entscheidender Bedeutung, wobei ihre Konfiguration für die Untersuchung beibehalten werden muss. Das `AWSSupport-ContainIAMPrincipal` Runbook bietet einen strukturierten, umkehrbaren Ansatz zur Eindämmung kompromittierter IAM- oder IDC-Identitäten, wodurch deren Zugriff auf Ressourcen effektiv blockiert und eine mögliche Ausbreitung der Sicherheitslücke verhindert wird. AWS

Dieser automatisierte Prozess ermöglicht eine Untersuchung ohne dauerhafte Änderung der Konfiguration der Identität und ermöglicht die Wiederherstellung des normalen Zugriffs, wenn dies als angemessen erachtet wird. Der Containment-Prozess behält den Benutzer oder die Rolle innerhalb von IAM oder den Benutzer innerhalb von IDC bei und isoliert ihn gleichzeitig effektiv von allen Netzwerkaktivitäten. Diese Isolierung verhindert, dass die enthaltene Identitätsressource mit Ressourcen in Ihrer Amazon Virtual Private Cloud kommuniziert oder auf Internetressourcen zugreift. Die Eindämmung ist so konzipiert, dass sie reversibel ist, sodass der normale Zugriff wiederhergestellt werden kann, wenn dies als angemessen erachtet wird.

Wie funktioniert es?

Das `AWSSupport-ContainIAMPrincipal` Runbook implementiert einen umfassenden Eindämmungsprozess für IAM-Benutzer, -Rollen und Identity Center-Benutzer. Wenn es im `Contain` Modus ausgeführt wird, validiert es zunächst alle Eingabeparameter und führt Sicherheitsüberprüfungen für den angegebenen Amazon S3 S3-Bucket durch. Anschließend sammelt es detaillierte Informationen über den Ziel-IAM-Principal und wendet je nach Prinzipaltyp geeignete Eindämmungsmaßnahmen an. Für IAM-Benutzer werden die Zugriffstasten deaktiviert, der Konsolenzugriff entfernt und eine Ablehnungsrichtlinie angehängt. Für IAM-Rollen wird eine Ablehnungsrichtlinie angehängt, die Berechtigungen für Sitzungen widerruft, die vor der Beschränkung erstellt wurden. Für Identity Center-Benutzer werden Berechtigungssätze und Gruppenmitgliedschaften entfernt und eine Ablehnungsrichtlinie angewendet. Während

des gesamten Vorgangs sichert das Runbook die ursprüngliche Konfiguration zur möglichen Wiederherstellung in einem Amazon S3 S3-Bucket. Wenn es im `Restore` Modus ausgeführt wird, versucht es, den Principal mithilfe der gesicherten Konfiguration in seinen Zustand vor der Beschränkung zurückzusetzen. Das Runbook bietet eine `DryRun` Option zur Vorschau von Änderungen, ohne sie zu übernehmen, und bietet umfassende Berichte sowohl zu erfolgreichen Vorgängen als auch zu Fehlerszenarien.

Important

- Verwendung erhöhter Rechte: In diesem SSM-Dokument werden verschiedene Vorgänge ausgeführt, für die erhöhte Rechte erforderlich sind, z. B. das Ändern von IAM- und IDC-Identitätsrichtlinien und das Anwenden von Quarantänekonfigurationen. Diese Aktionen könnten möglicherweise zu einer Rechteerweiterung führen oder sich auf andere Workloads auswirken, die von den Zielidentitäten abhängen. Sie sollten die Berechtigungen überprüfen, die der durch den `AutomationAssumeRole` Parameter angegebenen Rolle gewährt wurden, und sicherstellen, dass sie für den beabsichtigten Anwendungsfall geeignet sind. Weitere Informationen zu IAM-Berechtigungen finden Sie in der folgenden AWS Dokumentation:
  - Identity and Access Management (IAM) -Berechtigungen
  - AWS Systems Manager Manager-Automatisierungsberechtigungen
- Risiken der Nichtverfügbarkeit von Workloads: In diesem Systems Manager Manager-Dokument werden Isolierungsmaßnahmen durchgeführt, die möglicherweise zu einer Nichtverfügbarkeit oder Unterbrechung Ihrer Workloads führen können. Wenn es während eines Sicherheitsereignisses ausgeführt wird, schränkt es den Zugriff auf die betroffene Ressource ein, indem AWS API-Berechtigungen für die angegebenen IAM- und IDC-Identitäten entzogen werden, sodass diese keine API-Aufrufe oder -Aktionen ausführen können. AWS Dies könnte sich auf alle Anwendungen oder Dienste auswirken, die von diesen Identitäten abhängen.
- Erstellung zusätzlicher Ressourcen: Das Automatisierungsdokument kann abhängig von den Ausführungsparametern bedingt zusätzliche Ressourcen erstellen, z. B. einen Amazon Simple Storage Service (Amazon S3) -Bucket und darin gespeicherte Amazon S3-Objekte. Für diese Ressourcen fallen je nach Nutzung zusätzliche Gebühren an AWS .
- Risiken bei der Wiederherstellung: Wenn der Parameter Action auf gesetzt ist`Restore`, versucht dieses SSM-Dokument, die IAM- oder IDC-Identitätskonfiguration in ihren ursprünglichen Zustand zurückzuversetzen. Es besteht jedoch das Risiko, dass der Wiederherstellungsprozess fehlschlägt und die IAM- oder IDC-Identität inkonsistent

bleibt. Das Dokument enthält Anweisungen für die manuelle Wiederherstellung im Falle solcher Fehler. Sie sollten jedoch darauf vorbereitet sein, mögliche Probleme während des Wiederherstellungsprozesses zu lösen.

Es wird empfohlen, das Runbook gründlich zu überprüfen, seine möglichen Auswirkungen zu verstehen und es in einer Nicht-Produktionsumgebung zu testen, bevor Sie es in Ihrer Produktionsumgebung ausführen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Für den `AutomationAssumeRole` Parameter sind die folgenden Berechtigungen erforderlich, um das Runbook erfolgreich verwenden zu können:

- s3: GetBucketLocation
- s3: GetBucket
- s3: ListBucket
- s3: GetBucketPublicAccessBlocks
- s3: GetAccountPublicAccessBlocks
- s3: GetBucketPolicyStatus
- s3: GetBucketAcl
- s3: GetObject
- s3: CreateBucket
- s3: PutObject

- bin: GetUser
- ich bin: GetUserPolicy
- ich bin: GetRole
- ich bin: ListUserPolicies
- ich bin: ListAttachedUserPolicies
- ich bin: ListAccessKeys
- ich bin: ListMfaDevices
- ich bin: ListVirtual MFADevices
- ich bin: GetLoginProfile
- ich bin: GetPolicy
- ich bin: GetRolePolicy
- ich bin: ListPolicies
- ich bin: ListAttachedRolePolicies
- ich bin: ListRolePolicies
- ich bin: UpdateAccessKey
- ich bin: CreateAccessKey
- ich bin: DeleteLoginProfile
- ich bin: DeleteAccessKey
- ich bin: PutUserPolicy
- ich bin: DeleteUserPolicy
- iam: deaktivieren MFADevice
- ich bin: AttachRolePolicy
- ich bin: AttachUserPolicy
- ich bin: DeleteRolePolicy
- Ich bin: Tag MFADevice
- ich bin: PutRolePolicy
- ich bin: TagPolicy
- ich bin: TagRole
- ich bin: TagUser
- ich bin: UntagUser

- ich bin: UntagRole
- Organisationen: ListAccounts
- so: ListPermissionSetsProvisionedToAccount
- sso: GetInlinePolicyForPermissionSet
- sso: ListInstances
- sso-Verzeichnis: SearchUsers
- sso: ListPermissionSets
- sso: ListAccountAssignments
- sso-Verzeichnis: DescribeUser
- Identitätsspeicher: ListUsers
- Identitätsspeicher: ListGroups
- Identitätsspeicher: IsMemberInGroups
- Identitätsspeicher: ListGroupMemberships
- Verwalter von Geheimnissen: CreateSecret
- Verwalter von Geheimnissen: DeleteSecret
- so: DeleteAccountAssignment
- sso: PutInlinePolicyToPermissionSet
- sso: CreateAccountAssignment
- sso: DeleteInlinePolicyFromPermissionSet
- sso: TagResource
- sso: UntagResource
- Identitätsspeicher: DeleteGroupMembership
- Identitätsspeicher: CreateGroupMembership

Hier ist ein Beispiel für eine IAM-Richtlinie, die die erforderlichen Berechtigungen gewährt für: `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": "*"
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-ContainIAMPrincipalin der AWS Systems Manager Manager-Konsole zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - PrincipalType (Erforderlich):
     - Beschreibung: (Erforderlich) Der AWS IAM-Prinzipaltyp: IAM-Benutzer, IAM-Rolle oder Identity Center-Benutzer.
     - Typ: Zeichenfolge
     - Zulässige Werte: `IAM user|IAM role|Identity Center user`

- PrincipalName (Erforderlich):
  - Beschreibung: (Erforderlich) Der Name des IAM-Prinzipals. Geben Sie für Identity Center-Benutzer den Benutzernamen ein.
  - Typ: Zeichenfolge
  - Zulässiges Muster: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/+=,@]{1,1024}$`
- Aktion (erforderlich):
  - Beschreibung: (Erforderlich) Wählen Sie `Contain` diese Option, um den Ziel-IAM-Prinzipal `Restore` zu isolieren oder zu versuchen, den IAM-Prinzipal auf seine ursprüngliche Konfiguration aus einem vorherigen Backup zurückzusetzen.
  - Typ: Zeichenfolge
  - Zulässige Werte: `Contain|Restore`
- DryRun (Fakultativ):
  - Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, nimmt die Automatisierung keine Änderungen am Ziel-IAM-Prinzipal vor, sondern gibt das aus, was sie zu ändern versucht hätte, und zwar mit detaillierten Angaben zu jedem Schritt. Standardwert: `true`.
  - Typ: Boolescher Wert
  - Zulässige Werte: `true|false`
- ActivateDisabledKeys(Bedingt):
  - Beschreibung: (Bedingt) Wenn der Eingabeparameter Action auf `Restore` und der auf IAM-Benutzer gesetzt PrincipalType ist, bestimmt diese Option, ob diese Automatisierung versuchen soll, die zugehörigen Zugriffstasten zu aktivieren, falls sie deaktiviert sind. Bitte beachten Sie, dass die Integrität eines kompromittierten Zugriffsschlüssels nicht überprüft werden kann. AWS rät dringend davon ab, einen kompromittierten Schlüssel erneut zu aktivieren. Stattdessen ist es ratsam, neue Schlüssel zu generieren. Standardwert: `false`.
  - Typ: Boolescher Wert
  - Zulässige Werte: `true|false`
- Backups 3 BucketName (bedingt):
  - Beschreibung: (Bedingt) Der Amazon Amazon S3 S3-Bucket zum Sichern der IAM-Prinzipalkonfiguration, wenn die Aktion auf festgelegt ist, `Contain` oder zum Wiederherstellen der Konfiguration ab dem Zeitpunkt, an dem die Aktion aktiviert ist`Restore`. Beachten Sie, dass, wenn die angegebene Aktion lautet `Contain` und das Runbook nicht auf den Bucket zugreifen kann oder kein Wert angegeben wird, in Ihrem Konto ein neuer Bucket mit dem

Namen erstellt wird. awssupport-containiamprincipal-<random-string> Wenn auf true diesen Parameter gesetzt DryRun ist, ist dies erforderlich.

  - Typ: AWS::S3::Bucket::Name
- BackupS3 KeyName (bedingt):
  - Beschreibung: (Bedingt) Wenn Action auf gesetzt istRestore, gibt dies den Amazon Amazon S3 S3-Schlüssel an, mit dem die Automatisierung versucht, die IAM-Prinzipalkonfiguration wiederherzustellen. Der Amazon Amazon S3 S3-Schlüssel folgt normalerweise diesem Format:{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json. Der Schlüssel kann aus der Ausgabe einer früheren Ausführung der Containment-Automatisierung abgerufen werden.
  - Typ: Zeichenfolge
  - Zulässiges Muster: ^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$
- Backups 3 BucketAccess (bedingt):
  - Beschreibung: (Bedingt) Der ARN der IAM-Benutzer oder -Rollen, denen nach der Ausführung der Containment-Aktionen Zugriff auf den Amazon S3-Backup-Backup gewährt wird. Dieser Parameter ist erforderlich, wenn Action den Wert hat. Contain Der Benutzer AutomationAssumeRole, in dessen Kontext die Automatisierung ausgeführt wird, oder, falls er nicht vorhanden ist, wird automatisch zur Liste hinzugefügt.
  - Typ: StringList
  - Zulässiges Muster: ^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$
- TagIdentifier (Fakultativ):
  - Beschreibung: (Optional) Taggen Sie den IAM-Prinzipal mit einem Tag Ihrer Wahl im folgenden Format:Key=<EXAMPLE_KEY>,Value=<EXAMPLE_VALUE>. Mit dieser Option können Sie die IAM-Prinzipale verfolgen, auf die dieses Runbook abzielt. Hinweis: Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
  - Typ: Zeichenfolge
  - Zulässiges Muster: ^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\._\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\._\\:\\/@a-zA-Z0-9]{0,128}$

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:

- ValidateRequiredInputs

  Validiert die erforderlichen Eingabeparameter für die Automatisierung auf der Grundlage der `Action` angegebenen Parameter.

- CheckBackupS3BucketName

  Prüft, ob der Amazon Amazon S3 S3-Ziel-Bucket potenziell `write` öffentlichen Zugriff auf seine Objekte gewährt`read`. Im Falle eines Containment-Workflows wird ein neuer Amazon Amazon S3 S3-Bucket erstellt, falls der `BackupS3BucketName` Bucket nicht existiert.

- BranchOnAction

  Verzweigt die Automatisierung auf der Grundlage des angegebenen `Action` Werts.

- BranchOnPrincipalTypeAndDryRun

  Verzweigt die Automatisierung basierend auf dem Typ des IAM-Prinzipals (IAM-Benutzer, IAM-Rolle oder Identity Center-Benutzer) und ob sie im Modus ausgeführt wird. `DryRun`

- BranchOnPrincipalTypeForContain

  Verzweigt die Automatisierung nach dem in der Eingabe angegebenen `Contain` aktionsbasierten und dem IAM-Prinzipaltyp (IAM-Benutzer, IAM-Rolle oder Identity Center-Benutzer).

- Holen IAMUser

  Ruft die Erstellungszeit und den Benutzernamen des IAM-Zielbenutzers ab.

- Details abrufen IAMUser

  Ruft die Konfiguration des IAM-Zielbenutzers ab und speichert sie, einschließlich Inline-Richtlinien, verwalteten Richtlinien, Zugriffsschlüsseln, MFA-Geräten und Anmeldeprofilen.

- Updates (3) KeyForUser

  Aktualisiert die Automatisierungsvariable 'S3Key' anhand der Ausgabe des Schritts. `GetIAMUserDetails`

- Holen IAMRole

  Ruft die Erstellungszeit, den Rollennamen und den Pfad der IAM-Zielrolle ab.

- Details abrufen IAMRole

Ruft die Konfiguration der IAM-Zielrolle ab und speichert sie, einschließlich Inline-Richtlinien und verwalteter Richtlinien, die der Rolle zugeordnet sind.

- Updates (3) KeyForRole

  Aktualisiert die Automatisierungsvariable 'S3Key' anhand der Ausgabe des Schritts. `GetIAMRoleDetails`

- GetIdentityStoreId

  Ruft die ID der AWS IAM Identity Center-Instanz ab, die dem Konto zugeordnet ist. AWS

- Holen IDCUser

  Ruft die Benutzer-ID des Identity Center-Zielbenutzers mithilfe der Identity Store-ID ab.

- Sammeln Sie IDCUser Details

  Ruft die Konfiguration des Identity Center-Zielbenutzers ab und speichert sie, einschließlich Kontozuweisungen, zugehöriger Berechtigungssätze und Inline-Richtlinien.

- Updates (3) KeyFor IDCUser

  Aktualisiert die Automatisierungsvariable 'S3Key' anhand der Ausgabe des Schritts. `GatherIDCUserDetails`

- BranchOnIdentityContain

  Verzweigt die Automatisierung auf der Grundlage des Werts von `DryRun` und des IAM-Prinzipaltyps für die Aktion. `Contain`

- BranchOnDisableAccessKeys

  Verzweigt die Automatisierung basierend darauf, ob der IAM-Benutzer über Zugriffsschlüssel verfügt, die deaktiviert werden müssen.

- DisableAccessKeys

  Deaktiviert die aktiven IAM-Benutzerzugriffsschlüssel.

- BranchOnDisableConsoleAccess

  Verzweigt je nachdem, ob für den IAM-Benutzer der Zugriff auf die AWS Management Console aktiviert ist oder nicht.

- DisableConsoleAccess

Entfernt den kennwortbasierten Zugriff des IAM-Benutzers auf die Management Console. AWS

- AttachInlineDenyPolicyToUser

  Fügt dem IAM-Benutzer eine Ablehnungsrichtlinie hinzu, mit der er Berechtigungen für ältere Sitzungstoken entziehen kann.

- AttachInlineDenyPolicyToRole

  Fügt der IAM-Rolle eine Ablehnungsrichtlinie hinzu, um Berechtigungen für ältere Sitzungstoken zu widerrufen.

- RemovePermissionSets

  Entfernt die mit dem Identity Center-Benutzer verknüpften Berechtigungssätze.

- Entfernen IDCUser von IDCGroups

  Entfernt den Identity Center-Benutzer aus Identity Center-Gruppen.

- AttachInlineDenyPolicyToPermissionSet

  Fügt den Berechtigungssätzen, die dem Identity Center-Benutzer zugeordnet sind, eine Ablehnungsrichtlinie an.

- BranchOnReactivateKeys

  Verzweigt die Automatisierung auf der Grundlage des `ActivateDisabledKeys` Parameters während des Wiederherstellungsvorgangs.

- DetachInlineDenyPolicy

  Entfernt die Ablehnungsrichtlinie, die der IAM-Rolle während des Eindämmungsprozesses zugewiesen wurde.

- DetachInlineDenyPolicyFromPermissionSet

  Entfernt die Ablehnungsrichtlinie, die den Berechtigungssätzen während des Eindämmungsprozesses zugewiesen wurde.

- ReportContain

  Gibt detaillierte Informationen zu den Eindämmungsaktionen aus, die ausgeführt würden, wenn diese Einstellung auf gesetzt `DryRun` ist. `True`

- ReportRestore

Gibt detaillierte Informationen zu den Wiederherstellungsaktionen aus, die ausgeführt würden, wenn auf `True` gesetzt `DryRun` ist.

- ReportContainFailure

  Enthält umfassende Anweisungen zur manuellen Wiederherstellung der ursprünglichen Konfiguration des IAM-Prinzipals während eines Ausfallszenarios für den Containment-Workflow.

- ReportRestoreFailure

  Enthält detaillierte Anweisungen zum manuellen Abschließen der Wiederherstellung der ursprünglichen Konfiguration des IAM-Prinzipals während eines Ausfallszenarios für den Wiederherstellungs-Workflow.

7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   - EnthaltenIAMPrincipal. Ausgabe

     Enthält detaillierte Informationen zu den Containment-Aktionen, die ausgeführt werden, wenn Action auf Contain und auf DryRun False gesetzt ist. Enthält Informationen zum Backup-Speicherort, zu den angewandten Ablehnungsrichtlinien und zu den geänderten Konfigurationen.

   - WiederherstellenIAMPrincipal. Ausgabe

     Enthält detaillierte Informationen zu den Wiederherstellungsaktionen, die ausgeführt werden, wenn Action auf Restore und dann auf False gesetzt DryRun ist. Enthält Informationen zu den wiederhergestellten Konfigurationen und zu allen Problemen, die bei der Wiederherstellung aufgetreten sind.

   - ReportContain. Ausgabe

     Gibt detaillierte Informationen zu den Containment-Aktionen aus, die ausgeführt würden, wenn Action auf Contain gesetzt und auf True gesetzt DryRun ist. Beinhaltet einen Vergleich der aktuellen Konfigurationen und der Konfigurationen nach der Eindämmung.

   - ReportRestore. Ausgabe

     Gibt detaillierte Informationen zu den Wiederherstellungsaktionen aus, die ausgeführt würden, wenn Action auf Restore gesetzt und auf True gesetzt DryRun ist. Zeigt die aktuelle Konfiguration und die ursprüngliche Konfiguration an, die wiederhergestellt werden würde.

- ReportContainFailure. Ausgabe

  Enthält umfassende Anweisungen zur manuellen Wiederherstellung der ursprünglichen Konfiguration des IAM-Prinzipals während eines Ausfallszenarios für den Containment-Workflow.

- ReportRestoreFailure. Ausgabe

  Enthält detaillierte Anweisungen zum manuellen Abschließen der Wiederherstellung der ursprünglichen Konfiguration des IAM-Prinzipals bei einem Fehlschlagszenario für den Wiederherstellungs-Workflow.

Ausgaben

Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse:

- Contain. IAMPrincipal Output

  Enthält detaillierte Informationen zu den Containment-Aktionen, die ausgeführt werden, wenn Action auf Contain und auf DryRun False gesetzt ist. Enthält Informationen zum Backup-Speicherort, zu den angewandten Ablehnungsrichtlinien und zu den geänderten Konfigurationen.

- WiederherstellenIAMPrincipal. Ausgabe

  Enthält detaillierte Informationen zu den Wiederherstellungsaktionen, die ausgeführt werden, wenn Action auf Restore und dann auf False gesetzt DryRun ist. Enthält Informationen zu den wiederhergestellten Konfigurationen und zu allen Problemen, die bei der Wiederherstellung aufgetreten sind.

- ReportContain. Ausgabe

  Gibt detaillierte Informationen zu den Containment-Aktionen aus, die ausgeführt würden, wenn Action auf Contain gesetzt und auf True gesetzt DryRun ist. Beinhaltet einen Vergleich der aktuellen Konfigurationen und der Konfigurationen nach der Eindämmung.

- ReportRestore. Ausgabe

  Gibt detaillierte Informationen zu den Wiederherstellungsaktionen aus, die ausgeführt würden, wenn Action auf Restore gesetzt und auf True gesetzt DryRun ist. Zeigt die aktuelle Konfiguration und die ursprüngliche Konfiguration an, die wiederhergestellt werden würde.

- ReportContainFailure. Ausgabe

Enthält umfassende Anweisungen zur manuellen Wiederherstellung der ursprünglichen Konfiguration des IAM-Prinzipals während eines Ausfallszenarios für den Containment-Workflow.

- ReportRestoreFailure. Ausgabe

  Enthält detaillierte Anweisungen zum manuellen Abschließen der Wiederherstellung der ursprünglichen Konfiguration des IAM-Prinzipals bei einem Fehlschlagszenario für den Wiederherstellungs-Workflow.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Ausführen einer einfachen Automatisierung
- Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

AWSSupport-TroubleshootSAMLIssues

Beschreibung

Das AWSSupport-TroubleshootSAMLIssues Automation Runbook hilft bei der Diagnose von Problemen im Zusammenhang mit Security Assertion Markup Language (SAML), indem es die in Amazon Simple Storage Service (Amazon S3) gespeicherten SAML-Antwortdateien analysiert. Es führt eine umfassende Validierung durch, einschließlich Schemaverifizierung, Signaturvalidierung, Überprüfung von Zielgruppeneinschränkungen und Überprüfung der Ablaufzeit. Das Runbook dekodiert und extrahiert wichtige SAML-Elemente wie Aussteller, Assertionen, Betreff, Bedingungen, Signaturen und Attribute aus der SAML-Antwort. In Umgebungen, in denen SAML für den Zugriff auf AWS Ressourcen (wie Amazon Connect oder Amazon WorkSpaces Applications) über einen IAM-Identitätsanbieter verwendet wird, überprüft es, ob die Zertifikate in den SAML-Antwortsignaturen mit den im IAM Identity Provider konfigurierten Zertifikaten übereinstimmen.

Wie funktioniert das?

Das Runbook führt die folgenden Schritte aus:

- Überprüft das SAML-Antwortformat und die erforderlichen Elemente.

- Dekodiert und extrahiert SAML-Antwortkomponenten (Aussteller, Assertionen, Betreff, Bedingungen, Signaturen, Attribute).
- Überprüft digitale Signaturen anhand von IAM Identity Provider-Zertifikaten, sofern diese bereitgestellt werden.
- Überprüft die Zielgruppeneinschränkungen und die zeitliche Gültigkeit.
- Stellt detaillierte Diagnoseinformationen bereit, die die analysierte SAML-Struktur und die Validierungsergebnisse aufzeigen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Beispiel für eine Richtlinie:

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"
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Bevor Sie dieses Runbook verwenden können, müssen Sie eine Base64-kodierte SAML-Antwort (TXT-Datei) erfassen und in einem S3-Bucket speichern. Anweisungen zum Erfassen von SAML-Antworten finden Sie in diesem Dokument
2. Navigieren Sie `AWSSupport-TroubleshootSAMLIssues`im Systems Manager unter Dokumente zu.
3. Wählen Sie Execute automation (Automatisierung ausführen).
4. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, die es SSM Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - InputFileS3URI (erforderlich):
     - Beschreibung: (Erforderlich) Amazon Simple Storage Service (Amazon S3) URI der SAML-Antwort-TXT-Datei (z. B. s3://bucket - name/path/to/file .txt).
     - Typ: Zeichenfolge
     - Muster zulassen: `^s3://[a-z0-9][a-z0-9.-][a-z0-9](/.)?$`
   - S3 OutputPrefix (fakultativ):
     - <executionID of the runbook>Beschreibung: (Optional) Die Analyseausgabedateien werden im Eingabe-Bucket unter dem Namen „saml_analysis_ .json“ gespeichert. Sie können diesen Parameter verwenden, wenn Sie eine Datei mit einem bestimmten Präfix ausgeben möchten. <executionID of the runbook>Der Standardwert ist „output/“. In diesem Fall lautet die Datei-URI, die das Ergebnis ausgibt, 's3://bucket - name/output/saml _analysis_ .json'.
     - Typ: Zeichenfolge
     - Muster zulassen: `^[a-zA-Z0-9+=,.@\\-_/]*/$`
   - ExpectedAudience (Fakultativ):
     - Beschreibung: (Optional) Erwarteter Zielgruppenwert in der SAML-Antwort. Wenn nicht angegeben, verwenden `urn:amazon:webservices` wir. Wenn Sie in Ihrem IdP- und SP-Setup einen bestimmten Zielgruppenwert konfiguriert haben, geben Sie bitte das genaue Format an (z. B.`urn:amazon:webservices`,`https://signin.aws.amazon.com/saml`).
     - Typ: Zeichenfolge
     - Standard: urn:amazon:webservices

- IamIdProviderArn (Fakultativ):
  - Beschreibung: (Optional) Wenn Sie eine IAM-ID-Provider-Entität verwenden, um Ihren IdP direkt mit AWS IAM zu verknüpfen, geben Sie bitte deren ARN an (z. B.). `arn:aws:iam::<account-id>:saml-provider/<provider-name>`
  - Typ: Zeichenfolge
  - Muster zulassen: `^$|^arn:aws:iam::[0-9]{12}:saml-provider/[a-zA-Z0-9_-]+$`
- SAMLAuthenticationZeit (optional):
  - Beschreibung: (Optional) Datum und Uhrzeit der SAML-Authentifizierung. Die Zeitzone muss UTC sein. Muss im YYYY-MM-DDThh Format:mm:ss vorliegen (z. B. 2025-02-01T 10:00:00). Wenn dieser Parameter nicht angegeben wird, werden Ablaufprüfungen anhand des aktuellen Zeitstempels durchgeführt.
  - Typ: Zeichenfolge
  - Muster zulassen: `^$|^\\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[12]\\d|3[01])T(?:[01]\\d|2[0-3]):[0-5]\\d:[0-5]\\d$`
- S3 BucketOwnerRoleArn (fakultativ):
  - Beschreibung: (Optional) IAM-Rollen-ARN für den Zugriff auf die Amazon S3 S3-Buckets. Der ARN der IAM-Rolle mit den Berechtigungen zum Abrufen der Einstellungen für den öffentlichen Zugriff auf den Amazon S3 S3-Bucket und das Konto, zur Konfiguration der Bucket-Verschlüsselung, zum Bucket, zum Bucket ACLs, zum Bucket-Richtlinienstatus und zum Hochladen von Objekten in den Bucket. Wenn dieser Parameter nicht angegeben ist, verwendet das Runbook den `AutomationAssumeRole` (falls angegeben) oder den Benutzer, der dieses Runbook startet (falls `AutomationAssumeRole` nicht angegeben ist).
  - Typ: `AWS::IAM::Role::Arn`

5. Wählen Sie Ausführen aus.
6. Die Automatisierung wird initiiert.
7. Das Dokument führt die folgenden Schritte aus:
   - Bestätigen IAMIDProvider

     Überprüft den bereitgestellten IAM-ID-Provider-ARN, indem geprüft wird, ob er existiert und zugänglich ist. Wenn kein ARN angegeben wird, wird die Validierung übersprungen und der Schritt wird erfolgreich abgeschlossen.
   - Prüft S 3 BucketPublicStatus

Prüft, ob der Amazon S3 S3-Bucket anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen zulässt. Wenn der Bucket diese Berechtigungen zulässt, stoppt die Automatisierung bei diesem Schritt.

- Prüft (3) ObjectExistence

  Validiert den Zugriff auf die Amazon S3 S3-Buckets. Prüft, ob der Bucket und das Objekt existieren und ob die Automatisierung über die erforderlichen Berechtigungen verfügt, um aus der Quelle zu lesen und in das Ziel zu schreiben.

- Analysieren SAMLResponse

  Analysiert die SAML-Antwortdatei, indem die Prüfungen durchgeführt werden (Schemavalidierung, Signaturüberprüfung, Zielgruppenvalidierung, Ablaufprüfung). Generiert einen detaillierten JSON-Bericht und speichert ihn am angegebenen Amazon S3 S3-Speicherort.

8. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:
   - Der Abschnitt Ausgaben enthält Informationen über das Amazon S3 S3-Objekt, in dem die Analyseergebnisse beschrieben werden.
9. Das Amazon S3 S3-Objekt in den Analyseergebnissen ist eine JSON-Datei mit den folgenden Informationen:
   - validation_result: enthält grundlegende Validierungsergebnisse der SAML-Antwort.
     - saml_info: Wichtige SAML-Informationen, einschließlich Aussteller, Signaturen und Assertionen.
     - schema_validation: Ergebnisse der SAML-Schemavalidierung.
   - verification result: liefert detailliertere Diagnoseergebnisse.
     - Signatur: Ergebnisse der Signaturüberprüfung.
     - Zielgruppe: Ergebnisse der Überprüfung der Zielgruppeneinschränkungen.
     - Ablauf: Ergebnisse der Überprüfung der Ablaufzeit.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus

- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

Erkennung und Reaktion auf Vorfälle

AWS Systems Manager Automation bietet vordefinierte Runbooks für die Erkennung und Reaktion auf AWS Vorfälle. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSPremiumSupport-OnboardWorkloadToIDR

`AWSPremiumSupport-OnboardWorkloadToIDR`

Beschreibung

Das AWSPremiumSupport-OnboardWorkloadToIDRRunbook unterstützt AWS Enterprise Support-Kunden dabei, mithilfe von Incident Detection and Response einen Workload für die Überwachung und das Management kritischer AWS Vorfälle zu integrieren. Ein Workload kann als eine Sammlung von AWS Ressourcen definiert werden, die einer AWS Ressourcengruppe oder einer AWS Service AppRegistry Catalog-Anwendung zugeordnet sind. Wenn keine AWS Ressourcengruppe oder eine AWS Service AppRegistry Catalog-Anwendung angegeben ist, erstellt das Runbook in Ihrem Namen mithilfe von Tagfiltern oder der AWS CloudFormation Stack-ID, deren Ressourcen Sie in die Gruppe aufnehmen möchten, eine Ressourcengruppe. Wenn Sie den Parameter `CreateApplicationInsights` auf setzen`Yes`, stellt die Automatisierung eine Amazon CloudWatch Application Insights-Anwendung bereit, die verwendet AWS CloudFormation. CloudWatch Application Insights richtet empfohlene Metriken und Protokolle für ausgewählte Anwendungsressourcen mithilfe von CloudWatch Amazon-Statistiken, Protokollen und Ereignissen für Benachrichtigungen zu erkannten Problemen ein.

> **Important**
>
> Dieses Runbook führt abhängig von den angegebenen Eingabeparametern die folgenden Aktionen in Ihrem Konto aus:

- Erstellt eine neue AWS Ressourcengruppe unter Verwendung von „ AWS CloudFormation if“ `ResourceGroupName` oder `AppRegistryApplication` „not“. Nachdem der Stack erstellt wurde, versucht das Runbook, den Kündigungsschutz einzurichten.
- Kennzeichnet die dem Workload zugeordnete AWS Ressourcengruppe, einschließlich des `aws_idr` Tags.
- Erstellt eine auf Amazon CloudWatch Application Insights Resource basierende Anwendung, wenn der `CreateApplicationInsights` Eingabeparameter auf `Yes` gesetzt ist. Nachdem der Stack erstellt wurde, versucht das Runbook, den Terminierungsschutz für den Stack festzulegen.
- Installiert die `AWSServiceRoleForHealth_EventProcessor` Service-Linked Role (SLR), um Zugriff auf Incident Detection and Response für die Erfassung von Warnmeldungen zu gewähren, wenn der `InstallServiceLinkedRole` Eingabeparameter auf gesetzt ist. `Yes`
- Erstellt einen AWS Supportfall mit AWS Incident Detection and Response.

Important

Um dieses Runbook nutzen und AWS Incident Detection and Response nutzen zu können, benötigen Sie ein AWS Enterprise Support (gegen Aufpreis) oder ein Unified Operations-Abonnement. Weitere Informationen finden Sie unter Support Tarife vergleichen.

Wie funktioniert es?

Das Runbook führt die folgenden allgemeinen Schritte aus:

- Prüft, ob der aktuelle AWS Account Support Plan Enterprise ist; andernfalls endet die Automatisierung.
- Legt anhand der angegebenen Parameter fest, ob eine vorhandene AWS Ressourcengruppe verwendet oder eine neue erstellt werden soll.
- Generiert beim Erstellen einer neuen Ressourcengruppe eine AWS CloudFormation Vorlage und erstellt den Stapel mit den entsprechenden Tags.
- Versieht die Ressourcengruppe mit den erforderlichen AWS Incident-Detection- und Response-Tags.

- Installiert optional die serviceverknüpfte Rolle für AWS Incident Detection and Response.
- Erstellt optional eine Amazon CloudWatch Application Insights-Anwendung für eine verbesserte Überwachung.
- Erstellt einen AWS Support-Fall, um den Onboarding-Prozess abzuschließen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Beispiel für eine Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSPremiumSupport-OnboardWorkloadToIDR`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):
     - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem

Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

  - Typ: `AWS::IAM::Role::Arn`
- WorkloadName (Erforderlich):
  - Beschreibung: (Erforderlich) Der Name des Workloads. Wenn nicht angegeben, `ResourceGroupName` wird der Workload-Name verwendet, um eine neue AWS Ressourcengruppe mit dem Namen einzurichten`IDR-AWS-<WorkloadName>`.
  - Typ: `String`
  - Muster zulassen: `^[a-zA-Z0-9_-]{1,128}$`
- WorkloadDescription (Erforderlich):
  - Beschreibung: (Erforderlich) Die Beschreibung des Workloads. Geben Sie eine kurze Beschreibung ein, um die Anwendungsfälle dieses Workloads detailliert zu beschreiben. Bitte geben Sie den primären Endbenutzer und die Funktion dieses Workloads an.
  - Typ: `String`
  - Muster zulassen: `^[a-zA-Z0-9.:;,-_&() ]{1,1024}$`
- AppRegistryApplication (Fakultativ):
  - Beschreibung: (Optional) Der Name oder die ID der AWS Service AppRegistry Catalog-Anwendung. Falls nicht angegeben, müssen Sie eine Eingabe für angeben`ResourceGroupName`.
  - Typ: `String`
  - Muster zulassen: `^$|^[a-zA-Z0-9.-_]{1,128}$`
  - Standard: `""`
- ResourceGroupName (Fakultativ):
  - Beschreibung: (Optional) Der Name einer vorhandenen AWS Ressourcengruppe, falls er nicht angegeben `AppRegistryApplication` wird. Wenn Sie eine Ressourcengruppe erstellen möchten, müssen Sie eine Eingabe für eine neue Ressourcengruppe angeben `TagFilters` und optional `ResourceTypeFilters` eine neue AWS Ressourcengruppe erstellen.
  - Typ: `String`
  - Muster zulassen: `^$|^[a-zA-Z0-9_.-]{1,128}$`
  - Standard: `""`
- TagFilters (Bedingt):

    - Beschreibung: (Bedingt) Die Liste der Paare key/values (Zeichenfolge/Zeichenkettenliste), die mit den Tags verglichen werden, die an Ihre AWS Ressourcen angehängt sind. Dieser Parameter wird verwendet, um eine neue AWS Ressourcengruppe zu erstellen, wenn Sie kein `ResourceGroupName` vorhandenes oder angeben. `AppRegistryApplication`
    - Typ: `StringMap`
- ResourceTypeFilters (Bedingt):
    - Beschreibung: (Bedingt) Die Liste der Ressourcentypen, die von Resource Groups unterstützt werden.
    - Typ: `StringList`
    - Max. Anzahl Artikel: `10`
    - Standard: `AWS::AllSupported`
- InstallServiceLinkedRole (Fakultativ):
    - Beschreibung: (Optional) Wählen Sie `Yes` diese Option, um die `AWSServiceRoleForHealth_EventProcessor` serviceverknüpfte Rolle (SLR) zu installieren.
    - Typ: `String`
    - Zulässige Werte: `[Yes,No]`
    - Standard: `No`
- CreateApplicationInsights (Fakultativ):
    - Beschreibung: (Optional) Wählen Sie `Yes` diese Option, um eine auf Amazon CloudWatch Application Insights Resource basierende Anwendung auf Gruppenbasis zu erstellen.
    - Typ: `String`
    - Zulässige Werte: `[Yes,No]`
    - Standard: `No`
- ComplianceAndRegulatoryRequirements (Erforderlich):
    - Beschreibung: (Erforderlich) Geltende and/or regulatorische Compliance-Anforderungen für diesen Workload und alle Maßnahmen, die AWS nach einem Vorfall erforderlich sind.
    - Typ: `String`
    - Muster zulassen: `^[a-zA-Z0-9.:;,\\-_&() ]{1,1024}$`
- Nicht AWSComponents (optional):

  - Beschreibung: (Optional) Geben Sie bitte alle lokalen Komponenten oder AWS Komponenten anderer Anbieter für diesen Workload an? Falls ja, um welche handelt es sich dabei und welche Funktionen erfüllen sie?
  - Typ: `String`
  - Muster zulassen: `^$|^[a-zA-Z0-9.:;,\\-_&() ]{1,1024}$`
  - Standard: `""`
- UpstreamDownstreamDependencies (Fakultativ):
  - Beschreibung: (Optional) Einzelheiten zu allen upstream/downstream Komponenten, die nicht integriert sind und sich bei einem Ausfall auf diese Arbeitslast auswirken könnten.
  - Typ: `String`
  - Muster zulassen: `^$|^[a-zA-Z0-9.:;,\\-_&() ]{1,1024}$`
  - Standard: `""`
- FailoverDisasterRecoveryPlan (Fakultativ):
  - Beschreibung: (Optional) Geben Sie Einzelheiten zu allen manuellen oder automatisierten failover/disaster Wiederherstellungsplänen auf AZ- und regionaler Ebene an.
  - Typ: `String`
  - Muster zulassen: `^$|^[a-zA-Z0-9.:;,\\-_&() ]{1,1024}$`
  - Standard: `""`
- BridgeDetails (Fakultativ):
  - Beschreibung: (Optional) Die statische incident/crisis Verwaltungsbrücke, die von Ihrem Unternehmen eingerichtet wurde. Wenn Sie eine nicht statische Bridge verwenden, geben Sie Ihre bevorzugte Anwendung an. Diese Informationen AWS werden bei einem Vorfall abgefragt.
  - Typ: `String`
  - Zulässige Werte: `[Amazon Chime bridge, Non-Static bridge, Static bridge]`
  - Standard: `Amazon Chime bridge`
- SubscriptionStartDate (Erforderlich):
  - Beschreibung: (Erforderlich) Das Datum im `YYYY-MM-DD` Format, an dem Sie Ihr Abonnement für AWS Incident Detection and Response starten möchten.
  - Typ: `String`
  - Muster zulassen: `^(202[4-9]|20[3-9][0-9])-(0[1-9]|1[0-2])-(0[1-9]|[12][0-9]|3[01])$`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - AWSSupportPlan überprüfen:

     Prüft, ob der aktuelle AWS Account Support Plan Enterprise ist; andernfalls endet die Automatisierung.
   - BranchOnResourceGroup:

     Verzweigt die Automatisierung danach, ob eine bestehende AWS Ressourcengruppe bereitgestellt wurde. Falls nicht angegeben, erstellt die Automatisierung eine neue AWS Ressourcengruppe.
   - GetAppRegistryApplication:

     Ruft Metadateninformationen über die AWS Service AppRegistry Catalog-Anwendung ab, sofern diese bereitgestellt werden.
   - GenerateResourceGroupTemplate:

     Generiert eine AWS CloudFormation Vorlage für die AWS Ressourcengruppe mit den angegebenen Tagfiltern.
   - CreateResourceGroup:

     Erstellt eine neue AWS Ressourcengruppe mithilfe von AWS CloudFormation.
   - TagResourceGroup:

     Kennzeichnet die Ressourcengruppe mit den erforderlichen IDR-Tags (AWS Incident Detection and Response).
   - InstallServiceLinkedRole:

     Installiert auf AWS Anfrage die dienstbezogene Rolle Incident Detection and Response (IDR).
   - CreateApplicationInsightsApplication:

     Erstellt auf Anfrage eine Amazon CloudWatch Application Insights-Anwendung.
   - CreateAwsSupportCase:

     Erstellt einen AWS Supportfall mit AWS Incident Detection and Response.

7. Nach Abschluss der Ausführung finden Sie im Abschnitt Outputs die detaillierten Ergebnisse der Ausführung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows
- Beginnen Sie mit AWS Incident Detection and Response
- Erkennung von Arbeitslasten bei der Erkennung und Reaktion auf Vorfälle

Amazon Kinesis Data Streams

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Kinesis Data Streams bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableKinesisStreamEncryption

`AWS-EnableKinesisStreamEncryption`

Beschreibung

Das `AWS-EnableKinesisStreamEncryption` Runbook ermöglicht die Verschlüsselung auf Amazon Kinesis Data Streams (Kinesis Data Streams). Bei Producer-Anwendungen, die in einen verschlüsselten Stream schreiben, treten Fehler auf, wenn sie keinen Zugriff auf den Schlüssel AWS Key Management Service ()AWS KMS haben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- KinesisStreamName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Streams, für den Sie die Verschlüsselung aktivieren möchten.
- KeyId

  Typ: Zeichenfolge

  Standard: alias/aws/kinesis

  Beschreibung: (Erforderlich) Der vom Kunden verwaltete AWS KMS Schlüssel, den Sie für die Verschlüsselung verwenden möchten. Dieser Wert kann ein global eindeutiger Bezeichner, ein ARN für einen Alias oder einen Schlüssel oder ein Aliasname mit dem Präfix „alias/“ sein. Sie können den AWS verwalteten Schlüssel auch verwenden, indem Sie den Standardwert für den Parameter verwenden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

Dokumentschritte

- VerifyKinesisStreamStatus (`aws:waitforAwsResourceProperty`) - Überprüft den Status der Kinesis Data Streams.
- EnableKinesisStreamEncryption (`aws:executeAwsApi`) — Aktiviert die Verschlüsselung für die Kinesis Data Streams.
- VerifyKinesisStreamUpdateComplete (`aws:waitForAwsResourceProperty`) — Wartet darauf, dass der Status von Kinesis Data Streams wieder erreicht ist. `ACTIVE`
- VerifyKinesisStreamEncryption (`aws:assertAwsResourceProperty`) — Überprüft, ob die Verschlüsselung für die Kinesis Data Streams aktiviert ist.

AWS KMS

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS Key Management Service Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-CancelKeyDeletion
- AWSConfigRemediation-EnableKeyRotation

`AWSConfigRemediation-CancelKeyDeletion`

Beschreibung

Das `AWSConfigRemediation-CancelKeyDeletion` Runbook storniert das Löschen des AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels, den Sie angeben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- KeyId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des vom Kunden verwalteten Schlüssels, für den Sie den Löschvorgang abbrechen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CancelKeyDeletion`
- `kms:DescribeKey`

Dokumentschritte

- `aws:executeAwsApi`- Bricht das Löschen des vom Kunden verwalteten Schlüssels ab, den `KeyId` Sie im Parameter angeben.
- `aws:assertAwsResourceProperty`- Bestätigt, dass das Löschen von Schlüsseln für Ihren vom Kunden verwalteten Schlüssel deaktiviert ist.

`AWSConfigRemediation-EnableKeyRotation`

Beschreibung

Das `AWSConfigRemediation-EnableKeyRotation` Runbook ermöglicht die automatische Schlüsselrotation für den symmetrischen AWS Key Management Service (AWS KMS), vom Kunden verwalteten Schlüssel.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- KeyId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des vom Kunden verwalteten Schlüssels, für den Sie die automatische Schlüsselrotation aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die automatische Schlüsselrotation für den vom Kunden verwalteten Schlüssel, den Sie im `KeyId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Bestätigt, dass die automatische Schlüsselrotation für Ihren vom Kunden verwalteten Schlüssel aktiviert ist.

Lambda

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Lambda Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing
- AWSConfigRemediation-DeleteLambdaFunction
- AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK
- AWSConfigRemediation-MoveLambdaToVPC
- AWSSupport-RemediateLambdaS3Event
- AWSSupport-TroubleshootLambdaInternetAccess
- AWSSupport-TroubleshootLambdaS3Event

`AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing`

Beschreibung

Das `AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing` Runbook aktiviert AWS X-Ray Live-Tracing für die AWS Lambda Funktion, die Sie im Parameter angeben. `FunctionName`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- FunctionName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name oder der ARN der Lambda-Funktion, für die die Ablaufverfolgung aktiviert werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `lambda:UpdateFunctionConfiguration`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die Röntgenverfolgung für die Lambda-Funktion, die Sie im `FunctionName` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft, ob die Röntgenverfolgung für die Lambda-Funktion aktiviert wurde.

Ausgaben

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Antwort vom `UpdateFunctionConfiguration` API-Aufruf.

AWSConfigRemediation-DeleteLambdaFunction

Beschreibung

Das `AWSConfigRemediation-DeleteLambdaFunction` Runbook löscht die von Ihnen AWS Lambda angegebene Funktion.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- LambdaFunctionName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Lambda-Funktion, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

Dokumentschritte

- `aws:executeAwsApi`- Löscht die im Parameter angegebene Lambda-Funktion. `LambdaFunctionName`
- `aws:executeScript`— Überprüft, ob die Lambda-Funktion gelöscht wurde.

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

Beschreibung

Das `AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` Runbook verschlüsselt im Ruhezustand die Umgebungsvariablen für die AWS Lambda (Lambda-) Funktion, die Sie mit einem AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssel angeben. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass die Umgebungsvariablen Ihrer Lambda-Funktion gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Funktionen mit unterschiedlichen, vom Kunden verwalteten Schlüsseln zu verschlüsseln.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- FunctionName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name oder der ARN der Lambda-Funktion, deren Umgebungsvariablen Sie verschlüsseln möchten.
- KMSKeyArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des vom AWS KMS Kunden verwalteten Schlüssels, den Sie zur Verschlüsselung der Umgebungsvariablen Ihrer Lambda-Funktion verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Dokumentschritte

- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die `LastUpdateStatus` Eigenschaft aktiviert ist. `Successful`
- `aws:executeAwsApi`- Verschlüsselt die Umgebungsvariablen für die Lambda-Funktion, die Sie im `FunctionName` Parameter angeben, mithilfe des vom AWS KMS Kunden verwalteten Schlüssels, den `KMSKeyArn` Sie im Parameter angeben.
- `aws:assertAwsResourceProperty`— Bestätigt, dass die Verschlüsselung für die Umgebungsvariablen für Ihre Lambda-Funktion aktiviert ist.

AWSConfigRemediation-MoveLambdaToVPC

Beschreibung

Das `AWSConfigRemediation-MoveLambdaToVPC` Runbook verschiebt eine AWS Lambda (Lambda-) Funktion in eine Amazon Virtual Private Cloud (Amazon VPC).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- FunctionName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name der Lambda-Funktion, die zu einer Amazon VPC verschoben werden soll.

- SecurityGroupIds

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Sicherheitsgruppe, die IDs Sie den Elastic Network Interfaces (ENIs) zuweisen möchten, die mit Ihrer Lambda-Funktion verknüpft sind.

- SubnetIds

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Das Subnetz, für das IDs Sie die Elastic Network-Schnittstellen (ENIs) erstellen möchten, die Ihrer Lambda-Funktion zugeordnet sind.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Dokumentschritte

- `aws:executeAwsApi`- Aktualisiert die Amazon VPC-Konfiguration für die Lambda-Funktion, die Sie im `FunctionName` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die Lambda-Funktion aktiviert `LastUpdateStatus` ist. `successful`
- `aws:executeScript`— Überprüft, ob die Amazon VPC-Konfiguration der Lambda-Funktion erfolgreich aktualisiert wurde.

AWSSupport-RemediateLambdaS3Event

Beschreibung

Das `AWSSupport-TroubleshootLambdaS3Event` Runbook bietet eine automatisierte Lösung für die in den AWS Knowledge Center-Artikeln beschriebenen Verfahren Warum löst meine Amazon S3 S3-Ereignisbenachrichtigung nicht meine Lambda-Funktion aus? und warum erhalte ich die Fehlermeldung „Die folgenden Zielkonfigurationen können nicht validiert werden“, wenn ich eine Amazon S3 S3-Ereignisbenachrichtigung erstelle, um meine Lambda-Funktion auszulösen? Mit diesem Runbook können Sie ermitteln und beheben, warum eine Amazon Simple Storage Service (Amazon S3) -Ereignisbenachrichtigung die von Ihnen angegebene AWS Lambda Funktion nicht ausgelöst hat. Wenn in der Runbook-Ausgabe vorgeschlagen wird, die Parallelität Ihrer Lambda-Funktion zu validieren und zu konfigurieren, finden Sie weitere Informationen unter Asynchroner Aufruf und Funktionsskalierung.AWS Lambda

> **Note**
>
> Fehler „Die folgenden Zielkonfigurationen konnten nicht überprüft werden“ können auch aufgrund falscher Amazon S3-Ereigniskonfigurationen von Amazon Simple Notification Service (Amazon SNS) und Amazon Simple Queue Service (Amazon SQS) auftreten. Dieses Runbook überprüft nur Lambda-Funktionskonfigurationen. Wenn Sie nach der Verwendung des Runbooks immer noch die Fehlermeldung „Die folgenden Zielkonfigurationen können nicht validiert werden“ angezeigt wird, überprüfen Sie bitte alle vorhandenen Amazon SNS- und Amazon SQS Amazon S3 S3-Eventkonfigurationen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LambdaFunctionArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der Lambda-Funktion.
- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, dessen Ereignisbenachrichtigungen die Lambda-Funktion auslösen.
- Action

  Typ: Zeichenfolge

  Gültige Werte: Troubleshooting | Remediate

  Beschreibung: (Erforderlich) Die Aktion, die das Runbook ausführen soll. `Troubleshoot`Diese Option hilft bei der Identifizierung von Problemen, führt jedoch keine Mutationsaktionen durch, um das Problem zu lösen. `Remediate`Diese Option hilft bei der Identifizierung von Problemen und versucht, sie für Sie zu lösen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`

- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

Dokumentschritte

- `aws:branch`- Verzweigungen, die auf der für den `Action` Parameter angegebenen Eingabe basieren.

  Wenn der angegebene Wert wie folgt lautet`Troubleshoot`:

  - `aws:executeAutomation`- Führt das `AWSSupport-TroubleshootLambdaS3Event` Runbook aus.
  - `aws:executeAwsApi`- Überprüft die Ausgabe des `AWSSupport-TroubleshootLambdaS3Event` Runbooks, das im vorherigen Schritt ausgeführt wurde.

  Wenn der angegebene Wert wie folgt lautet`Remediate`:

  - `aws:executeScript`— Führt ein Skript aus, um die im Abschnitt Warum löst meine Amazon S3 S3-Ereignisbenachrichtigung meine Lambda-Funktion nicht aus? beschriebenen Probleme zu beheben. und warum erhalte ich die Fehlermeldung „Die folgenden Zielkonfigurationen können nicht validiert werden“, wenn ich eine Amazon S3 S3-Ereignisbenachrichtigung erstelle, um meine Lambda-Funktion auszulösen? Artikel im Knowledge Center.

Ausgaben

CheckOutput.Output

Korrigieren Sie das Lambdas3-Ereignis. Ausgabe

`AWSSupport-TroubleshootLambdaInternetAccess`

Beschreibung

Das `AWSSupport-TroubleshootLambdaInternetAccess` Runbook hilft Ihnen bei der Behebung von Internetzugriffsproblemen für eine AWS Lambda Funktion, die in Amazon Virtual Private Cloud (Amazon VPC) gestartet wurde. Ressourcen wie Subnetzrouten, Sicherheitsgruppenregeln und

ACL-Regeln (Network Access Control List) werden überprüft, um sicherzustellen, dass ausgehender Internetzugang zulässig ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- FunctionName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Lambda-Funktion, für die Sie Probleme mit dem Internetzugang beheben möchten.
- destinationIp

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ziel-IP-Adresse, zu der Sie eine ausgehende Verbindung herstellen möchten.
- destinationPort

  Typ: Zeichenfolge

Standard: 443

Beschreibung: (Optional) Der Zielport, über den Sie eine ausgehende Verbindung herstellen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

Dokumentschritte

- `aws:executeScript`- Überprüft die Konfiguration verschiedener Ressourcen in Ihrer VPC, in der die Lambda-Funktion gestartet wurde.
- `aws:branch`— Verzweigungen, die darauf basieren, ob sich die angegebene Lambda-Funktion in einer VPC befindet oder nicht.
- `aws:executeScript`- Überprüft die Routentabellenrouten für das Subnetz, in dem die Lambda-Funktion gestartet wurde, und stellt sicher, dass Routen zu einem NAT-Gateway (Network Address Translation) und einem Internet-Gateway vorhanden sind. Bestätigt, dass sich die Lambda-Funktion nicht in einem öffentlichen Subnetz befindet.
- `aws:executeScript`- Überprüft, ob die der Lambda-Funktion zugeordnete Sicherheitsgruppe ausgehenden Internetzugang auf der Grundlage der für die `destinationIp` Parameter und angegebenen Werte zulässt. `destinationPort`
- `aws:executeScript`- Überprüft die ACL-Regeln, die den Subnetzen der Lambda-Funktion zugeordnet sind, und das NAT-Gateway ermöglicht ausgehenden Internetzugang auf der Grundlage der für die Parameter und angegebenen Werte. `destinationIp` `destinationPort`

Ausgaben

checkVPC.vpc — Die ID der VPC, auf der Ihre Lambda-Funktion gestartet wurde.

CheckVPC.Subnet — Das der Subnetze, in denen IDs Ihre Lambda-Funktion gestartet wurde.

CheckVPC.SecurityGroups — Sicherheitsgruppen, die der Lambda-Funktion zugeordnet sind.

checkNACL.nacl — Analysenachricht mit Ressourcennamen. `LambdaIp`bezieht sich auf die private IP-Adresse der elastic network interface für Ihre Lambda-Funktion. Das `LambdaIpRules` Objekt wird nur für Subnetze generiert, die eine Route zu einem NAT-Gateway haben. Der folgende Inhalt ist ein Beispiel für die Ausgabe.

```
{
   "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 / destionation 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 / destionation port in Ingress rule"
   }
}
```

checkSecurityGroups.secgrps — Analyse für die Sicherheitsgruppe, die Ihrer Lambda-Funktion zugeordnet ist. Der folgende Inhalt ist ein Beispiel für die Ausgabe.

```
{
   "sg-123456789":{
```

```
      "Status":"Allowed",
      "Analysis":"This security group has allowed destintion IP and port in its
 outbuond rule."
   }
}
```

CheckSubnet.Subnets — Analyse für die Subnetze in Ihrer VPC, die Ihrer Lambda-Funktion zugeordnet sind. Der folgende Inhalt ist ein Beispiel für die Ausgabe.

```
{
   "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

Beschreibung

Das `AWSSupport-TroubleshootLambdaS3Event` Runbook bietet eine automatisierte Lösung für die in den AWS Knowledge Center-Artikeln beschriebenen Verfahren Warum löst meine Amazon S3 S3-Ereignisbenachrichtigung nicht meine Lambda-Funktion aus? und warum erhalte ich die Fehlermeldung „Die folgenden Zielkonfigurationen können nicht validiert werden“, wenn ich eine Amazon S3 S3-Ereignisbenachrichtigung erstelle, um meine Lambda-Funktion auszulösen? Mit diesem Runbook können Sie ermitteln, warum eine Amazon Simple Storage Service (Amazon S3) -Ereignisbenachrichtigung die von Ihnen angegebene AWS Lambda Funktion nicht ausgelöst hat. Wenn in der Runbook-Ausgabe vorgeschlagen wird, die Parallelität Ihrer Lambda-Funktion zu validieren und zu konfigurieren, finden Sie weitere Informationen unter Asynchroner Aufruf und Funktionsskalierung.AWS Lambda

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- LambdaFunctionArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der Lambda-Funktion, die die Amazon S3 S3-Ereignisbenachrichtigung auslöst.
- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, dessen Ereignisbenachrichtigungen die Lambda-Funktion auslösen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

Dokumentschritte

- `aws:executeScript`- Führt das Skript aus, um die Konfigurationseinstellungen für die Amazon S3 S3-Ereignisbenachrichtigung zu überprüfen. Validiert die ressourcenbasierte IAM-Richtlinie für Ihre Lambda-Funktion und generiert einen AWS Command Line Interface (AWS CLI) -Befehl, um die erforderlichen Berechtigungen hinzuzufügen, falls die erforderlichen Berechtigungen in der Richtlinie fehlen. Validiert die Ressourcenrichtlinien anderer Lambda-Funktionen, die Teil von Ereignisbenachrichtigungen für denselben S3-Bucket sind, und generiert einen AWS CLI Befehl als Ausgabe, wenn die erforderlichen Berechtigungen fehlen.

Ausgaben

Lambdas3Event.OUTPUT

Von Amazon verwaltete Workflows für Apache Airflow

AWS Systems Manager Automation bietet vordefinierte Runbooks für Amazon Managed Workflows für Apache Airflow. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-TroubleshootMWAAEnvironmentCreation

`AWSSupport-TroubleshootMWAAEnvironmentCreation`

Beschreibung

Das `AWSSupport-TroubleshootMWAAEnvironmentCreation` Runbook enthält Informationen zum Debuggen von Problemen bei der Erstellung von Amazon Managed Workflows for Apache Airflow (Amazon MWAA) -Umgebungen und zur Durchführung von Prüfungen zusammen mit den dokumentierten Gründen nach bestem Wissen und Gewissen, um den Fehler zu identifizieren.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Ruft die Details der Amazon MWAA-Umgebung ab.

- Überprüft die Berechtigungen der Ausführungsrolle.
- Überprüft, ob die Umgebung berechtigt ist, den angegebenen AWS KMS Schlüssel für die Protokollierung zu verwenden, und ob die erforderliche CloudWatch Protokollgruppe vorhanden ist.
- Analysiert die Protokolle in der angegebenen Protokollgruppe, um Fehler zu finden.
- Überprüft die Netzwerkkonfiguration, um zu überprüfen, ob die Amazon MWAA-Umgebung Zugriff auf die erforderlichen Endpunkte hat.
- Generiert einen Bericht mit den Ergebnissen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

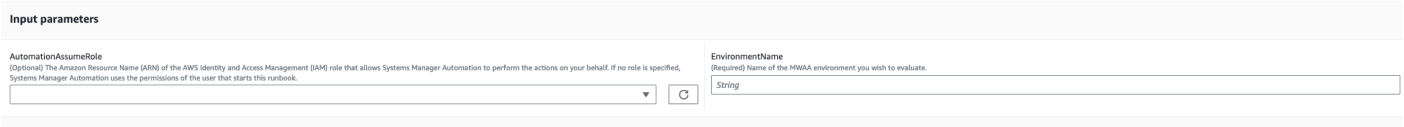
Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-TroubleshootMWAAEnvironmentCreationim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - EnvironmentName (Erforderlich):

Name der Amazon MWAA-Umgebung, die Sie bewerten möchten.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - **`GetMWAAEnvironmentDetails:`**

     Ruft die Details der Amazon MWAA-Umgebung ab. Schlägt dieser Schritt fehl, wird der Automatisierungsprozess angehalten und als angezeigt. `Failed`
   - **`CheckIAMPermissionsOnExecutionRole:`**

     Überprüft, ob die Ausführungsrolle über die erforderlichen Berechtigungen für Amazon MWAA-, Amazon S3- CloudWatch, CloudWatch Logs- und Amazon SQS-Ressourcen verfügt. Wenn ein vom Kunden verwalteter Schlüssel AWS Key Management Service (AWS KMS) erkannt wird, validiert die Automatisierung die erforderlichen Berechtigungen des Schlüssels. In diesem Schritt wird mithilfe der `iam:SimulateCustomPolicy` API festgestellt, ob die Automatisierungsausführungsrolle alle erforderlichen Berechtigungen erfüllt.
   - **`CheckKMSPolicyOnKMSKey:`**

     Prüft, ob die AWS KMS Schlüsselrichtlinie es der Amazon MWAA-Umgebung erlaubt, den Schlüssel für die Verschlüsselung CloudWatch von Protokollen zu verwenden. Wenn der AWS KMS Schlüssel AWS verwaltet wird, überspringt die Automatisierung diese Prüfung.
   - **`CheckIfRequiredLogGroupsExists:`**

     Prüft, ob die erforderlichen CloudWatch Protokollgruppen für die Amazon MWAA-Umgebung vorhanden sind. Wenn nicht, sucht die Automatisierung CloudTrail nach Ereignissen`CreateLogGroup`. `DeleteLogGroup` In diesem Schritt wird auch nach `CreateLogGroup` Ereignissen gesucht.
   - **`BranchOnLogGroupsFindings:`**

     Verzweigungen, die auf der Existenz von CloudWatch Protokollgruppen basieren, die sich auf die Amazon MWAA-Umgebung beziehen. Wenn mindestens eine Protokollgruppe vorhanden ist, analysiert die Automatisierung sie, um Fehler zu lokalisieren. Wenn keine Protokollgruppen vorhanden sind, überspringt die Automatisierung den nächsten Schritt.

- **CheckForErrorsInLogGroups:**

  Analysiert die CloudWatch Protokollgruppen, um Fehler zu finden.

- **GetRequiredEndPointsDetails:**

  Ruft die von der Amazon MWAA-Umgebung verwendeten Service-Endpunkte ab.

- **CheckNetworkConfiguration:**

  Überprüft, ob die Netzwerkkonfiguration der Amazon MWAA-Umgebung die Anforderungen erfüllt, einschließlich Prüfungen von Sicherheitsgruppen, Netzwerken ACLs, Subnetzen und Routingtabellenkonfigurationen.

- **CheckEndpointsConnectivity:**

  Ruft die `AWSSupport-ConnectivityTroubleshooter` untergeordnete Automatisierung auf, um die Konnektivität der Amazon MWAA mit den erforderlichen Endpunkten zu überprüfen.

- **CheckS3BlockPublicAccess:**

  Überprüft, ob der Amazon S3-Bucket der Amazon MWAA-Umgebung `Block Public Access` aktiviert wurde, und überprüft auch die allgemeinen Amazon S3 S3-Einstellungen für Block Public Access des Kontos.

- **GenerateReport:**

  Sammelt Informationen aus der Automatisierung und druckt das Ergebnis oder die Ausgabe jedes Schritts aus.

7. Wenn Sie den Vorgang abgeschlossen haben, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:

   - Überprüfen der Berechtigungen für die Ausführungsrolle der Amazon MWAA-Umgebung:

     Überprüft, ob die Ausführungsrolle über die erforderlichen Berechtigungen für Amazon MWAA-, Amazon S3- CloudWatch, CloudWatch Logs- und Amazon SQS-Ressourcen verfügt. Wenn ein vom Kunden verwalteter AWS KMS Schlüssel erkannt wird, validiert die Automatisierung die erforderlichen Berechtigungen des Schlüssels.

   - Überprüfung der AWS KMS Schlüsselrichtlinie für die Amazon MWAA-Umgebung:

     Überprüft, ob die Ausführungsrolle über die erforderlichen Berechtigungen für Amazon MWAA-, Amazon S3- CloudWatch, CloudWatch Logs- und Amazon SQS-Ressourcen verfügt. Wenn

ein vom Kunden verwalteter AWS KMS Schlüssel erkannt wird, überprüft die Automatisierung außerdem, ob die erforderlichen Berechtigungen für den Schlüssel vorhanden sind.

- Überprüfen der CloudWatch Protokollgruppen der Amazon MWAA-Umgebung:

  Überprüft, ob die erforderlichen CloudWatch Protokollgruppen für die Amazon MWAA-Umgebung vorhanden sind. Wenn dies nicht der Fall ist, überprüft die Automatisierung dann, ob CloudTrail Ereignisse gefunden wurden`CreateLogGroup`. `DeleteLogGroup`

- Überprüfung der Routentabellen der Amazon MWAA-Umgebung:

  Überprüft, ob die Amazon VPC-Routing-Tabellen in der Amazon MWAA-Umgebung ordnungsgemäß konfiguriert sind.

- Sicherheitsgruppen der Amazon MWAA-Umgebung überprüfen:

  Überprüft, ob die Amazon VPC-Sicherheitsgruppen der Amazon MWAA-Umgebung ordnungsgemäß konfiguriert sind.

- Überprüfen des Amazon MWAA-Umgebungsnetzwerks: ACLs

  Überprüft, ob die Amazon VPC-Sicherheitsgruppen in der Amazon MWAA-Umgebung ordnungsgemäß konfiguriert sind.

- Überprüfung der Subnetze der Amazon MWAA-Umgebung:

  Überprüft, ob die Subnetze der Amazon MWAA-Umgebung privat sind.

- Für die Überprüfung der Amazon MWAA-Umgebung war die Konnektivität der Endgeräte erforderlich:

  Überprüft, ob die Amazon MWAA-Umgebung auf die erforderlichen Endpunkte zugreifen kann. Zu diesem Zweck ruft die Automatisierung die Automatisierung auf. `AWSSupport-ConnectivityTroubleshooter`

- Überprüfen des Amazon S3-Buckets in der Amazon MWAA-Umgebung:

  Überprüft, ob der Amazon S3-Bucket der Amazon MWAA-Umgebung `Block Public Access` aktiviert wurde, und überprüft auch die Amazon S3 S3-Einstellungen für den Block Public Access des Kontos.

- Bei der Überprüfung der Amazon MWAA-Umgebung werden Gruppenfehler CloudWatch protokolliert:

  Analysiert die vorhandenen CloudWatch Protokollgruppen der Amazon MWAA-Umgebung, um Fehler zu lokalisieren.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage Support Automation Workflows

Neptune

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Neptune bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableNeptuneDbAuditLogsToCloudWatch
- AWS-EnableNeptuneDbBackupRetentionPeriod
- AWS-EnableNeptuneClusterDeletionProtection

AWS-EnableNeptuneDbAuditLogsToCloudWatch

Beschreibung

Das `AWS-EnableNeptuneDbAuditLogsToCloudWatch` Runbook hilft Ihnen, Audit-Logs für einen Amazon Neptune Neptune-DB-Cluster an Amazon Logs zu senden. CloudWatch

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DbClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID des Neptune-DB-Clusters, für den Sie Audit-Logs aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Dokumentschritte

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Gibt die ID des Neptune-DB-Clusters zurück.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Überprüft, ob der Neptune DB-Motortyp ist. `neptune`
- EnableNeptuneDbAuditLogs (`aws:executeAwsApi`) - Ermöglicht das Senden CloudWatch von Auditprotokollen für den Neptune-DB-Cluster.
- VerifyNeptuneDbStatus (`aws:waitAwsResourceProperty`) - Überprüft, ob der Neptune-DB-Clusterstatus lautet. `available`
- VerifyNeptuneDbAuditLogs (`aws:executeScript`) — Überprüft, ob die Audit-Logs erfolgreich für das Senden an Logs konfiguriert wurden. CloudWatch

AWS-EnableNeptuneDbBackupRetentionPeriod

Beschreibung

Das AWS-EnableNeptuneDbBackupRetentionPeriod Runbook unterstützt Sie bei der Aktivierung automatisierter Backups mit einer Aufbewahrungsdauer von Backups zwischen 7 und 35 Tagen für einen Amazon Neptune Neptune-DB-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DbClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID des Neptune-DB-Clusters, für den Sie Backups aktivieren möchten.
- BackupRetentionPeriod

  Typ: Ganzzahl

  Gültige Werte: 7-35

Beschreibung: (Erforderlich) Die Anzahl der Tage, an denen Backups aufbewahrt werden.

- PreferredBackupWindow

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein täglicher Zeitraum von mindestens 30 Minuten, in dem Backups erstellt werden. Der Wert muss in UTC (Universal Time Coordinated) angegeben sein und das folgende Format haben:`hh24:mm-hh24:mm`. Der Aufbewahrungszeitraum für Backups darf nicht mit dem bevorzugten Wartungsfenster kollidieren.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Dokumentschritte

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Gibt die ID des Neptune-DB-Clusters zurück.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Überprüft, ob der Neptune DB-Motortyp ist. `neptune`
- VerifyNeptuneDbStatus (`aws:waitAwsResourceProperty`) - Überprüft, ob der Neptune-DB-Clusterstatus lautet. `available`
- ModifyNeptuneDbRetentionPeriod (`aws:executeAwsApi`) - Legt den Aufbewahrungszeitraum für den Neptune-DB-Cluster fest.
- VerifyNeptuneDbBackupsEnabled (`aws:executeScript`) - Überprüft, ob der Aufbewahrungszeitraum und das Backup-Fenster erfolgreich festgelegt wurden.

AWS-EnableNeptuneClusterDeletionProtection

Beschreibung

Das AWS-EnableNeptuneClusterDeletionProtection Runbook aktiviert den Löschschutz für den von Ihnen angegebenen Amazon Neptune Neptune-Cluster.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DbClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Neptun-Clusters, für den Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- ssm:GetAutomationExecution

- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Dokumentschritte

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Gibt die ID des Neptune-DB-Clusters zurück.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Überprüft, ob der Engine-Typ des angegebenen DB-Clusters ist. `neptune`
- VerifyNeptuneStatus (`aws:waitForAwsResourceProperty`) — Überprüft, ob der Status des Clusters lautet. `available`
- EnableNeptuneDbDeletionProtection (`aws:executeAwsApi`) - Aktiviert den Löschschutz auf dem Neptune-DB-Cluster.
- VerifyNeptuneDbDeletionProtection (`aws:assertAwsResourceProperty`) - Überprüft, ob der Löschschutz auf dem DB-Cluster aktiviert ist.

Ausgaben

- EnableNeptuneDbDeletionProtection. EnableNeptuneDbDeletionProtectionResponse - Die Ausgabe des API-Vorgangs.

Amazon RDS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Relational Database Service bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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

Beschreibung

Das `AWS-CreateEncryptedRdsSnapshot` Runbook erstellt einen verschlüsselten Snapshot aus einer unverschlüsselten Amazon Relational Database Service (Amazon RDS) -Instance.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DBInstanceBezeichner

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon RDS-Instance, von der Sie einen Snapshot erstellen möchten.
- DBSnapshotBezeichner

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Namensvorlage für den Amazon RDS-Snapshot. Die Standard-Namensvorlage ist`DBInstanceIdentifier-yyyymmddhhmmss`.
- Verschlüsselter DBSnapshot Bezeichner

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name für den verschlüsselten Snapshot. Der Standardname ist der Wert, den Sie für den `DBSnapshotIdentifier` angehängten Parameter angeben. `-encrypted`

- InstanceTags

  Typ: Zeichenfolge

  Beschreibung: (Optional) Tags, die der DB-Instance hinzugefügt werden sollen. (Beispiel: key=tagKey1, value=tagValue1; key=tagKey2, value=tagValue2) '
- KmsKeyId

  Typ: Zeichenfolge

  Standard: `alias/aws/rds`

  Beschreibung: (Optional) Der ARN, die Schlüssel-ID oder der Schlüsselalias des vom Kunden verwalteten Schlüssels, den Sie zum Verschlüsseln des Snapshots verwenden möchten.
- SnapshotTags

  Typ: Zeichenfolge

  Beschreibung: (Optional) Tags, die dem Snapshot hinzugefügt werden sollen. (Beispiel: key=tagKey1, value=tagValue1; key=tagKey2, value=tagValue2) '

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds:CreateDBSnapshot`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Dokumentschritte

- `aws:executeScript`- Erstellt einen Snapshot der DB-Instance, die Sie im `DBInstanceIdentifier` Parameter angeben.
- `aws:executeScript`- Überprüft, ob der im vorherigen Schritt erstellte Snapshot existiert und existiert`available`.

- `aws:executeScript`- Kopiert den zuvor erstellten Snapshot in einen verschlüsselten Snapshot.
- `aws:executeScript`- Überprüft, ob der im vorherigen Schritt erstellte verschlüsselte Snapshot existiert.

Ausgaben

CopyRdsSnapshotToEncryptedRdsSnapshot. EncryptedSnapshotId - Die ID des verschlüsselten Amazon RDS-Snapshots.

AWS-CreateRdsSnapshot

Beschreibung

Erstellen Sie einen Amazon Relational Database Service (Amazon RDS) -Snapshot für eine Amazon RDS-Instance.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DBInstanceBezeichner

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die DBInstance ID-ID der RDS-Instance, aus der ein Snapshot erstellt werden soll.
- DBSnapshotBezeichner

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die DBSnapshot Identifikator-ID des zu erstellenden RDS-Snapshots.
- InstanceTags

  Typ: Zeichenfolge

  Beschreibung (optional): Tags, die für eine Instance erstellt werden sollen.
- SnapshotTags

  Typ: Zeichenfolge

  Beschreibung (optional): Tags, die für Snapshots erstellt werden sollen.

Dokumentschritte

create RDSSnapshot — Erstellt den RDS-Snapshot und gibt die Snapshot-ID zurück.

verifizieren RDSSnapshot — Überprüft, ob der im vorherigen Schritt erstellte Snapshot existiert.

Ausgaben

erstellenRDSSnapshot. SnapshotId — Die ID des erstellten Snapshots.

AWSConfigRemediation-DeleteRDSCluster

Beschreibung

Das `AWSConfigRemediation-DeleteRDSCluster` Runbook löscht den von Ihnen angegebenen Amazon Relational Database Service (Amazon RDS) -Cluster. AWS Config muss an dem Ort aktiviert sein, AWS-Region an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DBClusterID

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für den DB-Cluster, für den Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DeleteDBCluster`
- `rds:DeleteDBInstance`
- `rds:DescribeDBClusters`

Dokumentschritte

- `aws:executeScript`- Löscht den DB-Cluster, den Sie im `DBClusterId` Parameter angeben.

`AWSConfigRemediation-DeleteRDSClusterSnapshot`

Beschreibung

Das `AWSConfigRemediation-DeleteRDSClusterSnapshot` Runbook löscht den angegebenen Amazon Relational Database Service (Amazon RDS) -Cluster-Snapshot.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DBClusterSnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Amazon RDS-Cluster-Snapshot-ID, die gelöscht werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

Dokumentschritte

- `aws:branch`- Überprüft, ob sich der Cluster-Snapshot im `available` Status befindet. Wenn es nicht verfügbar ist, endet der Flow.
- `aws:executeAwsApi`— Löscht den angegebenen Amazon RDS-Cluster-Snapshot unter Verwendung der Cluster-Snapshot-ID der Datenbank (DB).
- `aws:executeScript`— Überprüft, ob der angegebene Amazon RDS-Cluster-Snapshot gelöscht wurde.

`AWSConfigRemediation-DeleteRDSInstance`

Beschreibung

Das `AWSConfigRemediation-DeleteRDSInstance` Runbook löscht die von Ihnen angegebene Amazon Relational Database Service (Amazon RDS) -Instance. Wenn Sie eine Datenbank-Instance (DB) löschen, werden alle automatisierten Backups für diese Instance gelöscht und können nicht wiederhergestellt werden. Manuelle DB-Snapshots werden nicht gelöscht. Wenn sich die DB-Instance, die Sie löschen möchten`failed`, im `incompatible-restore` Status`incompatible-network`, oder befindet, müssen Sie den `SkipFinalSnapshot` Parameter auf `true` setzen.

> **Note**
>
> Wenn sich die DB-Instance, die Sie löschen möchten, in einem Amazon Aurora Aurora-DB-Cluster befindet, löscht das Runbook die DB-Instance nicht, wenn es sich um eine Read Replica und die einzige Instance im DB-Cluster handelt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, die Sie löschen möchten.
- SkipFinalSnapshot

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt`true`, wird kein letzter Snapshot erstellt, bevor die DB-Instance gelöscht wird.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `rds:DeleteDBInstance`
- `rds:DescribeDBInstances`

Dokumentschritte

- `aws:executeAwsApi`- Ermittelt den Namen der DB-Instance aus dem Wert, den Sie im `DbiResourceId` Parameter angeben.
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie im `SkipFinalSnapshot` Parameter angeben.
- `aws:executeAwsApi`- Löscht die DB-Instance, die Sie im `DbiResourceId` Parameter angeben.
- `aws:executeAwsApi`- Löscht die DB-Instance, die Sie im `DbiResourceId` Parameter angeben, nachdem der endgültige Snapshot erstellt wurde.
- `aws:assertAwsResourceProperty`— Überprüft, ob die DB-Instance gelöscht wurde.

`AWSConfigRemediation-DeleteRDSInstanceSnapshot`

Beschreibung

Das `AWSConfigRemediation-DeleteRDSInstanceSnapshot` Runbook löscht den von Ihnen angegebenen Amazon Relational Database Service (Amazon RDS) -Instance-Snapshot. Nur Snapshots im Status werden gelöscht. `available` Dieses Runbook unterstützt nicht das Löschen von Snapshots aus Amazon Aurora Aurora-Datenbank-Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbSnapshotId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Snapshots, den Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Dokumentschritte

- `aws:executeAwsApi`- Erfasst den Status des im Parameter angegebenen Snapshots. `DbSnapshotId`
- `aws:assertAwsResourceProperty`- Bestätigt, dass der Status des Snapshots lautet`available`.
- `aws:executeAwsApi`- Löscht den im `DbSnapshotId` Parameter angegebenen Snapshot.
- `aws:executeScript`- Überprüft, ob der Snapshot gelöscht wurde.

AWSConfigRemediation-DisablePublicAccessToRDSInstance

Beschreibung

Das `AWSConfigRemediation-DisablePublicAccessToRDSInstance` Runbook deaktiviert den öffentlichen Zugriff für die von Ihnen angegebene Amazon Relational Database Service (Amazon RDS) -Datenbank-Instance (DB).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie den öffentlichen Zugriff deaktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Überprüft, ob sich die DB-Instances in einem `AVAILABLE` bestimmten Zustand befinden.
- `aws:executeAwsApi`— Deaktiviert den öffentlichen Zugriff auf Ihre DB-Instance.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die DB-Instance in einen `MODIFYING` Status wechselt.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass die DB-Instance in einen `AVAILABLE` Status wechselt.
- `aws:assertAwsResourceProperty`- Bestätigt, dass der öffentliche Zugriff auf der DB-Instance deaktiviert ist.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

Beschreibung

Das `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` Runbook aktiviert die `CopyTagsToSnapshot` Einstellung auf dem von Ihnen angegebenen Amazon Relational Database Service (Amazon RDS) -Cluster. Wenn Sie diese Einstellung aktivieren, werden alle Tags aus dem DB-Cluster in Snapshots des DB-Clusters kopiert. Standardmäßig werden sie nicht kopiert. AWS Config muss an dem Ort aktiviert sein AWS-Region , an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- ApplyImmediately

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für den DB-Cluster so schnell wie möglich asynchron angewendet.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbClusterResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für den DB-Cluster, für den Sie die `CopyTagsToSnapshot` Einstellung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `rds:ModifyDBCluster`

Dokumentschritte

- `aws:executeAwsApi`- Ermittelt die DB-Cluster-ID aus der DB-Cluster-Ressourcen-ID.
- `aws:assertAwsResourceProperty`- Bestätigt, dass sich der DB-Cluster in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`- Aktiviert die `CopyTagsToSnapshot` Einstellung in Ihrem DB-Cluster.
- `aws:assertAwsResourceProperty`- Bestätigt, dass die `CopyTagsToSnapshot` Einstellung in Ihrem DB-Cluster aktiviert ist.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

Beschreibung

Das `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance` Runbook aktiviert die `CopyTagsToSnapshot` Einstellung auf der Amazon Relational Database Service (Amazon RDS) -Instance, die Sie angeben. Wenn Sie diese Einstellung aktivieren, werden alle Tags aus der DB-Instance in Snapshots der DB-Instance kopiert. Standardmäßig werden sie nicht kopiert. AWS Config muss an dem Ort aktiviert sein AWS-Region , an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- ApplyImmediately

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für die DB-Instance so schnell wie möglich asynchron angewendet.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie die `CopyTagsToSnapshot` Einstellung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.

- `aws:assertAwsResourceProperty`— Bestätigt, dass sich die DB-Instance in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`— Aktiviert die `CopyTagsToSnapshot` Einstellung auf Ihrer DB-Instance.
- `aws:assertAwsResourceProperty`- Bestätigt, dass die `CopyTagsToSnapshot` Einstellung auf Ihrer DB-Instance aktiviert ist.

`AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance`

Beschreibung

Das `AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance` Runbook aktiviert Enhanced Monitoring auf der von Ihnen angegebenen Amazon RDS-Datenbank-Instance. Informationen zu Enhanced Monitoring finden Sie unter Enhanced Monitoring im Amazon RDS-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- MonitoringInterval

  Typ: Ganzzahl

  Gültige Werte: 1 | 5 | 10 | 15 | 30 | 60

  Beschreibung: (Erforderlich) Das Intervall in Sekunden, in dem Enhanced Monitoring-Metriken von der DB-Instance erfasst werden.
- MonitoringRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der IAM-Rolle, die es Amazon RDS ermöglicht, Enhanced Monitoring-Metriken an Amazon CloudWatch Logs zu senden.
- ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie Enhanced Monitoring aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Bestätigt, dass sich die DB-Instance in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`— Aktiviert die erweiterte Überwachung Ihrer DB-Instance.
- `aws:executeScript`— Bestätigt, dass Enhanced Monitoring auf Ihrer DB-Instance aktiviert ist.

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance

Beschreibung

Das `AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS` Runbook aktiviert die `AutoMinorVersionUpgrade` Einstellung auf der von Ihnen angegebenen Amazon RDS-Datenbank-Instance. Wenn Sie diese Einstellung aktivieren, werden kleinere Versions-Upgrades während des Wartungsfensters automatisch auf die DB-Instance angewendet.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie die `AutoMinorVersionUpgrade` Einstellung verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Bestätigt, dass sich die DB-Instance in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`— Aktiviert die `AutoMinorVersionUpgrade` Einstellung auf Ihrer DB-Instance.
- `aws:executeScript`— Bestätigt, dass die `AutoMinorVersionUpgrade` Einstellung auf Ihrer DB-Instance aktiviert ist.

`AWSConfigRemediation-EnableMultiAZOnRDSInstance`

Beschreibung

Das `AWSConfigRemediation-EnableMultiAZOnRDSInstance` Runbook ändert Ihre Amazon Relational Database Service (Amazon RDS) -Datenbank-Instance (DB) in eine Multi-AZ-Bereitstellung. Das Ändern dieser Einstellung führt nicht zu einem Nutzungsausfall. Die Änderung wird im nächsten Wartungsfenster übernommen, sofern Sie den Parameter nicht auf setzen. `ApplyImmediately` `true`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- ApplyImmediately

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für die DB-Instance so schnell wie möglich asynchron angewendet.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbiResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die AWS-Region eindeutige, unveränderliche Kennung für die DB-Instance, um die Einstellung zu aktivieren. `MultiAZ`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Dokumentschritte

- `aws:executeAwsApi`- Ruft den DB-Instance-Namen unter Verwendung des im Parameter angegebenen Werts ab. `DBInstanceId`
- `aws:executeAwsApi`- Überprüft, ob das ist`DBInstanceStatus`. `available`
- `aws:branch`- Prüft, ob `true` auf der DB-Instance, die Sie im `DbiResourceId` Parameter angeben, bereits auf eingestellt `MultiAZ` ist.
- `aws:executeAwsApi`- Ändert die `MultiAZ` Einstellung `true` auf der DB-Instance, die Sie im `DbiResourceId` Parameter angeben, auf.
- `aws:assertAwsResourceProperty`- Überprüft, ob `true` auf `MultiAZ` der DB-Instance, die Sie im `DbiResourceId` Parameter angeben, auf gesetzt ist.

`AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance`

Beschreibung

Das `AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance` Runbook aktiviert Performance Insights auf der von Ihnen angegebenen Amazon RDS-DB-Instance.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- DbiResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie Performance Insights aktivieren möchten.

- PerformanceInsightsKMSKeyID

  Typ: Zeichenfolge

  Standard: `alias/aws/rds`

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN), die Schlüssel-ID oder der Schlüsselalias des AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels, den Performance Insights zur Verschlüsselung aller potenziell sensiblen Daten verwenden soll. Wenn Sie den Schlüsselalias für diesen Parameter eingeben, stellen Sie dem Wert ein Präfix voran. **`alias/`** Wenn Sie keinen Wert für diesen Parameter angeben, Von AWS verwalteter Schlüssel wird der verwendet.

- PerformanceInsightsRetentionPeriod

  Typ: Ganzzahl

  Gültige Werte: 7, 731

  Standard: 7

  Beschreibung: (Optional) Die Anzahl der Tage, an denen Sie Performance Insights Insights-Daten aufbewahren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Bestätigt, dass der DB-Instance-Status lautet`available`.
- `aws:executeAwsApi`- Sammelt den ARN des vom AWS KMS Kunden verwalteten Schlüssels, der im `PerformanceInsightsKMSKeyId` Parameter angegeben ist.
- `aws:branch`— Prüft, ob der `PerformanceInsightsKMSKeyId` Eigenschaft der DB-Instance bereits ein Wert zugewiesen ist.
- `aws:executeAwsApi`— Aktiviert Performance Insights auf der DB-Instance, die Sie im `DbiResourceId` Parameter angeben.
- `aws:assertAwsResourceProperty`— Bestätigt, dass der für den `PerformanceInsightsKMSKeyId` Parameter angegebene Wert verwendet wurde, um die Verschlüsselung für Performance Insights auf der DB-Instance zu aktivieren.
- `aws:assertAwsResourceProperty`— Bestätigt, dass Performance Insights auf der DB-Instance aktiviert ist.

`AWSConfigRemediation-EnableRDSClusterDeletionProtection`

Beschreibung

Das `AWSConfigRemediation-EnableRDSClusterDeletionProtection` Runbook aktiviert den Löschschutz auf dem von Ihnen angegebenen Amazon Relational Database Service (Amazon RDS) -Cluster. AWS Config muss an dem Ort aktiviert sein AWS-Region , an dem Sie diese Automatisierung ausführen.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für den DB-Cluster, für den Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Dokumentschritte

- `aws:executeAwsApi`- Ermittelt den DB-Clusternamen aus der DB-Cluster-Ressourcen-ID.

- `aws:assertAwsResourceProperty`— Überprüft, ob der DB-Cluster-Status lautet. `available`
- `aws:executeAwsApi`— Aktiviert den Löschschutz auf dem DB-Cluster, den Sie im `ClusterId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft, ob der Löschschutz auf dem DB-Cluster aktiviert wurde.

AWSConfigRemediation-EnableRDSInstanceBackup

Beschreibung

Das `AWSConfigRemediation-EnableRDSInstanceBackup` Runbook ermöglicht Backups für die von Ihnen angegebene Amazon Relational Database Service (Amazon RDS) -Datenbank-Instance. Dieses Runbook unterstützt nicht die Aktivierung von Backups für Amazon Aurora Aurora-Datenbank-Instances.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- ApplyImmediately

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für die DB-Instance so schnell wie möglich asynchron angewendet.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BackupRetentionPeriod

  Typ: Ganzzahl

  Gültige Werte: 1—35

  Beschreibung: (Erforderlich) Die Anzahl der Tage, für die Backups aufbewahrt werden.
- DbiResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie Backups aktivieren möchten.
- PreferredBackupWindow

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der tägliche Zeitraum (in UTC), in dem Backups erstellt werden.

  Einschränkungen:
  - Muss im folgenden Format vorliegen `hh24:mi-hh24:mi`
  - Muss in koordinierter Weltzeit (UTC) angegeben werden
  - Darf nicht mit dem bevorzugten Wartungsfenster in Konflikt treten.
  - Muss mindestens 30 Minuten betragen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeScript`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID. Aktiviert Backups für Ihre DB-Instance. Bestätigt, dass Backups auf der DB-Instance aktiviert sind.

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

Beschreibung

Das `AWSConfigRemediation-EnableRDSInstanceDeletionProtection` Runbook aktiviert den Löschschutz für die von Ihnen angegebene Amazon RDS-Datenbank-Instance.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- ApplyImmediately

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn Sie `true` für diesen Parameter angeben, werden die Änderungen in dieser Anforderung und alle ausstehenden Änderungen unabhängig von der `PreferredMaintenanceWindow` Einstellung für die DB-Instance so schnell wie möglich asynchron angewendet.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DbInstanceResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, für die Sie den Löschschutz aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:executeAwsApi`— Aktiviert den Löschschutz für Ihre DB-Instance.
- `aws:assertAwsResourceProperty`— Bestätigt, dass der Löschschutz auf der DB-Instance aktiviert ist.

AWSConfigRemediation-ModifyRDSInstancePortNumber

Beschreibung

Das `AWSConfigRemediation-ModifyRDSInstancePortNumber` Runbook ändert die Portnummer, auf der die Amazon Relational Database Service (Amazon RDS) -Instance

Verbindungen akzeptiert. Wenn Sie diese Automatisierung ausführen, wird die Datenbank neu gestartet.

Diese Automatisierung ausführen (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- PortNumber

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Portnummer, über die die DB-Instance Verbindungen annehmen soll.
- RDSDBInstanceResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Ressourcen-ID für die DB-Instance, deren eingehende Portnummer Sie ändern möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Dokumentschritte

- `aws:executeAwsApi`— Ermittelt die DB-Instance-ID aus der DB-Instance-Ressourcen-ID.
- `aws:assertAwsResourceProperty`— Bestätigt, dass sich die DB-Instance in einem bestimmten `AVAILABLE` Zustand befindet.
- `aws:executeAwsApi`— Ändert die Nummer des eingehenden Ports, über den Ihre DB-Instance Verbindungen akzeptiert.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich die DB-Instance in einem bestimmten Zustand befindet. `MODIFYING`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich die DB-Instance in einem `AVAILABLE` bestimmten Zustand befindet.

`AWSSupport-ModifyRDSSnapshotPermission`

Beschreibung

Mit dem `AWSSupport-ModifyRDSSnapshotPermission` Runbook können Sie die Berechtigungen für mehrere Amazon Relational Database Service (Amazon RDS) -Snapshots ändern. Mit diesem Runbook können Sie Schnappschüsse erstellen `Public` oder `Private` diese mit anderen teilen. AWS-Konten Mit einem Standard-KMS-Schlüssel verschlüsselte Snapshots können nicht mit anderen Konten geteilt werden, die dieses Runbook verwenden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- AccountIds

  Typ: StringList

  Standard: keiner

  Beschreibung: (Optional) Die IDs Konten, mit denen Sie Snapshots teilen möchten. Dieser Parameter ist erforderlich, wenn Sie `No` den Wert des `Private` Parameters eingeben.

- AccountPermissionOperation

  Typ: Zeichenfolge

  Gültige Werte: hinzufügen | entfernen

  Standard: keiner

  Beschreibung: (Optional) Die Art des auszuführenden Vorgangs.

- Privat

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Beschreibung: (Erforderlich) Geben Sie `No` den Wert ein, wenn Sie Snapshots mit bestimmten Konten teilen möchten.

- SnapshotIdentifiers

Typ: StringList

Beschreibung: (Erforderlich) Die Namen der Amazon RDS-Snapshots, deren Berechtigungen Sie ändern möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`
- `rds:ModifyDBSnapshotAttribute`

Dokumentschritte

1. `aws:executeScript`- Überprüft die im IDs Parameter angegebenen Schnappschüsse. `SnapshotIdentifiers` Nach der Überprüfung von sucht das IDs Skript nach verschlüsselten Snapshots und gibt eine Liste aus, falls welche gefunden wurden.
2. `aws:branch`- Verzweigt die Automatisierung auf der Grundlage des Werts, den Sie für den `Private` Parameter eingeben.
3. `aws:executeScript`- Ändert die Berechtigungen der angegebenen Snapshots, um sie für die angegebenen Konten freizugeben.
4. `aws:executeScript`- Ändert die Berechtigungen der Snapshots, um sie von zu zu ändern. `Public` `Private`

Ausgaben

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts. Ergebnis

MakePrivate. Ergebnis

MakePrivate. Befehle

AWSPremiumSupport-PostgreSQLWorkloadReview

Beschreibung

Das `AWSPremiumSupport-PostgreSQLWorkloadReview` Runbook erfasst mehrere Schnappschüsse Ihrer Amazon Relational Database Service (Amazon RDS) PostgreSQL-Datenbanknutzungsstatistiken. Die erfassten Statistiken sind erforderlich, damit ein Experte von Support Proactive Services eine Betriebsprüfung durchführen kann. Die Statistiken werden mithilfe einer Reihe von benutzerdefinierten SQL- und Shell-Skripten gesammelt. Diese Skripts werden auf eine temporäre Amazon Elastic Compute Cloud (Amazon EC2) -Instance in Ihrer heruntergeladen AWS-Konto , die mit diesem Runbook erstellt wurde. Für das Runbook müssen Sie Anmeldeinformationen mit einem AWS Secrets Manager geheimen Schlüssel angeben, der ein Schlüssel-Wert-Paar aus Benutzername und Passwort enthält. Der Benutzername muss über Berechtigungen verfügen, um die standardmäßigen PostgreSQL-Statistikansichten und -funktionen abzufragen.

Dieses Runbook erstellt AWS-Konto mithilfe eines Stacks automatisch die folgenden AWS Ressourcen in Ihrem System. AWS CloudFormation Sie können die Stack-Erstellung mithilfe der CloudFormation Konsole überwachen.

- Eine Virtual Private Cloud (VPC) und eine Amazon EC2 EC2-Instance wurden in einem privaten Subnetz der VPC mit optionaler Konnektivität zum Internet über ein NAT-Gateway gestartet.
- Eine AWS Identity and Access Management (IAM-) Rolle, die der temporären Amazon EC2 EC2-Instance mit Berechtigungen zum Abrufen des geheimen Secrets Manager Manager-Werts zugewiesen ist. Die Rolle bietet auch Berechtigungen zum Hochladen von Dateien in einen Amazon Simple Storage Service (Amazon S3) -Bucket Ihrer Wahl und optional in einen Support Fall.
- Eine VPC-Peering-Verbindung, um Konnektivität zwischen Ihrer DB-Instance und der temporären Amazon EC2 EC2-Instance zu ermöglichen.
- Systems Manager-, Secrets Manager- und Amazon S3 S3-VPC-Endpoints, die an die temporäre VPC angeschlossen sind.
- Ein Wartungsfenster mit registrierten Aufgaben, die die temporäre Amazon EC2 EC2-Instance regelmäßig starten und stoppen, Datenerfassungsskripten ausführen und Dateien in einen Amazon S3 S3-Bucket hochladen. Für das Wartungsfenster wird auch eine IAM-Rolle erstellt, die Berechtigungen zur Ausführung der registrierten Aufgaben bereitstellt.

Wenn das Runbook abgeschlossen ist, wird der CloudFormation Stack, der zum Erstellen der erforderlichen AWS Ressourcen verwendet wird, gelöscht und der Bericht wird in den Amazon S3 S3-Bucket Ihrer Wahl hochgeladen, und optional wird ein Support Fall erstellt.

> **Note**
>
> Standardmäßig wird das Amazon EBS-Root-Volume der temporären Amazon EC2 EC2-Instance beibehalten. Sie können diese Option überschreiben, indem Sie den `EbsVolumeDeleteOnTermination` Parameter auf setzen. `true`

Voraussetzungen

- Enterprise Support-Abonnement Für dieses Runbook und die Proactive Services Workload Diagnostics and Reviews ist ein Enterprise Support-Abonnement erforderlich. Bevor Sie dieses Runbook verwenden, wenden Sie sich an Ihren Technical Account Manager (TAM) oder Specialist TAM (STAM), um weitere Anweisungen zu erhalten. Weitere Informationen finden Sie unter Proactive Services.Support
- Konto und AWS-Region Kontingente Stellen Sie sicher, dass Sie die maximale Anzahl an Amazon EC2 EC2-Instances nicht erreicht haben oder VPCs die Sie in Ihrem Konto und der Region, in der Sie dieses Runbook verwenden, erstellen können. Wenn Sie eine Erhöhung des Limits beantragen müssen, sehen Sie sich das Formular zur Erhöhung des Service-Limits an.
- Konfiguration der Datenbank
  1. Für die Datenbank, die Sie im `DatabaseName` Parameter angeben, sollte die `pg_stat_statements` Erweiterung konfiguriert sein. Wenn Sie nicht konfiguriert `pg_stat_statements` habens`hared_preload_libraries`, müssen Sie den Wert in der DB-Parametergruppe bearbeiten und die Änderungen übernehmen. Bei Änderungen am Parameter `shared_preload_libraries` müssen Sie Ihre DB-Instance neu starten. Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen. Wenn Sie `pg_stat_statements` mehr hinzufügen, `shared_preload_libraries` wird dies zu einem gewissen Leistungsaufwand führen. Dies ist jedoch nützlich, um die Leistung einzelner Kontoauszüge zu verfolgen. Weitere Informationen zur `pg_stat_statements` Erweiterung finden Sie in der PostgreSQL-Dokumentation. Wenn Sie die Erweiterung nicht konfigurieren oder wenn die `pg_stat_statements` Erweiterung nicht in der Datenbank vorhanden ist, die für die Statistikerfassung verwendet wird, wird die Analyse auf Abrechnungsebene nicht im Operational Review dargestellt.

2. Stellen Sie sicher, dass die `track_activities` Parameter `track_counts` und nicht ausgeschaltet sind. Wenn diese Parameter in der DB-Parametergruppe deaktiviert sind, sind keine aussagekräftigen Statistiken verfügbar. Wenn Sie diese Parameter ändern, müssen Sie Ihre DB-Instance neu starten. Weitere Informationen finden Sie unter Arbeiten mit Parametern auf Ihrer Amazon RDS for PostgreSQL PostgreSQL-DB-Instance.
3. Wenn der `track_io_timing` Parameter ausgeschaltet ist, werden die I/O Level-Statistiken nicht in die Betriebsüberprüfung einbezogen. Bei Änderungen `track_io_timing` müssen Sie Ihre DB-Instance neu starten, was je nach Arbeitslast der DB-Instance zu zusätzlichem Leistungsaufwand führt. Trotz des Leistungsaufwands bei kritischen Workloads liefert dieser Parameter nützliche Informationen zur I/O Zeit pro Abfrage.

Abrechnung und Gebühren AWS-Konto Ihnen werden die Kosten für die temporäre Amazon EC2 EC2-Instance, das zugehörige Amazon EBS-Volume, das NAT-Gateway und die während der Ausführung dieser Automatisierung übertragenen Daten in Rechnung gestellt. Standardmäßig erstellt dieses Runbook eine `t3.micro` Amazon Linux 2-Instance, um die Statistiken zu sammeln. Das Runbook startet und stoppt die Instance zwischen den Schritten, um die Kosten zu senken.

Datensicherheit und Verwaltung Dieses Runbook sammelt Statistiken, indem es die PostgreSQL-Statistikansichten und -funktionen abfragt. Stellen Sie sicher, dass die im `SecretId` Parameter angegebenen Anmeldeinformationen nur Leseberechtigungen für die Statistikansichten und -funktionen zulassen. Im Rahmen der Automatisierung werden die Sammlungsskripte in Ihren Amazon S3 S3-Bucket hochgeladen und befinden sich dorts3://*amzn-s3-demo-bucket*/*automation execution id*/queries/.

Diese Skripts sammeln Daten, die von einem AWS Spezialisten verwendet werden, um wichtige Leistungsindikatoren auf Objektebene zu überprüfen. Das Skript sammelt Informationen wie Tabellenname, Schemaname und Indexname. Wenn eine dieser Informationen vertrauliche Informationen wie Umsatzindikatoren, Benutzername, E-Mail-Adresse oder andere persönlich identifizierbare Informationen enthält, empfehlen wir, dass Sie diese Workload-Prüfung beenden. Wenden Sie sich an Ihren AWS TAM, um einen alternativen Ansatz für die Überprüfung der Arbeitslast zu besprechen.

Stellen Sie sicher, dass Sie über die erforderliche Genehmigung und Freigabe verfügen, um die im Rahmen dieser Automatisierung gesammelten Statistiken und Metadaten mit AWS anderen zu teilen.

Sicherheitsüberlegungen Wenn Sie den `UpdateRdsSecurityGroup` Parameter auf setzen`yes`, aktualisiert das Runbook die Ihrer DB-Instance zugeordnete Sicherheitsgruppe, um eingehenden Datenverkehr von der privaten IP-Adresse der temporären Amazon EC2 EC2-Instance zuzulassen.

Wenn Sie den `UpdateRdsRouteTable` Parameter auf setzen`yes`, aktualisiert das Runbook die Routing-Tabelle, die dem Subnetz zugeordnet ist, in dem Ihre DB-Instance läuft, um Traffic zur temporären Amazon EC2 EC2-Instance über die VPC-Peering-Verbindung zuzulassen.

Benutzererstellung Damit das Sammelskript eine Verbindung zu Ihrer Amazon RDS-Datenbank herstellen kann, müssen Sie einen Benutzer einrichten, der berechtigt ist, die Statistikansichten zu lesen. Dann müssen Sie die Anmeldeinformationen in Secrets Manager speichern. Wir empfehlen, einen neuen dedizierten Benutzer für diese Automatisierung zu erstellen. Wenn Sie einen separaten Benutzer erstellen, können Sie die im Rahmen dieser Automatisierung ausgeführten Aktivitäten prüfen und nachverfolgen.

1. Erstellen Sie einen neuen Benutzer.

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "CREATE USER <user_name> PASSWORD '<password>';"
   ```

2. Stellen Sie sicher, dass dieser Benutzer nur schreibgeschützte Verbindungen herstellen kann.

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "ALTER USER <user_name> SET default_transaction_read_only=true;"
   ```

3. Legen Sie Grenzwerte auf Benutzerebene fest.

   ```
   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. Erteilen Sie dem neuen Benutzer `pg_monitor` Berechtigungen, damit er auf die DB-Statistiken zugreifen kann. (Die `pg_monitor` Rolle ist Mitglied von `pg_read_all_settings`pg_read_all_stats, und`pg_stat_scan_table`.)

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "GRANT pg_monitor to <user_name>;"
   ```

Berechtigungen, die dem temporären Amazon EC2 EC2-Instance-Profil durch diese Systems Manager Manager-Automatisierung hinzugefügt wurden Die folgenden Berechtigungen werden der IAM-Rolle hinzugefügt, die der temporären Amazon EC2 EC2-Instance zugeordnet ist. Die `AmazonSSMManagedInstanceCore` verwaltete Richtlinie ist auch mit der IAM-Rolle verknüpft, sodass die Amazon EC2 EC2-Instance von Systems Manager verwaltet werden kann.

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"
        }
    ]
}
```

Durch diese Systems Manager Manager-Automatisierung zum temporären Wartungsfenster hinzugefügte Berechtigungen Die folgenden Berechtigungen werden automatisch der IAM-Rolle hinzugefügt, die den Windows-Wartungsaufgaben zugeordnet ist. Die Windows-Wartungsaufgaben starten, stoppen und senden Befehle an die temporäre Amazon EC2 EC2-Instance.

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"
        }
    ]
}
```

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DBInstanceBezeichner

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID Ihrer DB-Instance.

- DatabaseName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Datenbankname, der auf Ihrer DB-Instance gehostet wird.

- SecretId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN Ihres Secrets Manager Manager-Secrets, der das Schlüsselwertpaar aus Benutzername und Passwort enthält. Der CloudFormation Stack erstellt eine IAM-Richtlinie mit Berechtigungen für den `GetSecretValue` Vorgang mit diesem ARN. Die Anmeldeinformationen werden verwendet, damit die temporäre Instanz die Datenbankstatistiken sammeln kann. Wenden Sie sich an Ihren TAM oder STAM, um die erforderlichen Mindestberechtigungen zu besprechen.

- Bestätigen

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Geben Sie ein, **`yes`** ob Sie bestätigen, dass dieses Runbook temporäre Ressourcen in Ihrem Konto erstellt, um Statistiken von Ihrer DB-Instance zu sammeln. Wir empfehlen, sich mit Ihrem TAM oder STAM in Verbindung zu setzen, bevor Sie diese Automatisierung ausführen.

- SupportCase

  Typ: Zeichenfolge

Beschreibung: (Optional) Die Support Fallnummer, die Sie von Ihrem TAM oder STAM erhalten haben. Falls angegeben, aktualisiert das Runbook den Fall und fügt die gesammelten Daten an. Für diese Option muss die temporäre Amazon EC2 EC2-Instance über eine Internetverbindung verfügen, um auf den Support API-Endpunkt zugreifen zu können. Sie müssen den `AllowVpcInternetAccess` Parameter auf setzen. `true` Der Betreff der Groß- und Kleinschreibung muss den Ausdruck enthalten`AWSPremiumSupport-PostgreSQLWorkloadReview`.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon S3 S3-Bucket-Name in Ihrem Konto, in das Sie die von der Automatisierung gesammelten Daten hochladen möchten. Stellen Sie sicher, dass die Bucket-Richtlinie Prinzipalen, die keinen Zugriff auf den Inhalt des Buckets benötigen, keine unnötigen Lese- oder Schreibberechtigungen gewährt. Wir empfehlen, für diese Automatisierung einen neuen temporären Amazon S3 S3-Bucket zu erstellen. Das Runbook gewährt der IAM-Rolle, die der temporären Amazon EC2 EC2-Instance zugeordnet ist, Berechtigungen für den `s3:PutObject` API-Vorgang. Die hochgeladenen Dateien befinden sich in. `s3://`*`bucket name`*`/`*`automation execution id`*`/`

- InstanceType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Typ der temporären Amazon EC2 EC2-Instance, die die benutzerdefinierten SQL- und Shell-Skripts ausführt.

  Gültige Werte: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

  Standard: t3.micro

- VpcCidr

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der IP-Adressbereich in CIDR-Notation für die neue VPC (z. B.`172.31.0.0/16`). Stellen Sie sicher, dass Sie ein CIDR auswählen, das sich nicht mit einer vorhandenen VPC mit Konnektivität zu Ihrer DB-Instance überschneidet oder mit dieser übereinstimmt. Die kleinste VPC, die Sie erstellen können, verwendet eine /28-Subnetzmaske, und die größte VPC verwendet eine /16-Subnetzmaske.

Standard: 172.31.0.0/16

- StackResourcesNamePrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Namenspräfix und das Tag für den Namen der CloudFormation Stack-Ressourcen. Das Runbook erstellt die CloudFormation Stack-Ressourcen unter Verwendung dieses Präfixes als Teil des Namens und des Tags, die auf die Ressourcen angewendet werden. Die Struktur für das Schlüssel-Wert-Paar des Tags lautet. *StackResourcesNamePrefix*: {{automation:EXECUTION_ID}}

  Standard: Überprüfen AWSPostgre SQLWorkload

- Plan

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Zeitplan für das Wartungsfenster. Gibt an, wie oft die Aufgaben im Wartungsfenster ausgeführt werden. Der Standardwert ist jeder1 hour.

  Gültige Werte: 15 Minuten | 30 Minuten | 1 Stunde | 2 Stunden | 4 Stunden | 6 Stunden | 12 Stunden | 1 Tag | 2 Tage | 4 Tage

  Standard: 1 Stunde

- Dauer

  Typ: Ganzzahl

  Beschreibung: (Optional) Die maximale Dauer in Minuten, für die die Automatisierung ausgeführt werden soll. Die maximal unterstützte Dauer beträgt 8.640 Minuten (6 Tage). Der Standardwert ist 4.320 Minuten (3 Tage).

  Gültige Werte: 30-8640

  Standard: 4320

- UpdateRdsRouteTable

  Typ: Zeichenfolge

Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, aktualisiert das Runbook die Routing-Tabelle, die dem Subnetz zugeordnet ist, in dem Ihre DB-Instance ausgeführt wird. Eine IPv4-Route wird hinzugefügt, um den Datenverkehr über die neu erstellte VPC-Peering-Verbindung an die temporäre private IPV4 Adresse der Amazon EC2 EC2-Instance weiterzuleiten.

Zulässige Werte: true | false

Standard: false

- AllowVpcInternetAccess

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, erstellt das Runbook ein NAT-Gateway, um Internetkonnektivität für die temporäre Amazon EC2 EC2-Instance zur Kommunikation mit dem Support API-Endpunkt bereitzustellen. Sie können diesen Parameter so belassen, als `false` ob das Runbook nur die Ausgabe in Ihren Amazon S3 S3-Bucket hochladen soll.

  Zulässige Werte: true | false

  Standard: false

- UpdateRdsSecurityGroup

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, aktualisiert das Runbook die Ihrer DB-Instance zugeordnete Sicherheitsgruppe, um Datenverkehr von der privaten IP-Adresse der temporären Instance aus zuzulassen.

  Gültige Werte: false | true

  Standard: false

- EbsVolumeDeleteOnTermination

  Typ: Zeichenfolge

  Beschreibung: (Optional) Wenn auf gesetzt`true`, wird das Root-Volume der temporären Amazon EC2 EC2-Instance gelöscht, nachdem das Runbook abgeschlossen und der Stack gelöscht wurde. CloudFormation

Gültige Werte: false | true

Standard: false

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

1. aws:assertAwsResourceProperty- Bestätigt, dass sich die DB-Instance im available Status befindet.
2. aws:executeAwsApi- Sammelt Details über die DB-Instance.
3. aws:executeScript- Prüft, ob der im angegebene Amazon S3 S3-Bucket anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen S3BucketName zulässt.

4. `aws:executeScript`- Ruft den CloudFormation Vorlageninhalt aus dem Automation-Runbook-Anhang ab, der verwendet wird, um die temporären AWS Ressourcen in Ihrem AWS-Konto zu erstellen.
5. `aws:createStack`- Erstellt die CloudFormation Stack-Ressourcen.
6. `aws:waitForAwsResourceProperty`- Wartet, bis die von der CloudFormation Vorlage erstellte Amazon EC2 EC2-Instance läuft.
7. `aws:executeAwsApi`— Ruft die IDs für die temporäre Amazon EC2 EC2-Instance und die VPC-Peering-Verbindung ab, die von erstellt wurden. CloudFormation
8. `aws:executeAwsApi`— Ruft die IP-Adresse für die temporäre Amazon EC2 EC2-Instance ab, um die Konnektivität mit Ihrer DB-Instance zu konfigurieren.
9. `aws:executeAwsApi`— Kennzeichnet das Amazon EBS-Volume, das an die temporäre Amazon EC2 EC2-Instance angehängt ist.
10. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance die Statusprüfungen bestanden hat.
11. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance von Systems Manager verwaltet wird. Wenn bei diesem Schritt eine Zeitüberschreitung eintritt oder ein Fehler auftritt, startet das Runbook die Instance neu.
    a. `aws:executeAwsApi`— Startet die temporäre Amazon EC2 EC2-Instance neu, falls der vorherige Schritt fehlgeschlagen ist oder das Zeitlimit überschritten wurde.
    b. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance nach dem Neustart von Systems Manager verwaltet wird.
12. `aws:runCommand`- Installiert die Anwendungsanforderungen für den Metadatensammler auf der temporären Amazon EC2 EC2-Instance.
13. `aws:runCommand`- Konfiguriert den Zugriff auf Ihre DB-Instance, indem eine Konfigurationsdatei auf der temporären Amazon EC2 EC2-Instance erstellt wird.
14. `aws:executeAwsApi`— Erstellt ein Wartungsfenster, in dem die Metadaten-Collector-Anwendung regelmäßig mithilfe von Run Command ausgeführt werden kann. Das Wartungsfenster startet und stoppt die Instanz zwischen den Befehlen.
15. `aws:waitForAwsResourceProperty`- Wartet, bis das von der CloudFormation Vorlage erstellte Wartungsfenster bereit ist.
16. `aws:executeAwsApi`- Ruft das IDs für das Wartungsfenster und den Änderungskalender ab, die von CloudFormation erstellt wurden.
17. `aws:sleep`- Wartet bis zum Enddatum des Wartungsfensters.

18. `aws:executeAwsApi`- Schaltet das Wartungsfenster aus.
19. `aws:executeScript`- Ruft die Ergebnisse der Aufgaben ab, die während des Wartungsfensters ausgeführt wurden.
20. `aws:waitForAwsResourceProperty`- Wartet, bis das Wartungsfenster die letzte Aufgabe abgeschlossen hat, bevor der Vorgang fortgesetzt wird.
21. `aws:branch`- Verzweigt den Workflow je nachdem, ob Sie einen Wert für den `SupportCase` Parameter angegeben haben.
    a. `aws:changeInstanceState`- Startet die temporäre Amazon EC2 EC2-Instance und wartet, bis die Statusprüfungen bestanden sind, bevor der Bericht hochgeladen wird.
    b. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance von Systems Manager verwaltet wird. Wenn dieser Schritt das Timeout überschreitet oder fehlschlägt, startet das Runbook die Instance neu.
        i. `aws:executeAwsApi`— Startet die temporäre Amazon EC2 EC2-Instance neu, falls der vorherige Schritt fehlgeschlagen ist oder das Zeitlimit überschritten wurde.
        ii. `aws:waitForAwsResourceProperty`- Wartet, bis die temporäre Amazon EC2 EC2-Instance nach dem Neustart von Systems Manager verwaltet wird.
    c. `aws:runCommand`- Hängt den Metadatenbericht an den Support Fall an, wenn Sie einen Wert für den Parameter angegeben haben. `SupportCase` Das Skript komprimiert den Bericht und teilt ihn in 5 MB-Dateien auf. Die maximale Anzahl von Dateien, die das Skript an einen Support Fall anhängt, beträgt 12.
22. `aws:changeInstanceState`- Stoppt die temporäre Amazon EC2 EC2-Instance für den Fall, dass der CloudFormation Stack nicht gelöscht werden kann.
23. `aws:executeAwsApi`— Beschreibt die CloudFormation Stack-Ereignisse, falls die Runbooks den Stack nicht erstellen oder aktualisieren können. CloudFormation
24. `aws:waitForAwsResourceProperty`- Wartet, bis sich der CloudFormation Stack im Terminalstatus befindet, bevor er gelöscht wird.
25. `aws:executeAwsApi`- Löscht den CloudFormation Stapel mit Ausnahme des Wartungsfensters. Das Amazon EBS-Root-Volume, das der temporären Amazon EC2 EC2-Instance zugeordnet ist, wird beibehalten, wenn der `EbsVolumeDeleteOnTermination` Parameterwert auf gesetzt wurde. `false`

AWS-RebootRdsInstance

Beschreibung

Das `AWS-RebootRdsInstance` Runbook startet eine Amazon Relational Database Service (Amazon RDS) -DB-Instance neu, sofern sie nicht bereits neu gestartet wird.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon RDS-DB-Instance, die Sie neu starten möchten.

Dokumentschritte

RebootInstance - Startet die DB-Instance neu, falls sie nicht bereits neu gestartet wird.

WaitForAvailableState - Wartet darauf, dass die DB-Instance den Neustartvorgang abgeschlossen hat.

Ausgaben

Diese Automatisierung hat keine Ausgaben.

AWSSupport-ShareRDSSnapshot

Beschreibung

Das `AWSSupport-ShareRDSSnapshot` Runbook bietet eine automatisierte Lösung für das Verfahren, das im Knowledge Center-Artikel Wie kann ich einen verschlüsselten Amazon RDS-DB-Snapshot mit einem anderen Konto teilen? beschrieben wird. Wenn Ihr Amazon Relational Database Service (Amazon RDS) -Snapshot mit der Standardeinstellung verschlüsselt wurde Von AWS verwalteter Schlüssel, können Sie den Snapshot nicht teilen. In diesem Fall müssen Sie den Snapshot mit einem vom Kunden verwalteten Schlüssel kopieren und den Snapshot dann mit dem Zielkonto teilen. Diese Automatisierung führt diese Schritte mit dem Wert aus, den Sie im `SnapshotName` Parameter angeben, oder anhand des letzten Snapshots, der für die ausgewählte Amazon RDS-DB-Instance oder den ausgewählten Amazon RDS-DB-Cluster gefunden wurde.

> **Note**
>
> Wenn Sie keinen Wert für den `KMSKey` Parameter angeben, erstellt die Automatisierung einen neuen, vom AWS KMS Kunden verwalteten Schlüssel in Ihrem Konto, der zur Verschlüsselung des Snapshots verwendet wird.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AccountIds

  Typ: StringList

Beschreibung: (Erforderlich) Durch Kommas getrennte Liste der Konten, mit denen der Snapshot geteilt werden IDs soll.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Datenbank

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der Amazon RDS-DB-Instance oder des Clusters, dessen Snapshot Sie teilen möchten. Dieser Parameter ist optional, wenn Sie einen Wert für den `SnapshotName` Parameter angeben.

- KMSKey

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der vollständige Amazon-Ressourcenname (ARN) des vom AWS KMS Kunden verwalteten Schlüssels, der zur Verschlüsselung des Snapshots verwendet wurde.

- SnapshotName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die ID des DB-Clusters oder Instance-Snapshots, den Sie verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:DescribeDBSnapshots`

- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

Das `AutomationAssumeRole` erfordert die folgenden Aktionen, um das Runbook für einen DB-Cluster erfolgreich zu starten.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBClusters`
- `rds:DescribeDBClusterSnapshots`
- `rds:CopyDBClusterSnapshot`
- `rds:ModifyDBClusterSnapshotAttribute`

Die zur Ausführung der Automatisierung verwendete IAM-Rolle muss als Schlüsselbenutzer hinzugefügt werden, um den im Parameter angegebenen KMS-Schlüssel verwenden zu können. `ARNKmsKey` Informationen zum Hinzufügen von Schlüsselbenutzern zu einem KMS-Schlüssel finden Sie unter Ändern einer Schlüsselrichtlinie im AWS Key Management Service Entwicklerhandbuch.

Das `AutomationAssumeRole` erfordert die folgenden zusätzlichen Aktionen, um das Runbook erfolgreich zu starten, wenn Sie keinen Wert für den `KMSKey` Parameter angeben.

- `kms:CreateKey`
- `kms:ScheduleKeyDeletion`
- `kms:CreateGrant`
- `kms:DescribeKey`

Dokumentschritte

1. `aws:executeScript`- Überprüft, ob ein Wert für den `KMSKey` Parameter angegeben wurde, und erstellt einen vom AWS KMS Kunden verwalteten Schlüssel, falls kein Wert gefunden wird.
2. `aws:branch`- Überprüft, ob ein Wert für den `SnapshotName` Parameter angegeben wurde, und verzweigt entsprechend.
3. `aws:executeAwsApi`- Prüft, ob der bereitgestellte Snapshot von einer DB-Instance stammt.
4. `aws:executeScript`- Formatiert den `SnapshotName` Parameter und ersetzt Doppelpunkte durch einen Bindestrich.

5. `aws:executeAwsApi`- Kopiert den Snapshot mit dem angegebenen Wert. `KMSKey`
6. `aws:waitForAwsResourceProperty`- Wartet, bis der Vorgang zum Kopieren des Snapshots abgeschlossen ist.
7. `aws:executeAwsApi`- Teilt den neuen Snapshot mit dem `AccountIds` angegebenen.
8. `aws:executeAwsApi`- Prüft, ob der bereitgestellte Snapshot aus einem DB-Cluster stammt.
9. `aws:executeScript`- Formatiert den `SnapshotName` Parameter und ersetzt Doppelpunkte durch einen Bindestrich.
10. `aws:executeAwsApi`- Kopiert den Snapshot mit dem angegebenen Wert. `KMSKey`
11. `aws:waitForAwsResourceProperty`- Wartet, bis der Vorgang zum Kopieren des Snapshots abgeschlossen ist.
12. `aws:executeAwsApi`- Teilt den neuen Snapshot mit dem `AccountIds` angegebenen.
13. `aws:executeAwsApi`- Prüft, ob es sich bei dem für den `Database` Parameter angegebenen Wert um eine DB-Instance handelt.
14. `aws:executeAwsApi`- Prüft, ob es sich bei dem für den `Database` Parameter angegebenen Wert um einen DB-Cluster handelt.
15. `aws:executeAwsApi`- Ruft eine Liste von Snapshots für die angegebenen Daten ab. `Database`
16. `aws:executeScript`- Ermittelt den neuesten verfügbaren Snapshot aus der Liste, die im vorherigen Schritt zusammengestellt wurde.
17. `aws:executeAwsApi`- Kopiert den DB-Instance-Snapshot mit dem angegebenen Wert`KMSKey`.
18. `aws:waitForAwsResourceProperty`- Wartet, bis der Vorgang zum Kopieren des Snapshots abgeschlossen ist.
19. `aws:executeAwsApi`- Teilt den neuen Snapshot mit dem `AccountIds` angegebenen.
20. `aws:executeAwsApi`- Ruft eine Liste von Snapshots für den angegebenen ab. `Database`
21. `aws:executeScript`- Ermittelt den neuesten verfügbaren Snapshot aus der Liste, die im vorherigen Schritt zusammengestellt wurde.
22. `aws:executeAwsApi`- Kopiert den DB-Instance-Snapshot mit dem angegebenen Wert`KMSKey`.
23. `aws:waitForAwsResourceProperty`- Wartet, bis der Vorgang zum Kopieren des Snapshots abgeschlossen ist.
24. `aws:executeAwsApi`- Teilt den neuen Snapshot mit dem `AccountIds` angegebenen.
25. `aws:executeScript`- Löscht den vom AWS KMS Kunden verwalteten Schlüssel, der durch die Automatisierung erstellt wurde, wenn Sie keinen Wert für den `KMSKey` Parameter angegeben haben und die Automatisierung fehlschlägt.

AWS-StartRdsInstance

Beschreibung

Starten Sie eine Amazon Relational Database Service (Amazon RDS) -Instance.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID der Amazon RDS-Instance zum Starten.

AWS-StartStopAuroraCluster

Beschreibung

Dieses Runbook startet oder stoppt einen Amazon Aurora Aurora-Cluster.

> **Note**
>
> Um einen Cluster zu starten, muss er sich in einem `stopped` Status befinden. Um einen Cluster zu stoppen, muss er sich in einem `available` Status befinden. Dieses Runbook kann nicht verwendet werden, um einen Cluster zu starten oder zu stoppen, der ein Aurora Serverless v1-Cluster, ein Aurora-Multimaster-Cluster, Teil einer globalen Aurora-Datenbank oder ein Cluster ist, der Aurora-Parallelabfrage verwendet. Das Runbook kann verwendet werden, um einen Aurora Serverless v2-Cluster zu stoppen und zu starten.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- ClusterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Aurora-Clusters, den Sie beenden oder starten möchten.
- Action

Typ: Zeichenfolge

Gültige Werte: Start | Stop

Standard: Start

Beschreibung: (Erforderlich) Der Name des Aurora-Clusters, den Sie beenden oder starten möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `rds:DescribeDBClusters`
- `rds:StartDBCluster`
- `rds:StopDBCluster`

Dokumentschritte

- `aws:executeScript`- Startet oder stoppt den Cluster auf der Grundlage der Werte, die Sie für die angeben.

Ausgaben

StartStopAuroraCluster. ClusterName - Der Name des Aurora-Clusters

StartStopAuroraCluster. CurrentStatus - Der aktuelle Status des Aurora-Clusters

StartStopAuroraCluster.Message — Einzelheiten der Automatisierung

AWS-StopRdsInstance

Beschreibung

Stoppen Sie eine Amazon Relational Database Service (Amazon RDS) -Instance.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ID der Amazon RDS-Instance, die gestoppt werden soll.

AWSSupport-TroubleshootConnectivityToRDS

Beschreibung

Das `AWSSupport-TroubleshootConnectivityToRDS` Runbook diagnostiziert Verbindungsprobleme zwischen einer EC2-Instance und einer Amazon Relational Database Service Service-Instance. Die Automatisierung stellt sicher, dass die DB-Instance verfügbar ist, und überprüft dann die zugehörigen Sicherheitsgruppenregeln, Netzwerkzugriffskontrolllisten (Netzwerk ACLs) und Routing-Tabellen auf mögliche Verbindungsprobleme.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- DBInstanceBezeichner

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die DB-Instance-ID, mit der die Konnektivität getestet werden soll.
- SourceInstance

  Typ: Zeichenfolge

  Zulässiges Muster: ^i-[a-z0-9]{8,17}$

  Beschreibung: (Erforderlich) Die ID der EC2-Instance, von der die Konnektivität getestet werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`

- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- rds:DescribeDBInstances

Dokumentschritte

- aws:assertAwsResourceProperty- Bestätigt, dass der DB-Instance-Status lautetavailable.
- aws:executeAwsApi— Ruft Informationen über die DB-Instance ab.
- aws:executeAwsApi— Ruft Informationen über das DB-Instance-Netzwerk ab ACLs.
- aws:executeAwsApi— Ruft das CIDR des DB-Instance-Subnetzes ab.
- aws:executeAwsApi— Ruft Informationen über die EC2-Instance ab.
- aws:executeAwsApi— Ruft Informationen über das EC2-Instance-Netzwerk ab. ACLs
- aws:executeAwsApi— Ruft Informationen über die Sicherheitsgruppen ab, die der EC2-Instance zugeordnet sind.
- aws:executeAwsApi— Ruft Informationen über die Sicherheitsgruppen ab, die der DB-Instance zugeordnet sind.
- aws:executeAwsApi- Ruft Informationen über die Routing-Tabellen ab, die der EC2-Instance zugeordnet sind.
- aws:executeAwsApi— Ruft Informationen über die Haupt-Routing-Tabelle ab, die der Amazon VPC für die EC2-Instance zugeordnet ist.
- aws:executeAwsApi— Ruft Informationen über die Routing-Tabellen ab, die der DB-Instance zugeordnet sind.
- aws:executeAwsApi— Ruft Informationen über die Haupt-Routing-Tabelle ab, die der Amazon VPC für die DB-Instance zugeordnet ist.
- aws:executeScript— Wertet Sicherheitsgruppenregeln aus.
- aws:executeScript- Evaluiert das Netzwerk. ACLs
- aws:executeScript- Wertet Routentabellen aus.
- aws:sleep- Beendet die Automatisierung.

Ausgaben

RDSInstanceEigenschaften abrufen. DBInstanceIdentifier — Die in der Automatisierung verwendete DB-Instance.

RDSInstanceEigenschaften abrufen. DBInstanceStatus - Der aktuelle Status von DBInstance.

evalSecurityGroupRegeln. SecurityGroupEvaluation — Ergebnisse des Vergleichs der `SourceInstance` Sicherheitsgruppenregeln mit den Sicherheitsgruppenregeln der DB-Instance.

evalNetworkAclRegeln. NetworkAclEvaluation — Ergebnisse aus dem Vergleich des `SourceInstance` Netzwerks ACLs mit dem DB-Instance-Netzwerk ACLs.

evalRouteTableEinträge. RouteTableEvaluation - Ergebnisse aus dem Vergleich der `SourceInstance` Routentabelle mit den DB-Instance-Routen.

AWSSupport-TroubleshootRDSIAMAuthentication

Beschreibung

Das `AWSSupport-TroubleshootRDSIAMAuthentication` hilft bei der Fehlerbehebung AWS Identity and Access Management (IAM) bei der Authentifizierung für Amazon RDS for PostgreSQL, Amazon RDS for MySQL, Amazon RDS for MariaDB, Amazon Aurora PostgreSQL und Amazon Aurora MySQL-Instances. Verwenden Sie dieses Runbook, um die für die IAM-Authentifizierung mit einer Amazon RDS-Instance oder einem Aurora-Cluster erforderliche Konfiguration zu überprüfen. Es enthält auch Schritte zur Behebung der Verbindungsprobleme mit der Amazon RDS-Instance oder dem Aurora-Cluster.

> **Important**
>
> Dieses Runbook unterstützt Amazon RDS for Oracle oder Amazon RDS for Microsoft SQL Server nicht.

> **Important**
>
> Wenn eine Amazon EC2 EC2-Quellinstanz bereitgestellt wird und die Zieldatenbank Amazon RDS ist, wird eine untergeordnete Automatisierung `AWSSupport-TroubleshootConnectivityToRDS` aufgerufen, um die TCP-Konnektivität zu beheben. Die Ausgabe enthält auch Befehle, die Sie auf Ihrer Amazon EC2 EC2-Instance oder Ihrem Quellcomputer ausführen können, um mithilfe der IAM-Authentifizierung eine Verbindung zu den Amazon RDS-Instances herzustellen.

Wie funktioniert das?

Dieses Runbook besteht aus sechs Schritten:

- Schritt 1: ValidateInputs: Validiert die Eingaben für die Automatisierung.
- Schritt 2: branchOnSource EC2 Bereitgestellt: Überprüft, ob eine Amazon EC2 EC2-Instance-Quell-ID in den Eingabeparametern angegeben ist.
- Schritt 3: ValidierenRDSConnectivity: Validiert die Amazon RDS-Konnektivität von der Amazon EC2 EC2-Quellinstanz, sofern diese bereitgestellt wird.
- Schritt 4: ValidierenRDSIAMAuthentication: Überprüft, ob die IAM-Authentifizierungsfunktion aktiviert ist.
- Schritt 5: ValidierenIAMPolicies: Überprüft, ob die erforderlichen IAM-Berechtigungen für den angegebenen IAM-Benutzer/die angegebene IAM-Rolle vorhanden sind.
- Schritt 6: GenerateReport: Generiert einen Bericht mit den Ergebnissen der zuvor ausgeführten Schritte.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- RDSType

Typ: Zeichenfolge

Beschreibung: (Erforderlich): Wählen Sie den Typ der relationalen Datenbank aus, zu der Sie eine Verbindung herstellen und sich authentifizieren möchten.

Zulässige Werte: oder `Amazon RDS` `Amazon Aurora Cluster.`

- DBInstanceBezeichner

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Ziel-Amazon-RDS-Datenbank-Instance oder des Aurora-Datenbank-Clusters.

  Zulässiges Muster: `^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

  Max. Anzahl an Zeichen: 63

- SourceEc2InstanceIdentifier

  Typ: `AWS::EC2::Instance::Id`

  Beschreibung: (Optional) Die Amazon EC2 EC2-Instance-ID, wenn Sie von einer Amazon EC2-Instance aus, die in demselben Konto und derselben Region läuft, eine Verbindung zur Amazon RDS-Datenbank-Instance herstellen. Geben Sie diesen Parameter nicht an, wenn die Quelle keine Amazon EC2 EC2-Instance ist oder wenn der Amazon RDS-Zieltyp ein Aurora-Datenbank-Cluster ist.

  Standard: `""`

- DBIAMRoleName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der IAM-Rollenname, der für die IAM-basierte Authentifizierung verwendet wird. Geben Sie nur an, wenn der Parameter nicht `DBIAMUserName` angegeben wurde, andernfalls lassen Sie ihn leer. Es muss entweder `DBIAMRoleName` oder `DBIAMUserName` angegeben werden.

  Zulässiges Muster: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  Max. Anzahl an Zeichen: 64

Standard: ""

- DBIAMUserName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der IAM-Benutzername, der für die IAM-basierte Authentifizierung verwendet wird. Geben Sie nur an, wenn der `DBIAMRoleName` Parameter nicht angegeben wurde, andernfalls lassen Sie ihn leer. Es muss entweder `DBIAMRoleName` oder `DBIAMUserName` angegeben werden.

  Zulässiges Muster: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  Max. Anzahl an Zeichen: 64

  Standard: ""

- DBUserName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Datenbankbenutzername, der einem IAM role/user für die IAM-basierte Authentifizierung innerhalb der Datenbank zugeordnet ist. Die Standardoption * bewertet, ob die `rds-db:connect` Berechtigung für alle Benutzer in der Datenbank zulässig ist.

  Zulässiges Muster: `^[a-zA-Z0-9+=,.@*_-]{1,64}$`

  Max. Anzahl an Zeichen: 64

  Standard: *

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Anweisungen

1. Navigieren Sie AWSSupport-TroubleshootRDSIAMAuthenticationin der AWS Systems Manager Konsole zu.
2. Wählen Sie Automatisierung ausführen
3. Geben Sie für Eingabeparameter Folgendes ein:
   - AutomationAssumeRole(Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - RDSType(Erforderlich):

     Wählen Sie den Amazon RDS-Typ aus, mit dem Sie eine Verbindung herstellen und sich authentifizieren möchten. Wählen Sie aus den beiden zulässigen Werten: oder `Amazon RDS Amazon Aurora Cluster.`
   - DBInstanceBezeichner (erforderlich):

Geben Sie die ID der Ziel-Amazon-RDS-Datenbank-Instance oder des Aurora-Clusters ein, mit dem Sie eine Verbindung herstellen möchten, und verwenden Sie IAM-Anmeldeinformationen für die Authentifizierung.

- SourceEc2 InstanceIdentifier (optional):

  Geben Sie die Amazon EC2 EC2-Instance-ID an, wenn Sie von einer Amazon EC2-Instance aus, die sich im selben Konto und in derselben Region befindet, eine Verbindung zur Amazon RDS-Datenbank-Instance herstellen. Lassen Sie das Feld leer, wenn die Quelle nicht Amazon EC2 ist oder wenn der Amazon RDS-Zieltyp ein Aurora-Cluster ist.

- DBIAMRoleName (optional):

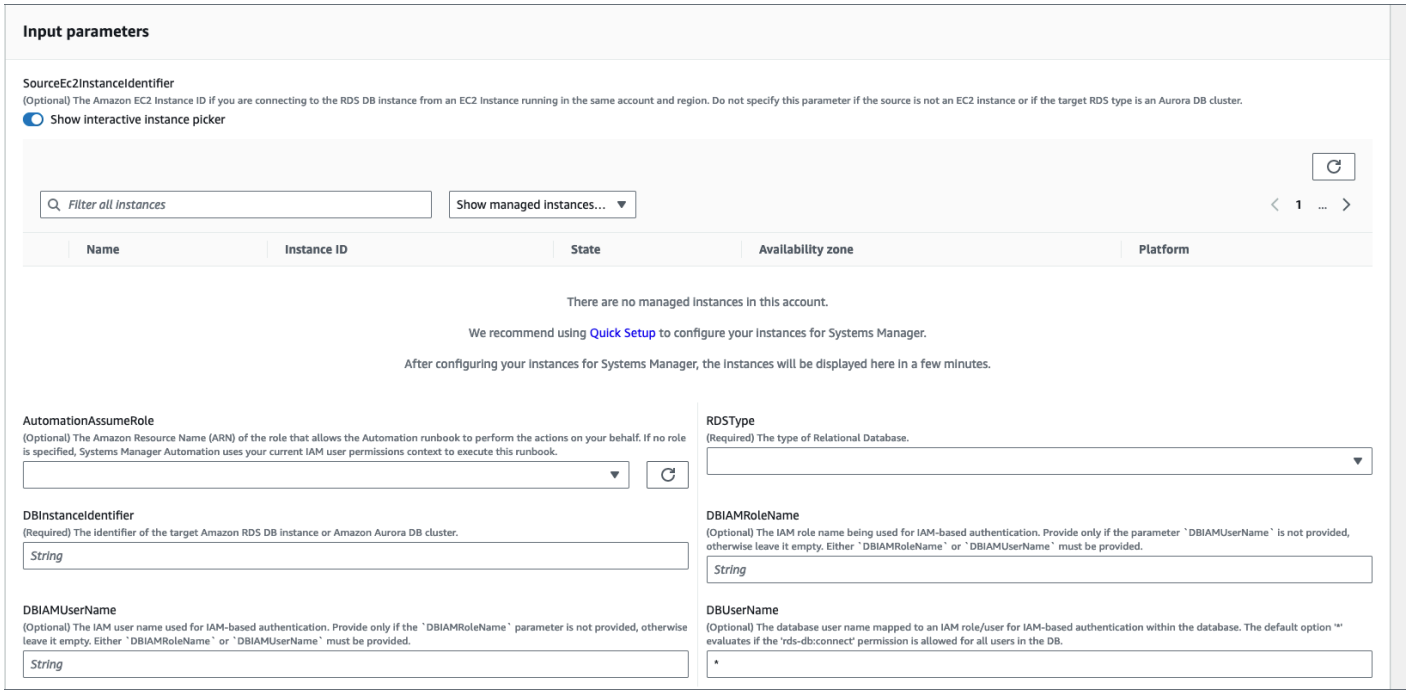
  Geben Sie den IAM-Rollennamen ein, der für die IAM-basierte Authentifizierung verwendet wird. Geben Sie das Feld nur an, wenn `DBIAMUserName` es nicht angegeben ist. Andernfalls lassen Sie das Feld leer. Es muss entweder `DBIAMRoleName` oder `DBIAMUserName` angegeben werden.

- DBIAMUserName (optional):

  Geben Sie den IAM-Benutzer ein, der für die IAM-basierte Authentifizierung verwendet wird. Geben Sie nur an, wenn nicht `DBIAMRoleName` angegeben, andernfalls lassen Sie das Feld leer. Es muss entweder `DBIAMRoleName` oder `DBIAMUserName` angegeben werden.

- DBUserName (fakultativ):

  Geben Sie den Datenbankbenutzer ein, der einer IAM-Rolle/einem IAM-Benutzer für die IAM-basierte Authentifizierung innerhalb der Datenbank zugeordnet ist. Die Standardoption * wird zur Auswertung verwendet. In diesem Feld ist nichts angegeben.



4. Wählen Sie Ausführen aus.
5. Beachten Sie, dass die Automatisierung initiiert wird.
6. Das Dokument führt die folgenden Schritte aus:
   - Schritt 1: Eingaben validieren:

     Validiert die Eingaben für die Automatisierung — `SourceEC2InstanceIdentifier` (optional), `DBInstanceIdentifier` oder, und oder`ClusterID`. `DBIAMRoleName` `DBIAMUserName` Es überprüft, ob die eingegebenen Eingabeparameter in Ihrem Konto und Ihrer Region vorhanden sind. Außerdem wird überprüft, ob der Benutzer einen der IAM-Parameter eingegeben hat (z. B. `DBIAMRoleName` oder). `DBIAMUserName` Darüber hinaus werden weitere Überprüfungen durchgeführt, z. B. ob sich die angegebene Datenbank im Status Verfügbar befindet.
   - Schritt 2: branchOnSource EC2 Vorausgesetzt:

     Überprüft, ob die Quelle Amazon EC2 in den Eingabeparametern angegeben ist und ob es sich bei der Datenbank um Amazon RDS handelt. Falls ja, wird mit Schritt 3 fortgefahren. Falls nicht, überspringt es Schritt 3, die Überprüfung der Amazon EC2-Amazon RDS-Konnektivität, und fährt mit Schritt 4 fort.
   - Schritt 3: validieren: RDSConnectivity

     Wenn die Quelle Amazon EC2 in den Eingabeparametern angegeben ist und es sich bei der Datenbank um Amazon RDS handelt, leitet Schritt 2 Schritt 3 ein. In diesem

Schritt `AWSSupport-TroubleshootConnectivityToRDS` wird die untergeordnete Automatisierung aufgerufen, um die Amazon RDS-Konnektivität von der Amazon EC2 EC2-Quelle aus zu validieren. Das untergeordnete Automatisierungs-Runbook `AWSSupport-TroubleshootConnectivityToRDS` überprüft, ob die erforderlichen Netzwerkkonfigurationen (Amazon Virtual Private Cloud [Amazon VPC], Sicherheitsgruppen, Network Access Control List [NACL], Amazon RDS-Verfügbarkeit) vorhanden sind, sodass Sie eine Verbindung von der Amazon EC2 EC2-Instance zur Amazon RDS-Instance herstellen können.

- Schritt 4: Bestätigen: RDSIAMAuthentication

  Überprüft, ob die IAM-Authentifizierungsfunktion auf der Amazon RDS-Instance oder dem Aurora-Cluster aktiviert ist.

- Schritt 5: validieren: IAMPolicies

  Überprüft, ob die erforderlichen IAM-Berechtigungen in dem user/role übergebenen IAM enthalten sind, damit sich die IAM-Anmeldeinformationen für den angegebenen Datenbankbenutzer (falls vorhanden) bei der Amazon RDS-Instance authentifizieren können.

- Schritt 6: Bericht generieren:

  Ruft alle Informationen aus den vorherigen Schritten ab und druckt das Ergebnis oder die Ausgabe jedes Schritts aus. Außerdem werden die Schritte aufgeführt, auf die verwiesen und ausgeführt werden muss, um mithilfe der IAM-Anmeldeinformationen eine Verbindung zur Amazon RDS-Instance herzustellen.

7. Wenn die Automatisierung abgeschlossen ist, finden Sie im Abschnitt Outputs die detaillierten Ergebnisse:

   - Überprüfen Sie die IAM-Benutzer-/Rollenberechtigung, um eine Verbindung zur Datenbank herzustellen:

     Überprüft, ob die erforderlichen IAM-Berechtigungen in dem user/role übergebenen IAM enthalten sind, damit sich die IAM-Anmeldeinformationen für den angegebenen Datenbankbenutzer (falls vorhanden) bei der Amazon RDS-Instance authentifizieren können.

   - Das IAM-basierte Authentifizierungsattribut für die Datenbank wird überprüft:

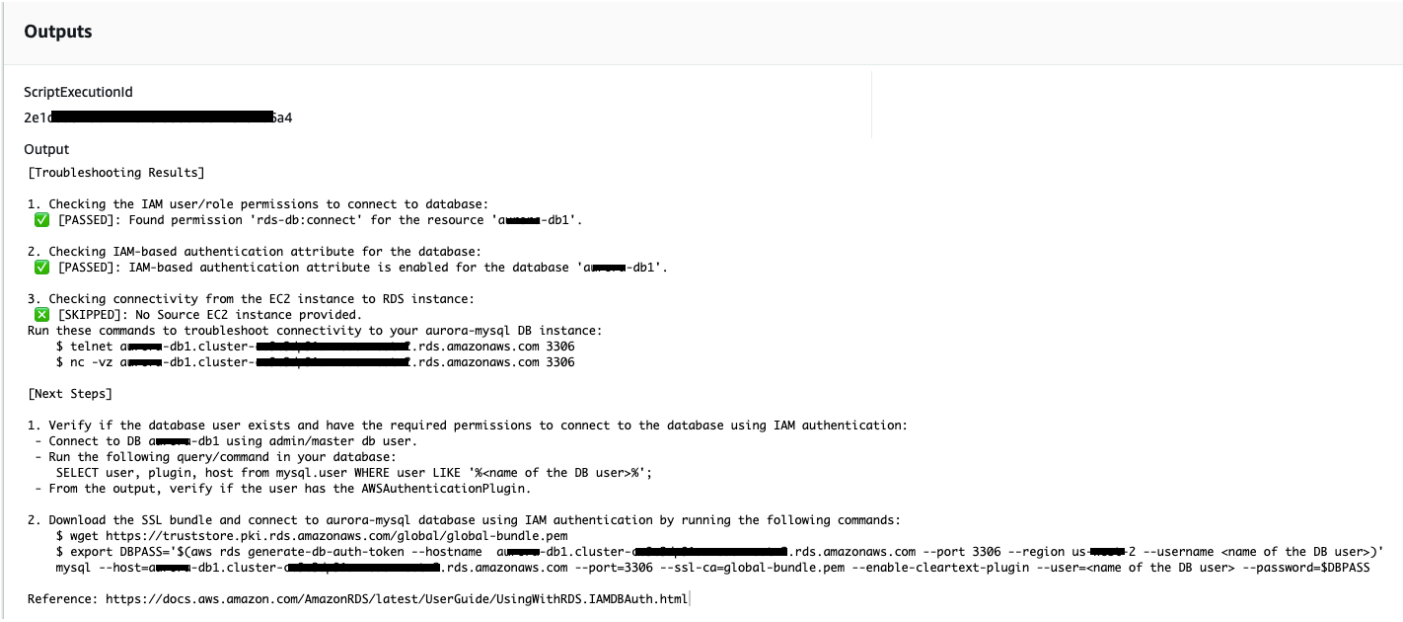
     Überprüft, ob die Funktion der IAM-Authentifizierung für den angegebenen Amazon RDS-Datenbank/Aurora-Cluster aktiviert ist.

   - Überprüfen der Konnektivität zwischen Amazon EC2 EC2-Instance und Amazon RDS-Instance:

Überprüft, ob die erforderlichen Netzwerkkonfigurationen (Amazon VPC, Sicherheitsgruppen, NACL, Amazon RDS-Verfügbarkeit) vorhanden sind, sodass Sie eine Verbindung von der Amazon EC2 EC2-Instance zur Amazon RDS-Instance herstellen können.

- Nächste Schritte:

  Führt die Befehle und Schritte auf, auf die verwiesen und ausgeführt werden muss, um mithilfe der IAM-Anmeldeinformationen eine Verbindung zur Amazon RDS-Instance herzustellen.



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWSSupport-ValidateRdsNetworkConfiguration

Beschreibung

`AWSSupport-ValidateRdsNetworkConfiguration`Durch die Automatisierung können Sie verhindern, dass Ihre bestehende Amazon Relational Database Service (Amazon RDS) /Amazon

Aurora/Amazon DocumentDB-Instance einen inkompatiblen Netzwerkstatus aufweist, bevor Sie diese ausführen oder ausführen. `ModifyDBInstance` `StartDBInstance` Wenn sich die Instance bereits im Status „Inkompatibles Netzwerk“ befindet, gibt das Runbook den Grund an.

Wie funktioniert es?

Dieses Runbook bestimmt, ob Ihre Amazon RDS-Datenbank-Instance in den Status „Inkompatibles Netzwerk“ wechselt, oder, falls dies der Fall ist, den Grund dafür, warum sie sich in einem inkompatiblen Netzwerkstatus befindet.

Das Runbook führt die folgenden Prüfungen anhand Ihrer Amazon RDS-Datenbank-Instance durch:

- Amazon Elastic Network Interface (ENI) -Kontingent pro Region.
- Alle Subnetze in der Datenbank-Subnetzgruppe sind vorhanden.
- Für die Subnetze sind ausreichend freie IP-Adressen verfügbar.
- (Für öffentlich zugängliche Amazon RDS-Instances) Einstellungen von VPC-Attributen (`enableDnsSupportundenableDnsHostnames`).

> **Important**
>
> Wenn Sie dieses Dokument für Amazon Aurora DocumentDB-Cluster verwenden, stellen Sie sicher, dass Sie `DBInstanceIdentifier` anstelle von `ClusterIdentifier` verwenden. Andernfalls schlägt das Dokument im ersten Schritt fehl.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `rds:DescribeDBInstances`
- `servicequotas:GetServiceQuota`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeSubnets`

Beispielrichtlinie:

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"
            ]
        }
    ]
}
```

Anweisungen

1. Navigieren Sie AWSSupport-ValidateRdsNetworkConfigurationin der AWS Systems Manager Konsole zum.
2. Wählen Sie Automatisierung ausführen

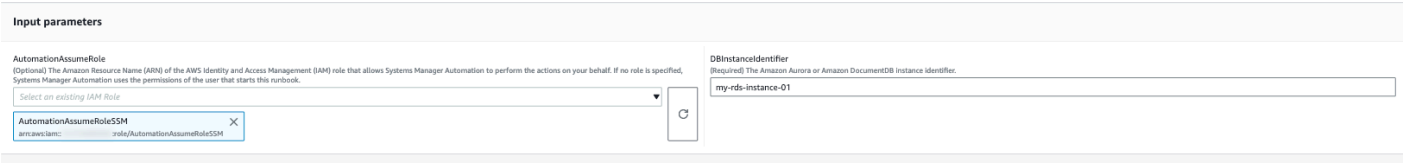
3. Geben Sie für Eingabeparameter Folgendes ein:

   - AutomationAssumeRole(Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

   - DBInstanceBezeichner (erforderlich):

     Geben Sie die Amazon Relational Database Service Instance Identifier ein.



4. Wählen Sie Ausführen aus.
5. Beachten Sie, dass die Automatisierung initiiert wird.
6. Das Dokument führt die folgenden Schritte aus:

   - Schritt 1 assertRdsState:

     Überprüft, ob die angegebene Instanz-ID existiert und einen der folgenden Zustände hat:`available`,`stopped`, oder`incompatible-network`.

   - Schritt 2 gatherRdsInformation:

     Sammelt die erforderlichen Informationen über die Amazon RDS-Instance, die später in der Automatisierung verwendet werden sollen.

   - Schritt 3: checkEniQuota

     Prüft, ob das aktuell verfügbare Kontingent von Amazon ENI für die Region verfügbar ist.

   - Schritt 4 validateVpcAttributes:

     Überprüft, ob die DNS-Parameter (`enableDnsSupport`und`enableDnsHostnames`) der Amazon VPC auf true gesetzt sind (oder nicht, wenn die Amazon RDS-Instance dies ist`PubliclyAccessible`).

   - Schritt 5: validateSubnetAttributes

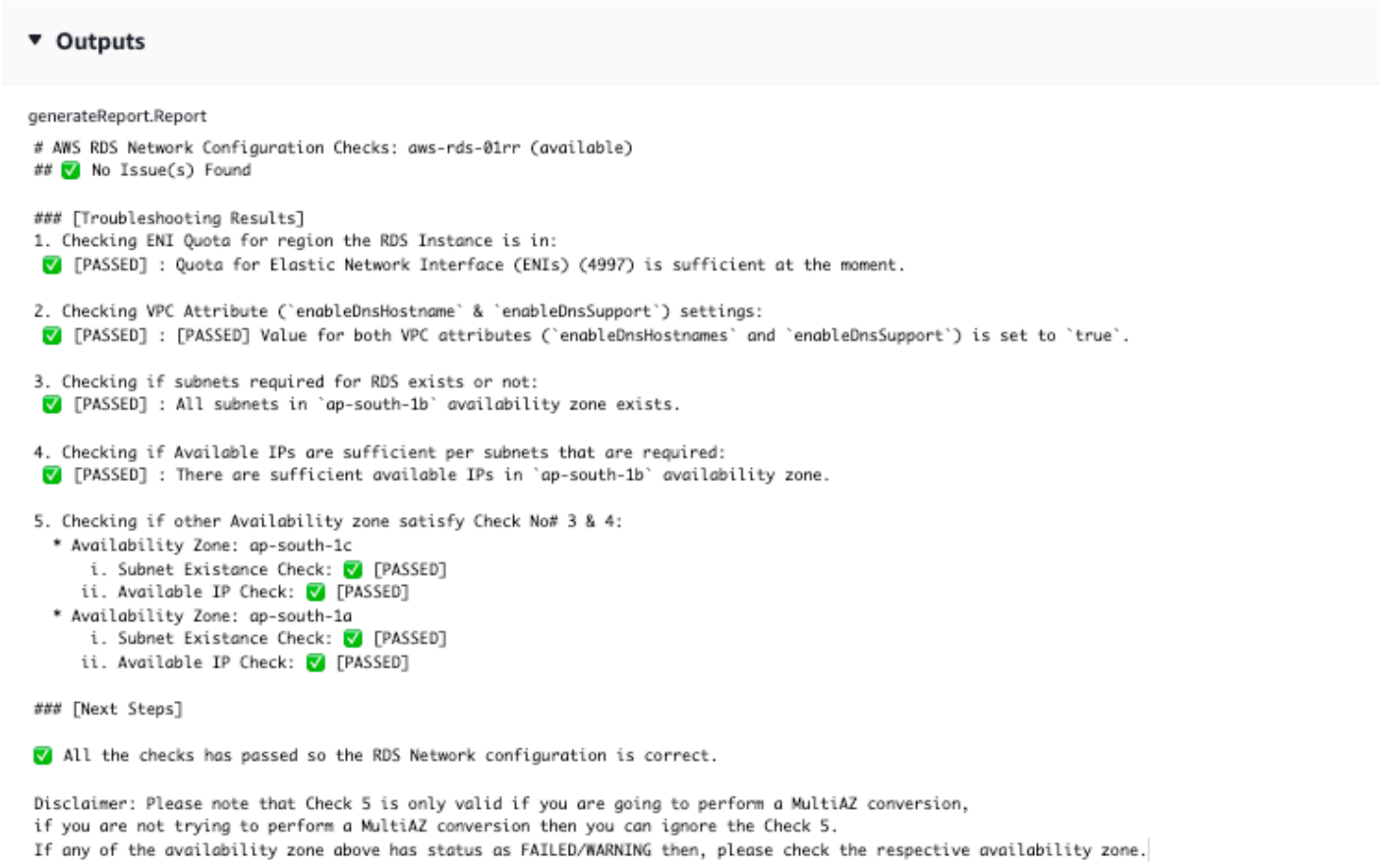
     Überprüft das Vorhandensein von Subnetzen im `DBSubnetGroup` und prüft, ob sie IPs für jedes Subnetz verfügbar sind.

- Schritt 6: Bericht generieren:

  Ruft alle Informationen aus den vorherigen Schritten ab und druckt das Ergebnis oder die Ausgabe jedes Schritts aus. Außerdem werden die Schritte aufgeführt, auf die verwiesen und ausgeführt werden muss, um mithilfe der IAM-Anmeldeinformationen eine Verbindung zur Amazon RDS-Instance herzustellen.

7. Wenn die Automatisierung abgeschlossen ist, finden Sie im Abschnitt Outputs die detaillierten Ergebnisse:

   Amazon RDS-Instance mit gültiger Netzwerkkonfiguration:



▼ **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 Existance Check: ✅ [PASSED]
     ii. Available IP Check: ✅ [PASSED]
  * Availability Zone: ap-south-1a
      i. Subnet Existance 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.
```

   Amazon RDS-Instance mit falscher Netzwerkkonfiguration (VPC-Attribut enableDnsHostnames ist auf „Falsch“ gesetzt):

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS Servicedokumentation

- Wie löse ich Probleme mit einer Amazon RDS-Datenbank, die sich in einem inkompatiblen Netzwerkstatus befindet?
- Wie löse ich Probleme mit einer Amazon DocumentDB DocumentDB-Instance, die sich in einem inkompatiblen Netzwerkstatus befindet?

Amazon Redshift

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Redshift bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-DeleteRedshiftCluster
- AWSConfigRemediation-DisablePublicAccessToRedshiftCluster
- AWSConfigRemediation-EnableRedshiftClusterAuditLogging
- AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot
- AWSConfigRemediation-EnableRedshiftClusterEncryption
- AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting
- AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster
- AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings
- AWSConfigRemediation-ModifyRedshiftClusterNodeType

`AWSConfigRemediation-DeleteRedshiftCluster`

Beschreibung

Das `AWSConfigRemediation-DeleteRedshiftCluster` Runbook löscht den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Amazon Redshift Redshift-Clusters, den Sie löschen möchten.
- SkipFinalClusterSnapshot

  Typ: Boolescher Wert

  Standard: false

  Beschreibung: (Optional) Wenn auf gesetzt, erstellt die Automatisierung einen Snapshot`false`, bevor der Amazon Redshift Redshift-Cluster gelöscht wird. Wenn auf gesetzt`true`, wird kein endgültiger Cluster-Snapshot erstellt.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DeleteCluster`
- `redshift:DescribeClusters`

Dokumentschritte

- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den `SkipFinalClusterSnapshot` Parameter angeben.

- `aws:executeAwsApi`— Löscht den im Parameter angegebenen Amazon Redshift Redshift-Cluster. `ClusterIdentifier`
- `aws:assertAwsResourceProperty`— Überprüft, ob der Amazon Redshift Redshift-Cluster gelöscht wurde.

`AWSConfigRemediation-DisablePublicAccessToRedshiftCluster`

Beschreibung

Das `AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` Runbook deaktiviert den öffentlichen Zugriff für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterIdentifier

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie den öffentlichen Zugriff deaktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Dokumentschritte

- `aws:executeAwsApi`- Deaktiviert den öffentlichen Zugriff für den im Parameter angegebenen Cluster. `ClusterIdentifier`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich der Status des Clusters ändert. `available`
- `aws:assertAwsResourceProperty`- Bestätigt, dass die Einstellung für öffentlichen Zugriff auf dem Cluster deaktiviert ist.

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

Beschreibung

Das `AWSConfigRemediation-EnableRedshiftClusterAuditLogging` Runbook aktiviert die Auditprotokollierung für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon Simple Storage Service (Amazon S3) -Buckets, in den Sie Protokolle hochladen möchten.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie die Audit-Protokollierung aktivieren möchten.
- S3 KeyPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Amazon S3 S3-Schlüsselpräfix (Unterordner), in das Sie Protokolle hochladen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

Dokumentschritte

- `aws:branch`- Verzweigt basierend darauf, ob ein Wert für den `S3KeyPrefix` Parameter angegeben wurde.
- `aws:executeAwsApi`- Aktiviert die Auditprotokollierung auf dem im `ClusterIdentifier` Parameter angegebenen Cluster.
- `aws:assertAwsResourceProperty`— Überprüft, ob die Auditprotokollierung auf dem Cluster aktiviert wurde.

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

Beschreibung

Das `AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` Runbook ermöglicht automatisierte Snapshots für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- AutomatedSnapshotRetentionPeriod

  Typ: Ganzzahl

  Gültige Werte: 1—35

  Beschreibung: (Erforderlich) Die Anzahl der Tage, für die automatische Snapshots aufbewahrt werden.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie automatische Snapshots aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert Automatisierungs-Snapshots auf dem im Parameter angegebenen Cluster. `ClusterIdentifier`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass sich der Status des Clusters ändert. `available`

- `aws:executeScript`- Bestätigt, dass automatische Snapshots auf dem Cluster aktiviert wurden.

AWSConfigRemediation-EnableRedshiftClusterEncryption

Beschreibung

Das `AWSConfigRemediation-EnableRedshiftClusterEncryption` Runbook ermöglicht die Verschlüsselung auf dem von Ihnen angegebenen Amazon Redshift Redshift-Cluster mithilfe eines AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass Ihre Amazon Redshift Redshift-Cluster gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Cluster mit unterschiedlichen, vom Kunden verwalteten Schlüsseln zu verschlüsseln. Dieses Runbook kann den vom AWS KMS Kunden verwalteten Schlüssel, der auf einem bereits verschlüsselten Cluster verwendet wird, nicht ändern. Um den vom AWS KMS Kunden verwalteten Schlüssel zu ändern, der zur Verschlüsselung eines Clusters verwendet wird, müssen Sie zuerst die Verschlüsselung auf dem Cluster deaktivieren.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie die Verschlüsselung aktivieren möchten.
- KMSKeyARN

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des vom AWS KMS Kunden verwalteten Schlüssels, den Sie zur Verschlüsselung der Clusterdaten verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert die Verschlüsselung auf dem im `ClusterIdentifier` Parameter angegebenen Amazon Redshift Redshift-Cluster.
- `aws:assertAwsResourceProperty`— Überprüft, ob die Verschlüsselung auf dem Cluster aktiviert wurde.

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

Beschreibung

Das `AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` Runbook ermöglicht erweitertes Virtual Private Cloud (VPC) -Routing für den von Ihnen angegebenen Amazon

Redshift Redshift-Cluster. Informationen zu erweitertem VPC-Routing finden Sie unter Amazon Redshift Enhanced VPC Routing im Amazon Redshift Management Guide.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie erweitertes VPC-Routing aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Dokumentschritte

- `aws:executeAwsApi`— Aktiviert erweitertes VPC-Routing auf dem im `ClusterIdentifier` Parameter angegebenen Cluster.
- `assertAwsResourceProperty`- Bestätigt, dass erweitertes VPC-Routing auf dem Cluster aktiviert wurde.

`AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster`

Beschreibung

Das `AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` Runbook erfordert, dass eingehende Verbindungen SSL für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster verwenden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie erweitertes VPC-Routing aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

Dokumentschritte

- `aws:executeAwsApi`- Ruft Parameterdetails aus dem im Parameter angegebenen Cluster ab. `ClusterIdentifier`
- `aws:executeAwsApi`- Aktiviert die `require_ssl` Einstellung für den im `ClusterIdentifier` Parameter angegebenen Cluster.
- `aws:assertAwsResourceProperty`- Bestätigt, dass die `require_ssl` Einstellung auf dem Cluster aktiviert wurde.
- `aws:executeScript`- Überprüft die `require_ssl` Einstellung für den Cluster.

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

Beschreibung

Das `AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` Runbook ändert die Wartungseinstellungen für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AllowVersionUpgrade

  Typ: Boolescher Wert

  Beschreibung: (Erforderlich) Wenn diese Option auf gesetzt ist`true`, werden Hauptversions-Upgrades während des Wartungsfensters automatisch auf den Cluster angewendet.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- AutomatedSnapshotRetentionPeriod

  Typ: Ganzzahl

  Gültige Werte: 1—35

  Beschreibung: (Erforderlich) Die Anzahl der Tage, an denen automatische Snapshots aufbewahrt werden.
- ClusterIdentifier

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, für den Sie erweitertes VPC-Routing aktivieren möchten.

- PreferredMaintenanceWindow

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der wöchentliche Zeitraum (in UTC), in dem die Systemwartung durchgeführt werden kann.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Dokumentschritte

- `aws:executeAwsApi`- Ändert die Wartungseinstellungen für den im Parameter angegebenen Cluster. `ClusterIdentifier`
- `aws:assertAwsResourceProperty`- Bestätigt, dass die geänderten Wartungseinstellungen für den Cluster konfiguriert wurden.

AWSConfigRemediation-ModifyRedshiftClusterNodeType

Beschreibung

Das `AWSConfigRemediation-ModifyRedshiftClusterNodeType` Runbook ändert den Knotentyp und die Anzahl der Knoten für den von Ihnen angegebenen Amazon Redshift Redshift-Cluster.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Datenbanken

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- Classic

  Typ: Boolescher Wert

  Beschreibung: (Optional) Wenn auf gesetzt`true`, wird für die Größenänderung der klassische Größenänderungsprozess verwendet.
- ClusterIdentifier

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die eindeutige Kennung des Clusters, dessen Knotentyp Sie ändern möchten.
- ClusterType

  Typ: Zeichenfolge

  Gültige Werte: Einzelknoten | Mehrknoten

  Beschreibung: (Erforderlich) Der Clustertyp, den Sie Ihrem Cluster zuweisen möchten.
- NodeType

Typ: Zeichenfolge

Gültige Werte: ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

Beschreibung: (Erforderlich) Der Knotentyp, den Sie Ihrem Cluster zuweisen möchten.

- NumberOfNodes

  Typ: Ganzzahl

  Gültige Werte: 2-100

  Beschreibung: (Optional) Die Anzahl der Knoten, die Sie Ihrem Cluster zuweisen möchten. Wenn es sich bei Ihrem Cluster um einen `single-node` Typ handelt, geben Sie keinen Wert für diesen Parameter an.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

Dokumentschritte

- `aws:executeScript`- Ändert den Knotentyp und die Anzahl der Knoten für den `ClusterIdentifier` im Parameter angegebenen Cluster.

Amazon S3

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Simple Storage Service bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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

Beschreibung

Das `AWS-ArchiveS3BucketToIntelligentTiering` Runbook erstellt oder ersetzt eine intelligente Tiering-Konfiguration für den von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, für den Sie eine intelligente Tiering-Konfiguration erstellen möchten.
- ConfigurationId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID für die intelligente Tiering-Konfiguration. Dies kann eine neue Konfigurations-ID oder die ID einer vorhandenen Konfiguration sein.
- NumberOfDaysToArchive

  Typ: Zeichenfolge

  Gültige Werte: 90-730

  Beschreibung: (Erforderlich) Die Anzahl der aufeinanderfolgenden Tage, nachdem ein Objekt in Ihrem Bucket für die Stufe Archive Access in Frage kommt.
- NumberOfDaysToDeepArchive

  Typ: Zeichenfolge

  Gültige Werte: 180-730

Beschreibung: (Erforderlich) Die Anzahl der aufeinanderfolgenden Tage, nachdem ein Objekt in Ihrem Bucket für den Übergang in die Stufe Deep Archive Access in Frage kommt.

- S3Prefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Schlüsselnamenpräfix der Objekte, auf die Sie die Konfiguration anwenden möchten.

- Tags (Markierungen)

  Typ: MapList

  Beschreibung: (Optional) Metadaten, die den Objekten zugewiesen sind, auf die Sie die Konfiguration anwenden möchten. Tags bestehen aus einem benutzerdefinierten Schlüssel und Wert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

Dokumentschritte

- PutsBucketIntelligentTieringConfiguration (aws:ExecuteScript) — Erstellt oder aktualisiert eine Amazon S3 Intelligent-Tiering-Konfiguration für den angegebenen Bucket.
- VerifyBucketIntelligentTieringConfiguration(aws: assertAwsResource Property) — Überprüft, ob die S3 Bucket Intelligent Configuration auf den angegebenen Bucket angewendet wurde.

AWS-ConfigureS3BucketLogging

Beschreibung

Aktivieren Sie die Protokollierung in einem Amazon Simple Storage Service (Amazon S3) -Bucket.

> **Important**
>
> Beachten Sie die folgenden wichtigen Informationen zur E-Mail-Grantee-ACL für die Amazon S3 PutBucketLoggingS3-API, die von diesem Runbook verwendet wird:
> Hinweis zum Ende des Supports: Ab dem 1. Oktober 2025 wird Amazon S3 die Unterstützung für die Erstellung neuer Zugriffssteuerungslisten (ACL) für E-Mail-Empfänger einstellen. E-Mail-Empfänger, die vor diesem Datum ACLs erstellt wurden, funktionieren weiterhin und sind weiterhin über die AWS-Managementkonsole, AWS CLI (CLI) und die REST-API zugänglich. SDKs Sie können jedoch keinen neuen E-Mail-Empfänger mehr erstellen. ACLs Zwischen dem 15. Juli 2025 und dem 1. Oktober 2025 werden Sie eine zunehmende Anzahl von HTTP 405-Fehlern bei Anfragen an Amazon S3 feststellen, wenn Sie versuchen, einen neuen E-Mail-Empfänger ACLs zu erstellen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BucketName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, für den Sie die Protokollierung konfigurieren möchten.

- GrantedPermission

  Typ: Zeichenfolge

  Gültige Werte: FULL_CONTROL | READ | WRITE

  Beschreibung: (Erforderlich) Die dem Berechtigungsempfänger zugewiesenen Berechtigungen für den Bucket.

- GranteeEmailAddress

  Typ: Zeichenfolge

  (Optional) E-Mail-Adresse des Berechtigungsempfängers

- GranteeId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die kanonische Benutzer-ID des Berechtigungsempfängers.

- GranteeType

  Typ: Zeichenfolge

  Gültige Werte: CanonicalUser | | Gruppe AmazonCustomerByEmail

  Beschreibung: (Erforderlich) Typ des Berechtigungsempfängers.

- GranteeUri

  Typ: Zeichenfolge

  Beschreibung: (Optional) URI der Berechtigungsempfängergruppe.

- TargetBucket

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Gibt den Bucket an, in dem Amazon S3 Serverzugriffsprotokolle speichern soll. In jedem Bucket, den Sie besitzen, können vier Protokolle sein. Sie können auch

mehrere Buckets konfigurieren, um ihre Protokolle zu demselben Ziel-Bucket zu senden. In diesem Fall sollten Sie TargetPrefix für jeden Quell-Bucket einen anderen auswählen, damit die bereitgestellten Protokolldateien anhand des Schlüssels unterschieden werden können.

- TargetPrefix

  Typ: Zeichenfolge

  Standard: /

  Beschreibung: (Optional) Gibt ein Präfix für die Schlüssel an, unter denen die Protokolldateien gespeichert werden.

AWS-ConfigureS3BucketVersioning

Beschreibung

Konfigurieren Sie die Versionierung für einen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, für den Sie die Versionierung konfigurieren möchten.
- VersioningState

  Typ: Zeichenfolge

  Gültige Werte: Aktiviert | Suspendiert

  Standard: Aktiviert

  Beschreibung: (Optional) Wird auf den VersioningConfiguration .Status angewendet. Bei der Einstellung „Aktiviert“ aktiviert dieser Prozess das Versioning für die Objekte in dem Bucket; alle dem Bucket hinzugefügten Objekte erhalten eine eindeutige Versions-ID. Wenn dieser Prozess auf gesetzt ist`Suspended`, deaktiviert er die Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten die Versions-ID. `null`

`AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock`

Beschreibung

Das `AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock` Runbook konfiguriert die Einstellungen für den öffentlichen Zugriffsblock von Amazon Simple Storage Service (Amazon S3) für einen Amazon S3-Bucket auf der Grundlage der Werte, die Sie in den Runbook-Parametern angeben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- BlockPublicAcls

  Typ: Boolescher Wert

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, blockiert Amazon S3 öffentliche Zugriffskontrolllisten (ACLs) für den S3-Bucket und Objekte, die in dem S3-Bucket gespeichert sind, den Sie im `BucketName` Parameter angeben.

- BlockPublicPolicy

  Typ: Boolescher Wert

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, blockiert Amazon S3 öffentliche Bucket-Richtlinien für den S3-Bucket, den Sie im `BucketName` Parameter angeben.

- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, den Sie konfigurieren möchten.

- IgnorePublicAcls

  Typ: Boolescher Wert

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, ignoriert Amazon S3 alle öffentlichen Daten ACLs für den S3-Bucket, den Sie im `BucketName` Parameter angeben.

- RestrictPublicBuckets

Typ: Boolescher Wert

Standard: true

Beschreibung: (Optional) Wenn auf gesetzt`true`, schränkt Amazon S3 die Richtlinien für öffentliche Buckets für den S3-Bucket ein, den Sie im `BucketName` Parameter angeben.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

Dokumentschritte

- `aws:executeAwsApi`- Erstellt oder ändert die `PublicAccessBlock` Konfiguration für den im Parameter angegebenen S3-Bucket. `BucketName`
- `aws:executeScript`- Gibt die `PublicAccessBlock` Konfiguration für den im `BucketName` Parameter angegebenen S3-Bucket zurück und überprüft anhand der in den Runbook-Parametern angegebenen Werte, ob die Änderungen erfolgreich vorgenommen wurden.

`AWSConfigRemediation-ConfigureS3PublicAccessBlock`

Beschreibung

Das `AWSConfigRemediation-ConfigureS3PublicAccessBlock` Runbook konfiguriert die Einstellungen für den öffentlichen Zugriff AWS-Konto von Amazon Simple Storage Service (Amazon S3) auf der Grundlage der Werte, die Sie in den Runbook-Parametern angeben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AccountId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Besitzers des S3-Buckets AWS-Konto , den Sie konfigurieren.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BlockPublicAcls

  Typ: Boolescher Wert

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, blockiert Amazon S3 öffentliche Zugriffskontrolllisten (ACLs) für S3-Buckets, deren Eigentümer die sind, die AWS-Konto Sie im `AccountId` Parameter angeben.
- BlockPublicPolicy

  Typ: Boolescher Wert

  Standard: true

Beschreibung: (Optional) Wenn auf gesetzt`true`, blockiert Amazon S3 öffentliche Bucket-Richtlinien für S3-Buckets, deren Eigentümer die sind, die AWS-Konto Sie im `AccountId` Parameter angeben.

- IgnorePublicAcls

  Typ: Boolescher Wert

  Standard: true

  Beschreibung: (Optional) Wenn diese Option auf gesetzt ist`true`, ignoriert Amazon S3 alle öffentlichen ACLs für S3-Buckets, deren Eigentümer die Buckets sind, die AWS-Konto Sie im Parameter angeben. `AccountId`

- RestrictPublicBuckets

  Typ: Boolescher Wert

  Standard: true

  Beschreibung: (Optional) Wenn auf gesetzt`true`, schränkt Amazon S3 öffentliche Bucket-Richtlinien für S3-Buckets ein, deren Eigentümer die sind, die AWS-Konto Sie im Parameter angeben. `AccountId`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

Dokumentschritte

- `aws:executeAwsApi`- Erstellt oder ändert die `PublicAccessBlock` Konfiguration für den im Parameter AWS-Konto angegebenen `AccountId` Wert.

- `aws:executeScript`- Gibt die `PublicAccessBlock` Konfiguration für den im `AccountId` Parameter AWS-Konto angegebenen Wert zurück und überprüft anhand der in den Runbook-Parametern angegebenen Werte, ob die Änderungen erfolgreich vorgenommen wurden.

AWS-CreateS3PolicyToExpireMultipartUploads

Beschreibung

Das `AWS-CreateS3PolicyToExpireMultipartUploads` Runbook erstellt eine Lebenszyklusrichtlinie für einen bestimmten Bucket, die bei unvollständigen, laufenden, mehrteiligen Uploads nach einer bestimmten Anzahl von Tagen abläuft. Dieses Runbook führt die neue Lebenszyklus-Richtlinie mit allen vorhandenen Lifecycle-Bucket-Richtlinien zusammen, die bereits existieren.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BucketName

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name des S3-Buckets, den Sie konfigurieren möchten.

- DaysUntilExpire

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Anzahl der Tage, die Amazon S3 wartet, bevor alle Teile des Uploads dauerhaft entfernt werden.

- RuleId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID, die zur Identifizierung der Lifecycle-Bucket-Regel verwendet wurde. Dies muss ein eindeutiger Wert sein.

- S3Prefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Schlüsselnamenpräfix der Objekte, auf die Sie die Konfiguration anwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

Dokumentschritte

- ConfigureExpireMultipartUploads (aws:ExecuteScript) — Konfiguriert die Lebenszyklusrichtlinie für den Bucket.
- VerifyExpireMultipartUploads (aws:ExecuteScript) — Überprüft, ob die Lebenszyklusrichtlinie für den Bucket konfiguriert wurde.

Ausgaben

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

AWS-DisableS3BucketPublicReadWrite

Beschreibung

Verwenden Sie Amazon Simple Storage Service (Amazon S3)`Block Public Access`, um den Lese- und Schreibzugriff für einen öffentlichen S3-Bucket zu deaktivieren. Weitere Informationen finden Sie unter Verwenden von Amazon S3 Block Public Access im Amazon Simple Storage Service-Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- S3 BucketName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) S3-Bucket, zu dem Sie den Zugriff einschränken möchten.

AWS-EnableS3BucketEncryption

Beschreibung

Konfiguriert die Standardverschlüsselung für einen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, in dem Sie den Inhalt verschlüsseln möchten.

- SSEAlgorithm

  Typ: Zeichenfolge

  Standard: AES256

  Beschreibung: (Optional) Der serverseitige Verschlüsselungsalgorithmus für die Standard-Verschlüsselung.

AWS-EnableS3BucketKeys

Beschreibung

Das `AWS-EnableS3BucketKeys` Runbook aktiviert Bucket Keys auf dem von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket. Dieser Schlüssel auf Bucket-Ebene erstellt während seines Lebenszyklus Datenschlüssel für neue Objekte. Wenn Sie keinen Wert für den `KmsKeyId` Parameter angeben, wird die serverseitige Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln (SSE-S3) für die Standardverschlüsselungskonfiguration verwendet.

> **Note**
>
> Amazon S3 Bucket Keys werden für die duale serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) -Schlüsseln (DSSE-KMS) nicht unterstützt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, für den Sie Bucket Keys aktivieren möchten.
- KMSKeyID

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN), die Schlüssel-ID oder der Schlüsselalias des AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels, den Sie für die serverseitige Verschlüsselung verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

Dokumentschritte

- ChooseEncryptionType (aws:branch) — Wertet den für den `KmsKeyId` Parameter angegebenen Wert aus, um festzustellen, ob SSE-S3 (AES256) oder SSE-KMS verwendet werden.
- PutBucketKeysKMS (aws:executeAwsApi) — Setzt die `BucketKeyEnabled` Eigenschaft `true` für den angegebenen S3-Bucket unter Verwendung des angegebenen auf. `KmsKeyId`

- PutBucketKeysAES256 (aws:executeAwsApi) — Setzt die `BucketKeyEnabled` Eigenschaft `true` für den angegebenen S3-Bucket mit AES256 Verschlüsselung auf.
- verifyS3 BucketKeysEnabled (aws: assertAwsResource Property) — Überprüft, ob die Bucket Keys auf dem Ziel-S3-Bucket aktiviert sind.

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

Beschreibung

Das `AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy` Runbook entfernt grundlegende Richtlinienanweisungen, die Platzhalter (`Principal: *`oder`Principal: "AWS": *`) für `Allow` Aktionen enthalten, aus Ihrer Amazon Simple Storage Service (Amazon S3) -Bucket-Richtlinie. Richtlinienerklärungen mit Bedingungen werden ebenfalls entfernt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BucketName

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, dessen Richtlinie Sie ändern möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

Dokumentschritte

- `aws:executeScript`- Ändert die Bucket-Richtlinie und überprüft, ob die wichtigsten Richtlinienanweisungen mit Platzhaltern aus dem Amazon S3 S3-Bucket entfernt wurden, den Sie im Parameter angeben. `BucketName`

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

Beschreibung

Das `AWSConfigRemediation-RestrictBucketSSLRequestsOnly` Runbook erstellt eine Bucket-Richtlinienanweisung für Amazon Simple Storage Service (Amazon S3), die HTTP-Anfragen an den von Ihnen angegebenen Amazon S3-Bucket ausdrücklich ablehnt.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets, den Sie HTTP-Anfragen ablehnen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutEncryptionConfiguration`
- `s3:PutBucketPolicy`

Dokumentschritte

- `aws:executeScript`— Erstellt eine Bucket-Richtlinie für den im `BucketName` Parameter angegebenen S3-Bucket, die HTTP-Anfragen explizit ablehnt.

AWSSupport-TroubleshootS3PublicRead

Beschreibung

Das AWSSupport-TroubleshootS3PublicRead Runbook diagnostiziert Probleme beim Lesen von Objekten aus dem öffentlichen Amazon Simple Storage Service (Amazon S3) -Bucket, den S3BucketName Sie im Parameter angeben. Eine Teilmenge der Einstellungen wird auch für Objekte im S3-Bucket analysiert.

Führen Sie diese Automatisierung aus (Konsole)

Einschränkungen

- Diese Automatisierung sucht nicht nach Zugriffspunkten, die öffentlichen Zugriff auf Objekte ermöglichen.
- Diese Automatisierung wertet keine Bedingungsschlüssel in der S3-Bucket-Richtlinie aus.
- Wenn Sie verwenden AWS Organizations, bewertet diese Automatisierung keine Richtlinien zur Servicekontrolle, um zu bestätigen, dass der Zugriff auf Amazon S3 zulässig ist.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- CloudWatchLogGroupName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Amazon CloudWatch Logs-Protokollgruppe, in die Sie die Automatisierungsausgabe senden möchten. Wenn keine Protokollgruppe gefunden wird, die dem von Ihnen angegebenen Wert entspricht, erstellt die Automatisierung anhand dieses Parameterwerts eine Protokollgruppe. Die Aufbewahrungsfrist für die durch diese Automatisierung erstellte Protokollgruppe beträgt 14 Tage.

- CloudWatchLogStreamName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der CloudWatch Log-Log-Stream, in den Sie die Automatisierungsausgabe senden möchten. Wenn kein Log-Stream gefunden wird, der dem von Ihnen angegebenen Wert entspricht, erstellt die Automatisierung einen Log-Stream mit diesem Parameterwert. Wenn Sie keinen Wert für diesen Parameter angeben, verwendet die Automatisierung den `ExecutionId` als Namen des Log-Streams.

- HttpGet

  Typ: Boolescher Wert

  Zulässige Werte: true | false

  Standard: true

  Beschreibung: (Optional) Wenn dieser Parameter auf gesetzt ist`true`, sendet die Automatisierung eine teilweise HTTP-Anfrage an die Objekte in der von `S3BucketName` Ihnen angegebenen Liste. Nur das erste Byte des Objekts wird mithilfe des Range-HTTP-Headers zurückgegeben.

- IgnoreBlockPublicAccess

  Typ: Boolescher Wert

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Wenn dieser Parameter auf gesetzt ist`true`, ignoriert die Automatisierung die Einstellungen für den öffentlichen Zugriff des S3-Buckets, den Sie im

`S3BucketName` Parameter angeben. Es wird nicht empfohlen, diesen Parameter gegenüber dem Standardwert zu ändern.

- MaxObjects

  Typ: Ganzzahl

  Gültige Werte: 1—25

  Standard: 5

  Beschreibung: (Optional) Die Anzahl der zu analysierenden Objekte im S3-Bucket, die Sie im `S3BucketName` Parameter angeben.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des S3-Buckets für die Fehlerbehebung.

- S3 PrefixName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Schlüsselnamenpräfix der Objekte, die Sie in Ihrem S3-Bucket analysieren möchten. Weitere Informationen finden Sie unter Objektschlüssel im Amazon Simple Storage Service-Benutzerhandbuch.

- StartAfter

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des Objektschlüssels, bei dem die Automatisierung mit der Analyse von Objekten in Ihrem S3-Bucket beginnen soll.

- ResourcePartition

  Typ: Zeichenfolge

  Zulässige Werte: `aws` | `aws-us-gov` | `aws-cn`

  Standard: `aws`

  Beschreibung: (Erforderlich) Die Partition, auf der sich Ihr S3-Bucket befindet.

- Verbose

Typ: Boolescher Wert

Zulässige Werte: true | false

Standard: false

Beschreibung: (Optional) Um während der Automatisierung detailliertere Informationen zurückzugeben, setzen Sie diesen Parameter auf`true`. Es werden nur Warn- und Fehlermeldungen zurückgegeben, wenn der Parameter auf gesetzt ist`false`.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Die `logs:PutLogEvents` Berechtigungen `logs:CreateLogGrouplogs:CreateLogStream`, und sind nur erforderlich, wenn Sie möchten, dass die Automatisierung Protokolldaten an CloudWatch Logs sendet.

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"
        }
    ]
}
```

Dokumentschritte

- `aws:assertAwsResourceProperty`- Bestätigt, dass der S3-Bucket existiert und zugänglich ist.
- `aws:executeScript`- Gibt den Standort des S3-Buckets und Ihre kanonische Benutzer-ID zurück.
- `aws:executeScript`- Gibt die Einstellungen für öffentliche Zugriffssperren für Ihr Konto und den S3-Bucket zurück.
- `aws:assertAwsResourceProperty`— Bestätigt, dass der S3-Bucket-Payer auf `BucketOwner` eingestellt ist. Wenn im S3-Bucket aktiviert `Requester Pays` ist, endet die Automatisierung.
- `aws:executeScript`- Gibt den Status der S3-Bucket-Richtlinie zurück und bestimmt, ob sie als öffentlich betrachtet wird. Weitere Informationen zu öffentlichen S3-Buckets finden Sie unter Die Bedeutung von „öffentlich“ im Amazon Simple Storage Service-Benutzerhandbuch.
- `aws:executeAwsApi`— Gibt die S3-Bucket-Richtlinie zurück.
- `aws:executeAwsApi`- Gibt alle Kontextschlüssel zurück, die in der S3-Bucket-Richtlinie gefunden wurden.

- `aws:assertAwsResourceProperty`— Bestätigt, ob die `GetObject` API-Aktion in der S3-Bucket-Richtlinie ausdrücklich abgelehnt wurde.
- `aws:executeAwsApi`— Gibt die Zugriffskontrollliste (ACL) für den S3-Bucket zurück.
- `aws:executeScript`- Erstellt eine CloudWatch Logs-Log-Gruppe und einen Log-Stream, wenn Sie einen Wert für den `CloudWatchLogGroupName` Parameter angeben.
- `aws:executeScript`- Basierend auf den Werten, die Sie in den Runbook-Eingabeparametern angeben, bewertet es, ob irgendwelche der während der Automatisierung gesammelten S3-Bucket-Einstellungen verhindern, dass Objekte von der Öffentlichkeit abgerufen werden. Dieses Skript führt die folgenden Funktionen aus:
  - Wertet die Einstellungen für öffentliche Zugangssperren aus
  - Gibt Objekte aus Ihrem S3-Bucket auf der Grundlage der Werte zurück, die Sie in den `StartAfter` Parametern `MaxObjectsS3PrefixName`, und angeben.
  - Gibt die S3-Bucket-Richtlinie zurück, um eine benutzerdefinierte IAM-Richtlinie für die von Ihrem S3-Bucket zurückgegebenen Objekte zu simulieren.
  - Führt eine teilweise HTTP-Anfrage an die zurückgegebenen Objekte aus, wenn der `HttpGet` Parameter auf `true` gesetzt ist. Nur das erste Byte des Objekts wird mithilfe des Range-HTTP-Headers zurückgegeben.
  - Überprüft den Schlüsselnamen des zurückgegebenen Objekts, um zu bestätigen, ob er mit einem oder zwei Punkten endet. Objektschlüsselnamen, die mit Punkten enden, können nicht von der Amazon S3 S3-Konsole heruntergeladen werden.
  - Prüft, ob der Besitzer des zurückgegebenen Objekts mit dem Besitzer des S3-Buckets übereinstimmt.
  - Prüft, ob die ACL des Objekts anonymen Benutzern `FULL_CONTROL` Berechtigungen gewährt `READ` oder gewährt.
  - Gibt Tags zurück, die dem Objekt zugeordnet sind.
  - Verwendet die simulierte IAM-Richtlinie, um zu bestätigen, ob es in der S3-Bucket-Richtlinie für die `GetObject` API-Aktion eine ausdrückliche Ablehnung für dieses Objekt gibt.
  - Gibt die Metadaten des Objekts zurück, um zu bestätigen, dass die Speicherklasse unterstützt wird.
  - Überprüft die serverseitigen Verschlüsselungseinstellungen des Objekts, um zu bestätigen, ob das Objekt mit einem AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssel verschlüsselt ist.

Ausgaben

AnalyzeObjects.bucket

AnalyzeObjects.objekt

AWSSupport-ConfigureS3ReplicationSameAndCrossAccount

Beschreibung

Das `AWSSupport-ConfigureS3ReplicationSameAndCrossAccount` Automation-Runbook konfiguriert die Amazon Simple Storage Service (Amazon S3) -Bucket-Replikation zwischen einem Quell- und Ziel-Bucket für dieselben oder kontenübergreifende Konten. Diese Automatisierung unterstützt die Replikation von Buckets, die mit serverseitiger Verschlüsselung mit Amazon S3-Managed Keys (SSE-S3) und serverseitiger Verschlüsselung mit (SSE-KMS) verschlüsselt wurden. AWS Key Management Service Es unterstützt auch präfix- und tagbasierte selektive Replikationsfilterung, Amazon S3 Replication Time Control (Amazon S3 RTC) mit 15-Minuten-SLA und die Replikation von Löschmarkern. Die Automatisierung führt die folgenden Aktionen aus:

- Überprüft Eingabeparameter und Bucket-Konfigurationen auf Kompatibilität.
- Überprüft die Verschlüsselungseinstellungen sowohl für Quell- als auch für Ziel-Buckets.
- Erstellt eine neue AWS Identity and Access Management (IAM-) Rolle mit den entsprechenden Berechtigungen für die Replikation, sofern diese nicht als Eingabe bereitgestellt wird.
- Konfiguriert Replikationsregeln auf der Grundlage bestimmter Parameter (Präfix, Tags oder ganzer Bucket).
- Aktiviert die Bucket-Versionierung, sofern sie nicht bereits aktiviert ist.
- Richtet die Replikationskonfiguration mit optionalen Funktionen wie Replication Time Control (RTC) und der Replikation von Löschmarkern ein.

⚠ Important

- Diese Automatisierung unterstützt keine Buckets mit vorhandenen Replikationsregeln. Der Quell-Bucket darf keine bestehende Replikationskonfiguration haben.
- Diese Automatisierung erstellt eine neue IAM-Rolle mit entsprechenden Berechtigungen für die Replikation, falls keine ReplicationRole S3-Eingabe bereitgestellt wird.

- Diese Automatisierung repliziert keine vorhandenen Objekte. Die Amazon S3 S3-Replikation gilt nur für Objekte, uploaded/created nachdem die Replikationskonfiguration aktiviert wurde.
- Für die kontoübergreifende Replikation müssen Sie eine IAM-Rolle im Zielkonto mit entsprechenden Berechtigungen für Amazon S3 S3-Operationen und AWS KMS -Operationen bereitstellen (falls der Bucket AWS KMS Verschlüsselung verwendet).
- Diese Automatisierung verwendet die `aws:approve` Aktion, die die Ausführung vorübergehend unterbricht, bis die designierten Principals die Konfigurationsänderungen genehmigen. Weitere Informationen finden Sie unter Automatisierung mit Genehmigern ausführen.

Wie funktioniert das?

Das Runbook führt die folgenden Schritte aus:

- ValidateInputParameters: Überprüft alle Eingabeparameter auf Richtigkeit und Kompatibilität, um eine korrekte Replikationskonfiguration sicherzustellen.
- PrepareApprovalMessage: Bereitet eine Genehmigungsnachricht mit allen Parametern der Replikationskonfiguration zur Überprüfung durch den Benutzer vor.
- RequestApproval: Fordert die Genehmigung autorisierter Benutzer an, bevor die Amazon S3 S3-Replikationskonfiguration zum Quell-Bucket hinzugefügt wird.
- CheckBucketEncryption: Überprüft die Verschlüsselungskonfiguration für Amazon S3 S3-Quell- und Ziel-Buckets, um die kompatiblen Replikationseinstellungen zu ermitteln.
- BranchOnEncryptionType: Verzweigt die Ausführung auf der Grundlage des Amazon S3 S3-Bucket-Verschlüsselungstyps, um die entsprechende Replikationskonfiguration für SSE-S3- oder SSE-KMS-verschlüsselte Buckets anzuwenden.
- SSES3Replikation konfigurieren: Konfiguriert die Amazon S3 S3-Replikation für Buckets, die mit serverseitiger Verschlüsselung mit Amazon S3-Managed Keys (SSE-S3) verschlüsselt wurden, einschließlich IAM-Rollen und Replikationsregeln.
- KonfigurierenSSEKMSReplication: Konfiguriert die Amazon S3 S3-Replikation für Buckets, die mit serverseitiger Verschlüsselung mit AWS KMS (SSE-KMS) verschlüsselt wurden, einschließlich IAM-Rollen, KMS-Schlüsselberechtigungen und Replikationsregeln.

- CleanupResources: Bereinigt die IAM-Rolle, die während einer fehlgeschlagenen Replikationskonfiguration erstellt wurde, wenn S3 nicht als Eingabe bereitgestellt wurde. ReplicationRole

Führen Sie diese Automatisierung aus (Konsole)

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- s3: ListBucket
- s3: GetBucketVersioning
- s3: GetEncryptionConfiguration
- s3: GetBucketLocation
- s3: GetReplicationConfiguration
- s3: PutBucketVersioning
- s3: PutReplicationConfiguration
- ich bin: ListRoles
- ich bin: GetRole
- ich bin: GetRolePolicy
- ich bin: ListRoleTags
- ich bin: ListAttachedRolePolicies
- ich bin: ListRolePolicies
- ich bin: SimulatePrincipalPolicy
- ich bin: CreateRole
- ich bin: TagRole
- ich bin: PassRole
- ich bin: DeleteRole
- ich bin: DeleteRolePolicy
- ich bin: DetachRolePolicy
- ich bin: PutRolePolicy
- Sätze: GetCallerIdentity

- sns:Publish
- kms: GetKeyPolicy (wenn Buckets SSE-KMS verwenden, Replikation für dasselbe Konto)
- kms: DescribeKey (wenn Buckets SSE-KMS verwenden, Replikation für dasselbe Konto)
- kms: PutKeyPolicy (wenn Buckets SSE-KMS verwenden, Replikation für dasselbe Konto)
- sts: AssumeRole (für kontoübergreifende Replikation)

CrossAccountReplicationRole (für kontenübergreifende Szenarien):

Für die kontoübergreifende Replikation müssen Sie CrossAccountReplicationRole im Zielkonto ein Konto mit den folgenden Berechtigungen angeben:

- s3: ListBucket
- s3: GetBucketVersioning
- s3: GetBucketLocation
- s3: GetBucketPolicy
- s3: GetEncryptionConfiguration
- s3: PutBucketVersioning
- s3: PutBucketPolicy
- kms: GetKeyPolicy (wenn der kontoübergreifende Ziel-Bucket SSE-KMS verwendet)
- kms: DescribeKey (wenn kontoübergreifender Ziel-Bucket SSE-KMS verwendet)
- kms: PutKeyPolicy (wenn kontoübergreifender Ziel-Bucket SSE-KMS verwendet)

S3 ReplicationRole (vom Kunden bereitgestellte Rolle):

Wenn Sie ein vorhandenes S3 bereitstellenReplicationRole, muss es über die folgenden Berechtigungen verfügen:

- s3: ListBucket
- s3: GetBucketLocation
- s3: GetReplicationConfiguration
- s3: GetObjectVersionAcl
- s3: GetObjectVersionTagging
- s3: GetObjectVersionForReplication
- s3: GetObjectTagging

- s3: ReplicateObject
- s3: ReplicateDelete
- s3: ReplicateTags
- s3: ObjectOwnerOverrideToBucketOwner
- kms:Decrypt (für SSE-KMS-Szenarien, KMS-Quellschlüssel)
- kms:Encrypt (für SSE-KMS-Szenarien, KMS-Zielschlüssel)
- kms: GenerateDataKey (für SSE-KMS-Szenarien, Ziel-KMS-Schlüssel)
- kms: ReEncrypt * (für SSE-KMS-Szenarien, Ziel-KMS-Schlüssel)

AutomationAssumeRoleBeispielrichtlinie für die Replikation desselben Kontos:

```
{
    "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**
>
> Die Policy-Anweisungen (KMSKeyReadOperations und KMSKeyMutatingOperations) sind nur erforderlich, wenn Buckets die SSE-KMS-Verschlüsselung verwenden.

AutomationAssumeRoleBeispielrichtlinie für kontenübergreifende Replikation:

```
{
    "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**
>
> - Die Policy-Anweisungen (KMSSourceKeyReadOperations und KMSSourceKeyMutatingOperations) sind nur erforderlich, wenn der Quell-Bucket die SSE-KMS-Verschlüsselung verwendet.
> - Ersetzen Sie CROSS_ACCOUNT_REPLICATION_ROLE_ARN durch den tatsächlichen Parameterwert, den Sie der Automatisierung zur Verfügung stellen. CrossAccountReplicationRole

CrossAccountReplicationRoleBeispiel für eine Richtlinie:

```
{
    "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**
>
> Die KMS-Anweisungen (KMSDestinationKeyReadOperations und KMSDestinationKeyMutatingOperations) sind nur erforderlich, wenn der Ziel-Bucket die SSE-KMS-Verschlüsselung verwendet. Entfernen Sie diese Anweisungen für SSE-S3-Szenarien.

Beispiel für eine CrossAccountReplicationRole Vertrauensrichtlinie:

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

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

> **Note**
>
> Ersetzen Sie AUTOMATION_ASSUME_ROLE_ARN durch den tatsächlichen Parameterwert, den Sie der Automatisierung zur Verfügung stellen. AutomationAssumeRole

Beispiel für eine ReplicationRole S3-Richtlinie:

```
{
    "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**
>
> - Die KMS-Anweisungen (KMSSourceKeyPermissions und KMSDestinationKeyPermissions) sind nur erforderlich, wenn Buckets die SSE-KMS-Verschlüsselung verwenden.
> - Die CrossAccountPermissions S3-Anweisung ist nur für die kontoübergreifende Bucket-Replikation erforderlich.

Beispiel für eine ReplicationRole S3-Vertrauensrichtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-ConfigureS3ReplicationSameAndCrossAccountim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Erforderlich):
     - Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
     - Typ: `AWS::IAM::Role::Arn`
   - SourceBucket (Erforderlich):
     - Beschreibung: (Erforderlich) Der Name des Amazon S3-Quell-Buckets, in dem die Replikationsregeln erstellt oder aktualisiert werden.
     - Typ: `AWS::S3::Bucket::Name`
   - DestinationBucket (Erforderlich):
     - Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Ziel-Buckets, in den Objekte repliziert werden.
     - Typ: `String`

  - Zulässiges Muster: `^[0-9a-z][a-z0-9\\-\\.]{3,63}$`
- SourceAccountId (Erforderlich):
  - Beschreibung: (Erforderlich) Die AWS Konto-ID, unter der sich der Quell-Bucket befindet.
  - Typ: `String`
  - Zulässiges Muster: `^[0-9]{12,13}$`
- DestinationAccountId (Erforderlich):
  - Beschreibung: (Erforderlich) Die AWS Konto-ID, unter der sich der Ziel-Bucket befindet.
  - Typ: `String`
  - Zulässiges Muster: `^[0-9]{12,13}$`
- SnsNotificationArn (Erforderlich):
  - Beschreibung: (Erforderlich) Der ARN eines Amazon Simple Notification Service (Amazon SNS) -Themas für Automatisierungsgenehmigungen.
  - Typ: `String`
  - Zulässiges Muster: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):sns:[a-z]{2}(-gov)?(-iso[a-z]?)?-[a-z]{2,10}-[0-9]{1,2}:\\d{12}:[0-9a-zA-Z-_]{1,256}(.fifo)?$`
- Genehmigende Personen (erforderlich):
  - Beschreibung: (Erforderlich) Die Liste der IAM-Benutzer, die user/role ARNs berechtigt sind, die Ausführung der Automatisierung zu genehmigen.
  - Typ: `StringList`
  - Zulässiges Muster: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::\\d{12}:(user|role)/[\\w+=,.@\\-/]+$`
- S3 ReplicationRole (optional):
  - Beschreibung: (Optional) Der ARN einer vorhandenen IAM-Rolle, die für Amazon S3 S3-Replikationsvorgänge verwendet werden soll. Diese Rolle muss berechtigt sein, aus dem Quell-Bucket zu lesen und in den Ziel-Bucket zu schreiben, einschließlich KMS-Berechtigungen, wenn Buckets SSE-KMS-Verschlüsselung verwenden. Falls nicht angegeben, erstellt die Automatisierung eine neue Rolle mit den entsprechenden Berechtigungen.
  - Typ: `String`
  - Zulässiges Muster: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::\\d{12}:role/[\\w+=,.@\\-/]+$`

  - Standard: ""
- CrossAccountReplicationRole (Fakultativ):
  - Beschreibung: (Optional) Der ARN einer IAM-Rolle im Zielkonto, den die Automatisierung annehmen kann. Dies ist für die kontenübergreifende Replikation erforderlich. Lassen Sie dieses Feld für die Replikation unter demselben Konto leer.
  - Typ: `String`
  - Zulässiges Muster: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::\\d{12}:role/[\\w+=,.@\\-/]+$`
  - Standard: ""
- ReplicateEntireBucket (Fakultativ):
  - Beschreibung: (Optional) Wenn auf gesetzt`true`, wird der gesamte Bucket repliziert und sowohl Präfix als auch Tags müssen leer sein. Wenn der Wert falsch ist, basiert die Replikation auf dem angegebenen Präfix oder den angegebenen Tags.
  - Typ: `Boolean`
  - Zulässige Werte: `[true, false]`
  - Standard: `true`
- ReplicationRuleStatus (Fakultativ):
  - Beschreibung: (Optional) Wenn auf gesetzt`true`, werden die erstellten Replikationsregeln aktiviert. Wenn auf gesetzt`false`, werden die erstellten Replikationsregeln auf Deaktiviert gesetzt.
  - Typ: `Boolean`
  - Zulässige Werte: `[true, false]`
  - Standard: `true`
- DeleteMarkerReplicationStatus (Fakultativ):
  - Beschreibung: (Optional) Wenn auf gesetzt`true`, aktiviert die Automatisierung die Replikation von Löschmarkern.
  - Typ: `Boolean`
  - Zulässige Werte: `[true, false]`
  - Standard: `false`
- ReplicationTimeControl (Fakultativ):
  - Beschreibung: (Optional) Wenn auf gesetzt`true`, wird Amazon S3 Replication Time Control (Amazon S3 RTC) mit 15-Minuten-SLA für vorhersehbare Replikationszeiten aktiviert.

- Typ: `Boolean`
- Zulässige Werte: `[true, false]`
- Standard: `false`

- ReplicaModifications (Fakultativ):
  - Beschreibung: (Optional) Wenn auf gesetzt`true`, wird die Replikation von Metadatenänderungen an Replikatobjekten aktiviert, sodass Änderungen an replizierten Objekten wieder mit der Quelle synchronisiert werden können.
  - Typ: `Boolean`
  - Zulässige Werte: `[true, false]`
  - Standard: `false`
- Präfix (optional):
  - Beschreibung: (Optional) Präfixfilter für die selektive Replikation von Objekten mit bestimmten Schlüsselpräfixen. Für eine korrekte Amazon S3 S3-Präfixfilterung muss das Präfix mit einem abschließenden Schrägstrich (/) enden.
  - Typ: `String`
  - Zulässiges Muster: `^$|^[a-zA-Z0-9!_'()\\-]*/+$`
  - Standard: `""`
- Schlagworte (optional):
  - Beschreibung: (Optional) JSON-Array mit Tags zum Filtern von Objekten, die repliziert werden sollen. Format für ein einzelnes Tag: [{"Key“:“ TagKey „, "Value“:“ TagValue „}] und für mehrere Tags: [{" Key“:“ TagKey 1", "Value“:“ TagValue 1"}, {"Key“:“ TagKey 2", "Value“:“ TagValue 2"}].
  - Typ: `String`
  - Zulässiges Muster: `^\\[((\\{\"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}\"\\})*)?\\]$`
  - Standard: `[]`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - ValidateInputParameters.

Überprüft alle Eingabeparameter auf Richtigkeit und Kompatibilität, um eine korrekte Replikationskonfiguration sicherzustellen.

- PrepareApprovalMessage:

  Bereitet die Genehmigungsnachricht mit allen Parametern der Replikationskonfiguration zur Überprüfung durch den Benutzer vor.

- RequestApproval:

  Fordert die Genehmigung autorisierter Benutzer an, bevor Sie mit den Änderungen der Amazon S3 S3-Replikationskonfiguration fortfahren.

- CheckBucketEncryption:

  Überprüft die Verschlüsselungskonfiguration für Amazon S3 S3-Quell- und Ziel-Buckets, um die kompatiblen Replikationseinstellungen zu ermitteln.

- BranchOnEncryptionType:

  Verzweigt die Ausführung auf der Grundlage des Amazon S3 S3-Bucket-Verschlüsselungstyps, um die entsprechende Replikationskonfiguration für SSE-S3- oder SSE-KMS-verschlüsselte Buckets anzuwenden.

- Replikation konfigurieren: SSES3

  Konfiguriert die Amazon S3 S3-Replikation für Buckets, die mit serverseitiger Verschlüsselung mit Amazon S3-Managed Keys (SSE-S3) verschlüsselt wurden, einschließlich IAM-Rollen und Replikationsregeln.

- Konfigurieren Sie: SSEKMSReplication

  Konfiguriert die Amazon S3 S3-Replikation für Buckets, die mit serverseitiger Verschlüsselung mit AWS KMS (SSE-KMS) verschlüsselt wurden, einschließlich IAM-Rollen, KMS-Schlüsselberechtigungen und Replikationsregeln.

- CleanupResources:

  Bereinigt IAM-Rollen, die während einer fehlgeschlagenen Replikationskonfiguration erstellt wurden, als S3 nicht vom Kunden bereitgestellt wurde. ReplicationRole

7. Überprüfen Sie nach Abschluss der Ausführung die Ergebnisse des Schritts „SSES3Replikation konfigurieren“ (für SSE-S3-verschlüsselte Buckets) oder des SSEKMSReplication Schritts „Konfigurieren“ (für SSE-KMS-verschlüsselte Buckets) auf die Ergebnisse der Ausführung,

einschließlich des Status der Replikationskonfiguration und der für die Replikation verwendeten IAM-Rolle.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

`AWSSupport-EmptyS3Bucket`

Beschreibung

Das `AWSSupport-EmptyS3Bucket` Automatisierungs-Runbook leert einen vorhandenen Amazon Simple Storage Service (Amazon S3) -Bucket mithilfe einer Konfigurationsregel für den Ablauf des Lebenszyklus.

> ⚠ Important
>
> - Amazon S3 S3-Buckets mit aktivierter Multi-Factor Authentication (MFA) werden nicht unterstützt.
> - Die durch dieses Runbook geänderten Lebenszyklusregeln löschen dauerhaft alle Objekte und ihre Versionen im angegebenen Amazon S3 S3-Bucket. Dauerhaft gelöschte Objekte können nicht wiederhergestellt werden. Weitere Informationen finden Sie unter Ablaufende Objekte.

Wie funktioniert es?

Das Runbook `AWSSupport-EmptyS3Bucket` führt die folgenden allgemeinen Schritte aus:

- Unterbricht die Bucket-Versionierung, falls diese Option aktiviert ist.
- Aktualisiert die Bucket-Richtlinie, sodass alle `s3:PutObject` API-Aufrufe verweigert werden (um neue Uploads zu verhindern, während der Bucket geleert wird).

- Aktualisiert die Lebenszyklusregeln, sodass alle Objekte gemäß den in den Eingabeparametern angegebenen Ablauftagen gelöscht werden.

> **Note**
>
> - Mit Amazon S3 Object Lock geschützte Objektversionen werden durch Lebenszykluskonfigurationen nicht gelöscht oder überschrieben.
> - Der Löschvorgang ist asynchron und kann einige Zeit in Anspruch nehmen, bis er abgeschlossen ist, nachdem die Runbook-Ausführung abgeschlossen ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden:

- ssm: DescribeAutomationExecutions
- ssm: GetAutomationExecution
- s3: GetBucketVersioning
- s3: PutBucketVersioning
- s3: GetBucketPolicy
- s3: GetBucketLifecycleConfiguration

- s3: GetLifecycleConfiguration
- s3: PutBucketPolicy
- s3: PutBucketLifecycleConfiguration
- s3: PutLifecycleConfiguration
- s3: DeleteBucketPolicy
- s3: DeleteBucketLifecycle

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-EmptyS3Bucket`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - S3BucketName:

     Der Name des Amazon S3 S3-Buckets, den Sie leeren möchten.
   - SNSTopicArn:

     Geben Sie den ARN des Amazon SNS SNS-Themas für die Genehmigungsbenachrichtigung an. Dieses Amazon SNS SNS-Thema wird verwendet, um Genehmigungsbenachrichtigungen zu senden, wenn dies während der Ausführung der Automatisierung erforderlich ist.
   - Genehmigungsurkunde:

     Geben Sie eine Liste der AWS authentifizierten Principals an, die die Aktion entweder genehmigen oder ablehnen können. Die maximale Anzahl von Genehmiger ist. `10` Sie können Prinzipale angeben, indem Sie eines der folgenden Formate verwenden: einen AWS Identity and Access Management (IAM-) Benutzernamen, einen IAM-Benutzer-ARN, einen IAM-Rollen-ARN oder einen IAM-Annahme-Rollen-Benutzer-ARN.
   - MinimumRequiredApprovals(Optional):

Die erforderliche Mindestanzahl an Genehmigungen zum Fortsetzen der Automatisierung. Wenn Sie keinen Wert angeben, verwendet das System standardmäßig. 1 Der Wert für diesen Parameter muss eine positive Zahl sein. Der Wert für diesen Parameter darf die Anzahl der Genehmiger nicht überschreiten, die durch den ApproverIAM-Parameter definiert ist.

- NoncurrentVersionExpirationDays(Optional):

  Geben Sie die Anzahl der Tage an, an denen veraltete Objektversionen ablaufen. Nach Ablauf löscht Amazon S3 permanent die nicht-aktuellen Objektversionen.

  - Standard: 1
  - Maximaler Wert: 365

- ExpirationDays (Fakultativ):

  Geben Sie den Ablauf für den Lebenszyklus des Objekts im Format Tage an.

  - Standard: 1
  - Maximaler Wert: 365

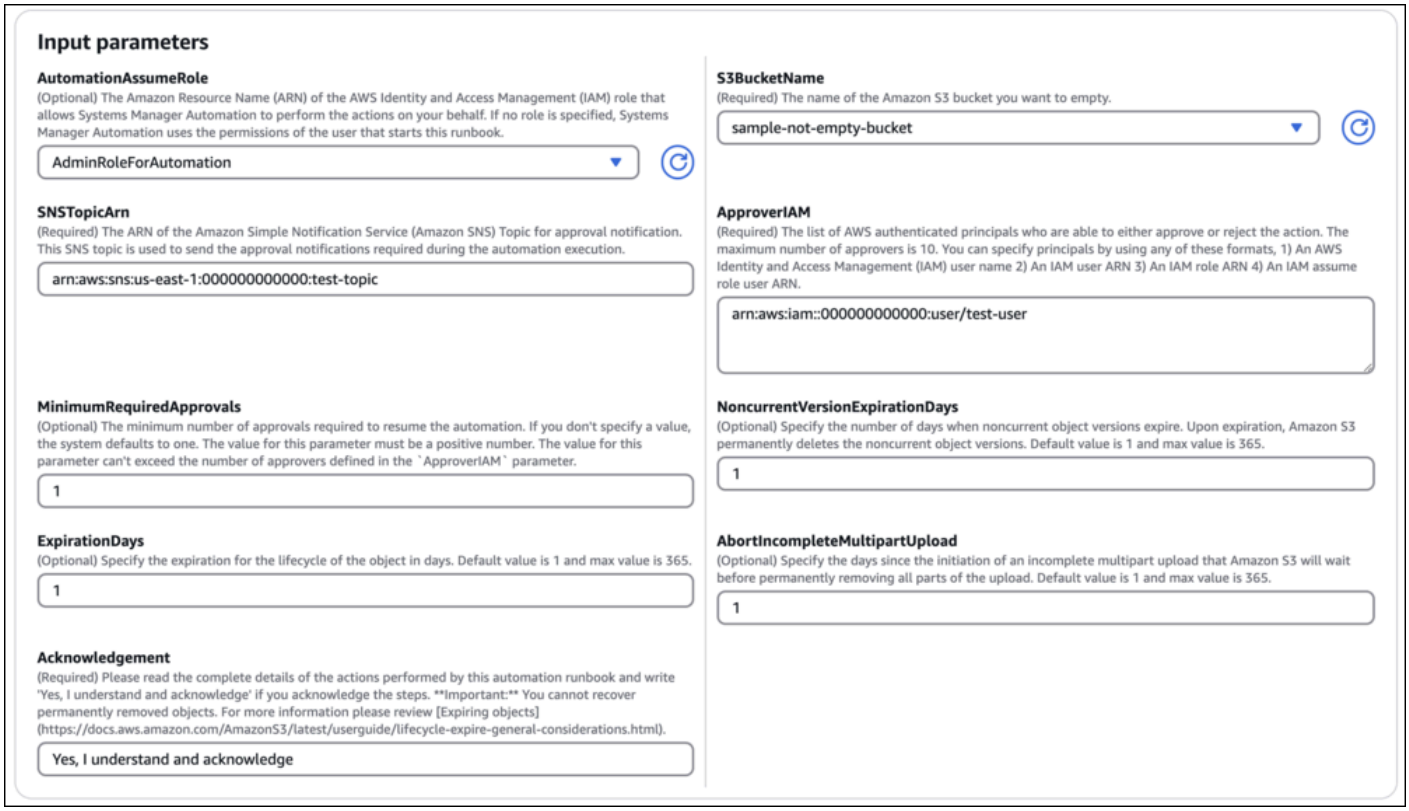
- AbortIncompleteMultipartUpload(Fakultativ):

  Geben Sie die Tage seit dem Start eines unvollständigen mehrteiligen Uploads an, die Amazon S3 abwartet, bevor alle Teile des Uploads dauerhaft entfernt werden.

  - Standard: 1
  - Maximaler Wert: 365

- Bestätigung:

  Bitte lesen Sie die vollständigen Einzelheiten der von diesem Automatisierungs-Runbook ausgeführten Aktionen und stimmen Sie zu, `Yes, I understand and acknowledge` wenn Sie die Schritte bestätigen.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - **`checkConcurrency`**:

     Stellt sicher, dass dieses Runbook nur einmal ausgeführt wird, das auf den angegebenen Amazon S3 S3-Bucket abzielt. Wenn das Runbook eine weitere laufende Ausführung findet, die auf denselben Bucket-Namen abzielt, gibt es einen Fehler zurück und wird beendet.
   - **`getBucketVersioningConfiguration`**:

     Ruft den Versionsstatus des angegebenen Amazon S3 S3-Buckets ab.
   - **`branchOnStoppingIfMFADeleteEnabled`**(bedingt):

     Stoppt die Automatisierung, wenn die Multi-Faktor-Authentifizierung (MFA) für den angegebenen Amazon S3 S3-Bucket aktiviert ist.
   - **`approvalToMakeChangesToTheProvidedS3Bucket`**:

Wartet auf die Genehmigung der designierten Principals, die Bucket-Versionierung zu deaktivieren und die Konfiguration der Bucket-Richtlinien und Lebenszyklusregeln für den angegebenen Amazon S3 S3-Bucket zu aktualisieren.

- **`branchOnBucketVersioningStatus`**(bedingt):

  Wenn die Versionierung für den angegebenen Amazon S3 S3-Bucket aktiviert ist, deaktivieren Sie sie, andernfalls fahren Sie mit der Aktualisierung der Bucket-Richtlinie und der Lebenszykluskonfiguration fort.

- **`suspendBucketVersioning`**:

  Unterbricht den Versionsstatus des angegebenen Amazon S3 S3-Buckets.

- **`updateBucketPolicyAndLifeCycleConfiguration`**:

  Fügt die Bucket-Richtlinie hinzu oder aktualisiert sie, um alle `s3:PutObject` Anfragen abzulehnen, und aktualisiert die Lebenszykluskonfiguration so, dass Objekte auf der Grundlage der vom Benutzer angegebenen Eingabeparameter ablaufen.

- **`branchOnFailingIfBucketPropertiesNotUpdated`**(bedingt):

  Überprüft den Status des `updateBucketPolicyAndLifeCycleConfiguration` Schritts und versucht, den ursprünglichen Status der Bucket-Versionierung wiederherzustellen, falls er durch Automatisierung geändert wurde.

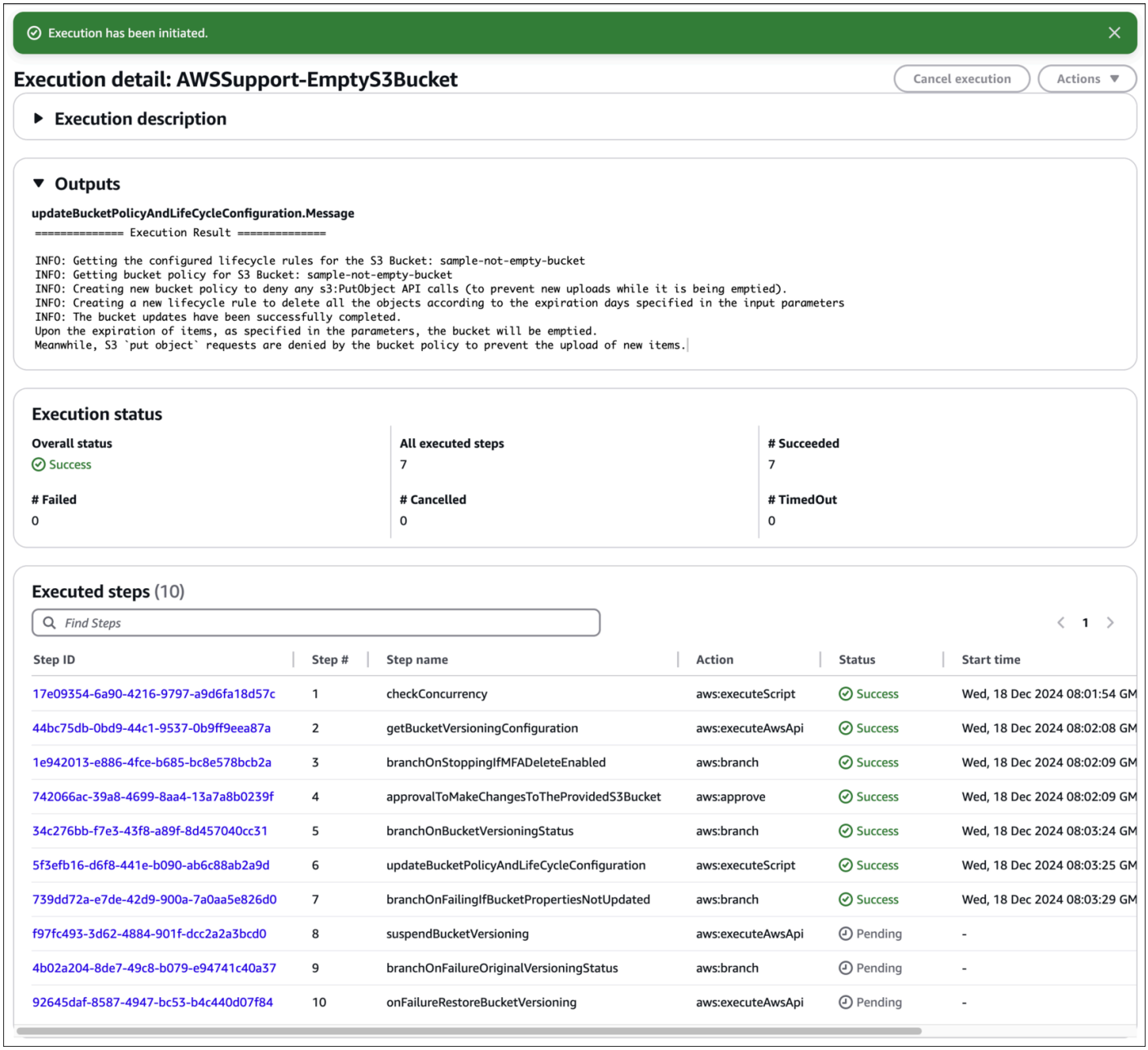
- **`branchOnFailureOriginalVersioningStatus`**(bedingt):

  Bei einem Fehler wird verzweigt, um den ursprünglichen Versionsstatus zu ermitteln. Falls durch diese Automatisierung aktiviert und gesperrt wurde, wird versucht, sie erneut zu aktivieren.

- **`onFailureRestoreBucketVersioning`**

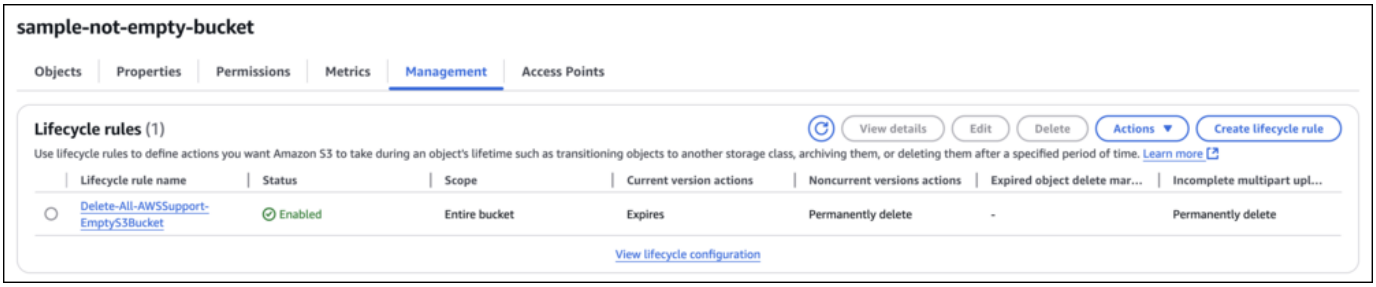
  Stellt den aktivierten Versionsverwaltungsstatus des angegebenen Amazon S3 S3-Buckets wieder her.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:



- Erfolgreiche Ausführung

  Dieser Workflow aktualisiert die Lebenszyklusregel des Buckets. Objekte werden gemäß der `Delete-All-AWSSupport-EmptyS3-Bucket` Lebenszyklusrichtlinie gelöscht.



- Ausführung eines Fehlers

  Ein teilweises Löschen wird nicht durchgeführt. Wenn die Ausführung fehlschlägt, werden der Lebenszyklus und andere Bucket-Einstellungen zurückgesetzt.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

Weitere Informationen zur Verwaltung von Amazon S3 S3-Buckets und -Objekten finden Sie unter Einen Bucket leeren.

AWSSupport-TroubleshootS3EventNotifications

Beschreibung

Das `AWSSupport-TroubleshootS3EventNotifications` AWS Systems Manager Automation-Runbook hilft bei der Fehlerbehebung bei Bucket-Ereignisbenachrichtigungen von Amazon Simple Storage Service (Amazon S3), die mit AWS Lambda Funktionen, Amazon Simple Notification Service (Amazon SNS) -Themen oder Amazon Simple Queue Service (Amazon SQS) -Warteschlangen konfiguriert sind. Es bietet einen Bericht über die Konfigurationseinstellungen der verschiedenen Ressourcen, die mit dem Amazon S3 S3-Bucket konfiguriert wurden, als Zielereignisbenachrichtigung.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Prüft, ob der Amazon S3 S3-Bucket in demselben Konto vorhanden `AWSSupport-TroubleshootS3EventNotifications` ist, in dem er ausgeführt wurde.
- Ruft mithilfe der API die als Ereignisbenachrichtigungen für den Amazon S3-Bucket konfigurierten Zielressourcen (AWS Lambda Funktion oder Amazon SNS-Thema oder Amazon SQS-Warteschlange) ab. GetBucketNotificationConfiguration
- Überprüft, ob die Zielressource existiert, und überprüft dann die ressourcenbasierte Richtlinie der Zielressourcen, um festzustellen, ob Amazon S3 auf dem Ziel veröffentlichen darf.
- Wenn Sie das Ziel mit einem Schlüssel AWS Key Management Service (AWS KMS) verschlüsselt haben, wird die Schlüsselrichtlinie überprüft, um festzustellen, ob Amazon S3 S3-Zugriff zulässig ist.
- Generiert einen Bericht über alle Prüfungen der Zielressourcen.

> **Important**
>
> - Dieses Runbook kann Konfigurationen für Ereignisbenachrichtigungen nur auswerten, wenn der Besitzer des Amazon S3 S3-Buckets mit dem AWS-Konto Besitzer identisch ist, auf dem das Automatisierungs-Runbook ausgeführt wird.
> - Darüber hinaus kann dieses Runbook keine Richtlinien für Zielressourcen auswerten, die auf einem anderen Server gehostet werden. AWS-Konto

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- S3 BucketName

  Typ: `AWS::S3::Bucket::Name`

  Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets, der mit Ereignisbenachrichtigungen konfiguriert ist.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Beispiel für eine IAM-Richtlinie für die Funktion „Automation Assume Role“

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": "*"
                            }
                        ]
                    }
```

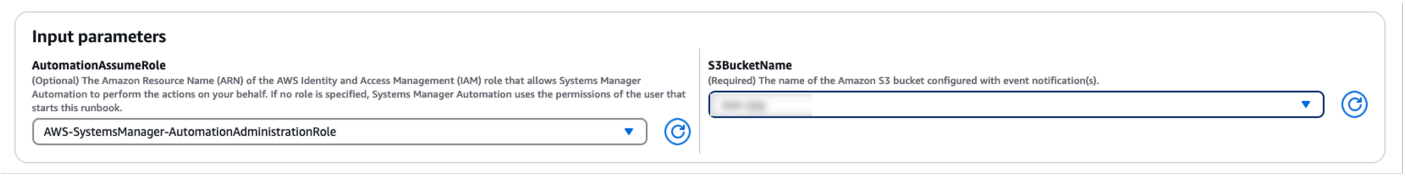
Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-TroubleshootS3EventNotificationsim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - S3 BucketName (erforderlich):

     Der Name des Amazon S3 S3-Buckets, der mit Ereignisbenachrichtigungen konfiguriert ist.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - ValidateInputs

     Überprüft, ob der angegebene Amazon S3 S3-Bucket zu demselben Konto gehört, in dem die Automatisierung ausgeführt wird, und ruft die Region ab, in der der Bucket gehostet wird.
   - GetBucketNotificationConfiguration

     Ruft die `GetBucketNotificationConfiguration` API auf, um die mit dem Amazon S3 S3-Bucket konfigurierten Event-Benachrichtigungen zu überprüfen und formatiert die Ausgabe.
   - BranchOnSQSResourceRichtlinie

     Gibt an, ob Amazon SQS SQS-Ressourcen in Ereignisbenachrichtigungen enthalten sind.
   - Richtlinie validieren SQSResource

Überprüft, ob die Ressourcenrichtlinie für Amazon SQS Queue-Attribute `sqs:SendMessage` berechtigt ist, Amazon S3 zu verwenden. Wenn die Amazon SQS SQS-Ressource verschlüsselt ist, wird geprüft, ob bei der Verschlüsselung kein AWS KMS Standardschlüssel verwendet wird, d. h.`aws/sqs`, ob die AWS KMS Schlüsselrichtlinie über Berechtigungen für Amazon S3 verfügt.

- BranchOnSNSResourceRichtlinie

  Gibt an, ob Amazon SNS SNS-Ressourcen in Ereignisbenachrichtigungen enthalten sind.

- Richtlinie validieren SNSResource

  Überprüft die Ressourcenrichtlinie für Amazon SNS Topic-Attribute hat die `sns:Publish` Berechtigung für Amazon S3. Wenn die Amazon SNS SNS-Ressource verschlüsselt ist, wird geprüft, ob bei der Verschlüsselung kein AWS KMS Standardschlüssel verwendet wird, d. h.`aws/sns`, ob die AWS KMS Schlüsselrichtlinie über Berechtigungen für Amazon S3 verfügt.

- BranchOnLambdaFunctionResourcePolicy

  Gibt an, ob Ereignisbenachrichtigungen AWS Lambda Funktionen enthalten.

- ValidateLambdaFunctionResourcePolicy

  Überprüft, ob die Ressourcenrichtlinie für die AWS Lambda Funktion über eine `lambda:InvokeFunction` Berechtigung für Amazon S3 verfügt.

- GenerateReport

  Gibt Details zu den Runbook-Schritten, Ausgaben und Empfehlungen zur Lösung von Problemen mit den mit dem Amazon S3 S3-Bucket konfigurierten Ereignisbenachrichtigungen zurück.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt „Ausgaben“ die detaillierten Ergebnisse der Ausführung:

   - Amazon SQS SQS-Ereignisbenachrichtigungen

     Wenn Amazon SQS SQS-Zielbenachrichtigungen für den Amazon S3 S3-Bucket konfiguriert sind, wird neben den Ergebnissen der Prüfungen eine Liste der Amazon SQS SQS-Warteschlangen angezeigt. Der Bericht umfasst die Amazon SQS SQS-Ressourcenprüfung, die Prüfung der Amazon SQS SQS-Zugriffsrichtlinien, die AWS KMS Schlüsselprüfung, die AWS KMS Schlüsselstatusprüfung und die Überprüfung der AWS KMS Schlüsselrichtlinien.

   - Amazon SNS SNS-Ereignisbenachrichtigungen

Wenn Amazon SNS-Zielbenachrichtigungen für den Amazon S3-Bucket konfiguriert sind, wird neben den Ergebnissen der Prüfungen eine Liste der Amazon SNS SNS-Themen angezeigt. Der Bericht umfasst die Amazon SNS SNS-Ressourcenprüfung, die Prüfung der Amazon SNS SNS-Zugriffsrichtlinien, die AWS KMS Schlüsselprüfung, die AWS KMS Schlüsselstatusprüfung und die Überprüfung der AWS KMS Schlüsselrichtlinien.

- AWS Lambda Benachrichtigungen über Ereignisse

  Wenn mit dem Amazon S3 S3-Bucket AWS Lambda Zielbenachrichtigungen konfiguriert sind, wird eine Liste der Lambda-Funktionen zusammen mit den Ergebnissen der Prüfungen angezeigt. Der Bericht umfasst die Lambda-Ressourcenprüfung und die Lambda-Zugriffsrichtlinienprüfung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWSSupport-ContainS3Resource

Beschreibung

Das `AWSSupport-ContainS3Resource` Runbook bietet eine automatisierte Lösung für das Verfahren, das im Artikel Support Automation Workflow (SAW) Runbook: Contain a AWS compromitted Amazon S3 Bucket beschrieben wird

Important

- Dieses Runbook führt verschiedene Operationen durch, für die erhöhte Rechte erforderlich sind, z. B. das Ändern von Amazon S3 S3-Bucket-Richtlinien, -Tags und öffentlichen Zugriffskonfigurationen. Diese Aktionen könnten möglicherweise zu einer Rechteeskalation führen oder sich auf andere Workloads auswirken, die vom ausgewählten Amazon S3 S3-Bucket abhängen. Sie sollten die Berechtigungen überprüfen, die der durch den `AutomationAssumeRole` Parameter angegebenen Rolle gewährt wurden, und sicherstellen, dass sie für den beabsichtigten Anwendungsfall geeignet sind. Weitere Informationen zu IAM-Berechtigungen finden Sie in der folgenden AWS Dokumentation: `Identity and Access Management (IAM) PermissionsAWS AWS Systems Manager Automation Permissions`.
- Dieses Runbook führt mutative Aktionen durch, die möglicherweise zur Nichtverfügbarkeit oder Unterbrechung Ihrer Workloads führen können. Insbesondere blockiert die `Contain` Aktion den gesamten Zugriff auf den angegebenen Amazon S3 S3-Bucket, mit Ausnahme der im `SecureRoles` Parameter angegebenen Rollen. Dies könnte sich auf alle Anwendungen oder Dienste auswirken, die auf den angestrebten Amazon S3 S3-Bucket angewiesen sind.
- Während der `Contain` Aktion kann dieses Runbook einen zusätzlichen Amazon S3 S3-Bucket (durch den `BackupS3BucketName` Parameter angegeben) erstellen, um die Sicherungskopie der Konfiguration des ursprünglichen Buckets zu speichern, falls diese noch nicht vorhanden ist.
- Wenn der `Action` Parameter auf gesetzt ist`Restore`, versucht dieses Runbook, die Konfiguration des Amazon S3 S3-Buckets auf der Grundlage der im `BackupS3BucketName` Bucket gespeicherten Sicherung in den ursprünglichen Zustand zurückzusetzen. Es besteht jedoch das Risiko, dass der Wiederherstellungsprozess fehlschlägt und der Amazon S3 S3-Bucket in einem inkonsistenten Zustand zurückbleibt. Das Runbook enthält Anweisungen für die manuelle Wiederherstellung im Falle solcher Fehler. Sie sollten jedoch darauf vorbereitet sein, mögliche Probleme während des Wiederherstellungsprozesses zu lösen.

Es wird empfohlen, das Runbook gründlich zu überprüfen, seine möglichen Auswirkungen zu verstehen und es in einer Nicht-Produktionsumgebung zu testen, bevor Sie es in Ihrer Produktionsumgebung ausführen.

Wie funktioniert es?

Dieses Runbook funktioniert je nach Ressourcentyp und Aktion unterschiedlich:

- Für Amazon S3 General Purpose Bucket`Containment`: Die Automatisierung blockiert den öffentlichen Zugriff auf den Bucket, deaktiviert die ACL-Konfiguration, erzwingt den Besitz von Bucket-Besitzern und legt eine restriktive Bucket-Richtlinie fest, die alle Amazon S3 S3-Aktionen für den Bucket verweigert, mit Ausnahme der zugelassenen aufgelisteten IAM-Rollen.
- Für Amazon S3 General Purpose Object`Containment`: Die Automatisierung blockiert den öffentlichen Zugriff auf den Bucket, deaktiviert die ACL-Konfiguration, erzwingt die Inhaberschaft des Bucket-Besitzers und legt eine restriktive Bucket-Richtlinie fest, die alle Amazon S3 S3-Aktionen für das Objekt mit Ausnahme der erlaubten aufgelisteten IAM-Rollen verweigert.
- Für Amazon S3 Directory Bucket`Containment`: Die Automatisierung legt eine restriktive Bucket-Richtlinie fest, die alle Amazon S3 S3-Aktionen für den Bucket verweigert, mit Ausnahme der aufgelisteten IAM-Rollen zulassen.
- Für Amazon S3 General Purpose Bucket`Restore`: Die Automatisierung setzt die Block Public Access-Konfiguration, die Bucket-ACL-Konfiguration, den Besitz des Bucket-Besitzers und die Bucket-Richtlinie auf die ursprüngliche Konfiguration vor der Beschränkung zurück.
- Für Amazon S3 General Purpose Object`Restore`: Die Automatisierung stellt die Konfiguration Block Public Access, Bucket ACL Konfiguration, Object ACL Configuration, Bucket Owner Object Owner und Bucket Policy auf die ursprüngliche Konfiguration vor der Eindämmung zurück.
- Für Amazon S3 Directory Bucket`Restore`: Durch die Automatisierung wird die Bucket-Richtlinie auf die ursprüngliche Konfiguration vor der Beschränkung zurückgesetzt.

Führen Sie diese Automatisierung aus (Konsole)

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattform

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- 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
- S3 Express: CreateSession
- s3express: DeleteBucketPolicy
- s3express: GetBucketPolicy
- s3express: PutBucketPolicy
- SMS: DescribeAutomationExecutions

Hier ist ein Beispiel für eine IAM-Richtlinie, die die erforderlichen Berechtigungen gewährt für: `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": "*"
        }
    ]
}
```

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-ContainS3Resourceim Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - BucketName (Erforderlich):
     - Beschreibung: (Erforderlich) Der Name des Amazon S3 S3-Buckets.

  - Typ: `AWS::S3::Bucket::Name`
- Aktion (erforderlich):
  - Beschreibung: (Erforderlich) Wählen Sie `Contain` diese Option, um die Amazon S3 S3-Ressource `Restore` zu isolieren oder zu versuchen, die Ressourcenkonfiguration aus einem früheren Backup auf ihren ursprünglichen Zustand zurückzusetzen.
  - Typ: Zeichenfolge
  - Zulässige Werte: `Contain|Restore`
- DryRun (Fakultativ):
  - Beschreibung: (Optional) Wenn diese Option auf true gesetzt ist, nimmt die Automatisierung keine Änderungen an der Amazon S3 S3-Zielressource vor, sondern gibt aus, was sie zu ändern versucht hätte. Standardwert: true.
  - Typ: Boolescher Wert
  - Zulässige Werte: `true|false`
- BucketKeyName (Fakultativ):
  - Beschreibung: (Optional) Der Schlüssel des Amazon S3 S3-Objekts, das Sie enthalten oder wiederherstellen möchten. Wird bei der Eindämmung auf Objektebene verwendet.
  - Typ: Zeichenfolge
  - Zulässiges Muster: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$`
- BucketRestrictAccess(Bedingt):
  - Beschreibung: (Bedingt) Der ARN der IAM-Benutzer oder -Rollen, denen nach der Ausführung der Containment-Aktionen Zugriff auf die Amazon S3 S3-Zielressource gewährt wird. Dieser Parameter ist erforderlich, wenn er auf gesetzt `Action` ist. `Contain`
  - Typ: StringList
  - Zulässiges Muster: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
- TagIdentifier (Fakultativ):
  - Beschreibung: (Optional) Ein Tag im Format Key=BatchId, Value=78925, das den Ressourcen hinzugefügt wird, die von diesem Runbook während des Containment-Workflows erstellt oder geändert wurden.
  - Typ: Zeichenfolge

    - Zulässiges Muster: `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{0,128}$`
- Backups 3 BucketName (bedingt):
    - Beschreibung: (Bedingt) Der Amazon S3 S3-Bucket zum Sichern der Zielressourcenkonfiguration, wenn das auf eingestellt `Action` ist, `Contain` oder zum Wiederherstellen der Konfiguration ab dem Zeitpunkt, an dem das eingestellt `Action` ist`Restore`.
    - Typ: `AWS::S3::Bucket::Name`
- BackupS3 KeyName (bedingt):
    - Beschreibung: (Bedingt) Wenn auf gesetzt `Action` ist`Restore`, gibt dies den Amazon S3 S3-Schlüssel an, mit dem die Automatisierung versucht, die Zielressourcenkonfiguration wiederherzustellen.
    - Typ: Zeichenfolge
    - Zulässiges Muster: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$`
- Backups 3 BucketAccess (bedingt):
    - Beschreibung: (Bedingt) Der ARN der IAM-Benutzer oder -Rollen, denen nach der Ausführung der Containment-Aktionen Zugriff auf den Amazon S3 S3-Backup-Backup gewährt wird. Dieser Parameter ist erforderlich, wenn er `Action` ist. `Contain`
    - Typ: StringList
    - Zulässiges Muster: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
- AutomationAssumeRole (Fakultativ):
    - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der IAM-Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
    - Typ: `AWS::IAM::Role::Arn`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
    - validateRequiredInputs

Validiert die erforderlichen Eingabeparameter für die Automatisierung auf der Grundlage der angegebenen Aktion.

- assertBucketExists

  Prüft, ob der Amazon S3 S3-Ziel-Bucket existiert und zugänglich ist.

- backupBucketPrePrüft

  Prüft, ob der Amazon S3 S3-Backup-Backup potenziell öffentlichen Lese- oder Schreibzugriff auf seine Objekte gewährt.

- backupTargetBucketMetadaten

  Beschreibt die aktuelle Konfiguration des Amazon S3 S3-Ziel-Buckets und lädt das Backup in den angegebenen Backup-Amazon S3-Bucket hoch.

- ContainBucket

  Führt Operationen auf Bucket-Ebene aus, um den Amazon S3 S3-Ziel-Bucket zu enthalten.

- BranchOnActionAndMode

  Verzweigt die Automatisierung auf der Grundlage der Eingabeparameter Action und DryRun.

- RestoreInstanceConfiguration

  Stellt die Amazon S3 S3-Bucket-Konfiguration aus dem Backup wieder her.

- containFinalOutput

  Konsolidiert die Containment-Aktivitäten in lesbarem Format.

- ReportContain

  Gibt Testlaufdetails für die Eindämmungsmaßnahmen aus.

- ReportRestore

  Gibt Details zum Probelauf für die Wiederherstellungsmaßnahmen aus.

- ReportRestoreFailure

  Enthält Anweisungen zur Wiederherstellung der ursprünglichen Konfiguration des Amazon S3 S3-Buckets während eines Fehlerszenarios für den Wiederherstellungs-Workflow.

- ReportContainmentFailure

Enthält Anweisungen zur Wiederherstellung der ursprünglichen Konfiguration des Amazon S3 S3-Buckets während eines Ausfallszenarios für den Containment-Workflow.

- FinalOutput

  Gibt die Details der Eindämmungsmaßnahmen aus.

7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:
   - ContainFinalOutput. Ausgabe

     Gibt die Details der von diesem Runbook ausgeführten Containment-Aktionen aus, wenn diese Option auf False gesetzt `DryRun` ist.
   - RestoreFinalOutput. Ausgabe

     Gibt die Details der von diesem Runbook ausgeführten Wiederherstellungsaktionen aus, wenn der Wert auf `DryRun` False gesetzt ist.
   - Enthält 3. Ausgabe ResourceDryRun

     Gibt die Details der Containment-Aktionen aus, die von diesem Runbook ausgeführt wurden, wenn der Wert auf True gesetzt `DryRun` ist.
   - Stellt S3 wieder her. Ausgabe ResourceDryRun

     Gibt die Details der von diesem Runbook ausgeführten Wiederherstellungsaktionen aus, wenn `DryRun` der Wert auf True gesetzt ist.
   - ReportContainmentFailure.Ausgabe

     Enthält Anweisungen zur Wiederherstellung der ursprünglichen Konfiguration der Amazon S3 S3-Zielressource während eines Ausfallszenarios für den Containment-Workflow.
   - ReportRestoreFailure. Ausgabe

     Enthält Anweisungen zum Wiederherstellen der ursprünglichen Konfiguration der Amazon S3 S3-Zielressource während eines Ausfallszenarios für den Wiederherstellungs-Workflow.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)

- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Support Sie Automatisierungs-Workflows

Amazon SES

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Simple Email Service bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSSupport-AnalyzeSESMessageSendingStatus
- AWSSupport-DeploySESSendingLogsToCloudWatchLogs

`AWSSupport-AnalyzeSESMessageSendingStatus`

Description

Das Runbook zur `AWSSupport-AnalyzeSESMessageSendingStatus` Automatisierung fasst den Status der E-Mail-Zustellung nicht zugestellter E-Mail-Nachrichten zusammen und gibt Ihnen Tipps, wie Sie herausfinden können, warum sie nicht zugestellt wurden. Das Runbook ruft E-Mail-Sendeereignisse von Amazon Simple Email Service (Amazon SES) ab, die in einer von Amazon SES veröffentlichten Amazon CloudWatch Logs-Gruppe gespeichert sind. Einzelheiten zur Veröffentlichung von Amazon SES SES-Veranstaltungen finden Sie unter Überwachung mithilfe der Veröffentlichung von Ereignissen mit Amazon Simple Email Service. Das Runbook enthält auch eine Zusammenfassung und den Zeitplan der E-Mail-Zustellungen sowie Empfehlungen, die sich möglicherweise auf nicht zugestellte E-Mail-Nachrichten auswirken können. Sie finden diese Nachrichten im Ausgabebereich jeder Ausführung. Bitte beachten Sie, dass dieses Runbook die Ereignisse erst nach der Bereitstellung des Event-Speichers beheben kann.

Wie funktioniert es?

Das Runbook führt die folgenden Schritte aus:

- Überprüft gleichzeitige Automatisierungsausführungen für dieselbe CloudWatch Protokollgruppe.

- Analysieren Sie Amazon SES SES-Ereignisse, die der vom Automatisierungsparameter IDs übermittelten Nachricht entsprechen.

- Geben Sie die Lieferzusammenfassungen im Ausgabebereich der Automatisierungsausführung aus.

> **Important**
>
> - Bevor Sie dieses Runbook ausführen, müssen Sie veröffentlichte Amazon SES SES-Ereignisse in einer durch den Automatisierungsparameter angegebenen CloudWatch Logs-Protokollgruppe speichern. Dieses Runbook analysiert nur Amazon SES SES-Ereignisse, die in der Protokollgruppe gespeichert sind.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `logs:StartQuery`
- `logs:GetQueryResults`
- `ses:GetIdentityMailFromDomainAttributes`

- `ses:GetSendQuota`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-AnalyzeSESMessageSendingStatus`im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

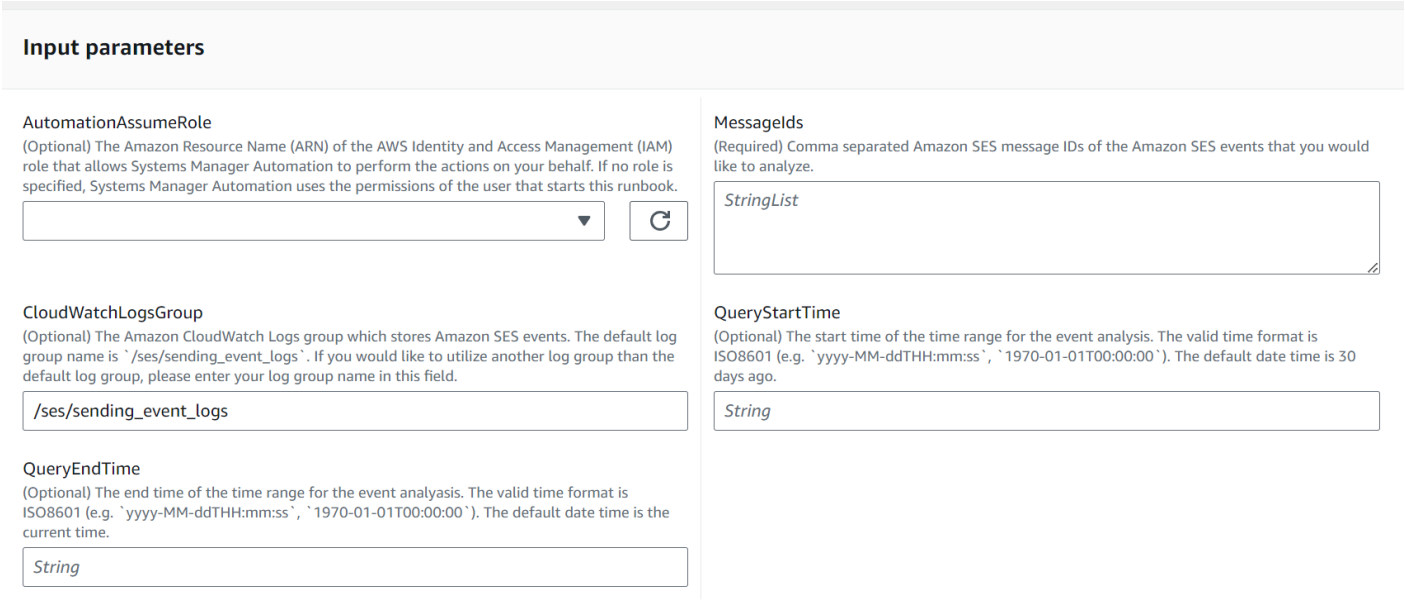
     Der Amazon-Ressourcenname (ARN) der Rolle AWS AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - MessageIds (Erforderlich)

     Durch Kommas getrennte Amazon Simple Email Service-Nachricht IDs von den Amazon Simple Email Service-Ereignissen, die Sie analysieren möchten.
   - CloudWatchLogsGroup (Fakultativ)

     Die Amazon CloudWatch Logs-Gruppe, in der Amazon Simple Email Service-Ereignisse gespeichert werden. Der Standardname der Protokollgruppe lautet `/ses/sending_event_logs`. Wenn Sie eine andere Protokollgruppe als die Standard-Protokollgruppe verwenden möchten, geben Sie bitte Ihren Protokollgruppennamen in dieses Feld ein. „,
   - QueryStartTime (Fakultativ)

     Die Startzeit des Zeitbereichs für die Ereignisanalyse. Das gültige Zeitformat ist ISO8601 (z. B. `YYYY-MM-DDTHH:MM:SS`, `1970-01-01T 00:00:00 `). Das Standarddatum ist vor 30 Tagen.
   - QueryEndTime (Fakultativ)

     Die Endzeit des Zeitbereichs für die Ereignisanalyse. Das gültige Zeitformat ist ISO8601 (z. B. `YYYY-MM-DDTHH:MM:SS`, `1970-01-01T 00:00:00 `). Die Standardzeit für Datum und Uhrzeit ist die aktuelle Uhrzeit.



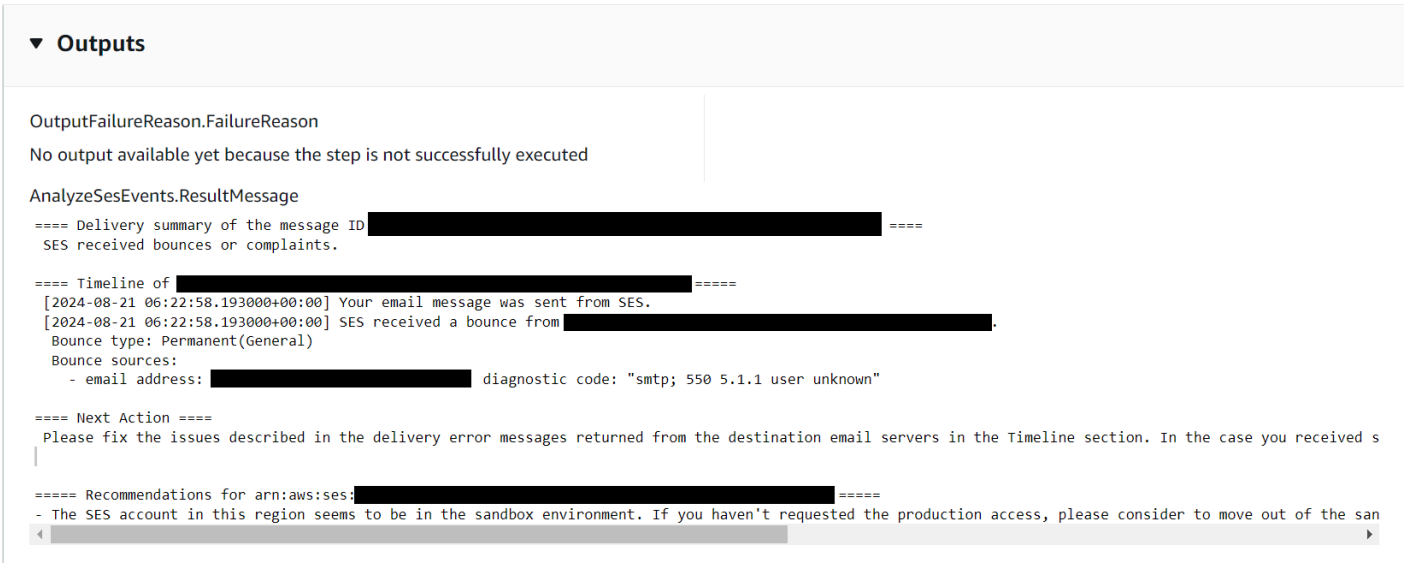
4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - **`CheckConcurrency:`**

     Stellt sicher, dass dieses Runbook nur einmal für die Amazon CloudWatch Logs-Gruppe ausgeführt wird. Wenn das Runbook eine weitere Ausführung findet, die auf dieselbe Protokollgruppe abzielt, gibt es einen Fehler zurück und wird beendet.
   - **`AnalyzeSesEvents:`**

     Analysieren Sie Amazon Simple Email Service-Ereignisse, die in der durch den Automatisierungsparameter angegebenen Amazon CloudWatch Logs-Gruppe gespeichert sind.
   - **`OutputFailureReason:`**

     Gibt Fehlermeldungen bei einem Ausführungsschritt aus, wenn der `AnalyzeSESMessageSendingStatus` Schritt fehlgeschlagen ist.
7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung:
   - Ergebnis der Analyse einer E-Mail-Nachricht, die aufgrund eines Bounces nicht zugestellt wurde

     Ausgabe einer automatisierten Ausführung für eine E-Mail-Nachricht, die das Zielpostfach aufgrund eines Bounces nicht erreicht hat.



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWSSupport-DeploySESSendingLogsToCloudWatchLogs

Beschreibung

Das AWSSupport-DeploySESSendingLogsToCloudWatchLogs Automation Runbook hilft bei der Konfiguration der Infrastruktur, die für die Veröffentlichung von Amazon Simple Email Service (Amazon SES) -Ereignissen in Amazon CloudWatch Logs (CloudWatch Logs) erforderlich ist. Dieses Runbook richtet die Komponenten ein, die für die Erfassung von E-Mail-Versandereignissen und deren Speicherung in CloudWatch Protokollen zur Überwachung und Analyse erforderlich sind. Weitere Informationen zur Veröffentlichung von Amazon SES-Ereignissen finden Sie unter Überwachen des E-Mail-Versands mithilfe von Amazon SES Event Publishing.

Wenn der `ApproveDeployAnalyticEnvironment` Parameter auf gesetzt ist`approve`, erstellt dieses Runbook neue AWS Ressourcen in Ihrem AWS Konto. Der CloudFormation Stapel wird nach der im `SleepTime` Parameter angegebenen Zeit automatisch gelöscht, sofern nicht auf `0` festgelegt.

Wie funktioniert es?

Dieses Runbook führt die folgenden Aktionen aus:

- Führt vorhandene Konfigurationssätze auf, für die Ereignisziele für Amazon Simple Notification Service (Amazon SNS) -Themen oder Lieferstreams konfiguriert sind.
- Erstellt die Infrastruktur, die für die Veröffentlichung von Amazon SES SES-Ereignissen in CloudWatch Logs erforderlich ist, wenn der `ApproveDeployAnalyticEnvironment` Parameter auf gesetzt ist`approve`.

Wenn der `ApproveDeployAnalyticEnvironment` Parameter auf gesetzt ist`approve`, erstellt das Runbook die folgenden Ressourcen:

- Ein CloudFormation Stack mit dem Namen`AWSSupport-SESSendingLogsToCloudWatchLogs`, der Folgendes beinhaltet:
  - Amazon SNS SNS-Thema mit AWS Key Management Service (AWS KMS) -Verschlüsselung
  - Amazon Simple Queue Service-Warteschlange (Amazon SQS)
  - AWS Lambda Funktion zur Verarbeitung von E-Mail-Versandereignissen
  - AWS Identity and Access Management (IAM) -Ausführungsrolle mit Berechtigungen für Amazon SQS und Logs CloudWatch
  - CloudWatch Logs (Protokollgruppe)
  - AWS KMS Schlüssel für die Verschlüsselung
  - Amazon SES SES-Konfigurationssatz mit Veranstaltungszielen
- Die Infrastruktur verarbeitet E-Mail-Sendeereignisse im folgenden Ablauf: Amazon SES SES-E-Mail-Versandereignisse → Amazon SES SES-Konfigurationssatz → Amazon SNS SNS-Thema → Amazon SQS SQS-Warteschlange → Lambda-Funktion → Protokolle CloudWatch
- Ordnet den erstellten Konfigurationssatz als Standardkonfigurationssatz für eine angegebene Amazon SES SES-Identität zu, wenn der `SesIdentity` Parameter angegeben wird.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

/

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Beispiel für eine Richtlinie:

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

Anweisungen

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie [AWSSupport-DeploySESSendingLogsToCloudWatchLogs](#)im Systems Manager unter Dokumente zu.
2. Wählen Sie Execute automation (Automatisierung ausführen).

3. Geben Sie für die Eingabeparameter Folgendes ein:

- AutomationAssumeRole (Fakultativ):
  - Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der IAM-Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
  - Typ: `AWS::IAM::Role::Arn`
- ApproveDeployAnalyticEnvironment (Optional):
  - Beschreibung: (Optional) Genehmigung zur Bereitstellung der Amazon SES SES-Infrastruktur für die Veröffentlichung von Ereignissen. Geben Sie ein`approve`, um den CloudFormation Stack und die zugehörigen Ressourcen zu erstellen. Wenn das Feld leer gelassen wird, zeigt das Runbook nur bestehende Konfigurationssätze mit oder Amazon SNS SNS-Ereigniszielen in der aktuellen Region an.
  - Typ: `String`
  - Muster zulassen: `^$|^approve$`
  - Standard: `""`
- SesIdentity (Fakultativ):
  - Beschreibung: (Optional) Amazon SES SES-Identität (E-Mail-Adresse oder Domain), die dem neu erstellten Konfigurationssatz als Standardkonfigurationssatz zugeordnet werden soll. Dadurch werden alle vorhandenen Standardkonfigurationen für die angegebene Identität überschrieben.
  - Typ: `String`
  - Standard: `""`
- CloudWatchLogGroupName (Optional):
  - Beschreibung: (Optional) Name der CloudWatch Logs-Protokollgruppe, die zum Speichern von Amazon SES SES-E-Mail-Sendeereignissen erstellt werden soll.
  - Typ: `String`
  - Muster zulassen: `^[0-9a-zA-Z_.#/\\-]{1,512}$`
  - Standard: `/ses/sending_event_logs`
- Maske PIIData (optional):
  - Beschreibung: (Optional) Geben Sie an, ob personenbezogene Daten (PII) wie Ziel-E-Mail-Adressen und E-Mail-Betreffzeilen in CloudWatch Protokollen maskiert werden sollen. Legen Sie fest`False`, dass diese Informationen in die Protokolle aufgenommen werden sollen.

- Typ: `String`
- Zulässige Werte: `[True, False]`
- Standard: `True`

- SleepTime (Fakultativ):
  - Beschreibung: (Optional) Wartezeit in Minuten, bis der CloudFormation Stack automatisch gelöscht wird. Die Standardeinstellung ist 24 Stunden (1.440 Minuten), maximal 7 Tage (10.080 Minuten). Auf einstellen, um automatisches `0` Löschen zu verhindern.
  - Typ: `String`
  - Muster zulassen: `^(?:[0-9]|[1-9]\\d{1,3}|100[0-7][0-9])$`
  - Standard: `1440`
- RetainCloudWatchLogsOnDeletion (Fakultativ):
  - Beschreibung: (Optional) Geben Sie an, ob die Protokollgruppe „ CloudWatch Logs“ beibehalten werden soll, wenn der CloudFormation Stack gelöscht wird. Stellen Sie auf `False` ein, um die Protokollgruppe zusammen mit dem Stack zu löschen.
  - Typ: `String`
  - Zulässige Werte: `[True, False]`
  - Standard: `True`
- UniqueId (Fakultativ):
  - Beschreibung: (Optional) Eine eindeutige Kennung für den Workflow.
  - Typ: `String`
  - Muster zulassen: `\\{\\{ automation:EXECUTION_ID \\}\\}|[a-zA-Z0-9-]+`
  - Standard: `{{ automation:EXECUTION_ID }}`
  - Max. Charaktere: `64`

4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - BranchOnValueOfParameterApproveDeployAnalyticEnvironment

     Legt auf der Grundlage des `ApproveDeployAnalyticEnvironment` Parameterwerts fest, ob die Amazon SES SES-Infrastruktur für die Veröffentlichung von Ereignissen bereitgestellt werden soll.
   - GetEligibleConfigurationSets

Ruft bestehende Amazon SES SES-Konfigurationssätze ab und identifiziert solche mit Ereigniszielen, die für Lieferstreams oder Amazon SNS SNS-Themen konfiguriert sind.

- CheckConcurrency

  Überprüft, ob kein vorhandener Stack vorhanden ist und dass keine anderen gleichzeitigen Ausführungen dieses Runbooks denselben Stack erstellen.

- DeploySesEventDestinations

  Erstellt den CloudFormation Stack, der die Amazon SES SES-Infrastruktur für die Veröffentlichung von Ereignissen enthält, einschließlich Amazon SNS SNS-Thema, Amazon SQS SQS-Warteschlange, Lambda-Funktion und CloudWatch Logs-Protokollgruppe.

- RelateConfigurationSetAsDefaultConfigurationSet

  Ordnet den neu erstellten Amazon SES SES-Konfigurationssatz als Standardkonfigurationssatz für die angegebene Amazon SES SES-Identität zu (falls vorhanden).

- SleepBeforeDeleteCloudFormationStack

  Wartet auf die im SleepTime Parameter angegebene Dauer, bevor mit dem Löschen des CloudFormation Stacks fortgefahren wird.

- DeleteCloudFormationStack

  Löscht den CloudFormation Stapel nach dem angegebenen Zeitraum.

7. Nach Abschluss der Ausführung finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.

Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

SageMaker KI

AWS Systems Manager Automation bietet vordefinierte Runbooks für Amazon SageMaker AI. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-DisableSageMakerNotebookRootAccess

`AWS-DisableSageMakerNotebookRootAccess`

Beschreibung

Das `AWS-DisableSageMakerNotebookRootAccess` Runbook deaktiviert den Root-Zugriff auf eine Amazon SageMaker AI-Notebook-Instance. Während der Automatisierung wird die Notebook-Instance gestoppt, um die erforderlichen Änderungen vorzunehmen. SageMaker AI Studio-Notebook-Instanzen werden nicht unterstützt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- NotebookInstanceName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der SageMaker AI-Notebook-Instanz, für die der Root-Zugriff deaktiviert werden soll.

- StartInstanceAfterUpdate

  Typ: Boolescher Wert

  Standard: true

  Beschreibung: (Optional) Legt fest, ob die Notebook-Instanz nach dem Deaktivieren des Root-Zugriffs gestartet wird. Die Standardeinstellung für diesen Parameter ist`true`. Wenn auf gesetzt`true`, wird die Instanz gestartet, nachdem der Root-Zugriff deaktiviert wurde. Wenn auf gesetzt`false`, verbleibt die Instanz in dem `stopped` Zustand, in dem der Root-Zugriff deaktiviert wurde.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

Dokumentschritte

- CheckNotebookInstanceStatus (aws:executeAwsApi): Prüft den aktuellen Status der Notebook-Instanz.

- StopOrUpdateNotebookInstance (aws:branch): Verzweigt basierend auf dem Status der Notebook-Instance.
- StopNotebookInstance (aws:executeAwsApi): Startet die Instance, wenn der Status lautet. `stopped`
- WaitForInstanceToStop (aws: waitForAwsResourceProperty): Überprüft, ob die `stopped` Instanz
- UpdateNotebookInstance (aws:executeAwsApi): Deaktiviert den Root-Zugriff auf der Notebook-Instanz.
- WaitForNotebookUpdate (aws: waitForAwsResourceProperty): Überprüft, ob der Root-Zugriff deaktiviert wurde und die Instance einen `stopped` Status hat.
- ChooseInstanceStart (aws:branch): Verzweigung, die darauf basiert, ob die Instance gestartet werden soll.
- StartNotebookInstance (aws:executeAwsApi): Startet die Notebook-Instanz.
- VerifyNotebookInstanceStatus (aws: waitForAwsResourceProperty): Überprüft, ob die Instanz aktiv ist, `available` bevor der Root-Zugriff deaktiviert wird.
- VerifyNotebookInstanceRootAccess (aws: assertAwsResource Property): Überprüft, ob die Root-Zugriffseinstellung für die Notebook-Instanz erfolgreich deaktiviert wurde.

Secrets Manager

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Secrets Manager Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-DeleteSecret
- AWSConfigRemediation-RotateSecret

`AWSConfigRemediation-DeleteSecret`

Beschreibung

Das `AWSConfigRemediation-DeleteSecret` Runbook löscht ein Geheimnis und alle darin gespeicherten Versionen. AWS Secrets Manager Sie können optional das Wiederherstellungsfenster angeben, in dem Sie das Geheimnis wiederherstellen können. Wenn Sie keinen Wert für den

`RecoveryWindowInDays` Parameter angeben, wird der Vorgang standardmäßig auf 30 Tage eingestellt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- RecoveryWindowInDays

  Typ: Ganzzahl

  Gültige Werte: 7-30

  Standard: 30

  Beschreibung: (Optional) Die Anzahl der Tage, an denen Sie das Geheimnis wiederherstellen können.
- SecretId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Geheimnisses, das Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager:DeleteSecret`
- `secretsmanager:DescribeSecret`

Dokumentschritte

- `aws:executeAwsApi`- Löscht das Geheimnis, das Sie im `SecretId` Parameter angeben.
- `aws:executeScript`- Überprüft, ob das Löschen des Geheimnisses geplant wurde.

`AWSConfigRemediation-RotateSecret`

Beschreibung

Das `AWSConfigRemediation-RotateSecret` Runbook rotiert ein in gespeichertes Geheimnis. AWS Secrets Manager

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- RotationInterval

  Typ: Intervall

  Gültige Werte: 1—365

  Beschreibung: (Erforderlich) Die Anzahl der Tage zwischen den Rotationen des Geheimnisses.

- RotationLambdaArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Lambda Funktion, die das Geheimnis rotieren kann.

- SecretId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Geheimnisses, das Sie rotieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

Dokumentschritte

- `aws:executeAwsApi`- Dreht das Geheimnis, das Sie im `SecretId` Parameter angeben.
- `aws:executeScript`- Überprüft, ob die Rotation für das Geheimnis aktiviert wurde.

Security Hub CSPM

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS Security Hub CSPM Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-EnableSecurityHub

`AWSConfigRemediation-EnableSecurityHub`

Beschreibung

Das `AWSConfigRemediation-EnableSecurityHub` Runbook aktiviert AWS Security Hub CSPM (Security Hub CSPM) für die AWS-Konto und AWS-Region wo Sie die Automatisierung ausführen. Informationen zu Security Hub CSPM finden Sie unter Was ist? AWS Security Hub CSPM im AWS Security Hub Benutzerhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- EnableDefaultStandards

  Typ: Boolescher Wert

  Standard: true

  Beschreibung: (Erforderlich) Wenn auf gesetzt`true`, sind die von Security Hub CSPM festgelegten Standardsicherheitsstandards aktiviert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert Security Hub CSPM im Girokonto und in der Region.
- `aws:executeAwsApi`— Überprüft, ob Security Hub CSPM aktiviert wurde.

AWS Shield

AWS Systems Manager Die Automatisierung bietet vordefinierte Runbooks für. AWS Shield Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSPremiumSupport-DDoSResiliencyAssessment

AWSPremiumSupport-DDoSResiliencyAssessment

Beschreibung

Das AWS Systems Manager Automation-Runbook hilft Ihnen dabei`AWSPremiumSupport-DDoSResiliencyAssessment`, Sicherheitslücken in DDo S zu überprüfen und die Konfiguration der Ressourcen entsprechend dem AWS Shield Advanced Schutz für Sie AWS-Konto zu konfigurieren. Es enthält einen Bericht mit den Konfigurationseinstellungen für Ressourcen, die anfällig für Distributed Denial of Service (DDoS) -Angriffe sind. Es wird verwendet, um die folgenden Ressourcen zu sammeln, zu analysieren und zu bewerten: Amazon Route 53, Amazon Load Balancers, CloudFront Amazon-Distributionen AWS Global Accelerator und AWS Elastic IPs für ihre Konfigurationseinstellungen gemäß den empfohlenen Best Practices for AWS Shield Advanced Protection. Der endgültige Konfigurationsbericht ist in einem Amazon S3 S3-Bucket Ihrer Wahl als HTML-Datei verfügbar.

Wie funktioniert er?

Dieses Runbook enthält eine Reihe von Prüfungen für die verschiedenen Arten von Ressourcen, die für den öffentlichen Zugriff aktiviert sind, und ob für sie Schutzmaßnahmen gemäß den Empfehlungen im AWS DDoS Best Practices Whitepaper konfiguriert wurden. Das Runbook führt Folgendes aus:

- Prüft, ob ein Abonnement für aktiviert AWS Shield Advanced ist.
- Wenn aktiviert, findet es heraus, ob Shield Advanced-geschützte Ressourcen vorhanden sind.
- Es findet alle globalen und regionalen Ressourcen im AWS-Konto und prüft, ob diese durch Shield geschützt sind.
- Es erfordert die Ressourcentyp-Parameter für die Bewertung, den Amazon S3 S3-Bucket-Namen und die Amazon S3 AWS-Konto S3-Bucket-ID (S3BucketOwner).
- Es gibt die Ergebnisse als HTML-Bericht zurück, der im bereitgestellten Amazon S3 S3-Bucket gespeichert ist.

Die Eingabeparameter `AssessmentType` entscheiden, ob die Prüfungen für alle Ressourcen durchgeführt werden. Standardmäßig sucht das Runbook nach allen Ressourcentypen. Wenn nur der `RegionalResources` Parameter `GlobalResources` oder ausgewählt ist, führt das Runbook Prüfungen nur für die ausgewählten Ressourcentypen durch.

> **Important**
>
> - Für den Zugriff auf `AWSPremiumSupport-*` Runbooks ist ein Abonnement für Business + Support, Enterprise Support oder Unified Operations erforderlich. Weitere Informationen finden Sie unter AWS Support Tarife vergleichen.
> - Für dieses Runbook ist ein `ACTIVE` AWS Shield Advanced Abonnement erforderlich.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- AssessmentType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Legt den Typ der Ressourcen fest, die für die DDo S-Resilienzbewertung bewertet werden sollen. Standardmäßig bewertet das Runbook sowohl globale als auch regionale Ressourcen. Für regionale Ressourcen beschreibt das Runbook alle Load Balancer für

Anwendungen (ALB) und Netzwerke (NLB) sowie die gesamte Auto Scaling Scaling-Gruppe in Ihrer /region. AWS-Konto

Zulässige Werte: `['Global Resources', 'Regional Resources', 'Global and Regional Resources']`

Standard: Globale und regionale Ressourcen

- S3 BucketName

  Typ: `AWS::S3::Bucket::Name`

  Beschreibung: (Erforderlich) Der Amazon S3 S3-Bucket-Name, in den der Bericht hochgeladen wird.

  Zulässiges Muster: `^[0-9a-z][a-z0-9\-\.]{3,63}$`

- S3 BucketOwnerAccount

  Typ: Zeichenfolge

  Beschreibung: (Optional) Derjenige AWS-Konto , dem der Amazon S3 S3-Bucket gehört. Bitte geben Sie diesen Parameter an, wenn der Amazon S3 S3-Bucket zu einem anderen gehört. AWS-Konto Andernfalls können Sie diesen Parameter leer lassen.

  Zulässiges Muster: `^$|^[0-9]{12,13}$`

- S3 BucketOwnerRoleArn

  Typ: `AWS::IAM::Role::Arn`

  Beschreibung: (Optional) Der ARN einer IAM-Rolle mit der Berechtigung, den Amazon S3 S3-Bucket zu beschreiben und den öffentlichen Zugriff zu AWS-Konto blockieren, falls sich der Bucket in einem anderen AWS-Konto befindet. Wenn dieser Parameter nicht angegeben ist, verwendet das Runbook den `AutomationAssumeRole` oder den IAM-Benutzer, der dieses Runbook startet (falls `AutomationAssumeRole` nicht angegeben). Weitere Informationen finden Sie im Abschnitt „Erforderliche Berechtigungen“ in der Runbook-Beschreibung.

  Zulässiges Muster: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- S3 BucketPrefix

  Typ: Zeichenfolge

Beschreibung: (Optional) Das Präfix für den Pfad innerhalb von Amazon S3 zum Speichern der Ergebnisse.

Zulässiges Muster: `^[a-zA-Z0-9][-./a-zA-Z0-9]{0,255}$|^$`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Beispiel für eine IAM-Richtlinie für die Funktion „Automation Assume Role“

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"
                }
            ]
```

```
}
```

Anweisungen

1. Navigieren Sie AWSPremiumSupport-DDoSResiliencyAssessmentin der AWS Systems Manager Konsole zu.
2. Wählen Sie Automatisierung ausführen
3. Geben Sie für Eingabeparameter Folgendes ein:
   - AutomationAssumeRole(Fakultativ):

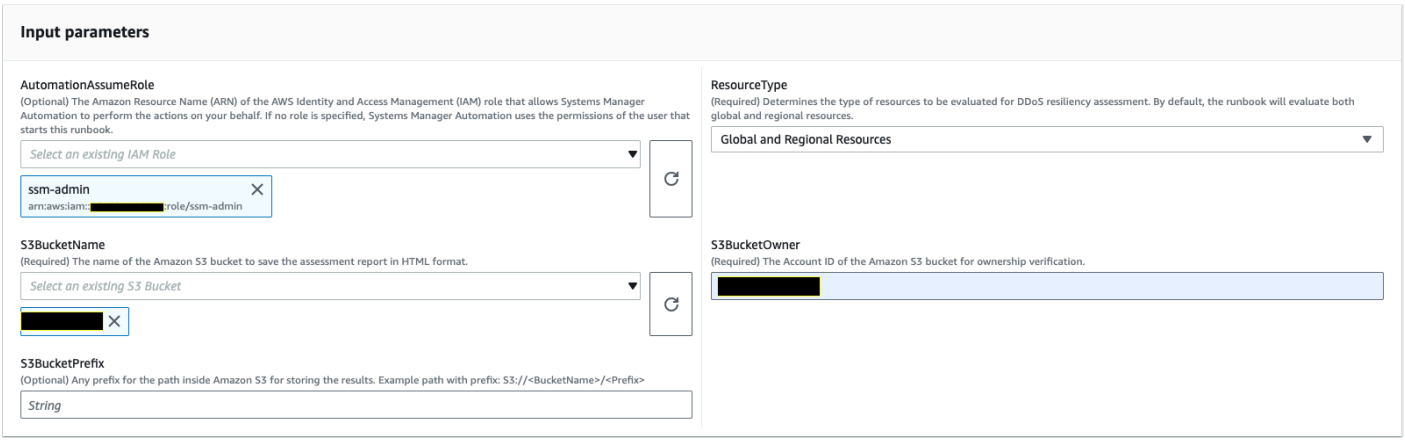
     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - AssessmentType(Optional):

     Bestimmt die Art der Ressourcen, die für die DDo S-Resilienzbewertung bewertet werden sollen. Standardmäßig bewertet das Runbook sowohl globale als auch regionale Ressourcen.
   - S3 BucketName (erforderlich):

     Der Name des Amazon S3 S3-Buckets, in dem der Bewertungsbericht im HTML-Format gespeichert werden soll.
   - S3 BucketOwner (optional):

     Die AWS-Konto ID des Amazon S3 S3-Buckets für die Eigentumsverifizierung. Die AWS-Konto ID ist erforderlich, wenn der Bericht in einem kontoübergreifenden Amazon S3 S3-Bucket veröffentlicht werden muss, und optional, wenn sich der Amazon S3 S3-Bucket in derselben Phase befindet AWS-Konto wie die Initiierung der Automatisierung.
   - S3 BucketPrefix (optional):

     Beliebiges Präfix für den Pfad innerhalb von Amazon S3 zum Speichern der Ergebnisse.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird eingeleitet.
6. Das Dokument führt die folgenden Schritte aus:
   - CheckShieldAdvancedState:

     Überprüft, ob das abonniert AWS-Konto ist AWS Shield Advanced und ob das Runbook Zugriff auf den Amazon S3 S3-Bucket hat.
   - S3: BucketSecurityChecks

     Überprüft, ob der in „S3BucketName“ angegebene Amazon S3-Bucket anonyme oder öffentliche Lese- oder Schreibzugriffsberechtigungen gewährt, ob für den Bucket die Verschlüsselung im Ruhezustand aktiviert ist und ob die in „S3BucketOwner“ angegebene AWS-Konto ID der Besitzer des Amazon S3 S3-Buckets ist.
   - BranchOnShieldAdvancedStatus:

     Branches dokumentieren Schritte auf der Grundlage des AWS Shield Advanced Abonnementstatus and/or Amazon S3 Bucket Ownership Status.
   - ShieldAdvancedConfigurationReview:

     Überprüft die Shield Advanced-Konfigurationen, um sicherzustellen, dass die mindestens erforderlichen Details vorhanden sind. Zum Beispiel: IAM-Zugriff für das AWS Shield Response-Team (SRT) -Team, Kontaktlistendetails und SRT-Status für proaktives Engagement.
   - ListShieldAdvancedProtections:

     Listet die durch Shield geschützten Ressourcen auf und erstellt für jeden Dienst eine Gruppe geschützter Ressourcen.
   - BranchOnResourceTypeAndCount:

Verzweigt Dokumentschritte auf der Grundlage des Werts des Parameters Resource Type und der Anzahl der durch Shield geschützten globalen Ressourcen.

- ReviewGlobalResources:

  Überprüft die von Shield Advanced geschützten globalen Ressourcen wie Route 53 Hosted Zones, CloudFront Distributions und Global Accelerators.

- BranchOnResourceType:

  Branches dokumentieren die Schritte auf der Grundlage des ausgewählten Ressourcentyps (Global, Regional oder beides).

- ReviewRegionalResources:

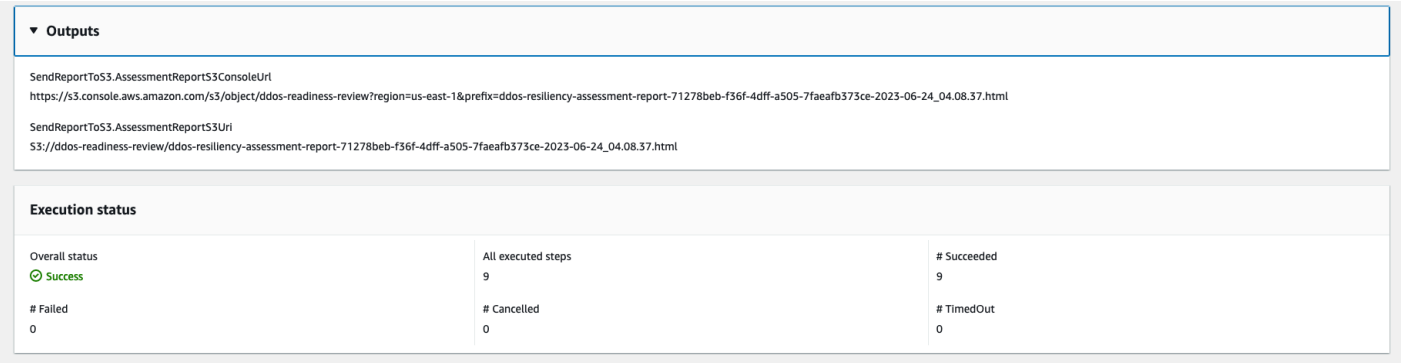
  Überprüft die von Shield Advanced geschützten regionalen Ressourcen wie Application Load Balancers, Network Load Balancers, Classic Load Balancers und Amazon Elastic Compute Cloud (Amazon EC2) Instances (Elastic). IPs

- SendReportToS3:

  Lädt die Details des DDo S Assessment Reports in den Amazon S3 S3-Bucket hoch.

7. Nach Abschluss des Vorgangs wird der URI für die HTML-Datei des Bewertungsberichts im Amazon S3 S3-Bucket bereitgestellt:

   S3-Konsolenlink und Amazon S3 S3-URI für den Bericht über die erfolgreiche Ausführung des Runbooks



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)

- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS Servicedokumentation

- AWS Shield Advanced

Amazon SNS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Simple Notification Service bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableSNSTopicDeliveryStatusLogging
- AWSConfigRemediation-EncryptSNSTopic
- AWS-PublishSNSNotification

`AWS-EnableSNSTopicDeliveryStatusLogging`

Beschreibung

Das `AWS-EnableSNSTopicDeliveryStatusLogging` Runbook konfiguriert die Protokollierung des Lieferstatus für einen Amazon Data Firehose-HTTP, Lambda- oder Amazon Simple Queue Service (Amazon SQS) -Endpunkt. `Platform application` Auf diese Weise kann Amazon SNS fehlgeschlagene Benachrichtigungen und einen Beispielprozentsatz erfolgreicher Warnmeldungen an Amazon CloudWatch protokollieren. Wenn die Protokollierung des Lieferstatus für das Thema bereits konfiguriert ist, ersetzt das Runbook die bestehende Konfiguration durch die neuen Werte, die Sie für die Eingabeparameter angeben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- EndpointType

  Typ: Zeichenfolge

  Zulässige Werte:
  - HTTP
  - Firehose
  - Lambda
  - Anwendung
  - SQS

  Beschreibung: (Erforderlich) Der Typ des Amazon SNS SNS-Themenendpunkts, für den Sie Benachrichtigungen zum Lieferstatus protokollieren möchten.
- TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon SNS SNS-Themas, für das Sie die Versandstatusprotokollierung konfigurieren möchten.
- SuccessFeedbackRoleArn

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, an die Amazon SNS Protokolle für erfolgreiche Benachrichtigungen sendet. CloudWatch

- SuccessFeedbackSampleRate

  Typ: Zeichenfolge

  Gültige Werte: 0-100

  Beschreibung: (Erforderlich) Der Prozentsatz der erfolgreichen Nachrichten, die für das angegebene Amazon SNS-Thema geprüft werden sollen.

- FailureFeedbackRoleArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der IAM-Rolle, an die Amazon SNS Protokolle für Fehlerbenachrichtigungen sendet. CloudWatch

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Dokumentschritte

- `aws:executeAwsApi`— Wendet den Wert für den `SuccessFeedbackRoleArn` Parameter auf das Amazon SNS SNS-Thema an.
- `aws:executeAwsApi`— Wendet den Wert für den `SuccessFeedbackSampleRate` Parameter auf das Amazon SNS SNS-Thema an.
- `aws:executeAwsApi`— Wendet den Wert für den `FailureFeedbackRoleArn` Parameter auf das Amazon SNS SNS-Thema an.

- `aws:executeScript`- Bestätigt, dass die Protokollierung des Lieferstatus für das Amazon SNS SNS-Thema aktiviert ist.

Ausgaben

VerifyDeliveryStatusLoggingEnabled. GetTopicAttributesResponse - Antwort von den `GetTopicAttributes` API-Operationen.

VerifyDeliveryStatusLoggingEnabled. VerifyDeliveryStatusLoggingEnabled - Meldung über die erfolgreiche Überprüfung der Protokollierung des Lieferstatus.

`AWSConfigRemediation-EncryptSNSTopic`

Beschreibung

Das `AWSConfigRemediation-EncryptSNSTopic` Runbook ermöglicht die Verschlüsselung des von Ihnen angegebenen Amazon Simple Notification Service (Amazon SNS) -Themas mithilfe eines AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssels. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass Ihre Amazon SNS SNS-Themen gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Themen mit unterschiedlichen, vom Kunden verwalteten Schlüsseln zu verschlüsseln.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- KmsKeyArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des vom AWS KMS Kunden verwalteten Schlüssels, den Sie zur Verschlüsselung des Amazon SNS-Themas verwenden möchten.

- TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon SNS SNS-Themas, das Sie verschlüsseln möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Dokumentschritte

- `aws:executeAwsApi`- Verschlüsselt das Amazon SNS SNS-Thema, das Sie im `TopicArn` Parameter angeben.
- `aws:assertAwsResourceProperty`— Bestätigt, dass die Verschlüsselung für das Amazon SNS SNS-Thema aktiviert ist.

AWS-PublishSNSNotification

Beschreibung

Veröffentlichen Sie eine Benachrichtigung auf Amazon SNS.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Fehlermeldung

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Nachricht für die SNS-Benachrichtigung.
- TopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des SNS-Themas, an das die Benachrichtigung veröffentlicht wird.

Amazon SQS

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon Simple Queue Service (Amazon SQS) bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableSQSEncryption

AWS-EnableSQSEncryption

Beschreibung

Das `AWS-EnableSQSEncryption` Runbook ermöglicht die Verschlüsselung im Ruhezustand für eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange. Eine Amazon SQS-Warteschlange kann mit von Amazon SQS verwalteten Schlüsseln (SSE-SQS) oder mit () verwalteten Schlüsseln AWS Key Management Service (SSE-KMS AWS KMS) verschlüsselt werden. Für den Schlüssel, den Sie Ihrer Warteschlange zuweisen, muss eine Schlüsselrichtlinie gelten, die Berechtigungen für alle Principals beinhaltet, die berechtigt sind, die Warteschlange zu verwenden. Wenn die Verschlüsselung aktiviert ist, werden anonyme `ReceiveMessage` Anfragen `SendMessage` und Anfragen an die verschlüsselte Warteschlange abgewiesen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- QueueUrl

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die URL der Amazon SQS SQS-Warteschlange, für die Sie die Verschlüsselung aktivieren möchten.
- KmsKeyId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der AWS KMS Schlüssel, der für die Verschlüsselung verwendet werden soll. Dieser Wert kann ein global eindeutiger Bezeichner, ein ARN für einen Alias oder einen Schlüssel oder ein Aliasname mit dem Präfix „alias/“ sein. Sie können den AWS verwalteten Schlüssel auch verwenden, indem Sie den Alias aws/sqs angeben.
- KmsDataKeyReusePeriodSeconds

  Typ: Zeichenfolge

  Gültige Werte: 60-86400

  Standard: 300

  Beschreibung: (Optional) Der Zeitraum in Sekunden, in dem eine Amazon SQS SQS-Warteschlange einen Datenschlüssel wiederverwenden kann, um Nachrichten zu verschlüsseln oder zu entschlüsseln, bevor sie erneut anruft. AWS KMS

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`

- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

Dokumentschritte

- SelectKeyType (`aws:branch`): Verzweigungen, die auf dem angegebenen Schlüssel basieren.
- PutAttributeSseKms (`aws:executeAwsApi`) — Aktualisiert die Amazon SQS SQS-Warteschlange, sodass sie den für die Verschlüsselung angegebenen AWS KMS Schlüssel verwendet.
- PutAttributeSseSqs (`aws:executeAwsApi`) — Aktualisiert die Amazon SQS SQS-Warteschlange, sodass sie den Standardschlüssel für die Verschlüsselung verwendet.
- VerifySqsEncryptionKms (`aws:assertAwsResourceProperty`) — Überprüft, ob die Verschlüsselung in der Amazon SQS SQS-Warteschlange aktiviert ist.
- VerifySqsEncryptionDefault (`aws:assertAwsResourceProperty`) — Überprüft, ob die Verschlüsselung in der Amazon SQS SQS-Warteschlange aktiviert ist.

Step Functions

AWS Systems Manager Automation bietet vordefinierte Runbooks für AWS Step Functions (Step Functions). Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-EnableStepFunctionsStateMachineLogging

`AWS-EnableStepFunctionsStateMachineLogging`

Beschreibung

Das `AWS-EnableStepFunctionsStateMachineLogging` Runbook aktiviert oder aktualisiert die Protokollierung auf dem von Ihnen angegebenen AWS Step Functions Zustandsmaschine. Die Mindestprotokollierungsebene muss auf `ALLERROR`, oder `FATAL` festgelegt sein.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Level

  Typ: Zeichenfolge

  Gültige Werte: ALL | ERROR | FATAL

  Beschreibung: (Erforderlich) Die URL der Amazon SQS SQS-Warteschlange, für die Sie die Verschlüsselung aktivieren möchten.
- LogGroupArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der Amazon CloudWatch Logs-Protokollgruppe, an die Sie State-Machine-Protokolle senden möchten.
- StateMachineArn

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der ARN der Zustandsmaschine, für die Sie die Anmeldung aktivieren möchten.

- IncludeExecutionData

  Typ: Boolesch

  Standard: False

  Beschreibung: (Optional) Legt fest, ob Ausführungsdaten in den Protokollen enthalten sind.

- TracingConfiguration

  Typ: Boolesch

  Standard: False

  Beschreibung: (Optional) Legt fest, ob die AWS X-Ray Ablaufverfolgung aktiviert ist.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `states:DescribeStateMachine`
- `states:UpdateStateMachine`

Dokumentschritte

- `EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)`- Aktualisiert den angegebenen Zustandsmaschine mit der angegebenen Protokollierungskonfiguration.
- `VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)`- Überprüft, ob die Protokollierung für den angegebenen Zustandsmaschine aktiviert wurde.

Ausgaben

- EnableStepFunctionsStateMachineLogging.Response — Antwort auf den UpdateStateMachine API-Aufruf.

Systems Manager

AWS Systems Manager Automation stellt vordefinierte Runbooks für Systems Manager bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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`

Beschreibung

Mit dem `AWS-BulkDeleteAssociation` Runbook können Sie bis zu 50 Systems Manager State Manager-Verknüpfungen gleichzeitig löschen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AssociationIds

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste IDs der Verknüpfungen, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:DeleteAssociation`

Dokumentschritte

- `aws:executeScript`- Löscht die Assoziationen, die Sie im `AssociationIds` Parameter angeben.

AWS-BulkEditOpsItems

Beschreibung

Mit dem `AWS-BulkEditOpsItems` Runbook können Sie den Status, den Schweregrad, die Kategorie oder die Priorität von AWS Systems Manager OpsItems bearbeiten. Mit dieser Automatisierung können maximal 50 Dateien OpsItems gleichzeitig bearbeitet werden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Kategorie

  Typ: Zeichenfolge

  Zulässige Werte:
  - Verfügbarkeit
  - Cost (Kosten)
  - Keine Änderung
  - Leistung

- Wiederherstellung
- Sicherheit

Standard: Keine Änderung

Beschreibung: (Optional) Die neue Kategorie, die Sie für die bearbeitete Datei angeben möchten OpsItems.

- OpsItemIds

Typ: StringList

Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste, die OpsItems IDs Sie bearbeiten möchten (z. B. OI-xxxxxxxxxxxx, OI-xxxxxxxxxxxx).

- Priorität

Typ: Zeichenfolge

Zulässige Werte:

- Keine Änderung
- 1
- 2
- 3
- 4
- 5

Standard: Keine Änderung

Beschreibung: (Optional) Die Wichtigkeit der bearbeiteten OpsItems Elemente im Vergleich zu anderen OpsItems im System.

- Schweregrad

Typ: Zeichenfolge

Zulässige Werte:

- Keine Änderung
- 1
- 2

- 3
- 4

Standard: Keine Änderung

Beschreibung: (Optional) Der Schweregrad der Bearbeitung OpsItems.

- WaitTimeBetweenEditsInSecs

Typ: Zeichenfolge

Gültige Werte: 0.0-2.0

Standardwert: 0.8

Beschreibung: (Optional) Die Zeit, die die Automatisierung zwischen dem Aufrufen des Vorgangs wartet. `UpdateOpsItems`

- Status

Typ: Zeichenfolge

Zulässige Werte:

- InProgress
- Keine Änderung
- Öffnen
- Gelöst

Standard: Keine Änderung

Beschreibung: (Optional) Der neue Status der Datei „Bearbeitet OpsItems“.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

Dokumentschritte

- `aws:executeScript`- Bearbeitet den, den OpsItems Sie im `OpsItemIds` Parameter angegeben haben, auf der Grundlage der Werte, die Sie für die Parameter`Category`, `PrioritySeverity`, und `Status` angeben.

AWS-BulkResolveOpsItems

Beschreibung

Das `AWS-BulkResolveOpsItems` Runbook löst Lösungen auf AWS Systems Manager OpsItems , die dem von Ihnen angegebenen Filter entsprechen. OpsItems Mit dem Parameter können Sie auch eine angeben OpsItemId , die zur Auflösung hinzugefügt werden soll. `OpsInsightsId` Wenn Sie einen Wert für den `S3BucketName` Parameter angeben, wird eine Ergebniszusammenfassung an den Amazon Simple Storage Service (Amazon S3) -Bucket gesendet. Um eine Benachrichtigung zu erhalten, sobald die Ergebniszusammenfassung an den Amazon S3 S3-Bucket gesendet wurde, geben Sie einen Wert für den `SnsTopicArn` Parameter an. Durch diese Automatisierung können maximal 1.000 Probleme OpsItems gleichzeitig behoben werden.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Filter

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Schlüssel-Wert-Paare von Filtern, um das zurückzugeben, das OpsItems Sie auflösen möchten. Beispiel, `[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`. Weitere Informationen zu den verfügbaren Optionen zum Filtern von OpsItems Antworten finden Sie OpsItemFiltersin der AWS Systems Manager API-Referenz.

- OpsInsightId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die zugehörige Ressourcen-ID, die Sie hinzufügen möchten, wurde aufgelöst OpsItems.

- S3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des Amazon S3 S3-Buckets, an den Sie die Ergebniszusammenfassung senden möchten.

- SnsMessage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Benachrichtigung, die Amazon Simple Notification Service (Amazon SNS) senden soll, wenn die Automatisierung abgeschlossen ist.

- SnsTopicArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN des Amazon SNS SNS-Themas, das Sie benachrichtigen möchten, wenn die Ergebnisübersicht an Amazon S3 gesendet wurde.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- s3:GetBucketAcl
- s3:PutObject
- sns:Publish
- ssm:DescribeOpsItems
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

Dokumentschritte

- aws:executeScript- Sammelt und löst sie auf der OpsItems Grundlage der von Ihnen angegebenen Filter auf. Wenn Sie einen Wert für den OpsInsightId Parameter angegeben haben, wird der Wert als zugehörige Ressource hinzugefügt.
- aws:executeScript— Wenn Sie einen Wert für den S3BucketName Parameter angegeben haben, wird eine Ergebniszusammenfassung an den Amazon S3 S3-Bucket gesendet.
- aws:executeScript— Wenn Sie einen Wert für den SnsTopicArn Parameter angegeben haben, wird eine Benachrichtigung an das Amazon SNS SNS-Thema gesendet, nachdem die Ergebniszusammenfassung an Amazon S3 gesendet wurde, einschließlich des SnsMessage Parameterwerts, falls angegeben.

AWS-ConfigureMaintenanceWindows

Beschreibung

Das AWS-ConfigureMaintenanceWindows Runbook hilft Ihnen, mehrere Systems Manager Manager-Wartungsfenster zu aktivieren oder zu deaktivieren.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- MaintenanceWindows

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste IDs der Wartungsfenster, die Sie aktivieren oder deaktivieren möchten.
- MaintenanceWindowsStatus

  Typ: Zeichenfolge

  Gültige Werte: „True“ | „False“

  Standard: „Falsch“

  Beschreibung: (Erforderlich) Legt fest, ob Wartungsfenster aktiviert oder deaktiviert sind. Geben Sie „True“ an, um Wartungsfenster zu aktivieren, und „False“, um sie zu deaktivieren.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

Dokumentschritte

- `aws:executeScript`- Erfasst den Status der Wartungsfenster, die Sie im `MaintenanceWindows` Parameter angeben, und aktiviert oder deaktiviert die Wartungsfenster.

AWS-CreateManagedLinuxInstance

Beschreibung

Erstellen Sie eine EC2-Instanz für Linux, die für Systems Manager konfiguriert ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux

Parameter

- AmiId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) AMI ID, die zum Starten der Instanz verwendet werden soll.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- GroupName

  Typ: Zeichenfolge

Standard: SSMSecurity GroupForLinuxInstances

Beschreibung: (Erforderlich) Name der Sicherheitsgruppe, die erstellt werden soll.

- HttpTokens

  Typ: Zeichenfolge

  Gültige Werte: optional | erforderlich

  Standard: optional

  Beschreibung: (Optional) IMDSv2 verwendet tokengestützte Sitzungen. Stellen Sie die Verwendung von HTTP-Token auf `optional` oder ein, um `required` zu bestimmen, ob dies optional oder IMDSv2 erforderlich ist.

- InstanceType

  Typ: Zeichenfolge

  Standard: t2.medium

  Beschreibung: (Erforderlich) Typ der zu startenden Instance. Standard ist t2.medium.

- KeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Schlüsselpaar für die Erstellung der Instance.

- RemoteAccessCidr

  Typ: Zeichenfolge

  Standard: 0.0.0.0/0

  Beschreibung: (Erforderlich) Erstellt eine Sicherheitsgruppe mit einem durch CIDR IPs angegebenen Port für SSH (Portbereich 22) (Standard ist 0.0.0.0/0). Wenn die Sicherheitsgruppe bereits vorhanden ist, wird sie nicht modifiziert, und auch die Regeln werden nicht geändert.

- RoleName

  Typ: Zeichenfolge

  Standard: SSMManaged InstanceProfileRole

Beschreibung: (Erforderlich) Zu erstellender Rollenname.

- StackName

  Typ: Zeichenfolge

  Standard: CreateManagedInstanceStack {{automation:execution_ID}}

  Beschreibung: (Optional) Geben Sie den Stack-Namen an, der von diesem Runbook verwendet wird

- SubnetId

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Erforderlich) Die neue Instance wird in diesem Subnetz oder, falls nicht angegeben, im Standard-Subnetz bereitgestellt.

- VpcId

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Erforderlich) Die neue Instance wird in dieser Amazon Virtual Private Cloud (Amazon VPC) oder in der Standard-Amazon-VPC bereitgestellt, falls nicht angegeben.

AWS-CreateManagedWindowsInstance

Beschreibung

Erstellen Sie eine EC2-Instanz für eineWindows Server, die für Systems Manager konfiguriert ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Windows

Parameter

Parameter

- AmiId

  Typ: Zeichenfolge

  Standard: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

  Beschreibung: (Erforderlich) AMI ID, die zum Starten der Instanz verwendet werden soll.
- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- GroupName

  Typ: Zeichenfolge

  Standard: SSMSecurity GroupForLinuxInstances

  Beschreibung: (Erforderlich) Name der Sicherheitsgruppe, die erstellt werden soll.
- HttpTokens

  Typ: Zeichenfolge

  Gültige Werte: optional | erforderlich

  Standard: optional

  Beschreibung: (Optional) IMDSv2 verwendet tokengestützte Sitzungen. Stellen Sie die Verwendung von HTTP-Token auf `optional` oder ein, um `required` zu bestimmen, ob dies optional oder IMDSv2 erforderlich ist.

- InstanceType

  Typ: Zeichenfolge

  Standard: t2.medium

  Beschreibung: (Erforderlich) Typ der zu startenden Instance. Standard ist t2.medium.

- KeyPairName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Schlüsselpaar für die Erstellung der Instance.

- RemoteAccessCidr

  Typ: Zeichenfolge

  Standard: 0.0.0.0/0

  Beschreibung: (Erforderlich) Erstellt eine Sicherheitsgruppe mit einem durch CIDR IPs angegebenen Port für RDP (Portbereich 3389) (Standard ist 0.0.0.0/0). Wenn die Sicherheitsgruppe bereits vorhanden ist, wird sie nicht modifiziert, und auch die Regeln werden nicht geändert.

- RoleName

  Typ: Zeichenfolge

  Standard: SSMManaged InstanceProfileRole

  Beschreibung: (Erforderlich) Zu erstellender Rollenname.

- StackName

  Typ: Zeichenfolge

  Standard: CreateManagedInstanceStack {{automation:execution_ID}}

  Beschreibung: (Optional) Geben Sie den Stack-Namen an, der von diesem Runbook verwendet wird

- SubnetId

  Typ: Zeichenfolge

Standard: Standard

Beschreibung: (Erforderlich) Die neue Instance wird in diesem Subnetz oder, falls nicht angegeben, im Standard-Subnetz bereitgestellt.

- VpcId

  Typ: Zeichenfolge

  Standard: Standard

  Beschreibung: (Erforderlich) Die neue Instance wird in dieser Amazon Virtual Private Cloud (Amazon VPC) oder in der Standard-Amazon-VPC bereitgestellt, falls nicht angegeben.

AWSConfigRemediation-EnableCWLoggingForSessionManager

Beschreibung

Das `AWSConfigRemediation-EnableCWLoggingForSessionManager` Runbook ermöglicht es AWS Systems Manager Session-Manager-Sitzungen (Session Manager), Ausgabeprotokolle in einer Amazon CloudWatch (CloudWatch) -Protokollgruppe zu speichern.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- DestinationLogGroup

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der CloudWatch Protokollgruppe.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:UpdateDocument`
- `ssm:CreateDocument`
- `ssm:UpdateDefaultDocumentVersion`
- `ssm:DescribeDocument`

Dokumentschritte

- `aws:executeScript`- Akzeptiert die CloudWatch Protokollgruppe, um das Dokument zu aktualisieren, in dem die Einstellungen für die Sitzungsausgabeprotokolle von Session Manager gespeichert sind, oder erstellt ein Dokument, falls es noch nicht vorhanden ist.

AWS-ExportOpsDataToS3

Beschreibung

Dieses Runbook ruft eine Liste von OpsData Zusammenfassungen im AWS Systems Manager Explorer ab und exportiert sie in ein Objekt in einem angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- columnFields

  Typ: StringList

  Beschreibung (erforderlich): Spaltenfelder zum Schreiben in die Ausgabedatei.
- -Filter

  Typ: Zeichenfolge

  Beschreibung: (Optional) Filter für die getOpsSummary Anfrage.
- resultAttribute

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Ergebnisattribut für die getOpsSummary Anfrage.
- s3 BucketName

  Typ: Zeichenfolge

Beschreibung (erforderlich): S3-Bucket, in den Sie die Ausgabedatei herunterladen.

- snsSuccessMessage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Nachricht, die gesendet werden soll, wenn Runbook fertig ist.

- snsTopicArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Amazon Simple Notification Service (Amazon SNS) -Thema ARN, um zu benachrichtigen, wenn der Download abgeschlossen ist.

- syncName

  Typ: Zeichenfolge

  Beschreibung (optional): der Name der Ressourcendatensynchronisierung.

Dokumentschritte

getOpsSummarySchritt — Ruft jetzt bis zu 5.000 Operationszusammenfassungen ab, um sie in eine CSV-Datei zu exportieren.

Ausgaben

OpsData Objekt — Wenn das Runbook erfolgreich ausgeführt wird, finden Sie das exportierte OpsData Objekt in Ihrem Ziel-S3-Bucket.

AWS-ExportPatchReportToS3

Beschreibung

Dieses Runbook ruft Listen mit Patch-Übersichtsdaten und Patch-Details in AWS Systems Manager Patch Manager ab und exportiert sie in CSV-Dateien in einem angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- assumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Dokument ausführt.
- s3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der S3-Bucket, in den Sie die Ausgabedatei herunterladen möchten.
- snsTopicArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Amazon Simple Notification Service (Amazon SNS) -Thema Amazon Resource Name (ARN), das benachrichtigt werden soll, wenn der Download abgeschlossen ist.
- snsSuccessMessage

  Typ: Zeichenfolge

  Beschreibung: (Optional) Text der Nachricht, die gesendet werden soll, wenn das Runbook fertig ist.
- targets

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Instanz-ID oder ein Platzhalterzeichen (*), um anzugeben, ob Patch-Daten für eine bestimmte Instance oder für alle Instances gemeldet werden sollen.

Dokumentschritte

ExportReportStep — Die Aktion für diesen Schritt hängt vom Wert des `targets` Parameters ab. Wenn `targets` es das Format von hat`instanceids=*`, ruft der Schritt bis zu 10.000 Patch-Zusammenfassungen für Instanzen in Ihrem Konto ab und exportiert die Daten in eine CSV-Datei.

Wenn `targets` das Format vorliegt`instanceids=<instance-id>`, ruft der Schritt sowohl die Patch-Zusammenfassung als auch alle Patches für die angegebene Instanz in Ihrem Konto ab und exportiert sie in eine CSV-Datei.

Ausgaben

PatchSummary/Patches-Objekt — Wenn das Runbook erfolgreich ausgeführt wird, wird das exportierte Patch-Berichtsobjekt in Ihren S3-Ziel-Bucket heruntergeladen.

`AWS-SetupInventory`

Beschreibung

Erstellen Sie eine Systems Manager Manager-Inventarzuordnung für eine oder mehrere verwaltete Instanzen. Das System erfasst Metadaten aus Ihren-Instances gemäß dem Zeitplan in der Zuordnung. Weitere Informationen finden Sie unter AWS Systems Manager Bestand.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- Anwendungen

  Typ: Zeichenfolge

Standard: Aktiviert

Beschreibung: (Optional) Erfassen von Metadaten über installierte Anwendungen.

- AssociatedDocName

  Typ: Zeichenfolge

  Standard: `AWS-GatherSoftwareInventory`

  Beschreibung: (Optional) Der Name des Runbooks, das zum Sammeln von Inventar aus der verwalteten Instanz verwendet wird.

- AssociationName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein Name für die Inventory-Zuordnung, die der Instance zugewiesen wird.

- AssocWaitTime

  Typ: Zeichenfolge

  Standard: M PT5

  Beschreibung: (Optional) Zeit, für die die Inventory-Erfassung unterbrochen werden soll, wenn die Startzeit für die Inventory-Zuordnung erreicht ist. Die Uhrzeit wird im ISO 8601-Format verwendet.

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- `AwsComponents`

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Sammeln Sie Metadaten für AWS Komponenten wie amazon-ssm-agent.

- CustomInventory

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen von benutzerdefinierten Bestandsmetadaten.

- Dateien

  Typ: Zeichenfolge

  Beschreibung: (Optional) Erfassen von Metadaten über Dateien auf Ihren Instances. Weitere Informationen zum Sammeln dieser Art von Inventardaten finden Sie unter Arbeiten mit Datei- und Windows-Registrierungsinventar. Erfordert SSMAgent Version 2.2.64.0 oder höher. Linux-Beispiel: `[{"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

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen zusätzlicher Informationen zu der Instance, einschließlich CPU-Modell, Geschwindigkeit und der Anzahl der Kerne, um nur einige zu nennen.

- InstanceIds

  Typ: Zeichenfolge

  Standard: *

  Beschreibung: (Erforderlich) EC2-Instances, die Sie inventarisieren möchten.

- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

- NetworkConfig

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen von Metadaten über Netzwerkkonfigurationen.

- OutputS3 BucketName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Name eines Amazon S3 S3-Buckets, in den Sie Inventarprotokolldaten schreiben möchten.

- OutputS3 KeyPrefix

  Typ: Zeichenfolge

  Beschreibung: (Optional) Ein Amazon S3 S3-Schlüsselpräfix (Unterordner), in das Sie Inventarprotokolldaten schreiben möchten.

- OutputS3Region

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name des Ortes AWS-Region , an dem Amazon S3 existiert.

- Plan

  Typ: Zeichenfolge

  Standard: cron(0 */30 * * * ? *)

  Beschreibung: (Optional) Ein cron-Ausdruck für den Inventory-Zuordnungplan. Der Standardwert ist alle 30 Minuten.

- Dienstleistungen

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional, nur Windows-Betriebssystem, erfordert SSMAgent Version 2.2.64.0 und höher) Sammeln Sie Daten für Servicekonfigurationen.

- WindowsRegistry

  Typ: Zeichenfolge

  Beschreibung: (Optional) Erfassen von Metadaten über Microsoft Windows Registry-Schlüssel. Weitere Informationen zum Sammeln dieser Art von Inventardaten finden Sie unter Arbeiten mit Datei- und Windows-Registrierungsinventar. Erfordert SSM Agent-Version 2.2.64.0 oder höher. Beispiel: [{"Path“ :"HKEY_CURRENT_CONFIG\ System“, "Recursive“ :true}, {"Path“ :"HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\ „," „: [“ „]}] MachineImage ValueNames AMIName

- WindowsRoles

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen von Informationen über Windows-Rollen auf der Instance. Gilt nur für Windows-Betriebssysteme. Erfordert SSMAgent Version 2.2.64.0 oder höher.

- WindowsUpdates

  Typ: Zeichenfolge

  Standard: Aktiviert

  Beschreibung: (Optional) Erfassen von Daten über alle Windows-Updates auf der Instance.

AWS-SetupManagedInstance

Beschreibung

Konfigurieren Sie eine Instanz mit einer AWS Identity and Access Management (IAM-) Rolle für den Systems Manager Manager-Zugriff.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der zu konfigurierenden EC2-Instance.

- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

- RoleName

  Typ: Zeichenfolge

  Standard: SSMRole ForManagedInstance

  Beschreibung: (Optional) Der Name der IAM-Rolle für die EC2-Instance. Wenn diese Rolle nicht vorhanden ist, wird sie erstellt. Stellen Sie bei der Angabe dieses Werts sicher, dass die Rolle die von Amazon SSMManaged InstanceCore verwaltete Richtlinie enthält.

AWS-SetupManagedRoleOnEC2Instance

Beschreibung

Konfigurieren Sie eine Instanz mit der SSMRole ForManagedInstance verwalteten IAM-Rolle für den Systems Manager Manager-Zugriff.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der zu konfigurierenden EC2-Instance.
- LambdaAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Rolle, die der von Automation erstellten Lambda-Funktion erlaubt, die Aktionen für Sie auszuführen. Wenn nicht angegeben, wird eine vorübergehende Rolle erstellt, um die Lambda-Funktion auszuführen.

- RoleName

  Typ: Zeichenfolge

  Standard: SSMRole ForManagedInstance

  Beschreibung: (Optional) Der Name der IAM-Rolle für die EC2-Instance. Wenn diese Rolle nicht vorhanden ist, wird sie erstellt. Stellen Sie bei der Angabe dieses Werts sicher, dass die Rolle die von Amazon SSMManaged InstanceCore verwaltete Richtlinie enthält.

`AWSSupport-TroubleshootManagedInstance`

Beschreibung

Mithilfe des `AWSSupport-TroubleshootManagedInstance` Runbooks können Sie ermitteln, warum eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance nicht als verwaltet von AWS Systems Manager gemeldet wird. In diesem Runbook wird die VPC-Konfiguration für die Instance überprüft, einschließlich Sicherheitsgruppenregeln, VPC-Endpoints, ACL-Regeln (Network Access Control List) und Routentabellen. Außerdem wird bestätigt, dass ein AWS Identity and Access Management (IAM-) Instanzprofil, das die erforderlichen Berechtigungen enthält, an die Instanz angehängt ist.

> **Important**
>
> Dieses Automatisierungs-Runbook bewertet IPv6 keine Regeln.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux, macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der EC2 Amazon-Instance, die nicht als von Systems Manager verwaltet gemeldet wird.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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`

Dokumentschritte

- `aws:executeScript`- Sammelt die Daten `PingStatus` der Instanz.
- `aws:branch`— Verzweigungen basieren darauf, ob die Instanz bereits meldet, dass sie von Systems Manager verwaltet wird.
- `aws:executeAwsApi`- Sammelt Details über die Instanz, einschließlich der VPC-Konfiguration.
- `aws:executeScript`— Falls zutreffend, sammelt zusätzliche Details zu VPC-Endpunkten, die für die Verwendung mit Systems Manager bereitgestellt wurden, und bestätigt, dass die mit dem VPC-Endpunkt verbundenen Sicherheitsgruppen eingehenden Datenverkehr über den TCP-Port 443 von der Instance zulassen.
- `aws:executeScript`- Überprüft, ob die Routentabelle Datenverkehr zum VPC-Endpunkt oder zu öffentlichen Systems Manager Manager-Endpunkten zulässt.
- `aws:executeScript`- Überprüft, ob die Netzwerk-ACL-Regeln Datenverkehr zum VPC-Endpunkt oder zu öffentlichen Systems Manager Manager-Endpunkten zulassen.
- `aws:executeScript`- Überprüft, ob ausgehender Datenverkehr zum VPC-Endpunkt oder zu öffentlichen Systems Manager Manager-Endpunkten von der Sicherheitsgruppe zugelassen wird, die der Instanz zugeordnet ist.
- `aws:executeScript`— Prüft, ob das mit der Instanz verknüpfte Instanzprofil eine verwaltete Richtlinie enthält, die die erforderlichen Berechtigungen bereitstellt.
- `aws:branch`— Verzweigungen, die auf dem Betriebssystem der Instanz basieren.
- `aws:executeScript`- Stellt einen Verweis auf das `ssmagent-toolkit-linux` Shell-Skript bereit.
- `aws:executeScript`- Stellt einen Verweis auf ein `ssmagent-toolkit-windows` PowerShell Skript bereit.
- `aws:executeScript`- Generiert die endgültige Ausgabe für die Automatisierung.
- `aws:executeScript`- Wenn der `PingStatus` der Instanz der Fall ist`Online`, wird zurückgegeben, dass die Instanz bereits von Systems Manager verwaltet wird.

`AWSSupport-TroubleshootPatchManagerLinux`

Beschreibung

Das `AWSSupport-TroubleshootPatchManagerLinux` Runbook behebt häufig auftretende Probleme, die zu einem Patch-Fehler auf Linux-basierten verwalteten Knoten führen können, mithilfe von Patch Manager, einem Tool in. AWS Systems Manager Das Hauptziel dieses Runbooks besteht darin, die Hauptursache des Fehlers beim Patch-Befehl zu ermitteln und einen Plan zur Behebung vorzuschlagen.

Wie funktioniert es?

Das `AWSSupport-TroubleshootPatchManagerLinux` Runbook berücksichtigt bei der Fehlerbehebung die von Ihnen angegebene ID/Command Instanz-ID des Paares. Wenn keine Befehls-ID angegeben wird, wird der letzte fehlgeschlagene Patch-Befehl innerhalb der letzten 30 Tage auf der angegebenen Instanz ausgewählt. Nach der Überprüfung des Befehlsstatus, der Erfüllung der Voraussetzungen und der Betriebssystemverteilung lädt das Runbook ein Log Analyzer-Paket herunter und führt es aus. Die Ausgabe enthält die Grundursache des Problems sowie die zur Behebung des Problems erforderlichen Maßnahmen.

Dokumenttyp

Automatisierung

Eigentümer

Amazon

Plattformen

- Amazon Linux 2 und AL2023
- Red Hat Enterprise Linux 8.X und 9.X
- Centos 8.X und 9.X
- SUSE 15.X

Parameter

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Anweisungen

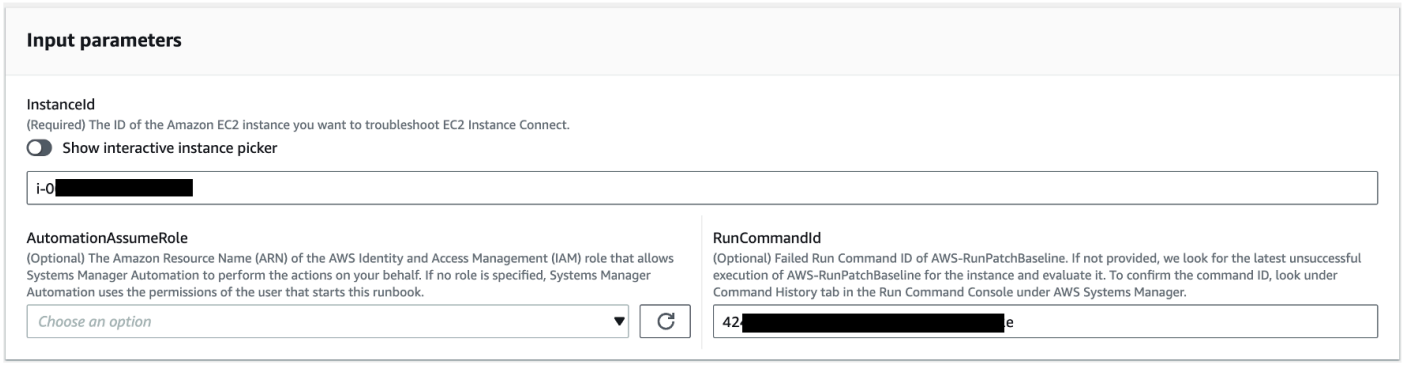
Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie `AWSSupport-TroubleshootPatchManagerLinux`in der AWS Systems Manager Konsole zum.
2. Wählen Sie Execute automation (Automatisierung ausführen).
3. Geben Sie für die Eingabeparameter Folgendes ein:
   - InstanceId (Erforderlich):

     Verwenden Sie die interaktive Instanzauswahl, um die ID des Linux-basierten SSM-verwalteten Knotens (Amazon Elastic Compute Cloud (Amazon EC2) oder Hybrid Activated Server) auszuwählen, für den der Patch-Befehl fehlgeschlagen ist, oder geben Sie die ID der SSM Managed Instance manuell ein.
   - AutomationAssumeRole (Optional):

     Geben Sie den ARN der IAM-Rolle ein, mit der Automation Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - RunCommandId (Optional):

     Geben Sie die Befehls-ID für den Fehler beim Ausführen des `AWS-RunPatchBaseline` Dokuments ein. Wenn Sie keine Befehls-ID angeben, sucht das Runbook auf der ausgewählten Instanz nach dem letzten fehlgeschlagenen Patch-Befehl innerhalb der letzten 30 Tage.



4. Wählen Sie Ausführen aus.
5. Die Automatisierung wird initiiert.
6. Das Dokument führt die folgenden Schritte aus:
   - CheckConcurrency:

     Stellt sicher, dass dieses Runbook nur einmal ausgeführt wird, das auf dieselbe Instanz abzielt. Wenn das Runbook eine weitere Ausführung feststellt, die auf dieselbe Instanz abzielt, gibt es einen Fehler zurück und wird beendet.
   - ValidateCommandID:

     Überprüft, ob die angegebene Befehls-ID als Eingabeparameter für das `AWS-RunPatchBaseline` SSM-Dokument ausgeführt wurde. Wenn keine Befehls-ID angegeben wird, berücksichtigt das Runbook die letzte fehlgeschlagene Ausführung `AWS-RunPatchBaseline` innerhalb der letzten 30 Tage auf der ausgewählten Instanz.
   - BranchOnCommandStatus:

     Bestätigt, dass der Status des angegebenen Befehls fehlgeschlagen ist. Andernfalls beendet das Runbook die Ausführung und generiert einen Bericht, der besagt, dass der angegebene Befehl erfolgreich ausgeführt wurde.
   - VerifyPrerequistes:

     Bestätigt, dass die oben genannten Voraussetzungen erfüllt sind.
   - GetPlatformDetails:

     Ruft die Distribution und Version des Betriebssystems (OS) ab.
   - GetDownloadURL:

     Ruft die Download-URL für das PatchManager Log Analyzer-Paket ab.

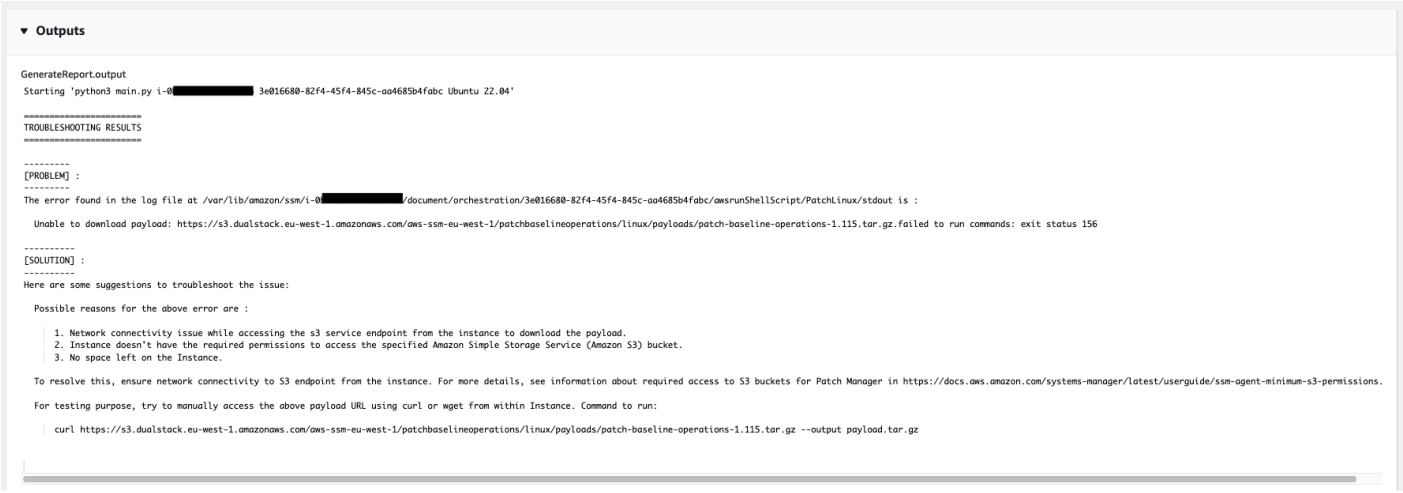
- EvaluatePatchManagerLogs:

  Lädt das PatchManager Log Analyzer-Python-Paket herunter und führt es auf der Instanz aus, um die Protokolldatei auszuwerten.

- GenerateReport:

  Generiert einen Abschlussbericht über die Ausführung des Runbooks, der das identifizierte Problem und den Lösungsvorschlag enthält.

7. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt „Ausgaben“ die detaillierten Ergebnisse der Ausführung:



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWSSupport-TroubleshootSessionManager

Beschreibung

Das `AWSSupport-TroubleshootSessionManager` Runbook hilft Ihnen bei der Behebung häufiger Probleme, die Sie daran hindern, mithilfe von Session Manager eine Verbindung zu

verwalteten Amazon Elastic Compute Cloud (Amazon EC2) -Instances herzustellen. Session Manager ist ein Tool in. AWS Systems Manager Dieses Runbook überprüft Folgendes:

- Prüft, ob die Instanz läuft und meldet, wie sie von Systems Manager verwaltet wird.
- Führt das `AWSSupport-TroubleshootManagedInstance` Runbook aus, wenn die Instanz nicht als von Systems Manager verwaltet gemeldet wird.
- Überprüft die Version des SSM-Agenten, der auf der Instanz installiert ist.
- Prüft, ob ein Instance-Profil, das eine empfohlene AWS Identity and Access Management (IAM-) Richtlinie für Session Manager enthält, an die Amazon EC2 EC2-Instance angehängt ist.
- Sammelt SSM-Agent-Protokolle von der Instance.
- Analysiert Ihre Session Manager-Einstellungen.
- Führt das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook aus, um die Konnektivität der Instance mit den Endpunkten für Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs (CloudWatch Logs) zu analysieren.

Überlegungen

- Verwaltete Hybrid-Knoten werden nicht unterstützt.
- Dieses Runbook prüft nur, ob eine empfohlene verwaltete IAM-Richtlinie an das Instanzprofil angehängt ist. Es analysiert weder IAM noch die in Ihrem AWS KMS Instanzprofil enthaltenen Berechtigungen.

> **Important**
>
> Das `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` Runbook verwendet VPC Reachability Analyzer, um die Netzwerkkonnektivität zwischen einer Quelle und einem Dienstendpunkt zu analysieren. Ihnen wird pro Analyselauf zwischen einer Quelle und einem Ziel in Rechnung gestellt. Weitere Informationen finden Sie unter Amazon VPC-Preise.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Amazon EC2 EC2-Instance, zu der Sie mit Session Manager keine Verbindung herstellen können.
- SessionPreferenceDocument

  Typ: Zeichenfolge

  Standard: SSM- SessionManagerRunShell

  Beschreibung: (Optional) Der Name Ihres Dokuments mit den Sitzungseinstellungen. Wenn Sie beim Starten von Sitzungen kein benutzerdefiniertes Dokument mit den Sitzungseinstellungen angeben, verwenden Sie den Standardwert.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

1. `aws:waitForAwsResourceProperty`: Wartet bis zu 6 Minuten, bis Ihre Ziel-Instance die Statusprüfungen bestanden hat.
2. `aws:executeScript`: Analysiert das Dokument mit den Sitzungseinstellungen.
3. `aws:executeAwsApi`: Ruft den ARN des Instanzprofils ab, das an Ihre Instance angehängt ist.
4. `aws:executeAwsApi`: Prüft, ob Ihre Instance als vom Systems Manager verwaltet gemeldet wird.
5. `aws:branch`: Verzweigungen basieren darauf, ob Ihre Instance als von Systems Manager verwaltet gemeldet wird.
6. `aws:executeScript`: Prüft, ob der auf Ihrer Instance installierte SSM-Agent Session Manager unterstützt.
7. `aws:branch`: Branches, die auf der Plattform Ihrer Instance basieren, um `ssm-cli` Logs zu sammeln.
8. `aws:runCommand`: Sammelt Logs, die `ssm-cli` von einer Linux macOS Oder-Instanz ausgegeben wurden.
9. `aws:runCommand`: Sammelt Logdateien, die `ssm-cli` von einer Windows Instanz ausgegeben wurden.
10. `aws:executeScript`: Analysiert die `ssm-cli` Protokolle.
11. `aws:executeScript`: Prüft, ob eine empfohlene IAM-Richtlinie an das Instanzprofil angehängt ist.
12. `aws:branch`: Legt fest, ob die `ssmmessages` Endpunktkonnektivität anhand von `ssm-cli` Protokollen bewertet werden soll.
13. `aws:executeAutomation`: Prüft, ob die Instanz eine Verbindung zu einem `ssmmessages` Endpunkt herstellen kann.
14. `aws:branch`: Legt anhand von `ssm-cli` Protokollen und Ihren Sitzungseinstellungen fest, ob die Amazon S3 S3-Endpunktkonnektivität bewertet werden soll.
15. `aws:executeAutomation`: Prüft, ob die Instance eine Verbindung zu einem Amazon S3 S3-Endpunkt herstellen kann.
16. `aws:branch`: Legt anhand von `ssm-cli` Protokollen und Ihren Sitzungspräferenzen fest, ob die AWS KMS Endpunktkonnektivität bewertet werden soll.
17. `aws:executeAutomation`: Prüft, ob die Instanz eine Verbindung zu einem AWS KMS Endpunkt herstellen kann.
18. `aws:branch`: Legt anhand von CloudWatch Protokollen und Ihren Sitzungseinstellungen fest, ob die Konnektivität des `ssm-cli` Logs-Endpunkts bewertet werden soll.

19. `aws:executeAutomation`: Prüft, ob die Instance eine Verbindung zu einem CloudWatch Logs-Endpunkt herstellen kann.
20. `aws:executeAutomation`: Führt das `AWSSupport-TroubleshootManagedInstance` Runbook aus.
21. `aws:executeScript`: Kompiliert die Ausgabe der vorherigen Schritte und gibt einen Bericht aus.

Gibt aus

- `generateReport.EvalReport`- Die Ergebnisse der vom Runbook durchgeführten Prüfungen im Klartext.

Drittanbieter

AWS Systems Manager Automation stellt vordefinierte Runbooks für Produkte und Dienste von Drittanbietern bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-CreateJiraIssue
- AWS-CreateServiceNowIncident
- AWS-RunPacker

`AWS-CreateJiraIssue`

Beschreibung

Erstellen Sie ein Problem in Jira.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AssigneeName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Benutzername der Person, der das Problem zugewiesen werden soll.
- DueDate

  Typ: Zeichenfolge

  Beschreibung: (Optional) Das Fälligkeitsdatum für das Problem im yyyy-mm-dd Format.
- IssueDescription

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine detaillierte Beschreibung des Problems.
- IssueSummary

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine kurze Zusammenfassung des Problems.
- IssueTypeName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Problemtyps, den Sie erstellen möchten (z. B. Aufgabe, Unteraufgabe, Fehler usw.).
- JiraURL

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die URL der Jira-Instance.
- JiraUsername

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Name des Benutzers, der das Problem erstellt.

- PriorityName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der Priorität des Problems.

- ProjectKey

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Schlüssel des Projekts, in dem das Problem erstellt wird.

- SSMParameterName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name eines verschlüsselten SSM-Parameter mit dem API-Schlüssel oder Passwort des Jira-Benutzers.

Dokumentschritte

`aws:createStack`- Erstellen Sie einen CloudFormation Stack, um eine Lambda-IAM-Rolle und -Funktion zu erstellen.

`aws:invokeLambdaFunction`- Rufen Sie die Lambda-Funktion auf, um das Jira-Problem zu erstellen

`aws:deleteStack`- Löscht den erstellten Stack CloudFormation .

Ausgaben

IssueId: ID des neu erstellten Jira-Problems

AWS-CreateServiceNowIncident

Beschreibung

Erstellen Sie einen Vorfall in der ServiceNow Incident-Tabelle.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Kategorie

  Typ: Zeichenfolge

  Beschreibung (optional): Die Kategorie des Vorfalls.

  Gültige Werte: Keine | Inquiry/Help | Software | Hardware | Netzwerk | Datenbank

  Standardwert: Keine
- Description

  Typ: Zeichenfolge

  Beschreibung (erforderlich): Eine detaillierte Erklärung zum Vorfall.
- Auswirkung

  Typ: Zeichenfolge

  Beschreibung (optional): Die Auswirkungen, die ein Vorfall auf das Geschäft hat.

Gültige Werte: Hoch | Mittel | Niedrig

Standardwert: Niedrig

- ServiceNowInstanceUsername

  Typ: Zeichenfolge

  Beschreibung (erforderlich): Der Name des Benutzers, der den Vorfall erstellt.

- ServiceNowInstancePassword

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name eines verschlüsselten SSM-Parameters, der das Passwort für den ServiceNow Benutzer enthält.

- ServiceNowInstanceURL

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die URL der ServiceNow Instanz

- ShortDescription

  Typ: Zeichenfolge

  Beschreibung (erforderlich): Eine kurze Beschreibung des Vorfalls.

- Unterkategorie

  Typ: Zeichenfolge

  Beschreibung (optional): Die Unterkategorie des Vorfalls.

  Gültige Werte: Keine | Antivirus | E-Mail | Interne Anwendung | Betriebssystem | CPU | Festplatte | Tastatur | Hardware | Speicher | Monitor | Maus | DHCP | DNS | IP-Adresse | VPN | Wireless | DB2 | MS SQL Server | Oracle

  Standardwert: Keine

Dokumentschritte

Push_Incident — Leitet die Informationen zum Vorfall an weiter. ServiceNow

Ausgaben

push_incident.IncidentId — Die erstellte Incident-ID.

AWS-RunPacker

Beschreibung

Dieses Runbook verwendet das HashiCorp Packer-Tool, um Packer-Vorlagen zu validieren, zu korrigieren oder zu erstellen, die zur Erstellung von Maschinenimages verwendet werden. Dieses Runbook verwendet Packer v1.7.2.

> **Note**
>
> Wenn Sie einen `vpc_id`-Wert angeben, müssen Sie auch den `subnet_id`-Wert eines öffentlichen Subnetzes angeben. Sofern Sie das IPv4 öffentliche Adressierungsattribut Ihres Subnetzes nicht ändern, müssen Sie es auch auf true setzen. `associate_public_ip_address`

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Force

  Typ: Boolescher Wert

  Beschreibung: Eine Packer-Option, mit der ein Builder ausgeführt wird, wenn Artefakte aus einem vorherigen Build ansonsten verhindern, dass ein Build ausgeführt wird.

- Mode

  Typ: Zeichenfolge

  Beschreibung: Der Modus oder der Befehl, in dem Packer bei der Validierung anhand der Vorlage verwendet werden soll. Zu den Optionen gehören `BuildValidate`, und`Fix`.

- TemplateFileName

  Typ: Zeichenfolge

  Beschreibung: der Name oder der Schlüssel der Vorlagendatei im S3-Bucket.

- Vorlagen 3 BucketName

  Typ: Zeichenfolge

  Beschreibung: der Name des S3-Buckets, der die Packer-Vorlage enthält.

Dokumentschritte

RunPackerProcessTemplate — Führt den ausgewählten Modus mit dem Packer-Tool anhand der Vorlage aus.

Ausgaben

RunPackerProcessTemplate.output — Die Standardausgabe aus dem Packer-Tool.

RunPackerProcessTemplate.fixed_template_key — Der Name der Vorlage, die in einem S3-Bucket gespeichert ist und nur verwendet werden soll, wenn sie im „Fix“ -Modus ausgeführt wird.

RunPackerProcessTemplate.s3_bucket — Der Name des S3-Buckets, der die feste Vorlage enthält, die nur verwendet werden soll, wenn sie im „Fix“ -Modus ausgeführt wird.

Amazon VPC

AWS Systems Manager Automation bietet vordefinierte Runbooks für Amazon Virtual Private Cloud. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- 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

Beschreibung

Dieses Runbook entfernt alle Eingangs- und Ausgangsregeln aus der von Ihnen angegebenen Sicherheitsgruppe.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- SecurityGroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, die Sie schließen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Dokumentschritte

- `aws:executeScript`- Entfernt alle Eingangs- und Ausgangsregeln aus der Sicherheitsgruppe, die Sie im Parameter angeben. `SecurityGroupId`

AWSSupport-ConfigureDNSQueryLogging

Beschreibung

Das `AWSSupport-ConfigureDNSQueryLogging` Runbook konfiguriert die Protokollierung für DNS-Abfragen, die ihren Ursprung in Ihrer Virtual Private Cloud (VPC) haben, oder für gehostete Zonen von Amazon Route 53. Sie können wählen, ob Sie Abfrageprotokolle in Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3) oder Amazon Data Firehose veröffentlichen möchten. Weitere Informationen zur Abfrageprotokollierung und Resolver-Abfrageprotokollierung finden Sie unter Öffentliche DNS-Abfrageprotokollierung und Resolver-Abfrageprotokollierung.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- LogDestinationArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der CloudWatch Logs-Gruppe, des Amazon S3 S3-Buckets oder des Firehose-Streams, an den Sie Abfrageprotokolle senden möchten. Beachten Sie, dass die öffentliche DNS-Abfrageprotokollierung von Route 53 nur CloudWatch Logs-Gruppen unterstützt. Wenn Sie keinen Wert für diesen Parameter angeben, erstellt die Automatisierung eine CloudWatch Logs-Gruppe mit dem Format `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID }` und einer IAM-Ressourcenrichtlinie zur Veröffentlichung der Abfrageprotokolle. Die durch die Automatisierung erstellte CloudWatch Protokollgruppe hat eine Aufbewahrungsfrist von 14 Tagen.

- QueryLogType

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Arten von Abfragen, die Sie protokollieren möchten.

  Gültige Werte: Public | Resolver/Private

  Standard: Öffentlich

- ResourceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Ressource, deren Abfragen Sie protokollieren möchten. Wenn Sie `Public` für den `QueryLogType` Parameter angeben, muss es sich bei der Ressource um die ID einer privaten gehosteten Route 53-Zone handeln. Wenn Sie `Resolver/Private` für den `QueryLogType` Parameter angeben, muss die Ressource die ID einer VPC sein.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Dokumentschritte

- aws:executeScript- Überprüft, ob die Ressource, die Sie für den ResourceId Parameter angeben, vorhanden ist, und prüft, ob der Ressourcentyp der erforderlichen QueryLogType Option entspricht.
- aws:executeScript- Überprüft, ob der Wert, den Sie für den LogDestinationArn Parameter angeben, dem erforderlichen Wert entspricht. QueryLogType
- aws:executeScript- Überprüft die erforderlichen Berechtigungen für Route 53, um Protokolle in der Protokollgruppe CloudWatch Logs zu veröffentlichen, und erstellt die erforderliche IAM-Ressourcenrichtlinie, falls diese nicht vorhanden ist.
- aws:executeScript- Aktiviert die DNS-Abfrageprotokollierung am ausgewählten Ziel.

AWSSupport-ConfigureTrafficMirroring

Beschreibung

Das AWSSupport-ConfigureTrafficMirroring Runbook konfiguriert die Verkehrsspiegelung, um Ihnen bei der Behebung von Verbindungsproblemen zwischen einem Load Balancer und Amazon Elastic Compute Cloud (Amazon EC2) -Instances zu helfen. Die Verkehrsspiegelung kopiert eingehenden und ausgehenden Datenverkehr von den Netzwerkschnittstellen, die mit Ihren Instances verbunden sind. Um die Verkehrsspiegelung zu konfigurieren, erstellt dieses Runbook die erforderlichen Ziele, Filter und Sitzungen. Standardmäßig konfiguriert das Runbook die Spiegelung für den gesamten eingehenden und ausgehenden Datenverkehr für alle Protokolle außer Amazon DNS. Wenn Sie den Datenverkehr von bestimmten Quellen und Zielen spiegeln möchten, können Sie

die Regeln für eingehenden und ausgehenden Datenverkehr nach Abschluss der Automatisierung ändern.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- Quelle: ENI

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die elastic network interface, für die Sie die Verkehrsspiegelung konfigurieren möchten.
- Target

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Das Ziel für den gespiegelten Datenverkehr. Sie müssen die ID einer Netzwerkschnittstelle, eines Network Load Balancer oder eines Gateway Load Balancer-Endpunkts angeben. Wenn Sie einen Network Load Balancer angeben, müssen UDP-Listener auf Port 4789 vorhanden sein.
- SessionNumber

Typ: Zeichenfolge

Gültige Werte: 1-32766

Beschreibung: (Erforderlich) Die Nummer der Spiegelsitzung, die Sie verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:CreateTrafficMirrorTarget`
- `ec2:CreateTrafficMirrorFilter`
- `ec2:CreateTrafficMirrorFilterRule`
- `ec2:CreateTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorFilter`
- `ec2:DeleteTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorFilterRule`
- `iam:ListRoles`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`

Dokumentschritte

- `aws:executeScript`- Führt ein Skript aus, um ein Ziel zu erstellen.
- `aws:executeAwsApi`- Erstellt eine Filterregel.
- `aws:executeAwsApi`- Erstellt eine Spiegelfilterregel für den gesamten eingehenden Datenverkehr.
- `aws:executeAwsApi`- Erstellt eine Spiegelfilterregel für den gesamten ausgehenden Datenverkehr.
- `aws:executeAwsApi`- Erstellt eine Traffic Mirror-Sitzung.
- `aws:executeAwsApi`- Löscht den Filter, wenn die Erstellung des Filters oder der Sitzung fehlschlägt.

- `aws:executeAwsApi`- Löscht das Ziel, wenn die Filter- oder Sitzungserstellung fehlschlägt.

Ausgaben

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget. Ziel IDOutput

AWSSupport-ConnectivityTroubleshooter

Beschreibung

Das `AWSSupport-ConnectivityTroubleshooter` Runbook diagnostiziert Verbindungsprobleme zwischen den folgenden Komponenten:

- AWS Ressourcen innerhalb einer Amazon Virtual Private Cloud (Amazon VPC)
- AWS Ressourcen in verschiedenen Amazon VPCs innerhalb desselben AWS-Region , die über VPC-Peering verbunden sind
- AWS Ressourcen in einer Amazon VPC und eine Internetressource, die ein Internet-Gateway verwendet
- AWS Ressourcen in einer Amazon VPC und eine Internetressource, die ein NAT-Gateway (Network Address Translation) verwendet

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Ziel-IP

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die IPv4 Adresse der Ressource, zu der Sie eine Verbindung herstellen möchten.

- DestinationPort

  Typ: Zeichenfolge

  Standard: true

  Beschreibung: (Erforderlich) Die Portnummer, zu der Sie eine Verbindung auf der Zielressource herstellen möchten.

- DestinationVpc

  Typ: Zeichenfolge

  Standard: Alle

  Beschreibung: (Optional) Die ID der Amazon VPC, mit der Sie die Konnektivität testen möchten.

- SourceIP

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die private IPv4 Adresse der AWS Ressource in Ihrer Amazon VPC, von der aus Sie die Konnektivität testen möchten.

- SourcePortRange

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Portbereich, der von der AWS Ressource in Ihrer Amazon VPC verwendet wird, von der aus Sie die Konnektivität testen möchten.

- SourceVpc

  Typ: Zeichenfolge

  Standard: Alle

  Beschreibung: (Optional) Die ID der Amazon VPC, von der aus Sie die Konnektivität testen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcPeeringConnections`

Dokumentschritte

- `aws:executeScript`- Sammelt Details zu der AWS Ressource, die Sie im `SourceIP` Parameter angeben.
- `aws:executeScript`- Ermittelt das Ziel des Netzwerkverkehrs von der AWS Ressource anhand der im vorherigen Schritt gesammelten Routen.
- `aws:branch`- Verzweigungen auf der Grundlage des Ziels des Netzwerkverkehrs.
- `aws:executeAwsApi`- Sammelt Details über die Zielressource.
- `aws:executeScript`— Bestätigt, dass die für die Amazon-Ziel-VPC zurückgegebene ID mit dem im `DestinationVpc` Parameter angegebenen Wert übereinstimmt, falls vorhanden.
- `aws:executeAwsApi`- Sammelt die Sicherheitsgruppenregeln für die Quell- und Zielressourcen.

- `aws:executeScript`- Bestätigt, ob die Sicherheitsgruppenregeln den erforderlichen Verkehr zwischen den Quell- und Zielressourcen zulassen.
- `aws:executeAwsApi`- Sammelt die Netzwerkzugriffskontrolllisten (NACLs), die den Subnetzen für die Quell- und Zielressourcen zugeordnet sind.
- `aws:executeScript`- Bestätigt, ob der benötigte Verkehr zwischen den Quell- und Zielressourcen NACLs zugelassen ist.
- `aws:executeScript`- Bestätigt, ob der Quelle eine öffentliche IP-Adresse zugeordnet ist, wenn das Routenziel ein Internet-Gateway ist.
- `aws:executeAwsApi`- Sammelt die Sicherheitsgruppenregeln für die Quellressource.
- `aws:executeScript`- Bestätigt, ob die Sicherheitsgruppenregeln den erforderlichen Verkehr von der Quell- zur Zielressource zulassen.
- `aws:executeAwsApi`- Sammelt die mit dem Subnetz NACLs verknüpften Daten für die Quellressource.
- `aws:executeScript`- Bestätigt, ob der benötigte Verkehr von der Quellressource NACLs zugelassen wird.
- `aws:executeAwsApi`- Sammelt Details über das NAT-Gateway.
- `aws:executeAwsApi`- Sammelt die mit dem Subnetz für das NAT-Gateway NACLs verknüpften Daten.
- `aws:executeScript`- Bestätigt, ob der benötigte Verkehr aus dem Subnetz für das NAT-Gateway NACLs zugelassen ist.
- `aws:executeScript`- Sammelt die Routen, die dem Subnetz für das NAT-Gateway zugeordnet sind.
- `aws:executeScript`- Bestätigt, ob das NAT-Gateway eine Route zu einem Internet-Gateway hat.
- `aws:executeAwsApi`- Sammelt Details über die VPC-Peering-Verbindung.
- `aws:executeScript`- Bestätigt, dass VPCs sich beide in derselben Region befinden und dass die für die Ziel-VPC zurückgegebene ID mit dem im `DestinationVpc` Parameter angegebenen Wert übereinstimmt, falls vorhanden.
- `aws:executeAwsApi`- Gibt das Subnetz der Zielressource zurück.
- `aws:executeScript`- Sammelt die Routen, die dem Subnetz für die Peering-VPC zugeordnet sind.
- `aws:executeScript`— Bestätigt, ob die Peering-VPC über eine Route zur Peering-Verbindung verfügt.

- `aws:executeScript`- Bestätigt, ob Datenverkehr von der Quellressource zulässig ist, wenn das Ziel von der Automatisierung nicht unterstützt wird.

AWSSupport-TroubleshootVPN

Beschreibung

Das `AWSSupport-TroubleshootVPN` Runbook hilft Ihnen dabei, Fehler in einer AWS Site-to-Site VPN Verbindung zu verfolgen und zu beheben. Die Automatisierung umfasst mehrere automatisierte Prüfungen, mit denen `IKEv2` Fehler im Zusammenhang mit AWS Site-to-Site VPN Verbindungstunneln `IKEv1` aufgespürt werden können. Die Automatisierung versucht, bestimmte Fehler und die entsprechende Lösung in einer Liste häufig auftretender Probleme zusammenzufassen.

Hinweis: Diese Automatisierung behebt die Fehler nicht. Sie läuft für den genannten Zeitraum und durchsucht die Protokollgruppe auf Fehler in der CloudWatch VPN-Protokollgruppe.

Wie funktioniert es?

Das Runbook führt eine Parametervalidierung durch, um zu bestätigen, ob die im Eingabeparameter enthaltene CloudWatch Amazon-Protokollgruppe existiert, ob die Protokollgruppe Protokollstreams enthält, die der VPN-Tunnelprotokollierung entsprechen, ob die VPN-Verbindungs-ID vorhanden ist und ob die Tunnel-IP-Adresse existiert. Es führt Logs Insights-API-Aufrufe für Ihre CloudWatch Protokollgruppe durch, die für die VPN-Protokollierung konfiguriert sind.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- LogGroupName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der CloudWatch Amazon-Protokollgruppe, der für die AWS Site-to-Site VPN Verbindungsprotokollierung konfiguriert ist

  Zulässiges Muster: `^[\.\-_/#A-Za-z0-9]{1,512}`

- VpnConnectionId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die AWS Site-to-Site VPN Verbindungs-ID, für die eine Fehlerbehebung durchgeführt werden soll.

  Zulässiges Muster: `^vpn-[0-9a-f]{8,17}$`

- Tunnel AIPAddress

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die IPv4 Adresse des Tunnels Nummer 1, die mit Ihrer verknüpft ist AWS Site-to-Site VPN.

  Zulässiges Muster: `^((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}$`

- Tunnel BIPAddress

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die IPv4 Adresse des Tunnels Nummer 2, die mit Ihrer verknüpft ist AWS Site-to-Site VPN.

  Zulässiges Muster: `^((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

Typ: Zeichenfolge

Beschreibung: (Erforderlich) Wählen Sie aus, welche IKE-Version Sie verwenden. Zulässige Werte: IKEv1, IKEv2

Zulässige Werte: `['IKEv1', 'IKEv2']`

- StartTimeinEpoch

  Typ: Zeichenfolge

  Beschreibung: (Optional) Startzeit für die Protokollanalyse. Sie können entweder StartTimeinEpoch/EndTimeinEpoch oder LookBackPeriod für die Protokollanalyse verwenden

  Zulässiges Muster: `^\d{10}|^$`

- EndTimeinEpoch

  Typ: Zeichenfolge

  Beschreibung: (Optional) Endzeit für die Protokollanalyse. Sie können entweder StartTimeinEpoch/EndTimeinEpoch oder LookBackPeriod für die Protokollanalyse verwenden. Wenn beides StartTimeinEpoch/EndTimeinEpoch und LookBackPeriod dann angegeben ist, hat LookBackPeriod es Vorrang

  Zulässiges Muster: `^\d{10}|^$`

- LookBackPeriod

  Typ: Zeichenfolge

  Beschreibung: (Optional) Zweistellige Zeitangabe in Stunden für die Rückschau zur Protokollanalyse. Gültiger Bereich: 01 — 99. Dieser Wert hat Vorrang, wenn Sie auch und angeben StartTimeinEpoch EndTime

  Zulässiges Muster: `^(\d?[1-9]|[1-9]0)|^$`

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`
- `ec2:DescribeVpnConnections`

Anweisungen

Hinweis: Diese Automatisierung funktioniert für die CloudWatch Protokollgruppen, die für Ihre VPN-Tunnelprotokollierung konfiguriert sind, wenn das Ausgabeformat für die Protokollierung JSON ist.

Gehen Sie wie folgt vor, um die Automatisierung zu konfigurieren:

1. Navigieren Sie AWSSupport-TroubleshootVPNin der AWS Systems Manager Konsole zum.
2. Geben Sie für die Eingabeparameter Folgendes ein:
   - AutomationAssumeRole (Fakultativ):

     Der Amazon-Ressourcenname (ARN) der Rolle AWS Identity and Access Management (IAM), der es Systems Manager Automation ermöglicht, die Aktionen in Ihrem Namen durchzuführen. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
   - LogGroupName (Erforderlich):

     Der Name der CloudWatch Amazon-Protokollgruppe, der überprüft werden soll. Dies muss die CloudWatch Protokollgruppe sein, an die VPN konfiguriert ist, um Protokolle zu senden.
   - VpnConnectionId (Erforderlich):

     Die AWS Site-to-Site VPN Verbindungs-ID, deren Protokollgruppe auf VPN-Fehler überprüft wird.
   - Tunnel AIPAddress (erforderlich):

     Die Tunnel-A-IP-Adresse, die Ihrer AWS Site-to-Site VPN Verbindung zugeordnet ist.
   - Tunnel BIPAddress (optional):

     Die IP-Adresse von Tunnel B, die Ihrer AWS Site-to-Site VPN Verbindung zugeordnet ist.
   - IKEVersion (Erforderlich):

Wählen Sie aus IKEversion , was Sie verwenden. Zulässige Werte: IKEv1, IKEv2.

- StartTimeinEpoch (Fakultativ):

  Der Beginn des Zeitbereichs, für den ein Fehler abgefragt werden soll. Der Bereich ist inklusiv, sodass die angegebene Startzeit in der Abfrage enthalten ist. Wird als Epochenzeit angegeben, die Anzahl der Sekunden seit dem 1. Januar 1970, 00:00:00 UTC.

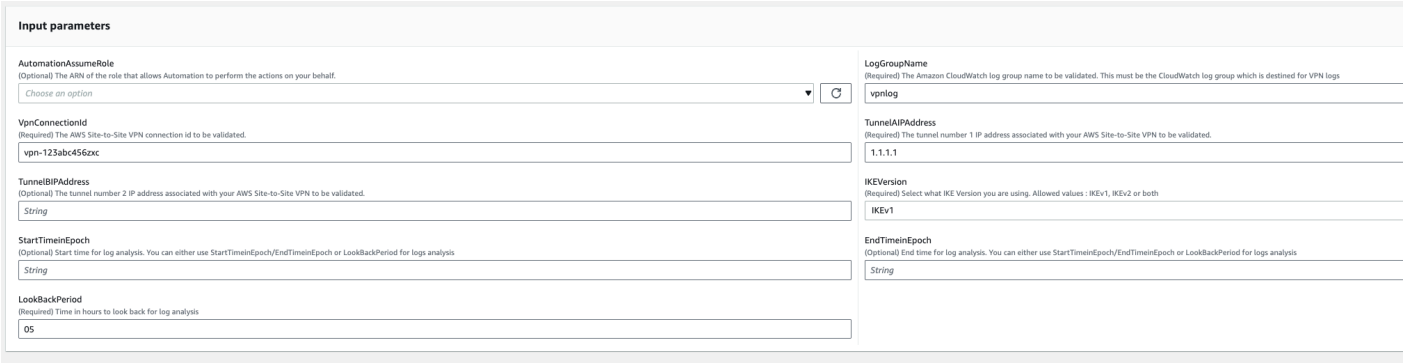
- EndTimeinEpoch (Fakultativ):

  Das Ende des Zeitraums, in dem nach Fehlern abgefragt werden soll. Der Bereich ist inklusiv, sodass die angegebene Endzeit in der Abfrage enthalten ist. Wird als Epochenzeit angegeben, die Anzahl der Sekunden seit dem 1. Januar 1970, 00:00:00 UTC.

- LookBackPeriod (Erforderlich):

  Zeit in Stunden, bis die Abfrage auf Fehler zurückblickt.

Hinweis: Konfigurieren Sie ein StartTimeinEpoch EndTimeinEpoch, oder, LookBackPeriod um den Zeitraum für die Protokollanalyse festzulegen. Geben Sie eine zweistellige Zahl in Stunden ein, um ab der Startzeit der Automatisierung nach Fehlern in der Vergangenheit zu suchen. Oder, wenn der Fehler innerhalb eines bestimmten Zeitraums in der Vergangenheit liegt, geben Sie statt von StartTimeinEpoch LookBackPeriod und EndTimeinEpoch an.



3. Wählen Sie Ausführen aus.
4. Die Automatisierung wird eingeleitet.
5. Das Automatisierungs-Runbook führt die folgenden Schritte aus:

   - Parametervalidierung:

     Führt eine Reihe von Validierungen für Eingabeparameter aus, die in der Automatisierung enthalten sind.

   - branchOnValidationOfLogGroup:

Prüft, ob die im Parameter angegebene Protokollgruppe gültig ist. Falls ungültig, wird die weitere Initiierung von Automatisierungsschritten gestoppt.

- branchOnValidationOfLogStream:

  Prüft, ob in der enthaltenen Protokollgruppe ein CloudWatch Protokollstream vorhanden ist. Falls ungültig, wird die weitere Initiierung von Automatisierungsschritten gestoppt.

- branchOnValidationOfVpnConnectionId:

  Überprüft, ob die im Parameter enthaltene VPN-Verbindungs-ID gültig ist. Falls ungültig, wird die weitere Initiierung von Automatisierungsschritten gestoppt.

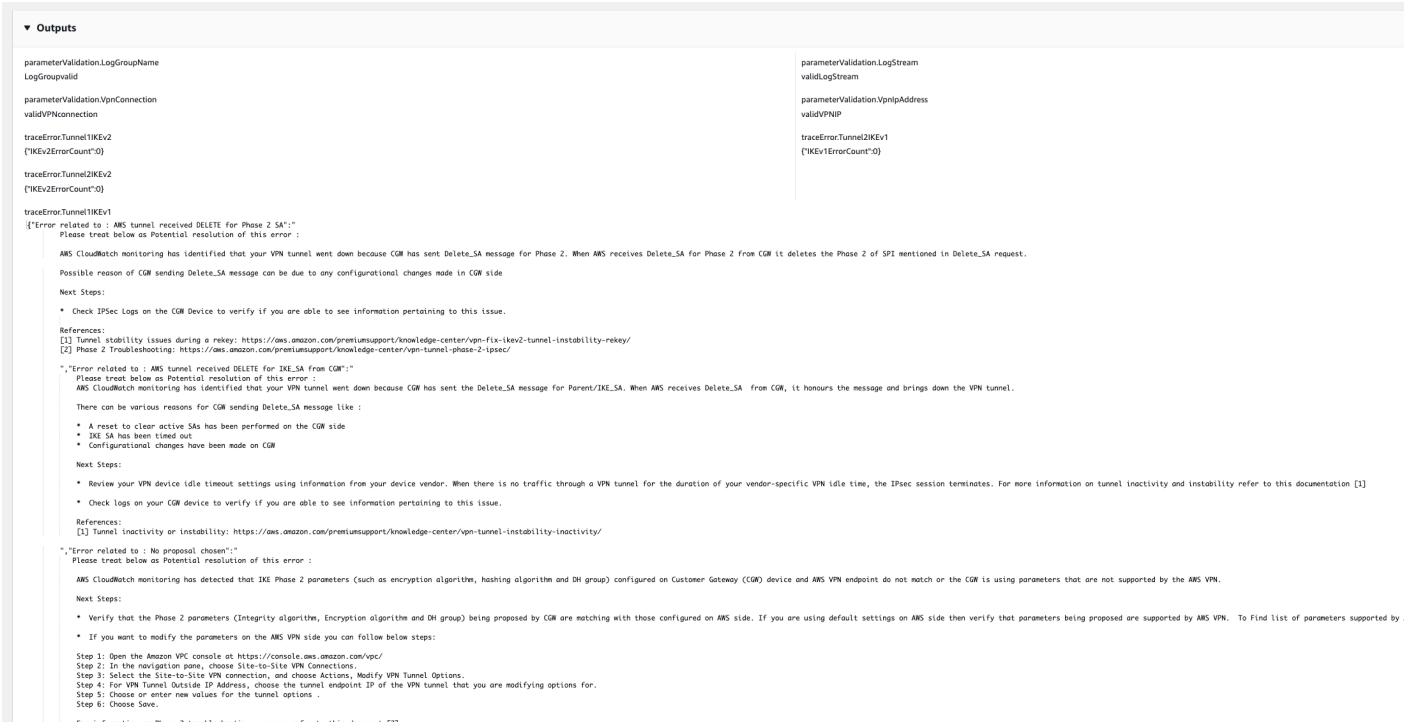
- branchOnValidationOfVpnIp:

  Prüft, ob die im Parameter angegebene Tunnel-IP-Adresse gültig ist oder nicht. Falls ungültig, wird die weitere Ausführung von Automatisierungsschritten gestoppt.

- TraceError:

  Führt einen Logs-Insight-API-Aufruf in Ihrer enthaltenen CloudWatch Protokollgruppe durch und sucht nach dem Fehler im Zusammenhang mit IKEv1/IKEv2 zusammen mit einem entsprechenden Lösungsvorschlag.

6. Wenn der Vorgang abgeschlossen ist, finden Sie im Abschnitt Ausgaben die detaillierten Ergebnisse der Ausführung.



Referenzen

Systems Manager Automation

- Führen Sie diese Automatisierung aus (Konsole)
- Führen Sie eine Automatisierung aus
- Eine Automatisierung einrichten
- Landingpage für Support-Automatisierungsworkflows

AWS Servicedokumentation

- Inhalt der Site-to-Site VPN-Protokolle

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Beschreibung

Das `AWSConfigRemediation-DeleteEgressOnlyInternetGateway` Runbook löscht das von Ihnen angegebene Internet-Gateway nur für ausgehenden Datenverkehr.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- EgressOnlyInternetGatewayId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Internet-Gateways für ausgehenden Datenverkehr, das Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteEgressOnlyInternetGateway`
- `ec2:DescribeEgressOnlyInternetGateways`

Dokumentschritte

- `aws:executeScript`- Löscht das im Parameter angegebene Internet-Gateway, das nur für ausgehenden Datenverkehr bestimmt ist. `EgressOnlyInternetGatewayId`
- `aws:executeScript`- Überprüft, ob das Internet-Gateway für ausgehenden Datenverkehr gelöscht wurde.

AWSConfigRemediation-DeleteUnusedENI

Beschreibung

Das `AWSConfigRemediation-DeleteUnusedENI` Runbook löscht ein elastic network interface (ENI) mit dem Anhangsstatus. `detached`

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- NetworkInterfaceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der ENI, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

Dokumentschritte

- `aws:executeAwsApi`- Löscht die ENI, die Sie im `NetworkInterfaceId` Parameter angeben.
- `aws:executeScript`- Überprüft, ob die ENI gelöscht wurde.

AWSConfigRemediation-DeleteUnusedSecurityGroup

Beschreibung

Das `AWSConfigRemediation-DeleteUnusedSecurityGroup` Runbook löscht die Sicherheitsgruppe, die Sie im `GroupId` Parameter angeben. Wenn Sie versuchen, eine Sicherheitsgruppe zu löschen, die mit einer Amazon Elastic Compute Cloud (Amazon EC2) -Instance verknüpft ist oder auf die von einer anderen Sicherheitsgruppe verwiesen wird, schlägt die Automatisierung fehl. Diese Automatisierung löscht keine Standardsicherheitsgruppe.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- GroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

Dokumentschritte

- `aws:executeAwsApi`- Gibt den Namen der Sicherheitsgruppe unter Verwendung des Werts zurück, den Sie im `GroupId` Parameter angeben.
- `aws:branch`- Bestätigt, dass der Gruppenname nicht „Standard“ ist.
- `aws:executeAwsApi`- Löscht die im `GroupId` Parameter angegebene Sicherheitsgruppe.
- `aws:executeScript`- Bestätigt, dass die Sicherheitsgruppe gelöscht wurde.

`AWSConfigRemediation-DeleteUnusedVPCNetworkACL`

Beschreibung

Das `AWSConfigRemediation-DeleteUnusedVPCNetworkACL` Runbook löscht eine Network Access Control List (ACL), die keinem Subnetz zugeordnet ist.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- NetworkAclId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Netzwerk-ACL, die Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

Dokumentschritte

- `aws:executeAwsApi`- Löscht die im Parameter angegebene Netzwerk-ACL. `NetworkAclId`
- `aws:executeScript`- Bestätigt, dass die im `NetworkAclId` Parameter angegebene Netzwerk-ACL gelöscht wurde.

`AWSConfigRemediation-DeleteVPCFlowLog`

Beschreibung

Das `AWSConfigRemediation-DeleteVPCFlowLog` Runbook löscht das von Ihnen angegebene VPC-Flow-Protokoll (Virtual Private Cloud).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- FlowLogId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Flow-Protokolls, das Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Dokumentschritte

- `aws:executeAwsApi`- Löscht das Flow-Protokoll, das Sie im `FlowLogId` Parameter angeben.

- `aws:executeScript`- Überprüft, ob das Flow-Protokoll gelöscht wurde.

AWSConfigRemediation-DetachAndDeleteInternetGateway

Beschreibung

Das `AWSConfigRemediation-DetachAndDeleteInternetGateway` Runbook trennt und löscht das von Ihnen angegebene Internet-Gateway. Wenn Amazon EC2 EC2-Instances in Ihrer Virtual Private Cloud (VPC) elastische IP-Adressen oder öffentliche IPv4 Adressen zugeordnet sind, schlägt das Runbook fehl.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- InternetGatewayId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Internet-Gateways, das Sie löschen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

Dokumentschritte

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Statuseigenschaft des virtuellen privaten Gateways ändert `available` oder das Zeitlimit überschritten wird.
- `aws:executeAwsApi`— Ruft eine angegebene Virtual Private Gateway-Konfiguration ab.
- `aws:branch`- Verzweigt auf der Grundlage des VpcAttachments Parameterwerts .state.

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Eigenschaft VpcAttachments .state des virtuellen privaten Gateways ändert `attached` oder das Zeitlimit überschritten wird.
- `aws:executeAwsApi`- Akzeptiert die ID des Virtual Private Gateways und die ID der Amazon VPC als Eingabe und trennt das Virtual Private Gateway von der Amazon VPC.
- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Eigenschaft VpcAttachments .state des virtuellen privaten Gateways ändert oder das Zeitlimit überschritten wird. `detached`

- `aws:executeAwsApi`- Akzeptiert die ID des virtuellen privaten Gateways als Eingabe und löscht sie.

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des Virtual Private Gateways als Eingabe und verifiziert deren Löschung.

`aws:executeAwsApi`- Erfasst die VPC-ID aus der Internet-Gateway-ID.

- `aws:executeAwsApi`- Trennt die Internet-Gateway-ID von der VPC.

- `aws:executeAwsApi`- Löscht das Internet-Gateway.

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

Beschreibung

Das `AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` Runbook trennt und löscht ein bestimmtes virtuelles privates Gateway von Amazon Elastic Compute Cloud (Amazon EC2), das an eine mit Amazon Virtual Private Cloud (Amazon VPC) erstellte Virtual Private Cloud (VPC) angehängt ist.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- VpnGatewayId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des virtuellen privaten Gateways, das gelöscht werden soll.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteVpnGateway`
- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

Dokumentschritte

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Statuseigenschaft des virtuellen privaten Gateways ändert `available` oder das Zeitlimit überschritten wird.
- `aws:executeAwsApi`— Ruft eine angegebene Virtual Private Gateway-Konfiguration ab.
- `aws:branch`- Verzweigt auf der Grundlage des VpcAttachments Parameterwerts .state.

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Eigenschaft VpcAttachments .state des virtuellen privaten Gateways ändert `attached` oder das Zeitlimit überschritten wird.
- `aws:executeAwsApi`- Akzeptiert die ID des Virtual Private Gateways und die ID der Amazon VPC als Eingabe und trennt das Virtual Private Gateway von der Amazon VPC.
- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des virtuellen privaten Gateways und wartet, bis sich die Eigenschaft VpcAttachments .state des virtuellen privaten Gateways ändert oder das Zeitlimit überschritten wird. `detached`

- `aws:executeAwsApi`- Akzeptiert die ID des virtuellen privaten Gateways als Eingabe und löscht sie.

- `aws:waitForAwsResourceProperty`- Akzeptiert die ID des Virtual Private Gateways als Eingabe und verifiziert deren Löschung.

AWS-DisableIncomingSSHOnPort22

Beschreibung

Das AWS-DisableIncomingSSHOnPort22 Runbook entfernt Regeln, die uneingeschränkten eingehenden SSH-Verkehr auf TCP-Port 22 für Sicherheitsgruppen zulassen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- SecurityGroupIds

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste IDs der Sicherheitsgruppen, für die Sie den SSH-Verkehr einschränken möchten.

Erforderliche IAM-Berechtigungen

Der AutomationAssumeRole Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Dokumentschritte

- `aws:executeAwsApi`- Entfernt alle Regeln, die eingehenden SSH-Verkehr auf TCP-Port 22 aus den Sicherheitsgruppen zulassen, die `SecurityGroupIds` Sie im Parameter angeben.

Ausgaben

DisableIncomingSSHTemplate. RestrictedSecurityGroupIds - Eine Liste IDs der Sicherheitsgruppen, bei denen die SSH-Regeln für eingehende Anrufe entfernt wurden.

`AWS-DisablePublicAccessForSecurityGroup`

Beschreibung

Dieses Runbook deaktiviert standardmäßige SSH- und RDP-Ports, die für alle IP-Adressen geöffnet sind.

> **Important**
>
> Dieses Runbook schlägt mit einem "fehl. InvalidPermission NotFound"Fehler für Sicherheitsgruppen, die beide der folgenden Kriterien erfüllen: 1) Die Sicherheitsgruppe befindet sich in einer nicht standardmäßigen VPC; und 2) Die Regeln für eingehende Nachrichten für die Sicherheitsgruppe geben keine offenen Ports an, die alle vier der folgenden Muster verwenden:
>
> - `0.0.0.0/0`
> - `::/0`
> - `SSH or RDP port + 0.0.0.0/0`
> - `SSH or RDP port + ::/0`

> **Note**
>
> Dieses Runbook ist in China nicht verfügbar. AWS-Regionen

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- GroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, für die die Ports deaktiviert werden sollen.
- IpAddressToBlock

  Typ: Zeichenfolge

  Beschreibung: (Optional) Zusätzliche IPv4 Adressen, von denen aus der Zugriff gesperrt werden soll, im Format`1.2.3.4/32`.

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Beschreibung

Das `AWSConfigRemediation-DisableSubnetAutoAssignPublicIP` Runbook deaktiviert das Attribut für die IPv4 öffentliche Adressierung für das von Ihnen angegebene Subnetz.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Subnetzes, für das Sie das Attribut für die automatische Zuweisung öffentlicher IPv4 Adressen deaktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`

- `ec2:ModifySubnetAttribute`

Dokumentschritte

- `aws:executeAwsApi`- Deaktiviert das Attribut für die automatische Zuweisung einer öffentlichen IPv4 Adresse für das Subnetz, das Sie im Parameter angegeben haben. `SubnetId`
- `aws:assertAwsResourceProperty`- Überprüft, ob das Attribut deaktiviert wurde.

AWSSupport-EnableVPCFlowLogs

Beschreibung

Das `AWSSupport-EnableVPCFlowLogs` Runbook erstellt Amazon Virtual Private Cloud (Amazon VPC) Flow Logs für Subnetze, Netzwerkschnittstellen und VPCs in Ihrem. AWS-Konto Wenn Sie ein Flow-Protokoll für ein Subnetz oder eine VPC erstellen, wird jede elastic network interface in diesem Subnetz oder dieser Amazon VPC überwacht. Flow-Protokolldaten werden in der Amazon CloudWatch Logs-Protokollgruppe oder dem von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket veröffentlicht. Weitere Informationen zu Flow-Protokollen finden Sie unter VPC Flow Logs im Amazon VPC-Benutzerhandbuch.

> **Important**
>
> Gebühren für Datenaufnahme und Archivierung von verkauften Protokollen fallen an, wenn Sie Flow-Protokolle in Logs oder Amazon CloudWatch S3 veröffentlichen. Weitere Informationen finden Sie unter Preise für Flow Logs

Führen Sie diese Automatisierung aus (Konsole)

> **Note**
>
> Stellen Sie bei der Auswahl `s3` als Protokollziel sicher, dass die Bucket-Richtlinie dem Log-Lieferdienst Zugriff auf den Bucket gewährt. Weitere Informationen finden Sie unter Amazon S3 S3-Bucket-Berechtigungen für Flow-Logs.

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

Linux,macOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- DeliverLogsPermissionArn

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN für die IAM-Rolle, der es Amazon Elastic Compute Cloud (Amazon EC2) ermöglicht, Flow-Logs in der CloudWatch Logs-Protokollgruppe in Ihrem Konto zu veröffentlichen. Wenn Sie `s3` für den `LogDestinationType` Parameter angeben, geben Sie keinen Wert für diesen Parameter an. Weitere Informationen finden Sie unter Veröffentlichen von CloudWatch Flow-Protokollen in Logs im Amazon VPC-Benutzerhandbuch.

- LogDestinationARN

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der ARN der Ressource, auf der die Flow-Protokolldaten veröffentlicht werden. Wenn für den `LogDestinationType` Parameter angegeben `cloud-watch-logs` ist, geben Sie den ARN der CloudWatch Logs-Protokollgruppe an, in der Sie Flow-Log-Daten veröffentlichen möchten. Alternativ können Sie stattdessen `LogGroupName` verwenden. Wenn für den `LogDestinationType` Parameter angegeben `s3` ist, müssen Sie für diesen Parameter den ARN des Amazon S3 S3-Buckets angeben, in dem Sie Flow-Protokolldaten veröffentlichen möchten. Sie können auch einen Ordner im Bucket angeben.

> **Important**
>
> Wenn `LogDestinationType` Sie sich für den ausgewählten Bucket entscheiden`s3`, sollten Sie sicherstellen, dass der ausgewählte Bucket den Best Practices für die Sicherheit von Amazon S3 Bucket entspricht und dass Sie die Datenschutzgesetze für Ihr Unternehmen und Ihre geografische Region einhalten.

- LogDestinationType

  Typ: Zeichenfolge

  Gültige Werte: cloud-watch-logs | s3

  Beschreibung: (Erforderlich) Legt fest, wo Flow-Protokolldaten veröffentlicht werden. Wenn Sie `LogDestinationType` als angeben`s3`, geben Sie nicht `DeliverLogsPermissionArn` oder an`LogGroupName`.

- LogFormat

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Felder, die in das Flow-Protokoll aufgenommen werden sollen, und die Reihenfolge, in der sie im Datensatz erscheinen sollen. Eine Liste der verfügbaren Felder finden Sie unter Flow-Protokolldatensätze im Amazon VPC-Benutzerhandbuch. Wenn Sie keinen Wert für diesen Parameter angeben, wird das Flow-Protokoll im Standardformat erstellt. Wenn Sie diesen Parameter angeben, müssen Sie mindestens ein Feld angeben.

- LogGroupName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name der CloudWatch Logs-Protokollgruppe, in der Flow-Log-Daten veröffentlicht werden. Wenn Sie `s3` für den `LogDestinationType` Parameter angeben, geben Sie keinen Wert für diesen Parameter an.

- ResourceIds

  Typ: StringList

  Beschreibung: (Erforderlich) Eine durch Kommas getrennte Liste der IDs Subnetze, Elastic Network Interfaces oder VPC, für die Sie ein Flow-Protokoll erstellen möchten.

- TrafficType

  Typ: Zeichenfolge

  Gültige Werte: ACCEPT | REJECT | ALL

  Beschreibung: (Erforderlich) Der Typ des zu protokollierenden Datenverkehrs. Sie können den Datenverkehr protokollieren, den die Ressource akzeptiert oder ablehnt, oder den gesamten Datenverkehr.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `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

Beispiel für eine Richtlinie

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/*"
            ]
        }
    ]
}
```

Dokumentschritte

- `aws:branch`- Verzweigt auf der Grundlage des für den `LogDestinationType` Parameter angegebenen Werts.
- `aws:executeScript`- Prüft, ob der Ziel-Amazon Simple Storage Service (Amazon S3) möglicherweise Lese - oder **`public`**Schreibzugriff auf seine Objekte gewährt.
- `aws:executeScript`- Erstellt eine Protokollgruppe, wenn kein Wert für den `LogDestinationARN` Parameter angegeben wurde, und für den `LogDestinationType` Parameter `cloud-watch-logs` wird ein Wert angegeben.
- `aws:executeScript`- Erstellt Flussprotokolle auf der Grundlage der in den Runbook-Parametern angegebenen Werte.

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

Beschreibung

Das `AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch` Runbook ersetzt ein vorhandenes Amazon VPC-Flow-Protokoll, das Flow-Protokolldaten in Amazon Simple Storage Service (Amazon S3) veröffentlicht, durch ein Flow-Protokoll, das Flow-Protokolldaten in der von Ihnen angegebenen Amazon CloudWatch Logs (CloudWatch Logs) -Protokollgruppe veröffentlicht.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DestinationLogGroup

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name der CloudWatch Logs-Protokollgruppe, in der Sie Flow-Protokolldaten veröffentlichen möchten.
- DeliverLogsPermissionArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN der AWS Identity and Access Management (IAM) -Rolle, die Sie verwenden möchten und der Amazon Elastic Compute Cloud (Amazon EC2) die erforderlichen Berechtigungen zum Veröffentlichen von Flow-Protokolldaten in Logs gewährt. CloudWatch

- FlowLogId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Flow-Protokolls, das auf Amazon S3 veröffentlicht wird, das Sie ersetzen möchten.
- MaxAggregationInterval

  Typ: Ganzzahl

  Gültige Werte: 60 | 600

  Beschreibung: (Optional) Das maximale Zeitintervall in Sekunden, in dem ein Paketfluss erfasst und in einem Flow-Protokolldatensatz zusammengefasst wird.
- TrafficType

  Typ: Zeichenfolge

  Gültige Werte: ACCEPT | REJECT | ALL

  Beschreibung: (Erforderlich) Der Typ der Flow-Protokolldaten, die Sie aufzeichnen und veröffentlichen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Dokumentschritte

- `aws:executeAwsApi`- Erfasst Details zu Ihrer VPC aus dem Wert, den Sie im `FlowLogId` Parameter angeben.

- `aws:executeAwsApi`- Erstellt ein Flow-Protokoll auf der Grundlage der Werte, die Sie für die Runbook-Parameter angeben.
- `aws:assertAwsResourceProperty`— Überprüft, ob das neu erstellte Flow-Protokoll in Logs veröffentlicht wird. CloudWatch
- `aws:executeAwsApi`— Löscht das Flow-Protokoll, das auf Amazon S3 veröffentlicht wird.
- `aws:executeScript`— Bestätigt, dass das auf Amazon S3 veröffentlichte Flow-Protokoll gelöscht wurde.

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

Beschreibung

Das `AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket` Runbook ersetzt ein vorhandenes Amazon VPC-Flow-Protokoll, das Flow-Protokolldaten in Amazon CloudWatch Logs (CloudWatch Logs) veröffentlicht, durch ein Flow-Protokoll, das Flow-Protokolldaten in dem von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket veröffentlicht.

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- Ziele: 3 BucketArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der ARN des Amazon S3 S3-Buckets, in dem Sie Flow-Protokolldaten veröffentlichen möchten.
- FlowLogId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Flow-Protokolls, das in CloudWatch Logs veröffentlicht wird, die Sie ersetzen möchten.
- MaxAggregationInterval

  Typ: Ganzzahl

  Gültige Werte: 60 | 600

  Beschreibung: (Optional) Das maximale Zeitintervall in Sekunden, in dem ein Paketfluss erfasst und in einem Flow-Protokolldatensatz zusammengefasst wird.
- TrafficType

  Typ: Zeichenfolge

  Gültige Werte: ACCEPT | REJECT | ALL

  Beschreibung: (Erforderlich) Der Typ der Flow-Protokolldaten, die Sie aufzeichnen und veröffentlichen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Dokumentschritte

- `aws:executeAwsApi`- Erfasst Details zu Ihrer VPC aus dem Wert, den Sie im `FlowLogId` Parameter angeben.
- `aws:executeAwsApi`- Erstellt ein Flow-Protokoll auf der Grundlage der Werte, die Sie für die Runbook-Parameter angeben.
- `aws:assertAwsResourceProperty`— Überprüft, ob das neu erstellte Flow-Protokoll auf Amazon S3 veröffentlicht wird.
- `aws:executeAwsApi`— Löscht das Flow-Protokoll, das in Logs veröffentlicht wird. CloudWatch
- `aws:executeScript`- Bestätigt, dass das in CloudWatch Logs veröffentlichte Flow-Protokoll gelöscht wurde.

AWS-ReleaseElasticIP

Beschreibung

Freigeben der angegebenen Elastic-IP-Adresse mithilfe der Zuordnungs-ID.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- AllocationId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Zuweisungs-ID der Elastic IP-Adresse.

AWS-RemoveNetworkACLUnrestrictedSSHRDP

Beschreibung

Das `AWS-RemoveNetworkACLUnrestrictedSSHRDP` Runbook entfernt alle ACL-Regeln (Network Access Control List) aus der angegebenen Netzwerk-ACL, die eingehenden Datenverkehr von allen Quelladressen zu Standard-SSH- und RDP-Anschlüssen zulassen. Regeln, die Portbereiche enthalten, die sich mit den standardmäßigen SSH- und RDP-Ports überschneiden, werden nicht entfernt.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen

ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- NetworkAclId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Netzwerk-ACL, für die Sie uneingeschränkte Regeln entfernen möchten, die eingehenden Datenverkehr von allen Quelladressen zu standardmäßigen SSH- und RDP-Anschlüssen zulassen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAclEntry`
- `ec2:DescribeNetworkAcls`

Dokumentschritte

- `aws:executeScript`- Entfernt alle Eingangsregeln, die Datenverkehr von allen Quelladressen der Sicherheitsgruppe zulassen, die Sie im Parameter angegeben haben. `SecurityGroupId`

Ausgaben

RemoveNaclEntriesAndVerify. VerificationMessage - Bestätigungsmeldungen der erfolgreich gelöschten Netzwerk-ACL-Regeln.

RemoveNaclEntriesAndVerify. RulesDeletedAndApiResponses - Die Netzwerk-ACL-Regeln, die gelöscht wurden, und die Antworten der `DeleteNetworkAclEntry` API-Operationen.

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules

Beschreibung

Das `AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules` Runbook entfernt alle Eingangsregeln aus der von Ihnen angegebenen Sicherheitsgruppe, die Datenverkehr von allen Quelladressen zulassen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- SecurityGroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, aus der Sie Eingangsregeln entfernen möchten, die Datenverkehr von allen Quelladressen zulassen.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

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

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Dokumentschritte

- `aws:executeScript`- Entfernt alle Eingangsregeln, die Datenverkehr von allen Quelladressen der Sicherheitsgruppe zulassen, die Sie im Parameter angegeben haben. `SecurityGroupId`

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

Beschreibung

Das `AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` Runbook entfernt alle Regeln aus der Standardsicherheitsgruppe der von Ihnen angegebenen Virtual Private Cloud (VPC).

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- GroupId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die ID der Sicherheitsgruppe, aus der Sie alle Regeln entfernen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Dokumentschritte

- `aws:assertAwsResourceProperty`- Bestätigt, dass die Sicherheitsgruppe, die Sie im `GroupId` Parameter angegeben haben, den Namen default trägt.
- `aws:executeScript`- Entfernt alle Regeln aus der Sicherheitsgruppe, die Sie im `GroupId` Parameter angegeben haben.

AWSSupport-SetupIPMonitoringFromVPC

Beschreibung

`AWSSupport-SetupIPMonitoringFromVPC`erstellt eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance im angegebenen Subnetz und überwacht das ausgewählte Ziel IPs (IPv4 oder IPv6), indem kontinuierlich Ping-, MTR-, Traceroute- und Tracetcp-Tests ausgeführt werden. Die Ergebnisse werden in Amazon CloudWatch Logs-Protokollen gespeichert, und Metrikfilter werden angewendet, um Latenz- und Paketverlust-Statistiken schnell in einem CloudWatch Dashboard zu visualisieren.

Zusätzliche Informationen

Die CloudWatch Logs-Daten können zur Fehlerbehebung im Netzwerk und zur Analyse der pattern/ trends. Additionally, you can configure CloudWatch alarms with Amazon SNS notifications when packet loss and/or Latenz, die einen bestimmten Schwellenwert erreicht hat, verwendet werden. Die

Daten können auch verwendet werden, wenn ein Fall eröffnet wird AWS Support, um ein Problem schnell zu isolieren und die Zeit bis zur Lösung bei der Untersuchung eines Netzwerkproblems zu verkürzen.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- CloudWatchLogGroupNamePrefix

  Typ: Zeichenfolge

  Standard: `/AWSSupport-SetupIPMonitoringFromVPC`

  Beschreibung: (Optional) Das Präfix wird für jede CloudWatch Protokollgruppe verwendet, die für die Testergebnisse erstellt wurde.
- CloudWatchLogGroupRetentionInDays

  Typ: Zeichenfolge

  Gültige Werte: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

Standard: 7

Beschreibung: (Optional) Die Anzahl der Tage, für die Sie die Netzwerküberwachungsergebnisse behalten möchten.

- InstanceType

  Typ: Zeichenfolge

  Gültige Werte: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

  Standard: t3.micro

  Beschreibung: (Optional) Der EC2-Instance-Typ für die Rescue-Instance. EC2 Empfohlene Größe: t3.micro.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Subnetz-ID für die Überwachungs-Instance. Beachten Sie, dass Sie, wenn Sie ein privates Subnetz angeben, sicherstellen müssen, dass ein Internetzugang vorhanden ist, damit die Monitor-Instance den Test einrichten kann (d. h. den CloudWatch Logs-Agent installieren, mit Systems Manager interagieren und CloudWatch).

- Ziel IPs

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Durch Kommas getrennte Liste der zu überwachenden IPv4s und/oder IPv6s zu überwachenden Objekte. Leerzeichen sind nicht zulässig. Die maximale Größe beträgt 255 Zeichen. Beachten Sie: Wenn Sie eine ungültige IP angeben, schlägt die Automatisierung fehl, und die Testeinrichtung wird zurückgesetzt.

- TestInstanceSecurityGroupId

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Sicherheitsgruppen-ID für die Testinstanz. Wenn nicht angegeben, erstellt die Automatisierung während der Instanzerstellung eine. Stellen Sie sicher, dass die Sicherheitsgruppe ausgehenden Zugriff auf die Überwachung IPs zulässt.

- TestInstanceProfileName

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Name eines vorhandenen IAM-Instanzprofils für die Testinstanz. Wenn nicht angegeben, erstellt die Automatisierung während der Instanzerstellung eines. Die Rolle muss über die folgenden Berechtigungen verfügen:`logs:CreateLogStream`, `logs:DescribeLogGroupslogs:DescribeLogStreams`, und `logs:PutLogEvents` und die AWS verwaltete Richtlinie`AmazonSSMManagedInstanceCore`.
- TestInterval

  Typ: Zeichenfolge

  Beschreibung: (Optional) Die Anzahl der Minuten zwischen den Testintervallen. Der Standardwert ist 1 Minute und das Maximum ist `10` Minuten.
- RetainDashboardAndLogsOnDeletion

  Typ: Zeichenfolge

  Beschreibung: (Optional) Geben Sie `False` an, dass das CloudWatch Amazon-Dashboard und die Protokolle beim Löschen des AWS AWS CloudFormation Stacks gelöscht werden sollen. Der Standardwert ist `True`. Standardmäßig werden das Dashboard und die Protokolle beibehalten und müssen manuell gelöscht werden, wenn sie nicht mehr benötigt werden.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

> **Warning**
>
> Es wird empfohlen, den `TestInstanceProfileName` Parameter zu übergeben oder Sicherheitsvorkehrungen zu treffen, um den Missbrauch veränderbarer IAM-Berechtigungen zu verhindern.

Es wird empfohlen, dass dem Benutzer, der die Automatisierung ausführt, die von Amazon SSMAutomation Role IAM verwaltete Richtlinie beigefügt ist. Außerdem muss der Benutzer die folgende Richtlinie an sein Benutzerkonto, seine Gruppe oder seine Rolle angefügt haben:

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"
        }
    ]
}
```

Wenn der `TestInstanceProfileName` Parameter angegeben wird, sind die folgenden IAM-Berechtigungen nicht erforderlich, um das Runbook auszuführen:

- iam: CreateRole
- ich bin: CreateInstanceProfile

- ich bin: DetachRolePolicy
- ich bin: AttachRolePolicy
- ich bin: AddRoleToInstanceProfile
- ich bin: RemoveRoleFromInstanceProfile
- ich bin: DeleteRole
- ich bin: DeleteRolePolicy
- ich bin: DeleteInstanceProfile

Dokumentschritte

1. **`aws:executeAwsApi`**- Beschreiben Sie das bereitgestellte Subnetz, um die VPC-ID und den IPv6 CIDR-Blockzuordnungsstatus abzurufen.
2. **`aws:executeScript`**— überprüft, ob das angegebene Ziel syntaktisch korrekt ist IPv4 und/oder die IPv6 Adressen korrekt IPs sind, ermittelt die Architektur des ausgewählten Instanztyps und stellt sicher, dass das Subnetz über eine IPv6 Pool-Zuordnung verfügt, falls es sich um eine Ziel-IP handelt. IPv6
3. **`aws:createStack`**- Erstellen Sie einen AWS CloudFormation Stack, der die Amazon EC2 EC2-Testinstanz, das IAM-Instance-Profil (falls nicht bereitgestellt), die Sicherheitsgruppe (falls nicht bereitgestellt), die CloudWatch Protokollgruppen und CloudWatch das Dashboard bereitstellt.

   (Cleanup) Wenn der Schritt fehlschlägt:

   `aws:executeScript`— Beschreiben Sie die CloudFormation Stack-Ereignisse, um die Fehlerursache zu ermitteln.

   `aws:deleteStack`- löscht den CloudFormation Stapel und alle zugehörigen Ressourcen.
4. **`aws:waitForAwsResourceProperty`**- warte, bis der CloudFormation Stapel fertig erstellt ist.

   (Cleanup) Wenn der Schritt fehlschlägt:

   `aws:executeScript`- Beschreiben Sie die CloudFormation Stack-Ereignisse, um die Fehlerursache zu ermitteln.

   `aws:deleteStack`- löscht den CloudFormation Stapel und alle zugehörigen Ressourcen.

5. **`aws:executeScript`**— Beschreiben Sie die CloudFormation Stack-Ressourcen, um die Testinstanz-ID, die Sicherheitsgruppen-ID, die IAM-Rolle, das Instanzprofil und den Dashboard-Namen zu erhalten.

   (Cleanup) Wenn der Schritt fehlschlägt:

   `aws:executeScript`— Beschreiben Sie die CloudFormation Stack-Ereignisse, um die Fehlerursache zu ermitteln.

   `aws:deleteStack`- löscht den CloudFormation Stapel und alle zugehörigen Ressourcen.

6. **`aws:waitForAwsResourceProperty`**- Warten Sie, bis die Testinstanz zu einer verwalteten Instanz wird.

   (Cleanup) Wenn der Schritt fehlschlägt:

   `aws:deleteStack`- löscht den CloudFormation Stack und alle zugehörigen Ressourcen.

7. **`aws:runCommand`**- installiert den CloudWatch Agenten auf der Testinstanz.

   (Cleanup) Wenn der Schritt fehlschlägt:

   `aws:deleteStack`- löscht den CloudFormation Stack und alle zugehörigen Ressourcen.

8. **`aws:runCommand`**- Definieren Sie die Netzwerktestskripte (MTR, Ping, Tracepath und Traceroute) für jedes der bereitgestellten Skripte. IPs

   (Cleanup) Wenn der Schritt fehlschlägt:

   `aws:deleteStack`- löscht den CloudFormation Stack und alle zugehörigen Ressourcen.

9. **`aws:runCommand`**- Starten Sie die Netzwerktests und planen Sie nachfolgende Ausführungen mit Cronjobs, die alle Minuten ausgeführt werden. TestInterval

   (Cleanup) Wenn der Schritt fehlschlägt:

   `aws:deleteStack`- löscht den CloudFormation Stack und alle zugehörigen Ressourcen.

10. **`aws:runCommand`**- konfigurieren Sie den CloudWatch Agenten so, dass er die Testergebnisse `/home/ec2-user/logs/` in die CloudWatch Logs überträgt.

    (Cleanup) Wenn der Schritt fehlschlägt:

    `aws:deleteStack`- löscht den CloudFormation Stack und alle zugehörigen Ressourcen.

11 **aws:runCommand**- konfigurieren Sie die Protokollrotation für die Testergebnisse in/home/ec2-user/logs/.

12 **aws:executeScript**- legt die Aufbewahrungsrichtlinie für alle vom CloudFormation Stapel erstellten CloudWatch Protokollgruppen fest.

13 **aws:executeScript**- Erstellen Sie Metrikfilter für CloudWatch Protokollgruppen für Ping-Latenz und Ping-Paketverlust.

(Cleanup) Wenn der Schritt fehlschlägt:

aws:deleteStack- löscht den CloudFormation Stapel und alle zugehörigen Ressourcen.

14 **aws:executeScript**- aktualisiert das CloudWatch Dashboard um Widgets für Statistiken zur Ping-Latenz und zum Verlust von Ping-Paketen.

(Cleanup) Wenn der Schritt fehlschlägt:

aws:executeAwsApi- lösche das CloudWatch Dashboard, falls es existiert.

aws:deleteStack- lösche den CloudFormation Stack und alle zugehörigen Ressourcen.

15 **aws:branch**- den SleepTime Parameter auswerten. Wenn auf gesetzt0, wird die Automatisierung beendet, ohne dass der Stapel gelöscht wird.

16 **aws:sleep**- Warten Sie die angegebene SleepTime Dauer, bevor Sie den CloudFormation Stapel löschen.

17 **aws:deleteStack**- löscht den CloudFormation Stapel. Basierend auf dem RetainDashboardAndLogsOnDeletion Parameter werden das CloudWatch Dashboard und die Protokollgruppen entweder beibehalten oder gelöscht.

(Bereinigung) Wenn das Löschen des Stacks fehlschlägt:

aws:executeScript- Beschreiben Sie die CloudFormation Stack-Ereignisse, um die Ursache für das Fehlschlagen beim Löschen zu ermitteln.

Ausgaben

updateCloudWatchArmaturenbrett. StackUrl - die URL des CloudFormation Stacks.

updateCloudWatchArmaturenbrett. DashboardUrl - die URL des CloudWatch Dashboards.

updateCloudWatchArmaturenbrett. DashboardName - der Name des CloudWatch Dashboards.

updateCloudWatchArmaturenbrett. LogGroups - die Liste der erstellten CloudWatch Protokollgruppen.

describeStackResources. HelperInstanceId - die Testinstanz-ID.

describeStackResources. StackName - der CloudFormation Stack-Name.

AWSSupport-TerminateIPMonitoringFromVPC

Beschreibung

`AWSSupport-TerminateIPMonitoringFromVPC`beendet einen IP-Überwachungstest, der zuvor von `AWSSupport-SetupIPMonitoringFromVPC` gestartet wurde. Daten im Zusammenhang mit der angegebenen Test-ID werden gelöscht.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- AutomationExecutionId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Die Ausführungs-ID der Automatisierung, von der Sie das `AWSSupport-SetupIPMonitoringFromVPC` Runbook zuvor ausgeführt haben. Alle Ressourcen, die dieser Ausführungs-ID zugeordnet sind, werden gelöscht.

- InstanceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Instance-ID für die Überwachungs-Instance.

- SubnetId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die Subnetz-ID für die Überwachungs-Instance.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

Es wird empfohlen, dass dem Benutzer, der die Automatisierung ausführt, die von Amazon SSMAutomation Role IAM verwaltete Richtlinie beigefügt ist. Darüber hinaus muss dem Benutzer, seiner Gruppe oder Rolle die folgende Richtlinie zugewiesen sein:

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"
        }
    ]
}
```

Dokumentschritte

1. `aws:assertAwsResourceProperty`- überprüfen AutomationExecutionId und InstanceId beziehen sich auf denselben Test.
2. `aws:assertAwsResourceProperty`- überprüfen SubnetId und InstanceId beziehen sich auf denselben Test.
3. `aws:executeAwsApi`- ruft die Testsicherheitsgruppe ab.
4. `aws:executeAwsApi`- löscht das CloudWatch Dashboard.
5. `aws:changeInstanceState`- beendet die Testinstanz.
6. `aws:executeAwsApi`- entfernt das IAM-Instanzprofil aus der Rolle.
7. `aws:executeAwsApi`- löscht das durch die Automatisierung erstellte IAM-Instanzprofil.
8. `aws:executeAwsApi`— löscht die CloudWatch Inline-Richtlinie aus der Rolle, die durch die Automatisierung erstellt wurde.
9. `aws:executeAwsApi`- Trennen Sie die von Amazon SSMManaged InstanceCore verwaltete Richtlinie von der Rolle, die durch die Automatisierung erstellt wurde.
10. `aws:executeAwsApi`- löscht die durch die Automatisierung erstellte IAM-Rolle.
11. `aws:executeAwsApi`- löscht die durch die Automatisierung erstellte Sicherheitsgruppe, falls sie existiert.

Ausgaben

Keine

AWS WAF

AWS Systems Manager Die Automatisierung stellt vordefinierte Runbooks für bereit. AWS WAF Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl
- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

AWS-AddWAFRegionalRuleToRuleGroup

Beschreibung

Das `AWS-AddWAFRegionalRuleToRuleGroup` Runbook fügt einer AWS WAF regionalen Regelgruppe eine bestehende AWS WAF regionale Regel hinzu. Nur AWS WAF klassische regionale Regelgruppen werden unterstützt. AWS WAF Klassische regionale Regelgruppen können maximal 10 Regeln haben.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- RuleGroupId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Regelgruppe, die Sie aktualisieren möchten.
- RulePriority

  Typ: Ganzzahl

Beschreibung: (Erforderlich) Die Priorität für die neue Regel. Die Regelpriorität bestimmt die Reihenfolge, in der Regeln in einer regionalen Gruppe bewertet werden. Regeln mit einem niedrigeren Wert haben eine höhere Priorität als Regeln mit einem höheren Wert. Der Wert muss eine eindeutige ganze Zahl sein. Wenn Sie einer regionalen Regelgruppe mehrere Regeln hinzufügen, müssen die Werte nicht aufeinander folgen.

- RuleId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID für die Regel, die Sie zu Ihrer regionalen Regelgruppe hinzufügen möchten.

- RuleAction

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Gibt die Aktion an, AWS WAF die ausgeführt wird, wenn eine Webanforderung den Bedingungen der Regel entspricht.

  Gültige Werte: ALLOW | BLOCK | COUNT

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

Dokumentschritte

- Get WAFChange Token (aws:executeAwsApi) — Ruft ein AWS WAF Änderungstoken ab, um sicherzustellen, dass das Runbook keine widersprüchlichen Anfragen an den Service sendet.

- Add WAFRule To WAFRegional RuleGroup (aws:ExecuteScript) — Fügt die angegebene Regel der regionalen Regelgruppe hinzu. AWS WAF
- VerifyChangeTokenPropagating (aws: waitForAwsResourceProperty) — Überprüft, ob das Änderungstoken den Status oder hat. `PENDING` `INSYNC`
- VerifyRuleAddedToRuleGroup (aws:ExecuteScript) — Überprüft, ob die angegebene AWS WAF Regel der regionalen Zielregelgruppe hinzugefügt wurde.

Ausgaben

- VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse - Ergebnis des Schritts zur Überprüfung, ob die neue Regel der regionalen Regelgruppe hinzugefügt wurde.
- VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse - Ausgabe des `ListActivatedRulesInRuleGroup` API-Vorgangs.

AWS-AddWAFRegionalRuleToWebAcl

Beschreibung

Das `AWS-AddWAFRegionalRuleToWebAcl` Runbook fügt eine bestehende AWS WAF regionale Regel, Regelgruppe oder ratenbasierte Regel zu einer regionalen AWS WAF Classic Web Access Control List (ACL) hinzu. Dieses Runbook aktualisiert keine vorhandenen regionalen AWS WAF Classic-Web-ACLs, die von verwaltet werden. AWS Firewall Manager

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

Typ: Zeichenfolge

Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- Web ACLId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Web-ACL, die Sie aktualisieren möchten.

- ActivatedRulePriority

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Priorität für die neue Regel. Die Regelpriorität bestimmt die Reihenfolge, in der Regeln in einer Web-ACL ausgewertet werden. Regeln mit einem niedrigeren Wert haben eine höhere Priorität als Regeln mit einem höheren Wert. Der Wert muss eine eindeutige ganze Zahl sein. Wenn Sie einer regionalen Web-ACL mehrere Regeln hinzufügen, müssen die Werte nicht aufeinander folgen.

- ActivatedRuleRuleId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID für die reguläre Regel, ratenbasierte Regel oder Gruppe, die Sie der Web-ACL hinzufügen möchten.

- ActivatedRuleAction

  Typ: Zeichenfolge

  Gültige Werte: ALLOW | BLOCK | COUNT

  Beschreibung: (Optional) Gibt die Aktion an, die AWS WAF ausgeführt wird, wenn eine Webanforderung den Bedingungen der Regel entspricht.

- ActivatedRuleType

  Typ: Zeichenfolge

  Gültige Werte: REGULAR | RATE_BASED | GROUP

Standard: REGULAR

Beschreibung: (Optional) Der Regeltyp, den Sie der Web-ACL hinzufügen. Dieses Feld ist zwar optional, beachten Sie jedoch, dass die Anforderung fehlschlägt, wenn Sie versuchen, einer Web-ACL eine `RATE_BASED` Regel hinzuzufügen, ohne den Typ festzulegen, da die Anforderung standardmäßig eine `REGULAR` Regel verwendet.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

Dokumentschritte

- DetermineWebACLNotIn FMSAnd RulePriority (aws:ExecuteScript) — Überprüft, ob sich die AWS WAF Web-ACL in einer Firewall Manager Manager-Sicherheitsrichtlinie befindet, und stellt sicher, dass die Prioritäts-ID nicht mit einer vorhandenen ACL in Konflikt steht.
- AddRuleOrRuleGroupToWebACL (aws:ExecuteScript) — Fügt die angegebene Regel zur Web-ACL hinzu. AWS WAF
- VerifyRuleOrRuleGroupAddedToWebAcl (aws:ExecuteScript) — Überprüft, ob die angegebene Regel zur Ziel-Web-ACL hinzugefügt wurde. AWS WAF

Ausgaben

- DetermineWebACLNotFMSAndRulePriorityIn. PrereqResponse: Ausgabe des `DetermineWebACLNotInFMSAndRulePriority` Schritts.
- VerifyRuleOrRuleGroupAddedToWebAcl. VerifyRuleOrRuleGroupAddedToWebACLResponse: Ausgabe des `AddRuleOrRuleGroupToWebACL` Schritts.

- VerifyRuleOrRuleGroupAddedToWebAcl. ListActivatedRulesOrRuleGroupsInWebACLResponse: Ausgabe des `VerifyRuleOrRuleGroupAddedToWebAcl` Schritts.

AWSConfigRemediation-EnableWAFClassicLogging

Beschreibung

Das `AWSConfigRemediation-EnableWAFClassicLogging` Runbook ermöglicht die Protokollierung bei Amazon Data Firehose (Firehose) für die von Ihnen angegebene AWS WAF Web Access Control List (Web ACL).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- DeliveryStreamName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Name des Firehose-Lieferstreams, an den Sie Protokolle senden möchten.

- Web ACLId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der AWS WAF Web-ACL, für die Sie die Anmeldung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

Dokumentschritte

- `aws:executeAwsApi`- Bestätigt, dass der von Ihnen angegebene Lieferdatenstrom `DeliveryStreamName` existiert.
- `aws:executeAwsApi`- Sammelt den ARN der im `WebACLId` Parameter angegebenen AWS WAF Web-ACL.
- `aws:executeAwsApi`- Aktiviert die Protokollierung für die Web-ACL.
- `aws:assertAwsResourceProperty`- Überprüft, ob die Protokollierung auf der AWS WAF Web-ACL aktiviert wurde.

AWSConfigRemediation-EnableWAFClassicRegionalLogging

Beschreibung

Das `AWSConfigRemediation-EnableWAFClassicRegionalLogging` Runbook ermöglicht die Protokollierung bei Amazon Data Firehose (Firehose) für die von Ihnen angegebene AWS WAF Web Access Control List (ACL).

Führen Sie diese Automatisierung (Konsole) aus

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.
- LogDestinationConfigs

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) des Firehose-Lieferstreams, an den Sie Protokolle senden möchten.
- Web ACLId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der AWS WAF Web-ACL, für die Sie die Anmeldung aktivieren möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

Dokumentschritte

- `aws:executeAwsApi`- Sammelt den ARN der im `WebACLId` Parameter angegebenen AWS WAF Web-ACL.
- `aws:executeAwsApi`- Aktiviert die Protokollierung für die Web-ACL.
- `aws:assertAwsResourceProperty`- Überprüft, ob die Protokollierung auf der AWS WAF Web-ACL aktiviert wurde.

`AWSConfigRemediation-EnableWAFV2Logging`

Beschreibung

Das `AWSConfigRemediation-EnableWAFV2Logging` Runbook ermöglicht die Protokollierung für eine AWS WAF (AWS WAF V2) Web Access Control List (Web ACL) mit dem angegebenen Amazon Data Firehose (Firehose) -Lieferstream.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- LogDestinationConfigs

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Firehose-Lieferstream-ARN, den Sie der Web-ACL zuordnen möchten.

  > **Note**
  >
  > Der Firehose-Lieferstream-ARN muss mit dem Präfix `aws-waf-logs-` beginnen. Beispiel, `aws-waf-logs-us-east-2-analytics`. Weitere Informationen finden Sie unter Amazon Data Firehose.

- WebAclArn

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) ARN der Web-ACL, für die die Protokollierung aktiviert wird.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

Dokumentschritte

- `aws:executeScript`- Aktiviert die Protokollierung für die AWS WAF V2-Web-ACL und überprüft, ob die Protokollierung die angegebene Konfiguration hat.

Amazon WorkSpaces

AWS Systems Manager Automation stellt vordefinierte Runbooks für Amazon WorkSpaces bereit. Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWS-CreateWorkSpace
- AWSSupport-RecoverWorkSpace

`AWS-CreateWorkSpace`

Beschreibung

Das `AWS-CreateWorkSpace` Runbook erstellt einen neuen WorkSpaces virtuellen Amazon-Desktop, auch bekannt als a WorkSpace, basierend auf den Werten, die Sie für die Eingabeparameter angeben. Weitere Informationen dazu WorkSpaces finden Sie unter Was ist Amazon WorkSpaces? im WorkSpaces Amazon-Administratorhandbuch.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.

- BundleId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Bundles, das für das WorkSpace verwendet werden soll.

- ComputeTypeName

  Typ: Zeichenfolge

  Gültige Werte: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

  Beschreibung: (Optional) Der Berechnungstyp für Ihren. WorkSpace

- DirectoryId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID des Verzeichnisses, zu dem Sie hinzugefügt werden WorkSpace sollen.

- RootVolumeEncryptionEnabled

  Typ: Boolescher Wert

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Ermittelt, ob das Root-Volume von verschlüsselt WorkSpace ist.

- RootVolumeSizeGib

  Typ: Ganzzahl

Beschreibung: (Erforderlich) Die Größe des Root-Volumes für WorkSpace.

- RunningMode

  Typ: Zeichenfolge

  Gültige Werte: ALWAYS_ON | AUTO_STOP

  Beschreibung: (Erforderlich) Der Laufmodus von. WorkSpace

- RunningModeAutoStopTimeoutInMinutes

  Typ: Ganzzahl

  Beschreibung: (Optional) Die Zeit nach dem Abmelden eines Benutzers, wenn der WorkSpaces beendet wird. Geben Sie einen Wert in 60-Minuten-Intervallen an.

- Tags (Markierungen)

  Typ: Zeichenfolge

  Beschreibung: (Optional) Tags, auf die Sie anwenden möchten. WorkSpace

- UserName

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Benutzername, dem zugeordnet werden soll WorkSpace.

- UserVolumeEncryptionEnabled

  Typ: Boolescher Wert

  Zulässige Werte: true | false

  Standard: false

  Beschreibung: (Optional) Legt fest, ob das Benutzervolume von verschlüsselt WorkSpace ist.

- UserVolumeSizeGib

  Typ: Ganzzahl

  Beschreibung: (Erforderlich) Die Größe des Benutzervolumes für WorkSpace.

- VolumeEncryptionKey

Typ: Zeichenfolge

Beschreibung: (Optional) Der symmetrische AWS Key Management Service Schlüssel, den Sie zum Verschlüsseln der auf Ihrem gespeicherten Daten verwenden möchten. WorkSpace

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

Dokumentschritte

- `aws:executeScript`- Erstellt eine, die auf den Werten WorkSpace basiert, die Sie für die Eingabeparameter angeben.
- `aws:waitForAwsResourceProperty`- Überprüft den Status von. WorkSpace `AVAILABLE`

Ausgaben

`CreateWorkspace.WorkspaceId`

AWSSupport-RecoverWorkSpace

Beschreibung

Das `AWSSupport-RecoverWorkSpace` Runbook führt Wiederherstellungsschritte auf dem WorkSpaces virtuellen Amazon-Desktop durch WorkSpace, den Sie angeben. Das Runbook startet das neu WorkSpace, und wenn der Status unverändert ist, stellt es auf der WorkSpace Grundlage der Werte`UNHEALTHY`, die Sie für die Eingabeparameter angeben, wieder her oder erstellt es neu. Bevor Sie dieses Runbook verwenden, empfehlen wir Ihnen, die Informationen zur WorkSpaces Problembehebung im WorkSpaces Amazon-Administratorhandbuch zu lesen.

> **Important**
>
> Das Wiederherstellen oder Neuerstellen eines WorkSpace ist eine potenziell zerstörerische Aktion, die zum Verlust von Daten führen kann. Dies liegt daran, dass der aus dem letzten

verfügbaren Snapshot wiederhergestellt WorkSpace wird und Daten, die aus Snapshots wiederhergestellt wurden, bis zu 12 Stunden alt sein können.
Mit der Wiederherstellungsoption werden sowohl das Stammvolume als auch das Benutzervolume auf der Grundlage der neuesten Snapshots neu erstellt. Mit der Neuerstellungsoption wird das Benutzer-Volume aus dem letzten Snapshot und das aus dem Image, das dem Bundle zugeordnet ist, WorkSpace aus dem es erstellt wurde, neu erstellt. WorkSpace Anwendungen, die installiert wurden, oder Systemeinstellungen, die nach der Erstellung geändert wurden, WorkSpace gehen verloren. Weitere Informationen zur Wiederherstellung und WorkSpaces Neuerstellung finden Sie unter Restore a WorkSpace und Rebuild a WorkSpace im Amazon WorkSpaces Administration Guide.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Optional) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann. Wenn keine Rolle angegeben ist, verwendet Systems Manager Automation die Berechtigungen des Benutzers, der dieses Runbook startet.
- Bestätigen

  Typ: Zeichenfolge

  Gültige Werte: Ja

Beschreibung: (Erforderlich) Die Eingabe von Ja bedeutet, dass Sie verstehen, dass bei den Wiederherstellungs- und Neuerstellungsaktionen versucht wird, die Daten WorkSpace aus dem letzten Snapshot wiederherzustellen, und dass Daten, die aus diesen Snapshots wiederhergestellt wurden, bis zu 12 Stunden alt sein können.

- Starten Sie neu

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Standard: Ja

  Beschreibung: (Erforderlich) Legt fest, ob der WorkSpace neu gestartet wurde.

- Neu aufbauen

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Standard: Nein

  Beschreibung: (Erforderlich) Legt fest, ob der neu erstellt WorkSpace wird.

- Wiederherstellen

  Typ: Zeichenfolge

  Gültige Werte: Ja | Nein

  Standard: Nein

  Beschreibung: (Erforderlich) Legt fest, ob WorkSpace das wiederhergestellt wurde.

- WorkspaceId

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Die ID der Datei, die WorkSpace Sie wiederherstellen möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

Dokumentschritte

- `aws:executeAwsApi`- Erfasst den Status von, den WorkSpace Sie im `WorkspaceId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft den Status von WorkSpace ist`AVAILABLE`,, `ERROR` `IMPAIREDSTOPPED`, oder. `UNHEALTHY`
- `aws:branch`- Filialen, die auf dem WorkSpace Bundesstaat basieren.
- `aws:executeAwsApi`- Startet das WorkSpace.
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den `Action` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet nach dem Start auf WorkSpace den Status.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der WorkSpace Status `UNHEALTHY` nach dem `AVAILABLE` Start zu`ERROR`,`IMPAIRED`, oder wechselt.
- `aws:executeAwsApi`- Erfasst den Status von WorkSpace nach dem Start.
- `aws:branch`- Verzweigungen, die auf dem Status von basieren, WorkSpace nachdem sie gestartet wurden.
- `aws:executeAwsApi`- Sammelt die verfügbaren Schnappschüsse für die Wiederherstellung oder Neuerstellung von. WorkSpace
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den Parameter angeben. `Reboot`
- `aws:executeAwsApi`- Startet den WorkSpace neu.

- `aws:executeAwsApi`- Erfasst den Status von WorkSpace nach dem Start.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Status von geändert wird WorkSpace . `REBOOTING`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der WorkSpace Status zu `AVAILABLEERROR`, oder `UNHEALTHY` nach dem Neustart wechselt.
- `aws:executeAwsApi`- Erfasst den Status von nach dem WorkSpace Neustart.
- `aws:branch`- Verzweigungen, die auf dem Status von nach dem WorkSpace Neustart basieren.
- `aws:branch`- Verzweigt auf der Grundlage des Werts, den Sie für den `Restore` Parameter angeben.
- `aws:executeAwsApi`- Stellt die wieder her WorkSpace. Schlägt die Wiederherstellung fehl, versucht das Runbook, den WorkSpace neu zu erstellen.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Status von geändert wird WorkSpace . `RESTORING`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der WorkSpace Status zu `AVAILABLEERROR`, oder `UNHEALTHY` nach der Wiederherstellung wechselt.
- `aws:executeAwsApi`- Sammelt den Zustand von WorkSpace nach der Wiederherstellung.
- `aws:branch`- Verzweigungen basieren auf dem Zustand der Datei WorkSpace nach der Wiederherstellung.
- `aws:branch`- Verzweigungen, die auf dem Wert basieren, den Sie für den `Rebuild` Parameter angeben.
- `aws:executeAwsApi`- Baut die WorkSpace neu auf.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Status des WorkSpace wechselt. `REBUILDING`
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der WorkSpace Status zu `AVAILABLEERROR`, oder `UNHEALTHY` nach dem Wiederaufbau wechselt.
- `aws:executeAwsApi`- Sammelt den Zustand von WorkSpace nach dem Wiederaufbau.
- `aws:assertAwsResourceProperty`- Bestätigt den Zustand des WorkSpace is`AVAILABLE`.

X-Ray

AWS Systems Manager Automation bietet vordefinierte Runbooks für. AWS X-Ray Ausführliche Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter Working with runbooks. Informationen zum Anzeigen von Runbook-Inhalten finden Sie unter. Runbook-Inhalte anzeigen

Themen

- AWSConfigRemediation-UpdateXRayKMSKey

AWSConfigRemediation-UpdateXRayKMSKey

Beschreibung

Das `AWSConfigRemediation-UpdateXRayKMSKey` Runbook ermöglicht die Verschlüsselung Ihrer AWS X-Ray Daten mithilfe eines AWS Key Management Service (AWS KMS) -Schlüssels. Dieses Runbook sollte nur als Grundlage verwendet werden, um sicherzustellen, dass Ihre AWS X-Ray Daten gemäß den empfohlenen Mindestsicherheitsmethoden verschlüsselt werden. Wir empfehlen, mehrere Datensätze mit unterschiedlichen KMS-Schlüsseln zu verschlüsseln.

Führen Sie diese Automatisierung aus (Konsole)

Art des Dokuments

Automatisierung

Eigentümer

Amazon

Plattformen

LinuxmacOS, Windows

Parameter

- AutomationAssumeRole

  Typ: Zeichenfolge

  Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN) der AWS Identity and Access Management (IAM) -Rolle, mit der Systems Manager Automation die Aktionen in Ihrem Namen ausführen kann.

- KeyId

  Typ: Zeichenfolge

Beschreibung: (Erforderlich) Der Amazon-Ressourcenname (ARN), die Schlüssel-ID oder der Schlüsselalias des KMS-Schlüssels, den Sie AWS X-Ray zum Verschlüsseln von Daten verwenden möchten.

Erforderliche IAM-Berechtigungen

Der `AutomationAssumeRole` Parameter erfordert die folgenden Aktionen, um das Runbook erfolgreich zu verwenden.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

Dokumentschritte

- `aws:executeAwsApi`- Aktiviert die Verschlüsselung Ihrer X-Ray-Daten mit dem KMS-Schlüssel, den Sie im `KeyId` Parameter angeben.
- `aws:waitForAwsResourceProperty`- Wartet darauf, dass der Verschlüsselungskonfigurationsstatus Ihres X-Ray erreicht ist`ACTIVE`.
- `aws:executeAwsApi`- Sammelt den ARN des Schlüssels, den Sie im `KeyId` Parameter angeben.
- `aws:assertAwsResourceProperty`- Überprüft, ob die Verschlüsselung auf Ihrem X-Ray aktiviert wurde.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.