



Guida per l'utente

AWS Systems Manager Riferimento al runbook di automazione



AWS Systems Manager Riferimento al runbook di automazione: Guida per l'utente

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Riferimento al runbook del servizio di automazione	1
Visualizza il contenuto del runbook	4
API Gateway	4
AWSConfigRemediation-DeleteAPIGatewayStage	4
AWSConfigRemediation-EnableAPIGatewayTracing	6
AWSConfigRemediation-UpdateAPIGatewayMethodCaching	7
AWS Batch	9
AWSSupport-TroubleshootAWSBatchJob	9
AWS CloudFormation	15
AWS-DeleteCloudFormationStack	15
AWS-EnableCloudFormationSNSNotification	16
AWS-RunCfnLint	18
AWSSupport-TroubleshootCFNCustomResource	20
AWS-UpdateCloudFormationStack	22
CloudFront	23
AWSConfigRemediation-EnableCloudFrontDefaultRootObject	24
AWSConfigRemediation-EnableCloudFrontAccessLogs	25
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity	27
AWSConfigRemediation-EnableCloudFrontOriginFailover	29
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS	30
CloudTrail	32
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail	32
AWS-EnableCloudTrail	34
AWS-EnableCloudTrailCloudWatchLogs	35
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS	37
AWS-EnableCloudTrailKmsEncryption	39
AWSConfigRemediation-EnableCloudTrailLogFileValidation	40
AWS-EnableCloudTrailLogFileValidation	41
AWS-QueryCloudTrailLogs	43
CloudWatch	45
AWS-ConfigureCloudWatchOnEC2Instance	45
AWS-EnableCWAAlarm	46
Amazon DocumentDB	49
AWS-EnableDocDbClusterBackupRetentionPeriod	49

CodeBuild	51
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMCMK	52
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject	53
AWS CodeDeploy	55
AWSSupport-TroubleshootCodeDeploy	55
AWS Config	57
AWSSupport-SetupConfig	57
Amazon Connect	60
AWSSupport-AssociatePhoneNumbersToConnectContactFlows	60
AWSSupport-CollectAmazonConnectContactFlowLog	68
AWS Directory Service	74
AWS-CreateDSManagementInstance	74
AWSSupport-TroubleshootADConnectorConnectivity	79
AWSSupport-TroubleshootDirectoryTrust	82
AWS AppSync	86
AWS-EnableAppSyncGraphQLApiLogging	86
Amazon Athena	88
AWS-EnableAthenaWorkGroupEncryptionAtRest	89
DynamoDB	91
AWS-ChangeDDBRWCapacityMode	91
AWS-CreateDynamoDBBackup	93
AWS-DeleteDynamoDbBackup	95
AWSConfigRemediation-DeleteDynamoDbTable	95
AWS-DeleteDynamoDbTableBackups	97
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable	98
AWSConfigRemediation-EnablePITRForDynamoDbTable	100
AWS-EnableDynamoDbAutoscaling	101
AWS-RestoreDynamoDBTable	105
AWS Database Migration Service	107
AWSSupport-TroubleshootDMSTableErrors	107
Amazon EBS	113
AWSSupport-AnalyzeEBSResourceUsage	114
AWS-ArchiveEBSSnapshots	120
AWS-AttachEBSVolume	122
AWSSupport-CalculateEBSPerformanceMetrics	123
AWS-CopySnapshot	130

AWS-CreateSnapshot	131
AWS-DeleteSnapshot	132
AWSConfigRemediation-DeleteUnusedEBSVolume	133
AWS-DeregisterAMIs	134
AWS-DetachEBSVolume	136
AWSConfigRemediation-EnableEbsEncryptionByDefault	137
AWS-ExtendEbsVolume	139
AWSSupport-ModifyEBSSnapshotPermission	141
AWSConfigRemediation-ModifyEBSVolumeType	143
Amazon EC2	145
AWS-ASGEnterStandby	147
AWS-ASGExitStandby	148
AWS-CreateImage	149
AWS-DeleteImage	151
AWS-PatchAsgInstance	152
AWS-PatchInstanceWithRollback	155
AWS-QuarantineEC2Instance	157
AWS-ResizeInstance	159
AWS-RestartEC2Instance	160
AWS-SetupJupyter	161
AWS-StartEC2Instance	165
AWS-StopEC2Instance	165
AWS-TerminateEC2Instance	166
AWS-UpdateLinuxAmi	167
AWS-UpdateWindowsAmi	170
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck	174
AWSConfigRemediation-EnforceEC2InstanceIMDSv2	175
AWSEC2-CloneInstanceAndUpgradeSQLServer	177
AWSEC2-CloneInstanceAndUpgradeWindows	181
AWSEC2-ConfigureSTIG	185
AWSEC2-PatchLoadBalancerInstance	221
AWSEC2-SQLServerDBRestore	223
AWSSupport-ActivateWindowsWithAmazonLicense	228
AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2	231
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD	236
AWSSupport-CheckXenToNitroMigrationRequirements	242

AWSSupport-ConfigureEC2Metadata	245
AWSSupport-ContainEC2Instance	248
AWSSupport-CopyEC2Instance	259
AWSSupport-EnableWindowsEC2SerialConsole	265
AWSSupport-ExecuteEC2Rescue	273
AWSSupport-ListEC2Resources	276
AWSSupport-ManageRDPSettings	279
AWSSupport-ManageWindowsService	281
AWSSupport-MigrateEC2ClassicToVPC	283
AWSSupport-MigrateXenToNitroLinux	289
AWSSupport-ResetAccess	302
AWSSupport-ResetLinuxUserPassword	304
AWSPremiumSupport-ResizeNitroInstance	311
AWSSupport-RestoreEC2InstanceFromSnapshot	318
AWSSupport-SendLogBundleToS3Bucket	323
AWSSupport-StartEC2RescueWorkflow	325
AWSPremiumSupport-TroubleshootEC2DiskUsage	335
AWSSupport-TroubleshootEC2InstanceConnect	340
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs	346
AWSSupport-TroubleshootRDP	349
AWSSupport-TroubleshootSSH	355
AWSSupport-TroubleshootSUSERegistration	359
AWSSupport-TroubleshootWindowsPerformance	361
AWSSupport-TroubleshootWindowsUpdate	368
AWSSupport-UpgradeWindowsAWSDrivers	375
Amazon ECS	379
AWSSupport-CollectECSInstanceLogs	379
AWS-InstallAmazonECSAgent	382
AWS-ECSRunTask	384
AWSSupport-TroubleshootECSContainerInstance	388
AWSSupport-TroubleshootECSTaskFailedToStart	390
AWS-UpdateAmazonECSAgent	394
Amazon EFS	396
AWSSupport-CheckAndMountEFS	396
Amazon EKS	399
AWSSupport-CollectEKSInstanceLogs	400

AWS-CreateEKSClusterWithFargateProfile	402
AWS-CreateEKSClusterWithNodegroup	405
AWS-DeleteEKSCluster	409
AWS-MigrateToNewEKSSelfManagedNodeGroup	412
AWSPremiumSupport-TroubleshootEKSCluster	418
AWSSupport-TroubleshootEKSWorkerNode	422
AWS-UpdateEKSCluster	424
AWS-UpdateEKSMangedNodeGroup	426
AWS-UpdateEKSSelfManagedLinuxNodeGroups	430
AWSSupport-SetupK8sApiProxyForEKS	434
AWSSupport-TroubleshootEbsCsiDriversForEks	445
Elastic Beanstalk	454
AWSSupport-CollectElasticBeanstalkLogs	454
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ..	457
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications	459
AWSSupport-TroubleshootElasticBeanstalk	460
Sistema di bilanciamento del carico elastico	463
AWSConfigRemediation-DropInvalidHeadersForALB	464
AWS-EnableCLBAccessLogs	465
AWS-EnableCLBConnectionDraining	467
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing	469
AWSConfigRemediation-EnableELBDeletionProtection	470
AWSConfigRemediation-EnableLoggingForALBAndCLB	472
AWSSupport-TroubleshootCLBConnectivity	473
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing	476
AWS-UpdateALBDesyncMitigationMode	478
AWS-UpdateCLBDesyncMitigationMode	480
Amazon EMR	482
AWSSupport-AnalyzeEMRLogs	482
AWSSupport-DiagnoseEMRLogsWithAthena	488
OpenSearch Servizio Amazon	496
AWSConfigRemediation-DeleteOpenSearchDomain	497
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain	498
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups	499
AWSSupport-TroubleshootOpenSearchRedYellowCluster	501
AWSSupport-TroubleshootOpenSearchHighCPU	507

EventBridge	513
AWS-AddOpsItemDedupStringToEventBridgeRule	514
AWS-DisableEventBridgeRule	515
AWS Glue	517
AWSSupport-TroubleshootGlueConnection	517
Amazon FSx	528
AWSSupport-ValidateFSxWindowsADConfig	528
GuardDuty	542
AWSConfigRemediation-CreateGuardDutyDetector	542
IAM	543
AWSSupport-TroubleshootIAMAccessDeniedEvents	544
AWS-AttachIAMToInstance	550
AWS-DeleteIAMInlinePolicy	553
AWSConfigRemediation-DeleteIAMRole	554
AWSConfigRemediation-DeleteIAMUser	556
AWSConfigRemediation-DeleteUnusedIAMGroup	558
AWSConfigRemediation-DeleteUnusedIAMPolicy	559
AWSConfigRemediation-DetachIAMPolicy	561
AWSConfigRemediation-EnableAccountAccessAnalyzer	562
AWSSupport-GrantPermissionsToIAMUser	564
AWSConfigRemediation-RemoveUserPolicies	569
AWSConfigRemediation-ReplaceIAMInlinePolicy	571
AWSConfigRemediation-RevokeUnusedIAMUserCredentials	572
AWSConfigRemediation-SetIAMPasswordPolicy	574
AWSSupport-ContainIAMPrincipal	577
Flusso di dati Amazon Kinesis	592
AWS-EnableKinesisStreamEncryption	592
AWS KMS	594
AWSConfigRemediation-CancelKeyDeletion	594
AWSConfigRemediation-EnableKeyRotation	595
Lambda	597
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing	597
AWSConfigRemediation-DeleteLambdaFunction	599
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK	600
AWSConfigRemediation-MoveLambdaToVPC	602
AWSSupport-RemediateLambdaS3Event	603

AWSSupport-TroubleshootLambdaInternetAccess	606
AWSSupport-TroubleshootLambdaS3Event	610
Amazon Managed Workflows for Apache Airflow	612
AWSSupport-TroubleshootMWAAEnvironmentCreation	612
Neptune	619
AWS-EnableNeptuneDbAuditLogsToCloudWatch	619
AWS-EnableNeptuneDbBackupRetentionPeriod	621
AWS-EnableNeptuneClusterDeletionProtection	623
Amazon RDS	624
AWS-CreateEncryptedRdsSnapshot	625
AWS-CreateRdsSnapshot	628
AWSConfigRemediation-DeleteRDSCluster	629
AWSConfigRemediation-DeleteRDSClusterSnapshot	631
AWSConfigRemediation-DeleteRDSInstance	632
AWSConfigRemediation-DeleteRDSInstanceSnapshot	634
AWSConfigRemediation-DisablePublicAccessToRDSInstance	635
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster	637
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance	639
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance	640
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS	642
AWSConfigRemediation-EnableMultiAZOnRDSInstance	644
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance	646
AWSConfigRemediation-EnableRDSClusterDeletionProtection	648
AWSConfigRemediation-EnableRDSInstanceBackup	649
AWSConfigRemediation-EnableRDSInstanceDeletionProtection	652
AWSConfigRemediation-ModifyRDSInstancePortNumber	653
AWSSupport-ModifyRDSSnapshotPermission	655
AWSPremiumSupport-PostgreSQLWorkloadReview	657
AWS-RebootRdsInstance	673
AWSSupport-ShareRDSSnapshot	674
AWS-StartRdsInstance	678
AWS-StartStopAuroraCluster	679
AWS-StopRdsInstance	681
AWSSupport-TroubleshootConnectivityToRDS	682
AWSSupport-TroubleshootRDSIAMAuthentication	684
AWSSupport-ValidateRdsNetworkConfiguration	692

Amazon Redshift	698
AWSConfigRemediation-DeleteRedshiftCluster	698
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster	700
AWSConfigRemediation-EnableRedshiftClusterAuditLogging	701
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot	703
AWSConfigRemediation-EnableRedshiftClusterEncryption	704
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting	706
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster	707
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings	709
AWSConfigRemediation-ModifyRedshiftClusterNodeType	711
Amazon S3	713
AWS-ArchiveS3BucketToIntelligentTiering	714
AWS-ConfigureS3BucketLogging	716
AWS-ConfigureS3BucketVersioning	718
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock	719
AWSConfigRemediation-ConfigureS3PublicAccessBlock	721
AWS-CreateS3PolicyToExpireMultipartUploads	724
AWS-DisableS3BucketPublicReadWrite	726
AWS-EnableS3BucketEncryption	726
AWS-EnableS3BucketKeys	728
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy	730
AWSConfigRemediation-RestrictBucketSSLRequestsOnly	731
AWSSupport-TroubleshootS3PublicRead	732
AWSSupport-EmptyS3Bucket	738
AWSSupport-TroubleshootS3EventNotifications	745
AWSSupport-ContainS3Resource	752
Amazon SES	761
AWSSupport-AnalyzeSESMessagesSendingStatus	761
SageMaker AI	765
AWS-DisableSageMakerNotebookRootAccess	765
Secrets Manager	768
AWSConfigRemediation-DeleteSecret	768
AWSConfigRemediation-RotateSecret	769
Security Hub	771
AWSConfigRemediation-EnableSecurityHub	771
AWS Shield	773

AWSPremiumSupport-DDoSResiliencyAssessment	773
Amazon SNS	782
AWS-EnableSNSTopicDeliveryStatusLogging	782
AWSConfigRemediation-EncryptSNSTopic	785
AWS-PublishSNSNotification	786
Amazon SQS	787
AWS-EnableSQSEncryption	788
Step Functions	790
AWS-EnableStepFunctionsStateMachineLogging	790
Systems Manager	792
AWS-BulkDeleteAssociation	793
AWS-BulkEditOpsItems	794
AWS-BulkResolveOpsItems	797
AWS-ConfigureMaintenanceWindows	800
AWS-CreateManagedLinuxInstance	801
AWS-CreateManagedWindowsInstance	804
AWSConfigRemediation-EnableCWLoggingForSessionManager	806
AWS-ExportOpsDataToS3	808
AWS-ExportPatchReportToS3	810
AWS-SetupInventory	811
AWS-SetupManagedInstance	816
AWS-SetupManagedRoleOnEC2Instance	817
AWSSupport-TroubleshootManagedInstance	818
AWSSupport-TroubleshootPatchManagerLinux	821
AWSSupport-TroubleshootSessionManager	824
Terze parti	830
AWS-CreateJiraIssue	830
AWS-CreateServiceNowIncident	832
AWS-RunPacker	834
Amazon VPC	836
AWS-CloseSecurityGroup	837
AWSSupport-ConfigureDNSQueryLogging	838
AWSSupport-ConfigureTrafficMirroring	842
AWSSupport-ConnectivityTroubleshooter	844
AWSSupport-TroubleshootVPN	848
AWSConfigRemediation-DeleteEgressOnlyInternetGateway	854

AWSConfigRemediation-DeleteUnusedENI	855
AWSConfigRemediation-DeleteUnusedSecurityGroup	857
AWSConfigRemediation-DeleteUnusedVPCNetworkACL	858
AWSConfigRemediation-DeleteVPCFlowLog	859
AWSConfigRemediation-DetachAndDeleteInternetGateway	861
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway	862
AWS-DisableIncomingSSHOnPort22	864
AWS-DisablePublicAccessForSecurityGroup	866
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP	867
AWSSupport-EnableVPCFlowLogs	868
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch	875
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket	877
AWS-ReleaseElasticIP	879
AWS-RemoveNetworkACLUnrestrictedSSHRDP	880
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules	882
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules	883
AWSSupport-SetupIPMonitoringFromVPC	884
AWSSupport-TerminateIPMonitoringFromVPC	897
AWS WAF	900
AWS-AddWAFRegionalRuleToRuleGroup	901
AWS-AddWAFRegionalRuleToWebAcl	903
AWSConfigRemediation-EnableWAFClassicLogging	906
AWSConfigRemediation-EnableWAFClassicRegionalLogging	907
AWSConfigRemediation-EnableWAFV2Logging	909
Amazon WorkSpaces	911
AWS-CreateWorkSpace	911
AWSSupport-RecoverWorkSpace	914
X-Ray	918
AWSConfigRemediation-UpdateXRayKMSKey	918
.....	cmxxi

Riferimento al runbook del servizio di automazione di Systems Manager

Per aiutarti a iniziare rapidamente, AWS Systems Manager fornisce runbook predefiniti. Questi runbook sono gestiti da Amazon Web Services Supporto AWS e AWS Config. Il riferimento al runbook descrive ciascuno dei runbook predefiniti forniti da Systems Manager e. Supporto AWS Config

Important

Se si esegue un flusso di lavoro di automazione che chiama altri servizi utilizzando un ruolo di servizio (IAM) AWS Identity and Access Management , tenere presente che tale ruolo di servizio deve essere configurato con l'autorizzazione per la chiamata di tali servizi. Questo requisito si applica a tutti i runbook Automation di AWS (runbook di AWS-*) come i runbook di AWS-ConfigureS3BucketLogging, AWS-CreateDynamoDBBackup, e AWS-RestartEC2Instance, per citarne alcuni. Questo requisito si applica anche a tutti i runbook di automazione personalizzati creati dall'utente che richiamano altri AWS servizi utilizzando azioni che richiamano altri servizi. Ad esempio, se utilizzi le operazioni `aws:executeAwsApi`, `aws:createStack` o `aws:copyImage`, allora dovrai configurare il ruolo di servizio con l'autorizzazione per richiamare questi servizi. Puoi abilitare le autorizzazioni per altri AWS servizi aggiungendo una policy in linea IAM al ruolo. Per ulteriori informazioni, consulta [Aggiungere una policy in linea di automazione per richiamare](#) altri servizi. AWS

Questo riferimento include argomenti che descrivono ciascuno dei runbook di Systems Manager di proprietà di AWS Supporto AWS, e AWS Config. I runbook sono organizzati in base ai pertinenti. Servizio AWS Ogni pagina fornisce una spiegazione dei parametri obbligatori e facoltativi che è possibile specificare quando si utilizza il runbook. Ogni pagina elenca anche i passaggi del runbook e l'eventuale output dell'automazione.

Questo riferimento non include una pagina separata per i runbook che richiedono l'approvazione, come il runbook `AWS-CreateManagedLinuxInstanceWithApproval` o `AWS-StopEC2InstanceWithApproval`. Qualsiasi nome di runbook che include `WithApproval` significa che il runbook include l'azione. [aws:approve](#) Questa azione sospende temporaneamente

un'automazione fino a quando i responsabili designati non approvano o rifiutano l'azione. Una volta raggiunto il numero richiesto di approvazioni, viene ripresa l'automazione.

[Per informazioni sull'esecuzione delle automazioni, consulta Esecuzione di un'automazione semplice.](#) Per informazioni sull'esecuzione di automazioni su più destinazioni, consulta [Esecuzione di automazioni che utilizzano obiettivi e](#) controlli di frequenza.

Argomenti

- [Visualizza il contenuto del runbook](#)
- [API Gateway](#)
- [AWS Batch](#)
- [AWS CloudFormation](#)
- [CloudFront](#)
- [CloudTrail](#)
- [CloudWatch](#)
- [Amazon DocumentDB](#)
- [CodeBuild](#)
- [AWS CodeDeploy](#)
- [AWS Config](#)
- [Amazon Connect](#)
- [AWS Directory Service](#)
- [AWS AppSync](#)
- [Amazon Athena](#)
- [DynamoDB](#)
- [AWS Database Migration Service](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [Amazon ECS](#)
- [Amazon EFS](#)
- [Amazon EKS](#)
- [Elastic Beanstalk](#)

- [Sistema di bilanciamento del carico elastico](#)
- [Amazon EMR](#)
- [OpenSearch Servizio Amazon](#)
- [EventBridge](#)
- [AWS Glue](#)
- [Amazon FSx](#)
- [GuardDuty](#)
- [IAM](#)
- [Flusso di dati Amazon Kinesis](#)
- [AWS KMS](#)
- [Lambda](#)
- [Amazon Managed Workflows for Apache Airflow](#)
- [Neptune](#)
- [Amazon RDS](#)
- [Amazon Redshift](#)
- [Amazon S3](#)
- [Amazon SES](#)
- [SageMaker AI](#)
- [Secrets Manager](#)
- [Security Hub](#)
- [AWS Shield](#)
- [Amazon SNS](#)
- [Amazon SQS](#)
- [Step Functions](#)
- [Systems Manager](#)
- [Terze parti](#)
- [Amazon VPC](#)
- [AWS WAF](#)
- [Amazon WorkSpaces](#)

- [X-Ray](#)

Visualizza il contenuto del runbook

È possibile visualizzare il contenuto dei runbook nella console Systems Manager.

Per visualizzare il contenuto dei runbook

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegliere Documents (Documenti).

oppure

Se la AWS Systems Manager home page si apre per prima, scegli l'icona del menu



per aprire il riquadro di navigazione, quindi scegli Documenti nel riquadro di navigazione.

3. Nella sezione Categorie, scegli Documenti di automazione.
4. Scegliere un documento, quindi scegliere View details (Visualizza dettagli).
5. Scegliere la scheda Content (Contenuti).

API Gateway

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon API Gateway.

Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

AWSConfigRemediation-DeleteAPIGatewayStage

Descrizione

Il `AWSConfigRemediation-DeleteAPIGatewayStage` runbook elimina una fase di Amazon API Gateway (API Gateway). AWS Config deve essere abilitato nel luogo in Regione AWS cui esegui questa automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `StageArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) della fase API Gateway che desideri eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

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

Fasi del documento

- `aws:executeScript`- Elimina lo stadio API Gateway specificato nel `StageArn` parametro.

AWSConfigRemediation-EnableAPIGatewayTracing

Descrizione

Il `AWSConfigRemediation-EnableAPIGatewayTracing` runbook consente il tracciamento su una fase di Amazon API Gateway (API Gateway). AWS Config deve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- StageArn

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) dello stadio API Gateway su cui desideri abilitare il tracing.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Abilita il tracciamento nella fase API Gateway specificata nel `StageArn` parametro.

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

Descrizione

Il `AWSConfigRemediation-UpdateAPIGatewayMethodCaching` runbook aggiorna l'impostazione del metodo cache per una risorsa di fase Amazon API Gateway.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- CachingAuthorizedMethods

Tipo: StringList

Descrizione: (Obbligatorio) I metodi autorizzati per abilitare la memorizzazione nella cache. L'elenco deve essere una combinazione di DELETEGET, HEAD, OPTIONS, PATCHPOST, e PUT. La memorizzazione nella cache è abilitata per i metodi selezionati e disabilitata per i metodi non selezionati. La memorizzazione nella cache è abilitata per tutti i metodi se ANY è selezionata e disabilitata per tutti i metodi se NONE è selezionata.

- StageArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN della fase API Gateway per l'RESTAPI.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Accetta l'ID della risorsa dello stage come input, aggiorna l'impostazione del metodo cache per una fase API Gateway utilizzando l'azione `UpdateStage API` e verifica l'aggiornamento.

AWS Batch

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Batch Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-TroubleshootAWSBatchJob](#)

AWSSupport-TroubleshootAWSBatchJob

Descrizione

Il `AWSSupport-TroubleshootAWSBatchJob` runbook consente di risolvere i problemi che impediscono a un AWS Batch job di passare dallo stato precedente. `RUNNABLE STARTING`

Come funziona?

Questo runbook esegue i seguenti controlli:

- Se l'ambiente di calcolo è in uno stato `INVALID` or `DISABLED`.
- Se il `Max vCPU` parametro dell'ambiente di calcolo è sufficientemente grande da contenere il volume di lavori nella coda dei lavori.
- Se i job richiedono più risorse v CPUs o di memoria rispetto a quelle fornite dai tipi di istanza dell'ambiente di calcolo.
- Se i processi devono essere eseguiti su istanze basate su GPU ma l'ambiente di calcolo non è configurato per utilizzare istanze basate su GPU.
- Se il gruppo Auto Scaling per l'ambiente di calcolo non è riuscito ad avviare le istanze.
- Se le istanze avviate possono unirsi al cluster Amazon Elastic Container Service (Amazon ECS) sottostante, in caso contrario, esegue il runbook. [AWSSupport-TroubleshootECSContainerInstance](#)

- Se c'è un problema di autorizzazioni che blocca azioni specifiche necessarie per eseguire il lavoro.

Important

- Questo runbook deve essere avviato nella stessa AWS regione del job il cui stato è bloccato. RUNNABLE
- Questo runbook può essere avviato per i AWS Batch lavori pianificati su istanze Amazon ECS o AWS Fargate Amazon Elastic Compute Cloud (Amazon). EC2 Se l'automazione viene avviata per un AWS Batch processo su Amazon Elastic Kubernetes Service (Amazon EKS), l'iniziazione si interrompe.
- Se le istanze sono disponibili per eseguire il job ma non riescono a registrare il cluster Amazon ECS, questo runbook avvia il runbook di `AWSSupport-TroubleshootECSTaskInstance` automazione per cercare di determinare il motivo. Per ulteriori informazioni, consulta il runbook. [AWSSupport-TroubleshootECSTaskInstance](#)

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- JobId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del AWS Batch Job il cui RUNNABLE stato è bloccato.

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

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Istruzioni

1. Accedere a [AWSSupport-TroubleshootAWSBatchJob](#) nella AWS Systems Manager console.
2. Seleziona Execute Automation
3. Per i parametri di input, inserisci quanto segue:
 - `AutomationAssumeRole`(Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `JobId`(Obbligatorio):

L'ID del AWS Batch Job bloccato nello RUNNABLE stato.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Choose an option

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

b9e32

4. Seleziona Esegui.

5. Notate che l'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- PreflightPermissionChecks:

Esegue controlli preliminari delle autorizzazioni IAM rispetto all'utente/ruolo iniziante. Se mancano delle autorizzazioni, questo passaggio fornisce le azioni API mancanti nella sezione Global Output.

- ProceedOnlyIfUserHasPermission:

I rami dipendono dal fatto che si disponga delle autorizzazioni necessarie per eseguire tutte le azioni richieste per il runbook.

- AWSBatchJobEvaluation:

Esegue controlli sul AWS Batch Job verificandone l'esistenza e lo RUNNABLE stato.

- ProceedOnlyIfBatchJobExistsAndIsInRunnableStato:

Succursali in base al fatto che il lavoro esista e sia RUNNABLE disponibile.

- BatchComputeEnvironmentEvaluation:

Esegue controlli rispetto all'ambiente di AWS Batch calcolo.

- ProceedOnlyIfComputeEnvironmentChecksAreOK:

Filiali in base all'esito dei controlli dell'ambiente di calcolo.

- UnderlyingInfraEvaluation:

Esegue controlli rispetto all'Auto Scaling Group o Spot Fleet Request sottostante.

- ProceedOnlyIfInstancesNotJoiningEcsCluster:

Filiali in base all'eventuale presenza di istanze che non si uniscono al cluster Amazon ECS.

- EcsAutomationRunner:

Esegue l'automazione Amazon ECS per le istanze che non entrano a far parte del cluster.

- ExecutionResults:

Genera output in base ai passaggi precedenti.

7. Dopo il completamento, viene fornito l'URI per il file HTML del rapporto di valutazione:

Collegamento alla console S3 e URI Amazon S3 per il report sull'esecuzione riuscita del runbook

▼ Outputs

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

[INFO]: Reviewing Compute Environment "ComputeEnvironment-eqMKnNEEWmt8eY":
[ERROR]: Job "411-██████████606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-eqMKnNEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/updating-compute-environments.html
[WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-eqMKnNEEWmt8eY".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your Instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html
[ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.

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

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

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

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

[INFO]: Reviewing Compute Environment "ComputeEnvironment-eqMKnNEEWmt8eY":
[ERROR]: Job "411-██████████606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-eqMKnNEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/updating-compute-environments.html
[WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-eqMKnNEEWmt8eY".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your Instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html
[ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.
```

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS CloudFormation

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS CloudFormation
Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

AWS-DeleteCloudFormationStack

Descrizione

Eliminare una AWS CloudFormation pila.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- StackNameOrId

Tipo: stringa

Descrizione: (Obbligatorio) Nome o ID univoco dello CloudFormation stack da eliminare

AWS-EnableCloudFormationSNSNotification

Descrizione

Il AWS-EnableCloudFormationSNSNotification runbook abilita le notifiche Amazon Simple Notification Service (Amazon SNS) per lo stack AWS CloudFormation (AWS CloudFormation) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- StackArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN o il nome dello AWS CloudFormation stack per cui desideri abilitare le notifiche Amazon SNS.

- NotificationArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN dell'argomento Amazon SNS che desideri associare allo stack. AWS CloudFormation

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm: GetAutomationExecution
- ssm: StartAutomationExecution
- formazione di nuvole: DescribeStacks
- formazione di nuvole: UpdateStack
- kms:Decrypt
- kms:GenerateDataKey
- sns:Publish
- sqs: GetQueueAttributes

Fasi del documento

- CheckCfnSnsLimits (aws:executeScript) - Verifica che il numero massimo di argomenti di Amazon SNS non sia già stato associato AWS CloudFormation allo stack specificato.
- EnableCfnSnsNotification (aws:executeAwsApi) - Abilita le notifiche Amazon SNS per lo AWS CloudFormation stack.
- VerificationCfnSnsNotification (aws:executeScript) - Verifica che le notifiche Amazon SNS siano state abilitate per AWS CloudFormation lo stack.

Output

`CheckCfnSnsLimits`. `NotificationArnList` - Un elenco di quelli ARNs che ricevono notifiche Amazon SNS per lo AWS CloudFormation stack.

`VerificationCfnSnsNotification`. `VerifySnsTopicsResponse` - Risposta dell'operazione API che conferma che le notifiche di Amazon SNS sono state abilitate per AWS CloudFormation lo stack.

AWS-RunCfnLint

Descrizione

Questo runbook utilizza un [AWS CloudFormation Linter](#) (`cfn-python-lint`) per convalidare i modelli YAML e JSON rispetto alle specifiche delle risorse. AWS CloudFormation Il AWS-RunCfnLint runbook esegue controlli aggiuntivi, ad esempio garantendo che siano stati immessi valori validi per le proprietà delle risorse. Se la convalida non ha esito positivo, il passaggio `RunCfnLintAgainstTemplate` non riesce e l'output dello strumento linter viene fornito in un messaggio di errore. Questo runbook utilizza `cfn-lint` v0.24.4.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `ConfigureRuleFlag`

Tipo: stringa

Descrizione: (Facoltativo) Opzioni di configurazione per passare una regola al parametro `--configure-rule`.

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

- FormatFlag

Tipo: stringa

Descrizione: (Facoltativo) Valore da passare al parametro `--format` per specificare il formato di output.

Valori validi: Default | quiet | parseable | json

Impostazione predefinita: Default

- IgnoreChecksFlag

Tipo: stringa

Descrizione: (Facoltativa) IDs delle regole da passare al parametro `--ignore-checks`. Queste regole non sono controllate.

Esempio: E1001, E1003, W7001

- IncludeChecksFlag

Tipo: stringa

Descrizione: (Facoltativa) IDs delle regole da passare al parametro. `--include-checks` Queste regole sono controllate.

Esempio: E1001, E1003, W7001

- InfoFlag

Tipo: stringa

Descrizione: (Facoltativo) Opzione per il parametro `--info`. Includere l'opzione per abilitare ulteriori informazioni di registrazione sull'elaborazione del modello.

Impostazione predefinita: false

- **TemplateFileName**

Tipo: stringa

Descrizione: il nome o la chiave del file modello nel bucket S3.

- **Modelli 3 BucketName**

Tipo: stringa

Descrizione: il nome del bucket S3 contenente il modello di packer.

- **RegionsFlag**

Tipo: stringa

Descrizione: (Facoltativo) Valori da passare al `--regions` parametro for per testare il modello rispetto a quanto specificato. Regioni AWS

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

Fasi del documento

RunCfnLintAgainstTemplate — Esegue lo `cfn-python-lint` strumento sul AWS CloudFormation modello specificato.

Output

RunCfnLintAgainstTemplate.output — Lo stdout dello strumento. `cfn-python-lint`

AWSSupport-TroubleshootCFNCustomResource

Descrizione

Il **AWSSupport-TroubleshootCFNCustomResource** runbook aiuta a diagnosticare il motivo per cui uno AWS CloudFormation stack non è riuscito a creare, aggiornare o eliminare una risorsa personalizzata. Il runbook controlla il token di servizio utilizzato per la risorsa personalizzata e il messaggio di errore restituito. Dopo aver esaminato i dettagli della risorsa personalizzata, l'output del runbook fornisce una spiegazione del comportamento dello stack e le procedure di risoluzione dei problemi per la risorsa personalizzata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- StackName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome dello AWS CloudFormation stack in cui la risorsa personalizzata ha avuto esito negativo.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- cloudformation:ListStackResources
- ec2:DescribeRouteTables
- ec2:DescribeNatGateways

- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeSubnets`
- `logs:FilterLogEvents`

Fasi del documento

- `validateCloudFormationStack`- Verifica che lo AWS CloudFormation stack esista nello stesso e. Account AWS Regione AWS
- `checkCustomResource`- Analizza lo AWS CloudFormation stack, verifica la risorsa personalizzata guasta e fornisce informazioni su come risolvere i problemi relativi alla risorsa personalizzata guasta.

AWS-UpdateCloudFormationStack

Descrizione

Aggiorna uno AWS CloudFormation stack utilizzando un AWS CloudFormation modello archiviato in un bucket Amazon S3.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `LambdaAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo assunto da Lambda

- `StackNameOrId`

Tipo: stringa

Descrizione: (Obbligatorio) Nome o ID univoco dello AWS CloudFormation stack da aggiornare

- `TemplateUrl`

Tipo: stringa

Descrizione: (Obbligatoria) posizione del bucket S3 che contiene il modello aggiornato CloudFormation (ad es. `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`)

CloudFront

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. CloudFront Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

AWSConfigRemediation-EnableCloudFrontDefaultRootObject

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontDefaultRootObject` runbook configura l'oggetto root predefinito per la distribuzione Amazon CloudFront (CloudFront) specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- CloudFrontDistributionId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della CloudFront distribuzione per cui desideri configurare l'oggetto root predefinito.

- DefaultRootObject

Tipo: stringa

Descrizione: (Obbligatorio) L'oggetto che desideri CloudFront restituire quando una richiesta di un visualizzatore punta all'URL principale.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Configura l'oggetto root predefinito per la CloudFront distribuzione specificata nel `CloudFrontDistributionId` parametro.

AWSConfigRemediation-EnableCloudFrontAccessLogs

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontAccessLogs` runbook consente la registrazione degli accessi per la distribuzione Amazon CloudFront (CloudFront) specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon Simple Storage Service (Amazon S3) in cui desideri archiviare i log di accesso. I bucket in af-south-1, ap-east-1, eu-south-1 e me-south-1 non sono supportati. Regione AWS

- CloudFrontId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della distribuzione a cui desideri abilitare la registrazione degli accessi. CloudFront

- IncludeCookies

Tipo: Booleano

Valori validi: true | false

Descrizione: (Obbligatorio) Imposta questo parametro su true, se desideri che i cookie vengano inclusi nei log di accesso.

- Prefix

Tipo: stringa

Descrizione: (Facoltativo) Una stringa opzionale che desideri aggiungere CloudFront come prefisso al registro filenames degli accessi della tua distribuzione, ad esempio, `myprefix/`

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

- `cloudfront:GetDistribution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:UpdateDistribution`
- `s3:GetBucketLocation`
- `s3:GetBucketAcl`
- `s3:PutBucketAcl`

Note

L'`s3:GetBucketLocationAPI` può essere utilizzata solo per i bucket S3 nello stesso account. Non puoi utilizzarla per bucket S3 con più account.

Fasi del documento

- `aws:executeScript`- Abilita la registrazione degli accessi per la CloudFront distribuzione specificata nel parametro. `CloudFrontDistributionId`

AWSConfigRemediation- EnableCloudFrontOriginAccessIdentity

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity` runbook abilita l'identità di accesso all'origine per la distribuzione Amazon CloudFront (CloudFront) specificata. Questa automazione assegna la stessa CloudFront Origin Access Identity a tutte le Origin del tipo Origin di Amazon Simple Storage Service (Amazon S3) senza identità di accesso all'origine per la distribuzione specificata. CloudFront Questa automazione non concede l'autorizzazione di lettura all'identità di accesso di origine per accedere CloudFront agli oggetti nel tuo bucket Amazon S3. È necessario aggiornare le autorizzazioni del bucket Amazon S3 per consentire l'accesso.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- CloudFrontDistributionId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della CloudFront distribuzione su cui desideri abilitare il failover di origine.

- OriginAccessIdentityId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'identità di accesso di CloudFront origine da associare all'origine.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Abilita l'identità di accesso all'origine per la CloudFront distribuzione specificata nel `CloudFrontDistributionId` parametro e verifica che l'identità di accesso all'origine sia stata assegnata.

AWSConfigRemediation-EnableCloudFrontOriginFailover

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontOriginFailover` runbook abilita il failover di origine per la distribuzione Amazon CloudFront (CloudFront) specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `CloudFrontDistributionId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della CloudFront distribuzione su cui desideri abilitare il failover di origine.

- **OriginGroupId**

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gruppo di origine.

- **PrimaryOriginId**

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'origine principale nel gruppo di origine.

- **SecondaryOriginId**

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'origine secondaria nel gruppo di origine.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Abilita il failover di origine per la CloudFront distribuzione specificata nel `CloudFrontDistributionId` parametro e verifica che il failover sia stato abilitato.

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

Descrizione

Il `AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS` runbook abilita la politica del protocollo del visualizzatore per la distribuzione Amazon CloudFront (CloudFront) specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- CloudFrontDistributionId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della CloudFront distribuzione su cui desideri abilitare la policy del protocollo del visualizzatore.

- ViewerProtocolPolicy

Tipo: stringa

Valori validi: https-only, redirect-to-https

Descrizione: (Obbligatorio) Il protocollo che gli utenti possono utilizzare per accedere ai file nell'origine.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution

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

Fasi del documento

- `aws:executeScript`- Abilita la politica del protocollo del visualizzatore per la CloudFront distribuzione specificata nel `CloudFrontDistributionId` parametro e verifica che la politica sia stata assegnata.

CloudTrail

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS CloudTrail Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

Descrizione

Il `AWSConfigRemediation-CreateCloudTrailMultiRegionTrail` runbook crea un AWS CloudTrail (CloudTrail) trail che invia file di log da più file Regioni AWS al bucket Amazon Simple Storage Service (Amazon S3) di tua scelta.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 in cui desideri caricare i log.

- KeyPrefix

Tipo: stringa

Descrizione: (Facoltativo) Il prefisso chiave di Amazon S3 che segue il nome del bucket che hai designato per la consegna dei file di registro.

- TrailName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del CloudTrail percorso da creare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeAwsApi`- Accetta il nome del percorso e il nome del bucket Amazon S3 come input e crea un percorso. CloudTrail
- `aws:executeAwsApi`- Abilita la registrazione sul percorso creato e avvia la consegna dei log al bucket Amazon S3 specificato.
- `aws:assertAwsResourceProperty`- Verifica che il CloudTrail percorso sia stato creato.

AWS-EnableCloudTrail

Descrizione

Crea un AWS CloudTrail percorso e configura la registrazione su un bucket S3.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- S3 BucketName

Tipo: stringa

Descrizione: (obbligatoria) nome del bucket S3 designato per la pubblicazione dei file di log.

Note

Il bucket S3 deve esistere e la policy del bucket deve concedere a CloudTrail l'autorizzazione di scrittura nel bucket stesso. Per informazioni, consulta [Amazon S3 Bucket Policy](#) per. CloudTrail

- TrailName

Tipo: stringa

Descrizione: (obbligatorio) nome del nuovo trail.

AWS-EnableCloudTrailCloudWatchLogs

Descrizione

Questo runbook aggiorna la configurazione di uno o più AWS CloudTrail trail per inviare eventi a un gruppo di log di Amazon CloudWatch Logs.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- CloudWatchLogsLogGroupArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del gruppo di log CloudWatch Logs in cui verranno CloudTrail consegnati i log.

- CloudWatchLogsRoleArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo IAM CloudWatch Logs Logs presuppone la scrittura nel gruppo di log specificato.

- TrailNames

Tipo: StringList

Descrizione: (Obbligatorio) Un elenco separato da virgole dei nomi dei CloudTrail percorsi di cui si desidera inviare gli eventi a Logs. CloudWatch

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Aggiorna i CloudTrail percorsi specificati per inviare gli eventi al gruppo di log CloudWatch Logs specificato.

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

Descrizione

Il `AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS` runbook crittografa un percorso AWS CloudTrail (CloudTrail) utilizzando la chiave gestita dal cliente AWS Key Management Service (AWS KMS) specificata. Questo runbook deve essere usato solo come base per garantire che i CloudTrail percorsi siano crittografati secondo le migliori pratiche di sicurezza minime consigliate. Ti consigliamo di crittografare più percorsi con chiavi KMS diverse. CloudTrail i file digest non sono crittografati. Se in precedenza avete impostato il `EnableLogFileValidation` parametro su `true` per il percorso, consultate la sezione «Utilizzare la crittografia lato server con chiavi AWS KMS gestite» dell'argomento [Procedure consigliate per la sicurezza CloudTrail preventiva](#) nella Guida per l'AWS CloudTrail utente per ulteriori informazioni.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- KMSKeyId

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN, l'ID della chiave o l'alias della chiave gestita dal cliente che desideri utilizzare per crittografare la traccia specificata nel parametro. `TrailName`

- TrailName

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN o il nome del percorso che desideri aggiornare per essere crittografato.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeAwsApi`- Abilita la crittografia sulla traccia specificata nel `TrailName` parametro.
- `aws:executeAwsApi`- Raccoglie l'ARN per la chiave gestita dal cliente specificata nel `KMSKeyId` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la crittografia sia stata abilitata durante il percorso. `CloudTrail`

AWS-EnableCloudTrailKmsEncryption

Descrizione

Questo runbook aggiorna la configurazione di uno o più AWS CloudTrail percorsi per utilizzare la crittografia AWS Key Management Service (AWS KMS).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- KMSKeyId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della chiave gestita dal cliente che desideri utilizzare per crittografare la traccia specificata nel `TrailName` parametro. Il valore può essere un nome alias preceduto da «alias/», un ARN completamente specificato in un alias o un ARN completamente specificato in una chiave.

- TrailNames

Tipo: StringList

Descrizione: (Obbligatorio) Un elenco separato da virgole dei percorsi che desideri aggiornare per la crittografia.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Abilita AWS KMS la crittografia sui percorsi specificati nel `TrailName` parametro.

AWSConfigRemediation-EnableCloudTrailLogFileValidation

Descrizione

Il `AWSConfigRemediation-EnableCloudTrailLogFileValidation` runbook consente la convalida dei file di registro per il percorso. AWS CloudTrail

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- TrailName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome o Amazon Resource Name (ARN) del percorso per il quale desideri abilitare la convalida dei log.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- aws:executeAwsApi- Abilita la convalida del registro per il AWS CloudTrail percorso specificato nel TrailName parametro.
- aws:assertAwsResourceProperty- Verifica che la convalida dei log sia abilitata per il percorso.

AWS-EnableCloudTrailLogFileValidation

Descrizione

Il AWS-EnableCloudTrailLogFileValidation runbook consente la convalida dei file di registro per i AWS CloudTrail percorsi specificati.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- TrailNames

Tipo: StringList

Descrizione: (Obbligatorio) Un elenco separato da virgole dei nomi dei CloudTrail percorsi per i quali si desidera abilitare la convalida dei log.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- cloudtrail:GetTrail
- cloudtrail:UpdateTrail

Fasi del documento

- `aws:executeScript`- Abilita la convalida dei log per i AWS CloudTrail percorsi specificati nel `TrailNames` parametro.

AWS-QueryCloudTrailLogs

Descrizione

Il `AWS-QueryCloudTrailLogs` runbook crea una tabella Amazon Athena dal bucket Amazon Simple Storage Service (Amazon S3) S3) di tua scelta contenente () log. AWS CloudTrail CloudTrail. Dopo aver creato la tabella, l'automazione esegue le query SQL specificate dall'utente e quindi elimina la tabella.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `Query`

Tipo: stringa

Descrizione: (Obbligatoria) La query SQL che si desidera eseguire.

- **SourceBucketPath**

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 contenente i file di CloudTrail log da interrogare.

- **TableName**

Tipo: stringa

Descrizione: (Facoltativo) Il nome della tabella Athena creata dall'automazione.

Impostazione predefinita: cloudtrail_logs

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

- `aws:executeAwsApi`- Crea una tabella Athena.
- `aws:executeAwsApi`- Esegue la stringa di query specificata nel Query parametro.
- `aws:executeScript`- Esegue sondaggi e attende il completamento della query.
- `aws:executeAwsApi`- Ottiene i risultati della query.
- `aws:executeAwsApi`- Elimina la tabella creata dall'automazione.

CloudWatch

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. CloudWatch
Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

AWS-ConfigureCloudWatchOnEC2Instance

Descrizione

Abilita o disabilita il monitoraggio CloudWatch dettagliato di Amazon sulle istanze gestite.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon su cui desideri abilitare il CloudWatch monitoraggio.

- properties

Tipo: stringa

Descrizione: (Facoltativo) Questo parametro non è supportato. È elencato qui per la compatibilità con le versioni precedenti.

- status

Valori validi: Abilitato | Disabilitato

Descrizione: (facoltativo) specifica se abilitare o disabilitare CloudWatch.

Impostazione predefinita: Enabled

Fasi del documento

configureCloudWatch - Si configura CloudWatch sull' EC2 istanza Amazon con lo stato specificato.

Output

Questa automazione non ha alcun risultato.

AWS-EnableCWAlarm

Descrizione

Il `AWS-EnableCWAlarm` runbook crea allarmi Amazon CloudWatch (CloudWatch) per AWS le risorse Account AWS che non ne hanno già uno. CloudWatch gli allarmi vengono creati per le seguenti risorse: AWS

- Istanze Amazon Elastic Compute Cloud (Amazon EC2)
- Volumi Amazon Elastic Block Store (Amazon EBS)
- Bucket Amazon Simple Storage Service (Amazon S3)
- Cluster Amazon Relational Database Service (Amazon RDS)

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `ComparisonOperator`

Tipo: stringa

Valori validi: `GreaterThanEqualToThreshold` | `GreaterThanThreshold` | `GreaterThanUpperThreshold` | `LessThanLowerOrGreaterThanUpperThreshold` | `LessThanLowerThreshold` | `LessThanEqualToThreshold` | `LessThanThreshold`

Descrizione: (Obbligatoria) L'operazione aritmetica da utilizzare per confrontare la statistica e la soglia specificate.

- MetricName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della metrica associata all'allarme.

- Periodo

Tipo: integer

Valori validi: 10 | 30 | 60 | Un multiplo di 60

Descrizione: (Obbligatorio) Il periodo, in secondi, durante il quale viene applicata la statistica.

- Risorsa ARNs

Tipo: StringList

Descrizione: (Obbligatorio) Un elenco separato da virgole ARNs delle risorse per cui creare un CloudWatch allarme

- Statistic

Tipo: stringa

Valori validi: Media | Massimo | Minimo | SampleCount | Somma

Descrizione: (Obbligatoria) La statistica per la metrica associata all'allarme.

- Threshold

Tipo: integer

Descrizione: (Obbligatorio) Il valore da confrontare con la statistica specificata.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudwatch:PutMetricAlarm`

Fasi del documento

- `aws:executeScript`- Crea un CloudWatch allarme in base ai valori specificati nei parametri del runbook per le risorse specificate nel `ResourceARNs` parametro.

Output

Abilita. `CWAlarm FailedResources`: Una mappatura delle risorse ARNs per le quali non è stato creato un CloudWatch allarme e il motivo dell'errore.

Abilita. `CWAlarm SuccessfulResources`: Un elenco di risorse ARNs per le quali è stato creato correttamente un CloudWatch allarme.

Amazon DocumentDB

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon DocumentDB (con compatibilità con MongoDB). Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-EnableDocDbClusterBackupRetentionPeriod](#)

AWS-EnableDocDbClusterBackupRetentionPeriod

Descrizione

Il `AWS-EnableDocDbClusterBackupRetentionPeriod` runbook consente un periodo di conservazione dei backup per il cluster Amazon DocumentDB specificato. Questa funzionalità imposta il numero totale di giorni per i quali viene conservato un backup automatico. Per modificare un cluster, il cluster deve essere nello stato disponibile con un tipo di motore `docdb`.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DBClusterResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della risorsa per il cluster Amazon DocumentDB per cui desideri abilitare il periodo di conservazione del backup.

- BackupRetentionPeriod

Tipo: integer

Descrizione: (Obbligatorio) Il numero di giorni per i quali vengono conservati i backup automatici. Deve essere un valore compreso tra 7 e 35 giorni.

- PreferredBackupWindow

Tipo: stringa

Descrizione: (Facoltativo) Un intervallo di tempo giornaliero in Universal Time Coordinated (UTC) nel formato hh24:mm-hh24:mm, ad esempio 07:14-07:44. Il valore deve essere di almeno 30 minuti e non può essere in conflitto con la finestra di manutenzione preferita.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- docdb:DescribeDBClusters

- `docdb:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- `GetDocDbClusterIdentifier` (`aws:executeAwsApi`) - Restituisce l'identificatore del cluster Amazon DocumentDB utilizzando l'ID di risorsa fornito.
- `VerifyDocDbEngine` (`aws:assertAwsResourceProperty`) - Verifica che il tipo `docdb` di motore Amazon DocumentDB serva a prevenire modifiche involontarie ad altri tipi di motore Amazon RDS.
- `VerifyDocDbStatus` (`aws:waitAwsResourceProperty`) - Verifica che lo stato del cluster Amazon DocumentDB sia `available`
- `ModifyDocDbRetentionPeriod` (`aws:executeAwsApi`) - Imposta il periodo di conservazione utilizzando i valori forniti per il cluster Amazon DocumentDB specificato.
- `VerifyDocDbBackupsEnabled` (`aws:executeScript`) - Verifica che il periodo di conservazione per il cluster Amazon DocumentDB e la finestra di backup preferita, se specificata, siano state impostate correttamente.

Output

`ModifyDocDbRetentionPeriod`. `ModifyDbClusterResponse` - Risposta dall'operazione `ModifyDBCluster` API.

`VerifyDocDbBackupsEnabled`. `VerifyDbClusterBackupsEnabledResponse` - Output della `VerifyDocDbBackupsEnabled` fase di conferma dell'avvenuta modifica del cluster Amazon DocumentDB.

CodeBuild

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS CodeBuild Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

Descrizione

Il `AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK` runbook crittografa gli artefatti di compilazione di un progetto AWS CodeBuild (CodeBuild) utilizzando la chiave gestita dal cliente AWS Key Management Service (AWS KMS) specificata. AWS Config deve essere abilitato nel luogo in Regione AWS cui si esegue questa automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- KMSKeyId

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) della chiave gestita AWS KMS dal cliente che desideri utilizzare per crittografare il CodeBuild progetto specificato nel parametro.

`ProjectId`

- ProjectId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del CodeBuild progetto di cui desideri crittografare gli artefatti di build.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeAwsApi`- Raccoglie il nome del CodeBuild progetto dall'ID del progetto.
- `aws:executeAwsApi`- Abilita la crittografia sul CodeBuild progetto specificato nel `ProjectId` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la crittografia sia stata abilitata nel CodeBuild progetto.

Output

`UpdateLambdaConfig`. `UpdateFunctionConfigurationResponse` - Risposta dalla chiamata `UpdateFunctionConfiguration` API.

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

Descrizione

Il `AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject` runbook elimina le variabili di `AWS_SECRET_ACCESS_KEY` ambiente `AWS_ACCESS_KEY_ID` e dal progetto AWS

CodeBuild (CodeBuild) specificato. AWS Config deve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- ResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del CodeBuild progetto di cui desideri eliminare le variabili di ambiente chiave di accesso.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

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

Fasi del documento

- `aws:executeScript`- Elimina le variabili di ambiente della chiave di accesso per il CodeBuild progetto specificato nel `ResourceId` parametro.

AWS CodeDeploy

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS CodeDeploy Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-TroubleshootCodeDeploy](#)

AWSSupport - TroubleshootCodeDeploy

Descrizione

Il `AWSSupport-TroubleshootCodeDeploy` runbook aiuta a diagnosticare il motivo per cui una AWS CodeDeploy distribuzione non è riuscita su un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Il runbook riporta i passaggi per aiutarti a risolvere il problema o a risolverlo ulteriormente. CodeDeploy Vengono inoltre fornite le migliori pratiche per aiutarti a evitare problemi simili in futuro.

Questo runbook può aiutarti a risolvere i seguenti problemi:

- L' CodeDeploy agente non è installato o non è in esecuzione sull' EC2istanza Amazon
- L' EC2 istanza Amazon non ha un profilo di istanza AWS Identity and Access Management (IAM) collegato
- Il profilo dell'istanza IAM collegato all' EC2 istanza Amazon non dispone delle autorizzazioni Amazon Simple Storage Service (Amazon S3) richieste
- Manca una revisione archiviata in Amazon S3 oppure il bucket Amazon S3 utilizzato si trova in Regione AWS un'istanza diversa dall'istanza Amazon EC2
- Problemi relativi ai file delle specifiche dell'applicazione () AppSpec

- Errori «Il file esiste già nella posizione»
- Hook di eventi del ciclo di vita CodeDeploy gestiti non riusciti
- Hook per eventi del ciclo di vita gestiti dal cliente non riusciti
- Eventi di scalabilità durante l'implementazione

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DeploymentId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della distribuzione che non è riuscita.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon in cui la distribuzione non è riuscita.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeAwsApi`- Verifica i valori forniti per i parametri `DeploymentId` and `InstanceId`.
- `aws:executeScript`- Raccoglie informazioni dall' EC2istanza Amazon come lo stato dell'istanza e i dettagli del profilo dell'istanza IAM.
- `aws:executeScript`- Esamina la distribuzione specificata e restituisce un'analisi del motivo per cui l'implementazione non è riuscita.

AWS Config

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Config Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-SetupConfig](#)

AWSSupport-SetupConfig

Descrizione

Il `AWSSupport-SetupConfig` runbook crea un ruolo collegato al servizio AWS Identity and Access Management (IAM), un registratore di configurazione basato su e un canale di AWS Config distribuzione con un bucket AWS Config Amazon Simple Storage Service (Amazon S3) in cui invia istantanee di configurazione e file di cronologia della configurazione. Se specifichi valori per i `AggregatorAccountRegion` parametri `AggregatorAccountId` and, il runbook crea anche autorizzazioni per l'aggregazione dei dati al fine di raccogliere dati di configurazione e conformità da

più o meno dati. AWS Config Account AWS Regioni AWS Per ulteriori informazioni sull'aggregazione dei dati da più account e regioni, consulta [Aggregazione di dati multiaccount e più regioni nella Guida per gli sviluppatori](#). AWS Config

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AggregatorAccountId

Tipo: stringa

Descrizione: (Facoltativo) L'ID del Account AWS luogo in cui verrà aggiunto un aggregatore per aggregare i dati di AWS Config configurazione e conformità provenienti da più account e. Regioni AWS Questo account viene utilizzato anche dall'aggregatore per autorizzare gli account di origine.

- AggregatorAccountRegion

Tipo: stringa

Descrizione: (Facoltativo) La regione in cui verrà aggiunto un aggregatore per aggregare i dati di AWS Config configurazione e conformità di più account e regioni.

- IncludeGlobalResourcesRegion

Tipo: stringa

Predefinito: us-east-1

Descrizione: (Obbligatorio) Per evitare di registrare i dati delle risorse globali in ogni regione, specifica una regione da cui registrare i dati delle risorse globali.

- Partizione

Tipo: stringa

Impostazione predefinita: aws

Descrizione: (Obbligatoria) La partizione da cui si desidera raccogliere i dati di AWS Config configurazione e conformità.

- S3 BucketName

Tipo: stringa

Impostazione predefinita: aws-config-delivery-channel

Descrizione: (Facoltativo) Il nome che desideri applicare al bucket Amazon S3 creato per il canale di distribuzione. L'ID dell'account viene aggiunto alla fine del nome.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

- `aws:executeScript`- Crea un ruolo IAM collegato al servizio, AWS Config se non ne esiste già uno.
- `aws:executeScript`- Crea un registratore di configurazione se non ne esiste già uno.
- `aws:executeScript`- Crea un bucket Amazon S3 da utilizzare nel canale di distribuzione se non ne esiste già uno.
- `aws:executeScript`- Crea un canale di distribuzione utilizzando le risorse create dal runbook.
- `aws:executeAwsApi`- Avvia il registratore di configurazione.
- `aws:executeScript`- Se sono stati specificati i valori per i `AggregatorAccountRegion` parametri `AggregatorAccountId` and, vengono configurate le autorizzazioni per l'aggregazione dei dati per più account e più regioni.

Amazon Connect

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Connect. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

AWSSupport-AssociatePhoneNumbersToConnectContactFlows

Descrizione

Ti `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` aiuta ad associare i numeri di telefono ai flussi di contatti nella tua istanza Amazon Connect. Fornendo le mappature dei numeri di telefono e dei flussi di contatti in un file di input con valori separati da virgole (CSV),

il runbook associa il maggior numero possibile di numeri di telefono ai flussi di contatti entro 14,5 minuti. Il runbook produce un file CSV con tutte le coppie di numeri di telefono e flussi di contatti che non è riuscito ad associare entro il limite di tempo, in modo da poterle inserire nella prossima esecuzione.

Come funziona?

Il runbook ti `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` aiuta ad associare i numeri di telefono ai flussi di contatti nella tua istanza Amazon Connect utilizzando un file CSV di dati di mappatura archiviato in un bucket Amazon Simple Storage Service (Amazon S3). [Il file CSV di input deve essere allineato al seguente formato, con valori in formato E.164. PhoneNumber](#)

Esempio del file CSV di input

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

Il runbook di automazione crea anche i seguenti file nella posizione di destinazione specificata in `and.DestinationFileBucket DestinationFilePath`

- **automation:EXECUTION_ID/ResourceIdList.csv**: un file temporaneo che contiene le `ContactFlowId` coppie `PhoneNumberId` and necessarie per l'AssociatePhoneNumberContactFlowAPI.
- **automation:EXECUTION_ID/ErrorResourceList.csv**: Un file che contiene il numero di telefono e le coppie del flusso di contatti che non è stato possibile elaborare a causa di un errore, ad esempio `ResourceNotFoundException` nel formato `diPhoneNumber,ContactFlowName,ErrorMessage`.
- **automation:EXECUTION_ID/NonProcessedResourceList.csv**: Un file che contiene il numero di telefono e le coppie di flussi di contatti che non sono state elaborate. Il runbook tenta di elaborare il maggior numero possibile di numeri di telefono e flussi di contatti entro 14,5 minuti (15 minuti di timeout della AWS Lambda funzione - 30 secondi di buffer). Se alcuni numeri di telefono o flussi di contatti non possono essere elaborati a causa del vincolo di tempo, il runbook li include in un file CSV da utilizzare come input per la successiva esecuzione del runbook.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
  "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"
}
]
}

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-AssociatePhoneNumbersToConnectContactFlows](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - AutomationAssumeRole (Facoltativo)

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ConnectInstanceId (Obbligatorio)

L'ID della tua istanza Amazon Connect.

- SourceFileBucket (Obbligatorio)

Il bucket Amazon S3 che archivia il file CSV che contiene il numero di telefono e le coppie di flussi di contatti.

- SourceFilePath (Obbligatorio)

La chiave oggetto Amazon S3 del file CSV che contiene il numero di telefono e le coppie di flussi di contatti. Ad esempio `path/to/input.csv`.

- DestinationFileBucket (Obbligatorio)

Il bucket Amazon S3 in cui l'automazione inserirà un file intermedio e un rapporto sui risultati.

- DestinationFilePath (Facoltativo)

Il percorso dell'oggetto Amazon S3 DestinationFileBucket in cui archiviare un file intermedio e un report sui risultati. Ad esempio, se si specificapath/to/files/, i file vengono archiviati in `s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`

- S3 BucketOwnerAccount (opzionale)

Il numero di AWS account proprietario del bucket Amazon S3 in cui desideri caricare il registro del flusso di contatti. Se non specifichi questo parametro, i runbook utilizzano l'ID AWS account dell'utente o del ruolo in cui viene eseguita l'automazione.

- S3 BucketOwnerRoleArn (opzionale)

L'ARN del ruolo IAM con le autorizzazioni per ottenere le impostazioni di accesso pubblico del bucket Amazon S3 e dell'account, la configurazione della crittografia dei bucket, il bucket, lo stato della policy del bucket e il ACLs caricamento di oggetti nel bucket. Se questo parametro non è specificato, il runbook utilizza l'utente (se specificato) o l'utente che avvia questo runbook `AutomationAssumeRole` (se non è specificato). `AutomationAssumeRole` Consulta la sezione sulle autorizzazioni richieste nella descrizione del runbook.

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

4. Seleziona Esegui.

5. L'automazione si avvia.

6. Il documento esegue le seguenti operazioni:

- CheckConnectInstanceExistence

Verifica se l'istanza Amazon Connect fornita `ConnectInstanceId` esiste.

- Controlla S3 BucketPublicStatus

Verifica se i bucket Amazon S3 specificati in `SourceFileBucket` e `DestinationFileBucket` consentono autorizzazioni di accesso anonime o pubbliche in lettura o scrittura.

- CheckSourceFileExistenceAndSize

Verifica se il file CSV di origine specificato in `SourceFilePath` esiste e se la dimensione del file supera il limite di 25 MiB.

- GenerateResourceIdMap

Scarica il file CSV di origine specificato in `SourceFilePath` and identify `PhoneNumberId` e `ContactFlowId` per ogni risorsa. Al termine, carica un file CSV che contiene `PhoneNumber`, `PhoneNumberIdContactFlowName`, e nel bucket Amazon S3 `ContactFlowId` di destinazione specificato in `DestinationFileBucket`. Se `PhoneNumberId` non può essere identificato per un determinato numero, il file sarà vuoto nel file CSV.

- **AssociatePhoneNumbersToContactFlows**

Crea una AWS Lambda funzione nel tuo account utilizzando uno AWS CloudFormation stack. La AWS Lambda funzione associa ogni numero a un flusso di contatti elencato nel file CSV di origine specificato in `SourceFileBucket` e `SourceFilePath` e lo AWS CloudFormation stack richiama la funzione. La AWS Lambda funzione associa il maggior numero possibile di numeri di telefono ai flussi di contatto prima del timeout (15 minuti). L'elenco dei numeri di telefono e dei flussi di contatti che non è stato possibile elaborare a causa di un errore viene caricato in `[automation:EXECUTION_ID]/ErrorResourceList.csv`. Vengono caricati quelli che non è stato possibile elaborare a causa di un eccesso del numero massimo di numeri di telefono che possono essere elaborati in un'unica esecuzione `[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. Se questo passaggio fallisce, passa alla `DescribeCloudFormationErrorFromStackEvents` fase che mostra il motivo dell'errore in base agli eventi AWS CloudFormation dello stack.

- **WaitForPhoneNumberContactFlowAssociationCompletion**

Attende che venga creata la AWS Lambda funzione che mappa i numeri di telefono ai flussi di contatti e che lo AWS CloudFormation stack completi la sua chiamata.

- **GenerateReport**

Genera il rapporto che contiene il numero di numeri di telefono mappati ai flussi di contatti, quelli che non è stato possibile elaborare a causa di un errore e quelli che non hanno potuto essere elaborati a causa di un eccesso del numero massimo di numeri di telefono che possono essere elaborati in un'unica esecuzione. Il rapporto mostra anche la posizione (URI Amazon S3 e URL della console Amazon S3) di `[automation:EXECUTION_ID]/NonProcessedResourceList.csv` o, se `[automation:EXECUTION_ID]/ErrorResourceList.csv` applicabile.

- **DeleteCloudFormationStack**

Elimina lo AWS CloudFormation stack, inclusa la funzione Lambda per la mappatura.

- **DescribeCloudFormationErrorFromStackEvent**

Descrive gli errori della pila del AWS CloudFormation passo.

`AssociatePhoneNumbersToContactFlows`

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- `GenerateReport.OutputPayload`

Emissione delle associazioni tra numeri di telefono e flussi di contatti. Questo rapporto contiene le seguenti informazioni:

- Il numero di coppie di numeri di telefono e flussi di contatti elencati nel file CSV di input
 - Il numero di numeri di telefono associati ai flussi di contatti, come specificato nel file CSV di input
 - Il numero di numeri di telefono che non è stato possibile associare ai flussi di contatti a causa di un errore
 - Il numero di numeri di telefono che non sono stati associati ai flussi di contatti a causa di vincoli di tempo
 - La posizione (URI Amazon S3 e URL della console Amazon S3) del file CSV che contiene il numero di telefono e le coppie di flussi di contatti che non è stato possibile associare a causa di un errore
 - La posizione (URI Amazon S3 e URL della console Amazon S3) del file CSV che contiene il numero di telefono e le coppie di flussi di contatti che non erano associate a causa di vincoli di tempo
- `DescribeCloudFormationErrorFromStackEvents.Events`

Output che mostra gli eventi AWS CloudFormation dello stack se il `AssociatePhoneNumbersToContactFlows` passaggio fallisce.

Output di esecuzione con un numero limitato di numeri di telefono e flussi di contatti

```
▼ Outputs

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

GenerateReport.OutputPayload
{"Payload": "
=====
Amazon Connect Phone Number Mapping Result
=====
* Phone number and Contact Flow pairs listed in the provided input: 7
* Phone numbers associated with Contact Flow processed: 7
* Phone numbers that could not be associated with Contact Flow due to an error: 0
* Phone numbers that weren't associated with Contact Flow due to the time constraint: 0
"}
~j|
```

Output di esecuzione con un gran numero di numeri di telefono e flussi di contatti e numeri di telefono che non sono stati associati a causa di errori o vincoli di tempo

```

▼ Outputs

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

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

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

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

```

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWSSupport-CollectAmazonConnectContactFlowLog

Descrizione

Il runbook di AWSSupport-CollectAmazonConnectContactFlowLog automazione viene utilizzato per raccogliere i log del flusso di contatti di Amazon Connect per un ID di contatto specifico. Fornendo l'ID dell'istanza e l'ID del contatto di Amazon Connect, il runbook cerca il contatto nei log del flusso di contatti dal gruppo di CloudWatch log di Amazon e li carica nel bucket Amazon Simple Storage Service (Amazon S3) specificato nel parametro di richiesta. Il runbook genera un output che fornisce l'URL della console Amazon S3 e il comando AWS CLI per scaricare i log.

Come funziona?

Il runbook di AWSSupport-CollectAmazonConnectContactFlowLog automazione aiuta a raccogliere i log del flusso di contatti di Amazon Connect per un ID di contatto specifico archiviato nel gruppo di CloudWatch log configurato e li carica in un bucket Amazon S3 specificato. Per

contribuire alla sicurezza dei log raccolti dal flusso di contatti di Amazon Connect, l'automazione valuta la configurazione del bucket Amazon S3 per determinare se il bucket concede autorizzazioni `read` pubbliche `write` o di accesso ed è di proprietà dell'account specificato nel parametro. `AWS S3BucketOwnerAccountId` Se il tuo bucket Amazon S3 utilizza la crittografia lato server con AWS Key Management Service chiavi (SSE-KMS), assicurati che l'utente o il ruolo AWS Identity and Access Management (IAM) che esegue questa automazione disponga delle autorizzazioni sulla chiave. `kms:GenerateDataKey` AWS KMS Per ulteriori informazioni sui log generati dalla tua istanza Amazon Connect, consulta [Flow logs stored in an Amazon CloudWatch log group](#).

Important

Le query di CloudWatch Logs Insights comportano addebiti in base alla quantità di dati interrogati. Ai clienti del piano gratuito viene addebitato solo l'importo per l'utilizzo che supera le Service Quotas. Per ulteriori informazioni, consulta [Prezzi di Amazon CloudWatch](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
  "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"
    }
}
]
}

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSsupport-CollectAmazonConnectContactFlowLog](#) Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:

- **AutomationAssumeRole (Facoltativo):**

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- **ConnectInstanceId (Obbligatorio):**

L'ID della tua istanza Amazon Connect.

- **ContactId (Obbligatorio):**

L'ID del contatto per cui desideri raccogliere il registro del flusso di contatti.

- **S3 BucketName (obbligatorio):**

Il nome del bucket Amazon S3 nel tuo account in cui desideri caricare il log del flusso di contatti. Assicurati che la bucket policy non conceda autorizzazioni di lettura/scrittura non necessarie a parti che non hanno bisogno di accedere ai log raccolti.

- **S3 (opzionale): ObjectPrefix**

Il percorso dell'oggetto Amazon S3 nel bucket Amazon S3 per un log del flusso di contatti caricato. Ad esempio, se lo specifichi `CollectedLogs`, il log verrà caricato come `s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId][AWSAccountId].gz`. Se non si specifica questo parametro, viene utilizzato l'ID di esecuzione di Systems Manager Automation, ad esempio: `s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog_[ContactId]_[AWSAccountId].gz`. Nota: se si specifica un valore per `S3ObjectPrefix` ed si esegue questa automazione utilizzando lo stesso `[ContactId]`, il registro del flusso di contatti verrà sovrascritto.

- **S3 BucketOwnerAccount (opzionale):**

Il numero di AWS account proprietario del bucket Amazon S3 in cui desideri caricare il log del flusso di contatti. Se non specifichi questo parametro, il runbook utilizza l'ID AWS account dell'utente o del ruolo in cui viene eseguita l'automazione.

- **S3 BucketOwnerRoleArn (opzionale):**

L'ARN del ruolo IAM con le autorizzazioni per ottenere le impostazioni di accesso pubblico del bucket e dell'account Amazon S3, la configurazione della crittografia del bucket, lo stato della policy del bucket e il caricamento di ACLs oggetti nel bucket. Se questo parametro non

è specificato, il runbook utilizza l'utente (se specificato) o l'utente che avvia questo runbook `AutomationAssumeRole` (se non è specificato). `AutomationAssumeRole` Vedi la sezione sulle autorizzazioni richieste nella descrizione del runbook.

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. SSMAutomationRole C	ConnectInstanceId (Required) The ID of your Amazon Connect instance. fedcba98-7654-3210-fedc-ba9876543210
ContactId (Required) The ID of the contact that you want to collect Contact Flow Log for. 01234567-89ab-cdef-0123-456789abcdef	S3BucketName (Required) The Amazon S3 bucket name in your account where you want to upload Contact Flow Log. Make sure that bucket policy does not grant unnecessary read/write permissions to parties that do not need access to the collected logs. saw-example-bucket C
S3ObjectPrefix (Optional) The Amazon S3 object path in the Amazon S3 bucket for an uploaded the Contact Flow Log. For example, if you specify 'CollectedLogs', the log will be uploaded as 's3://your-s3-bucket/CollectedLogs/ContactFlowLog_{ContactId}_{AWSAccountId}.gr'. If you do not specify this parameter, the SSM Automation execution ID is used, example: 's3://your-s3-bucket/automation-EXECUTION_ID/ContactFlowLog_{ContactId}_{AWSAccountId}.gr'. Note: If you specify a value for 'S3ObjectPrefix' and you run this automation using the same [ContactId], the Contact Flow Log will be overwritten. String	S3BucketOwnerAccount (Optional) The AWS Account Number that owns the Amazon S3 bucket where you want to upload the Contact Flow Log. If you do not specify this parameter, the runbooks uses the AWS account ID of the user or role in which the Automation runs. String
S3BucketOwnerRoleArn (Optional) The ARN of the IAM role with permissions to get the Amazon S3 bucket and account block public access settings, bucket encryption configuration, the bucket ACLs, the bucket policy status, and upload objects to the bucket. If this parameter is not specified, the runbook uses the 'AutomationAssumeRole' (if specified) or user that starts this runbook (if 'AutomationAssumeRole' is not specified). Please see the required permissions section in the runbook description. C	

4. Seleziona Esegui.

5. L'automazione inizia.

6. Il documento esegue le seguenti operazioni:

- CheckConnectInstanceExistence

Verifica se l'istanza Amazon Connect fornita in `ConnectInstanceId` è ACTIVE.

- Controlla S3 BucketPublicStatus

Verifica se il bucket Amazon S3 specificato in `S3BucketName` consente autorizzazioni di accesso anonime o pubbliche in lettura o scrittura.

- GenerateLogSearchTimeRange

Genera `StartTime` e `EndTime` per il `StartQuery` passaggio in base all'API `InitiationTimestamp` e `LastUpdateTimestamp` restituita dall'API. `DescribeContactStartTimes` sarà un'ora prima `InitiationTimestamp` e `EndTime` sarà un'ora dopo `LastUpdateTimestamp`.

- StartQuery

Avvia un log di query per il file fornito `ContactId` nel gruppo di log CloudWatch Logs associato all'istanza Amazon Connect fornita in `ConnectInstanceId`. Le query scadono dopo 60 minuti di esecuzione. Se la query scade, riduci l'intervallo di tempo in cui viene effettuata la ricerca. Puoi visualizzare le interrogazioni attualmente in corso e la cronologia delle query recenti nella CloudWatch console. Per ulteriori informazioni, consulta [Visualizzare le query in esecuzione o la cronologia delle query](#).

- WaitForQueryCompletion

Attende il completamento del registro CloudWatch delle query di Logs fornito `ContactId`. Si noti che la query scade dopo 60 minuti di esecuzione. Se la query scade, riduci l'intervallo di tempo in cui viene eseguita la ricerca. Puoi visualizzare le query attualmente in corso e la cronologia delle query recenti nella console Amazon Connect. Per ulteriori informazioni, consulta [Visualizza le query in esecuzione o la cronologia delle query](#).

- `UploadContactFlowLog`

Ottiene il risultato della query e carica il log del flusso di contatti nel bucket Amazon S3 specificato in `S3BucketName`

- `GenerateReport`

Restituisce l'URL della console Amazon S3 in cui è stato caricato il log del flusso di contatti e un comando AWS CLI di esempio che puoi utilizzare per scaricare il file di registro.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- `GenerateReport.OutputPayload`

Output che indica che il runbook ha recuperato correttamente i log del flusso di contatti per il contatto specificato. Questo report contiene anche l'URL della console Amazon S3 e un comando AWS CLI di esempio per scaricare il file di registro.

▼ Outputs

`GenerateReport.OutputPayload`

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

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

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

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

- S3 Console URL for the Contact Flow Log file

`https://s3.console.aws.amazon.com/s3/object/saw-example-bucket?region=us-west-2&prefix=01234567-89ab-cdef-0123-456789abcdef/ContactFlowLog_01234567-89ab-cdef-0123-456789abcdef_123456789012.gz`

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

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

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)

- [Pagina iniziale Support Automation Workflows](#)

AWS Directory Service

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Directory Service
Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

AWS-CreateDSManagementInstance

Descrizione

Il AWS-CreateDSManagementInstance runbook crea un'istanza Windows di Amazon Elastic Compute Cloud EC2 (Amazon) che puoi usare per gestire la tua AWS Directory Service directory. L'istanza di gestione non può essere utilizzata per gestire le directory AD Connector.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AmiID

Tipo: stringa

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

Descrizione: (Obbligatorio) L'ID del Amazon Machine Image (AMI) che desideri utilizzare per avviare l'istanza di gestione.

- DirectoryId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della AWS Directory Service directory che desideri gestire. L'istanza viene aggiunta alla directory specificata.

- IamInstanceProfileName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome specificato viene applicato al profilo dell'istanza IAM creato dall'automazione e collegato all'istanza di gestione.

- InstanceType

Tipo: stringa

Impostazione predefinita: `t3.medium`

Valori consentiti:

- 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

Descrizione: (Obbligatorio) Il tipo di istanza che desideri avviare.

- KeyPairName

Tipo: stringa

Descrizione: (Facoltativo) La coppia di chiavi da utilizzare durante la creazione dell'istanza. Se non si specifica un valore, all'istanza non viene associata alcuna coppia di key pair.

- RemoteAccessCidr

Tipo: stringa

Descrizione: (Obbligatorio) Il blocco CIDR da cui si desidera consentire il traffico RDP (porta 3389). Il blocco CIDR specificato viene applicato a una regola in entrata che viene aggiunta al gruppo di sicurezza creato dall'automazione.

- SecurityGroupName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome specificato viene applicato al gruppo di sicurezza creato dall'automazione e associato all'istanza di gestione.

- Tag

Tipo: MapList

Descrizione: (Facoltativo) Una coppia chiave-valore da applicare alle risorse create dall'automazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie dettagli sulla directory specificata nel `DirectoryId` parametro.
- `aws:executeAwsApi`- Ottiene il blocco CIDR del cloud privato virtuale (VPC) in cui è stata avviata la directory.
- `aws:executeAwsApi`- Crea un gruppo di sicurezza utilizzando il valore specificato nel `SecurityGroupName` parametro.
- `aws:executeAwsApi`- Crea una regola in entrata per il gruppo di sicurezza appena creato che consente il traffico RDP dal CIDR specificato nel parametro. `RemoteAccessCidr`
- `aws:executeAwsApi`- Crea un ruolo IAM e un profilo di istanza utilizzando il valore specificato nel parametro. `IamInstanceProfileName`
- `aws:executeAwsApi`- Avvia un' EC2 istanza Amazon in base ai valori specificati nei parametri del runbook.
- `aws:executeAwsApi`- Crea un AWS Systems Manager documento per aggiungere l'istanza appena lanciata alla tua directory.
- `aws:runCommand`- Unisce la nuova istanza alla tua directory.
- `aws:runCommand`- Installa gli strumenti di amministrazione remota del server sulla nuova istanza.

AWSSupport-TroubleshootADConnectorConnectivity

Descrizione

Il `AWSSupport-TroubleshootADConnectorConnectivity` runbook verifica i seguenti prerequisiti per un AD Connector:

- Verifica se il traffico richiesto è consentito dalle regole del gruppo di sicurezza e dell'elenco di controllo degli accessi alla rete (ACL) associate ad AD Connector.
- Verifica se gli endpoint VPC CloudWatch dell'interfaccia AWS Systems Manager AWS Security Token Service, e Amazon sono presenti nello stesso cloud privato virtuale (VPC) di AD Connector.

Quando i controlli dei prerequisiti vengono completati correttamente, il runbook avvia due istanze Amazon Elastic Compute Cloud (Amazon EC2) Linux t2.micro nelle stesse sottoreti del tuo AD Connector. I test di connettività di rete vengono quindi eseguiti utilizzando le utilità `and. netcat` `nslookup`

[Esegui questa automazione \(console\)](#)

Important

L'utilizzo di questo runbook potrebbe comportare costi aggiuntivi per le EC2 istanze Amazon, Account AWS i volumi Amazon Elastic Block Store e Amazon Machine Image (AMI) creato durante l'automazione. Per ulteriori informazioni, consulta i prezzi di [Amazon Elastic Compute Cloud e i prezzi](#) di [Amazon Elastic Block Store](#).

Se il `aws:deletestack` passaggio non riesce, vai alla AWS CloudFormation console per eliminare manualmente lo stack. Il nome dello stack creato da questo runbook inizia con. `AWSSupport-TroubleshootADConnectorConnectivity` Per informazioni sull'eliminazione degli AWS CloudFormation stack, vedere [Eliminazione di uno stack](#) nella Guida per l'utente.AWS CloudFormation

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DirectoryId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della directory AD Connector a cui desideri risolvere i problemi di connettività.

- Ec2 InstanceProfile

Tipo: stringa

Numero massimo di caratteri: 128

Descrizione: (Obbligatorio) Il nome del profilo di istanza che si desidera assegnare alle istanze avviate per eseguire i test di connettività. Il profilo di istanza specificato deve avere la AmazonSSMManagedInstanceCore policy o autorizzazioni equivalenti allegate.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che la directory specificata nel `DirectoryId` parametro è un AD Connector.
- `aws:executeAwsApi`- Raccoglie informazioni su AD Connector.
- `aws:executeAwsApi`- Raccoglie informazioni sui gruppi di sicurezza associati ad AD Connector.
- `aws:executeAwsApi`- Raccoglie informazioni sulle regole ACL di rete associate alle sottoreti per AD Connector.
- `aws:executeScript`- Valuta le regole del gruppo di sicurezza AD Connector per verificare che il traffico in uscita richiesto sia consentito.
- `aws:executeScript`- Valuta le regole ACL di rete AD Connector per verificare che il traffico di rete in uscita e in entrata richiesto sia consentito.

- `aws:executeScript`- Verifica se gli AWS Systems Manager endpoint dell' CloudWatchinterfaccia AWS Security Token Service e Amazon esistono nello stesso VPC dell'AD Connector.
- `aws:executeScript`- Compila gli output dei controlli eseguiti nei passaggi precedenti.
- `aws:branch`- Suddivide l'automazione in base all'output dei passaggi precedenti. L'automazione si interrompe qui se mancano le regole in uscita e in entrata richieste per i gruppi di sicurezza e la rete. ACLs
- `aws:createStack`- Crea uno AWS CloudFormation stack per avviare EC2 istanze Amazon per eseguire test di connettività.
- `aws:executeAwsApi`- Raccoglie le IDs EC2 istanze Amazon appena lanciate.
- `aws:waitForAwsResourceProperty`- Attende che la prima EC2 istanza Amazon appena lanciata venga segnalata come gestita da AWS Systems Manager.
- `aws:waitForAwsResourceProperty`- Attende che la seconda EC2 istanza Amazon appena lanciata venga segnalata come gestita da AWS Systems Manager.
- `aws:runCommand`- Esegue test di connettività di rete sugli indirizzi IP dei server DNS locali dalla prima istanza Amazon EC2 .
- `aws:runCommand`- Esegue test di connettività di rete sugli indirizzi IP dei server DNS locali dalla seconda istanza Amazon EC2 .
- `aws:changeInstanceState`- Arresta le EC2 istanze Amazon utilizzate per i test di connettività.
- `aws:deleteStack`- Elimina lo stack. AWS CloudFormation
- `aws:executeScript`- Fornisce istruzioni su come eliminare manualmente lo AWS CloudFormation stack se l'automazione non riesce a eliminare lo stack.

AWSSupport-TroubleshootDirectoryTrust

Descrizione

Il `AWSSupport-TroubleshootDirectoryTrust` runbook diagnostica i problemi di creazione di fiducia tra Microsoft Active Directory AWS Managed Microsoft AD e Microsoft Active Directory. L'automazione garantisce che il tipo di directory supporti i trust, quindi verifica le regole dei gruppi di sicurezza associati, gli elenchi di controllo degli accessi alla rete (rete ACLs) e le tabelle di routing per potenziali problemi di connettività.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DirectoryId

Tipo: stringa

Pattern consentito: `^d-[a-z0-9]{10}$`

Descrizione: (Obbligatorio) L'ID del file da risolvere. AWS Managed Microsoft AD

- RemoteDomainCidrs

Tipo: StringList

Modello consentito: `^(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])(\((3[0-2]|[1-2][0-9]|1[0-9]))$`

Descrizione: (Obbligatorio) I CIDR del dominio remoto con cui si sta tentando di stabilire una relazione di trust. È possibile aggiungerne più di CIDRs uno utilizzando valori separati da virgole. Ad esempio: 172.31.48.0/20, 192.168.1.10/32.

- RemoteDomainName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome di dominio completo del dominio remoto con cui si sta stabilendo una relazione di trust.

- RequiredTrafficACL

Tipo: stringa

Descrizione: (Obbligatorio) I requisiti di porta predefiniti per AWS Managed Microsoft AD. Nella maggior parte dei casi, non è necessario modificare il valore predefinito.

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

- RequiredTrafficSG

Tipo: stringa

Descrizione: (Obbligatorio) I requisiti di porta predefiniti per AWS Managed Microsoft AD. Nella maggior parte dei casi, non è necessario modificare il valore predefinito.

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

- TrustId

Tipo: stringa

Descrizione: (facoltativo) L'ID della relazione di trust da risolvere.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

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

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che il tipo di cartella è AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Ottiene informazioni su AWS Managed Microsoft AD.
- `aws:branch`- Automazione delle filiali se viene fornito un valore per il parametro `TrustId` di input.
- `aws:executeAwsApi`- Ottiene informazioni sulla relazione di fiducia.
- `aws:executeAwsApi`- Ottiene gli indirizzi IP DNS del server di inoltro condizionale per `RemoteDomainName`
- `aws:executeAwsApi`- Ottiene informazioni sulle route IP che sono state aggiunte a. AWS Managed Microsoft AD
- `aws:executeAwsApi`- Ottiene CIDRs le AWS Managed Microsoft AD sottoreti.
- `aws:executeAwsApi`- Ottiene informazioni sui gruppi di sicurezza associati a. AWS Managed Microsoft AD
- `aws:executeAwsApi`- Ottiene informazioni sulla rete ACLs associata a AWS Managed Microsoft AD.
- `aws:executeScript`- Conferma che i valori `RemoteDomainCidrs` sono validi. Conferma che AWS Managed Microsoft AD dispone di server d'inoltro condizionali per e che le route IP necessarie sono state aggiunte agli indirizzi IP AWS Managed Microsoft AD se non `RemoteDomainCidrs` sono RFC 1918. `RemoteDomainCidrs`
- `aws:executeScript`- Valuta le regole dei gruppi di sicurezza.
- `aws:executeScript`- Valuta la rete. ACLs

Output

`evalDirectorySecurityGroup.output`: risulta dalla valutazione se le regole del gruppo di sicurezza associate a AWS Managed Microsoft AD consentono il traffico necessario per la creazione di fiducia.

evalAclEntries.output - Risulta dalla valutazione se la rete ACLs associata alla AWS Managed Microsoft AD consente il traffico necessario per la creazione di fiducia.

evaluateRemoteDomainCIDR.Output - Risultati della valutazione se si tratta di valori validi.

RemoteDomainCidrs Conferma che AWS Managed Microsoft AD dispone di server d'inoltro condizionali per e che le RemoteDomainCidrs route IP necessarie sono state aggiunte agli indirizzi IP se non sono RFC 1918. AWS Managed Microsoft AD RemoteDomainCidrs

AWS AppSync

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS AppSync Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-EnableAppSyncGraphQLApiLogging](#)

AWS - EnableAppSyncGraphQLApiLogging

Descrizione

Il AWS-EnableAppSyncGraphQLApiLogging runbook consente la registrazione a livello di campo e la registrazione a livello di richiesta per l'API GraphQL specificata. AWS AppSync Il runbook applicherà le modifiche all'API GraphQL specificata anche se la registrazione è già stata abilitata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `Apild`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'API per cui si desidera abilitare la registrazione.

- `FieldLogLevel`

Tipo: stringa

Valori validi: `ERROR` | `ALL`

Descrizione: (Obbligatorio) Il livello di registrazione del campo.

- `CloudWatchLogsRoleArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo di servizio che AWS AppSync si presuppone di pubblicare su Amazon Logs. CloudWatch

- `ExcludeVerboseContent`

Tipo: Booleano

Impostazione predefinita: `False`

Descrizione: (Facoltativo) Imposta su `True` per escludere informazioni come intestazioni, contesto e modelli di mappatura valutati, indipendentemente dal livello di registrazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`

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

Fasi del documento

- `aws: executeAwsApi` - Raccoglie il tipo di autenticazione e le informazioni di configurazione rilevanti per il tipo di autenticazione principale.
- `aws:branch` - Filiali basate sul tipo di autenticazione.
- `aws: executeAwsApi` - Aggiorna la configurazione di registrazione per l'API AWS AppSync GraphQL in base ai valori specificati per i parametri di input del runbook.

Output

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Risposta dalla chiamata. `UpdateGraphQLApi`
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Risposta alla `UpdateGraphQLApi` chiamata.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Risposta alla `UpdateGraphQLApi` chiamata.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Risposta alla `UpdateGraphQLApi` chiamata.

Amazon Athena

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Athena. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-EnableAthenaWorkGroupEncryptionAtRest](#)

AWS-EnableAthenaWorkGroupEncryptionAtRest

Descrizione

Il AWS-EnableAthenaWorkGroupEncryptionAtRest runbook abilita la crittografia a riposo per il gruppo di lavoro Amazon Athena specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- WorkGroup

Tipo: stringa

Descrizione: (Obbligatorio) Il gruppo di lavoro per cui si desidera abilitare la crittografia a riposo.

- EncryptionOption

Tipo: stringa

Valori validi: SSE_S3 | SSE_KMS | CSE_KMS

Descrizione: (Obbligatorio) Specificate l'opzione di crittografia utilizzata. Puoi scegliere la crittografia lato server con chiavi gestite Amazon S3 (SSE_S3), la crittografia lato server con chiavi gestite (SSE_KMS) o la crittografia lato client AWS KMS con chiavi gestite (CSE_KMS). AWS KMS

- KmsKeyId

Tipo: stringa

Descrizione: (Facoltativo) Se utilizzi un'opzione di AWS KMS crittografia, specifica l'ARN della chiave, l'ID della chiave o l'alias della chiave che desideri utilizzare.

- EnableMinimumEncryptionConfiguration

Tipo: Booleano

Impostazione predefinita: True

Descrizione: (Facoltativo) Applica un livello minimo di crittografia per il gruppo di lavoro per i risultati di query e calcoli scritti su Amazon S3. Se abilitata, gli utenti del gruppo di lavoro possono impostare la crittografia solo al livello minimo impostato dall'amministratore o superiore quando inviano le query. Questa impostazione non si applica ai gruppi di lavoro abilitati per Spark.

- EnforceWorkGroupConfiguration

Tipo: Booleano

Impostazione predefinita: True

Descrizione: (Facoltativo) Se impostata su True, le impostazioni per il gruppo di lavoro hanno la precedenza sulle impostazioni lato client. Se impostato su False, vengono utilizzate le impostazioni lato client.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:branch` - Rami basati sull'opzione di crittografia specificata nel parametro. `EncryptionOption`
- `aws:executeAwsApi` - Questo passaggio aggiorna il gruppo di lavoro Athena con l'impostazione di crittografia specificata.
- `aws:executeAwsApi` - Aggiorna l'Athena Work Group con l'impostazione di crittografia specificata.
- `aws:assertAwsResourceProperty` - Verifica che la crittografia per il gruppo di lavoro sia stata abilitata.

DynamoDB

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon DynamoDB. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

AWS-ChangeDDBRWCapacityMode

Descrizione

Il `AWS-ChangeDDBRWCapacityMode` runbook modifica la modalità di capacità di lettura/scrittura per una o più tabelle Amazon DynamoDB (DynamoDB) in modalità on demand o in modalità provisioning.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- CapacityMode

Tipo: stringa

Valori validi: PROVISIONED | PAY_PER_REQUEST

Descrizione: (Obbligatoria) La modalità di capacità di lettura/scrittura desiderata. Quando si passa dalla capacità su richiesta (pay-per-request) alla capacità fornita, è necessario impostare i valori della capacità fornita iniziale. I valori della capacità iniziale assegnata sono stimati in base alla capacità di lettura e scrittura consumata dalla tabella e dagli indici secondari globali negli ultimi 30 minuti.

- ReadCapacityUnits

Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero massimo di letture fortemente coerenti consumate al secondo prima che DynamoDB restituisca un'eccezione di limitazione.

- **TableNames**

Tipo: stringa

Descrizione: (Obbligatorio) Elenco separato da virgole di nomi di tabelle DynamoDB per modificare la modalità di capacità di lettura/scrittura per..

- **WriteCapacityUnits**

Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero massimo di scritture consumate al secondo prima che DynamoDB restituisca un'eccezione di limitazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Modifica la modalità di capacità di lettura/scrittura per le tabelle DynamoDB specificate nel parametro. `TableNames`

Output

`DDBRWCapacityCambia` modalità. `SuccessesTables` - Elenco di nomi di tabelle DynamoDB in cui la modalità di capacità è stata modificata con successo

`Cambia modalitàDDBRWCapacity`. `FailedTables` - Elenco di mappe dei nomi delle tabelle DynamoDB in cui la modifica della modalità di capacità non è riuscita e il motivo dell'errore.

AWS-CreateDynamoDBBackup

Descrizione

Crea un backup di una tabella Amazon DynamoDB.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- BackupName

Tipo: stringa

Descrizione: (obbligatorio) nome del backup da creare.

- LambdaAssumeRole

Tipo: stringa

Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

- TableName

Tipo: stringa

Descrizione: (obbligatorio) nome della tabella DynamoDB.

AWS-DeleteDynamoDbBackup

Descrizione

Elimina il backup di una tabella Amazon DynamoDB.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- BackupArn

Tipo: stringa

Descrizione: (obbligatorio) ARN del backup della tabella DynamoDB da eliminare.

AWSConfigRemediation-DeleteDynamoDbTable

Descrizione

Il `AWSConfigRemediation-DeleteDynamoDbTable` runbook elimina la tabella Amazon DynamoDB (DynamoDB) specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `TableName`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della tabella DynamoDB che desideri eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

- `dynamodb:DescribeTable`

Fasi del documento

- `aws:executeScript`- Elimina la tabella DynamoDB specificata nel parametro. `TableName`
- `aws:executeScript`- Verifica che la tabella DynamoDB sia stata eliminata.

AWS-DeleteDynamoDbTableBackups

Descrizione

Elimina i backup delle tabelle DynamoDB in base ai giorni di conservazione o al conteggio.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `LambdaAssumeRole`

Tipo: stringa

Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

- RetentionCount

Tipo: stringa

Impostazione predefinita: 10

Descrizione: (facoltativo) numero di backup da conservare per la tabella. Se esiste un numero di backup maggiore del numero specificato, verranno eliminati i backup meno recenti che superano tale numero. Entrambi RetentionCount o RetentionDays possono essere utilizzati, non entrambi.

- RetentionDays

Tipo: stringa

Descrizione: (facoltativo) numero di giorni durante i quali conservare i backup della tabella. I backup precedenti al numero di giorni specificato vengono eliminati. L'uno RetentionCount o l'altro RetentionDays possono essere usati, non entrambi.

- TableName

Tipo: stringa

Descrizione: (obbligatorio) nome della tabella DynamoDB.

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

Descrizione

Il AWSConfigRemediation-EnableEncryptionOnDynamoDbTable runbook crittografa una tabella Amazon DynamoDB (DynamoDB) utilizzando la chiave gestita dal cliente AWS KMS() specificata per AWS Key Management Service il parametro. KMSKeyId

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- KMSKeyId

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN della chiave gestita dal cliente che desideri utilizzare per crittografare la tabella DynamoDB specificata nel parametro. TableName

- TableName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della tabella DynamoDB che desideri crittografare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeAwsApi`- Crittografa la tabella DynamoDB specificata nel parametro. `TableName`
- `aws:waitForAwsResourceProperty`- Verifica che la `Enabled` proprietà della tabella `SSESpecification` DynamoDB sia impostata su. `true`
- `aws:assertAwsResourceProperty`- Verifica che la tabella DynamoDB sia crittografata con la chiave gestita dal cliente specificata nel parametro. `KMSKeyId`

AWSConfigRemediation-EnablePITRForDynamoDbTable

Descrizione

Il `AWSConfigRemediation-EnablePITRForDynamoDbTable` runbook abilita point-in-time il ripristino (PITR) sulla tabella Amazon DynamoDB specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `TableName`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della tabella DynamoDB su cui abilitare il ripristino. point-in-time

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeAwsApi`- Abilita il point-in-time ripristino sulla tabella DynamoDB specificata nel parametro. `TableName`
- `aws:assertAwsResourceProperty`- Conferma che point-in-time il ripristino è abilitato nella tabella DynamoDB.

AWS-EnableDynamoDbAutoscaling

Descrizione

Il `AWS-EnableDynamoDbAutoscaling` runbook abilita l'Application Auto Scaling per la tabella Amazon DynamoDB con capacità fornita specificata. Application Auto Scaling regola dinamicamente la capacità di throughput assegnata in risposta ai modelli di traffico. Per ulteriori informazioni, consulta [Gestire automaticamente la capacità di throughput con la scalabilità automatica di DynamoDB nella Amazon DynamoDB Developer Guide](#).

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- TableName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della tabella DynamoDB su cui si desidera abilitare l'Application Auto Scaling.

- MinReadCapacity

Tipo: integer

Descrizione: (Obbligatorio) Il numero minimo di unità di capacità di lettura del throughput assegnate per la tabella DynamoDB.

- MaxReadCapacity

Tipo: integer

Descrizione: (Obbligatorio) Il numero massimo di unità di capacità di lettura del throughput assegnate per la tabella DynamoDB.

- TargetReadCapacityUtilization

Tipo: integer

Descrizione: (Obbligatorio) L'utilizzo della capacità di lettura desiderata. L'utilizzo previsto è la percentuale del throughput assegnato consumato in un determinato momento. È possibile impostare i valori di utilizzo target con scalabilità automatica tra il 20 e il 90 per cento.

- ReadScaleOutCooldown

Tipo: integer

Descrizione: (Obbligatorio) La quantità di tempo, espressa in secondi, di attesa per l'entrata in vigore di una precedente attività di scalabilità orizzontale della capacità di lettura.

- ReadScaleInCooldown

Tipo: integer

Descrizione: (Obbligatorio) La quantità di tempo, in secondi, dopo il completamento di un'attività di scalabilità in base alla capacità di lettura prima che possa iniziare un'altra attività scalabile.

- MinWriteCapacity

Tipo: integer

Descrizione: (Obbligatorio) Il numero minimo di unità di scrittura di throughput assegnate per la tabella DynamoDB.

- MaxWriteCapacity

Tipo: integer

Descrizione: (Obbligatorio) Il numero massimo di unità di scrittura di throughput assegnate per la tabella DynamoDB.

- TargetWriteCapacityUtilization

Tipo: integer

Descrizione: (Obbligatorio) L'utilizzo della capacità di scrittura desiderata. L'utilizzo previsto è la percentuale del throughput assegnato consumato in un determinato momento. È possibile impostare i valori di utilizzo target con scalabilità automatica tra il 20 e il 90 per cento.

- WriteScaleOutCooldown

Tipo: integer

Descrizione: (Obbligatorio) La quantità di tempo, in secondi, di attesa per l'entrata in vigore di una precedente attività di scalabilità orizzontale della capacità di scrittura.

- WriteScaleInCooldown

Tipo: integer

Descrizione: (Obbligatorio) La quantità di tempo in secondi dopo il completamento di un'attività di scalabilità in base alla capacità di scrittura prima che possa iniziare un'altra attività scalabile.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

- `RegisterAppAutoscalingTargetWrite` (`aws:executeAwsApi`) - Configura Application Auto Scaling nella tabella DynamoDB specificata.
- `RegisterAppAutoscalingTargetWriteDelay` (`aws:sleep`) - Dorme per evitare la limitazione delle API.
- `PutScalingPolicyWrite` (`aws:executeAwsApi`) - Configura l'utilizzo della capacità di scrittura di destinazione per la tabella DynamoDB.
- `PutScalingPolicyWriteDelay` (`aws:sleep`) - Dorme per evitare la limitazione delle API.
- `RegisterAppAutoscalingTargetRead` (`aws:executeAwsApi`) - Configura le unità di capacità di lettura minima e massima per la tabella DynamoDB.
- `RegisterAppAutoscalingTargetReadDelay` (`aws:sleep`) - Dorme per evitare la limitazione delle API.
- `PutScalingPolicyRead` (`aws:executeAwsApi`) - Configura l'utilizzo della capacità di lettura prevista per la tabella DynamoDB.
- `VerifyDynamoDbAutoscalingEnabled` (`aws:executeScript`) - Verifica che l'Application Auto Scaling sia abilitato per la tabella DynamoDB in base ai valori specificati.

Output

- `RegisterAppAutoscalingTargetWrite.Risposta`
- `PutScalingPolicyWrite.Risposta`
- `RegisterAppAutoscalingTargetRead.Risposta`
- `PutScalingPolicyRead.Risposta`

- VerifyDynamoDbAutoscalingEnabled.DynamoDbAutoscalingEnabledResponse

AWS-RestoreDynamoDBTable

Descrizione

Il AWS-RestoreDynamoDBTable runbook ripristina la tabella Amazon DynamoDB specificata point-in-time utilizzando recovery (PITR).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EnablePointInTimeRecoverAsNeeded

Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Facoltativo) Determina se l'automazione attiva il point-in-time ripristino in base alle esigenze per ripristinare la tabella.

- GlobalSecondaryIndexOverride

Tipo: stringa

Descrizione: (Facoltativo) I nuovi indici secondari globali per sostituire gli indici secondari esistenti per la nuova tabella.

- LocalSecondaryIndexOverride

Tipo: stringa

Descrizione: (Facoltativo) I nuovi indici secondari locali per sostituire gli indici secondari esistenti per la nuova tabella.

- RestoreDateTime

Tipo: stringa

Descrizione: (Obbligatorio) Il point-in-time ripristino in cui desideri ripristinare la tabella negli ultimi 35 giorni. Specificate la data e l'ora utilizzando il seguente formato: DD/MM/YYYY HH:MM:SS

- SourceTableArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN della tabella che desideri ripristinare.

- SseSpecificationOverride

Tipo: stringa

Descrizione: (Facoltativo) Le impostazioni di crittografia lato server da utilizzare per la nuova tabella.

- TargetTableName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della tabella da ripristinare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- dynamodb:BatchWriteItem

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

Fasi del documento

- `aws:executeScript`- Ripristina la tabella DynamoDB specificata nel `TargetTableName` parametro utilizzando il ripristino. point-in-time

AWS Database Migration Service

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Database Migration Service Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-TroubleshootDMSTableErrors](#)

AWSSupport-TroubleshootDMSTableErrors

Descrizione

Il runbook di AWS Systems Manager `AWSSupport-TroubleshootDMSTableErrors` automazione consente di automatizzare il processo di risoluzione dei problemi relativo all'attività di migrazione del database `Table errors` o alla replica senza server di. AWS Database Migration Service Questi errori si verificano quando le tabelle non riescono a migrare dall'endpoint di origine (database di origine) all'endpoint di destinazione (database di destinazione) tramite l'attività di migrazione del database o la replica serverless creata in servizio. AWS DMS Questo runbook analizza i messaggi di errore di firma contenuti nei log, concentrandosi in particolare sui CloudWatch log delle attività per le

tradizionali attività di migrazione del database e sui log serverless per la replica serverless. Fornisce inoltre suggerimenti mirati e procedure di correzione per i messaggi di errore più comuni riscontrati durante le migrazioni. `Table error AWS DMS`

Come funziona?

Il runbook esegue i seguenti passaggi:

- Recupera informazioni sull' AWS DMS ARN fornito, che può essere un'attività di migrazione del database o una replica serverless.
- Verifica se la AWS DMS risorsa fornita è stata avviata almeno una volta controllando il `FreshStartDate` valore nella risposta API (per il task di migrazione del database) e `DescribeReplicationTasks DescribeReplications` API (per la replica senza server). Se la risorsa non è stata avviata, l'automazione genera un errore.
- Se la risorsa è stata avviata, l'automazione verifica la presenza di tabelle negli `TableError` stati utilizzando `TableStatistics` le informazioni. Se non vengono rilevati errori, l'automazione termina il flusso di lavoro dopo la visualizzazione di un messaggio di conferma che non sono stati rilevati errori di tabella nell'attività di migrazione del database o nella replica serverless specificata.
- Se vengono trovate tabelle con `TableError` stato, l'automazione verifica se la CloudWatch registrazione è abilitata per la risorsa specificata. AWS DMS Se la registrazione non è abilitata, l'automazione termina il flusso di lavoro dopo aver visualizzato un messaggio che indica che la registrazione non è abilitata.

Nota: CloudWatch la registrazione dovrebbe essere abilitata, poiché l'automazione si basa su questi registri per analizzare e identificare i problemi relativi alle tabelle in stato. `TableError`

- Se la registrazione è abilitata, l'automazione analizza CloudWatch i log e genera un report per ogni tabella che è in stato. `TableError` Il rapporto include suggerimenti per i messaggi di errore più comuni e fornisce i log degli errori pertinenti per aiutare a identificare e risolvere i problemi che impediscono la corretta migrazione delle tabelle dall'endpoint di AWS DMS origine all'endpoint di destinazione. AWS DMS

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DMSArn

Tipo: stringa

Descrizione: (obbligatorio) ARN dell'attività di migrazione del database o della replica serverless

Modello consentito: `^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

Tipo: stringa

Descrizione: (Facoltativo) Questo parametro definisce l'inizio dell'intervallo di tempo per l'analisi dei CloudWatch log di una determinata attività di migrazione del database o della replica serverless. Se forniti, verranno raccolti e analizzati solo i log generati da quel momento specifico in poi. Tieni presente che esiste la possibilità che il flusso di lavoro si verifichi un timeout se l'intervallo di tempo tra `startDate` e `endDate` è troppo lungo. Il valore deve essere fornito nel formato data/ora ISO 6081.

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

- EndTimeRange

Tipo: stringa

Descrizione: (Facoltativo) Questo parametro imposta la fine dell'intervallo di tempo per l'analisi dei CloudWatch log di una determinata attività di migrazione del database o della replica serverless. Se forniti, verranno raccolti e analizzati solo i log generati fino a quel momento specifico. Tieni presente che esiste la possibilità che il flusso di lavoro si verifichi un timeout se l'intervallo di tempo tra `startDate` e `endDate` è troppo lungo. Il valore deve essere fornito nel formato data/ora ISO 6081.

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

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Esempio di politica IAM per l'automazione Assume Role

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

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-TroubleshootDMSTableErrors](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:

- AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DMSArn

ARN dell'attività di migrazione del database o replica senza server con errori di tabella.

- StartTimeRange

(Facoltativo) Formato data/ora ISO 6081 che definisce l'inizio dell'intervallo di tempo per l'analisi dei CloudWatch log di una determinata attività di migrazione del database o della replica senza server.

- EndTimeRange

(Facoltativo) Formato data/ora ISO 6081 che definisce la fine dell'intervallo di tempo per l'analisi dei CloudWatch log di una determinata attività di migrazione del database o della replica serverless.

4. Seleziona il pulsante Esegui nella parte inferiore della pagina.
5. L'automazione si avvia.

6. Il documento esegue le seguenti operazioni:

- `convalidare DMSInput TypeAndGatherDetails`

Convalida l'input AWS DMS ARN fornito e raccoglie i dettagli di base dell'attività di migrazione del database o della replica serverless necessari nei passaggi successivi.

- `branchOnTableErrori`

Suddivide il flusso di lavoro in base al numero di errori di tabella rilevati nel passaggio precedente. Se il conteggio è maggiore di 0, procedi al `branchOnCWLoggingStatus` passaggio -. Altrimenti, procedi al `outputNoTableErrors` passaggio -.

- `outputNoTableErrori`

Invia un messaggio che indica che gli errori di tabella non sono stati rilevati nell'attività di migrazione del database specificata o nella replica serverless.

- `Stato BranchOn CWLogging`

Suddivide il flusso di lavoro in base allo stato CloudWatch di registrazione rilevato nel passaggio precedente. Se abilitato, procedi al `gatherTableDetails` passaggio -. Altrimenti, procedi al `outputNoCWLoggingEnabled` passaggio -.

- `OutputNo abilitato CWLogging`

Emette un messaggio che indica che la CloudWatch registrazione non è abilitata nell'attività di migrazione del database specificata o nella replica senza server.

- `gatherTableDetails`

Raccoglie i `FullLoadEndTime` timestamp delle tabelle con errori e calcola i valori dell'intervallo di tempo per analizzare i log. CloudWatch

- `analyzeCloudWatchLog`

Analizza i log trovati nel gruppo di CloudWatch log in base ai messaggi di errore relativi alla firma e restituisce il rapporto all'utente.

7. Al termine dell'esecuzione, consulta la sezione Output per i risultati dettagliati dell'esecuzione.

- Output di «Nessun errore di tabella trovato»

Se non vengono rilevati errori di tabella nell'attività di migrazione del database o nella replica serverless fornita, l'automazione mostra l'output con lo stesso risultato.

Se CloudWatch la registrazione non è abilitata nell'attività di migrazione del database o nella replica serverless fornita, l'automazione mostra l'output che indica lo stesso e fornisce i passaggi per abilitare la registrazione.

- Rapporto di analisi del registro

Genera un rapporto che identifica `Table error` lo stato delle tabelle in base all'attività di migrazione del database fornita o alla replica senza server, distinguendo i tipi di errore, elencando i messaggi di errore riscontrati e fornendo passaggi e suggerimenti di correzione mirati per ciascuna tabella identificata.

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

Amazon EBS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic Block Store. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, consulta [Visualizza il contenuto del runbook](#)

Argomenti

- [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

Descrizione

Il runbook di AWSSupport-AnalyzeEBSResourceUsage automazione viene utilizzato per analizzare l'utilizzo delle risorse su Amazon Elastic Block Store (Amazon EBS). Analizza l'utilizzo dei volumi e identifica i volumi, le immagini e le istantanee abbandonati in una determinata regione. AWS

Come funziona?

Il runbook svolge le seguenti quattro attività:

1. Verifica l'esistenza di un bucket Amazon Simple Storage Service (Amazon S3) o crea un nuovo bucket Amazon S3.
2. Raccoglie tutti i volumi Amazon EBS nello stato disponibile.
3. Raccoglie tutte le istantanee di Amazon EBS per cui è stato eliminato il volume di origine.
4. Raccoglie tutte le Amazon Machine Images (AMIs) che non sono utilizzate da istanze Amazon Elastic Compute Cloud (Amazon EC2) non terminate.

Il runbook genera report CSV e li archivia in un bucket Amazon S3 fornito dall'utente. Il bucket fornito deve essere protetto seguendo le migliori pratiche di AWS sicurezza descritte alla fine. Se il bucket Amazon S3 fornito dall'utente non esiste nell'account, il runbook crea un nuovo bucket Amazon S3 con il formato del nome, crittografato con una chiave personalizzata AWS Key Management Service (AWS KMS)<User-provided-name>-awssupport-YYYY-MM-DD, con il controllo delle versioni degli oggetti abilitato, l'accesso pubblico bloccato e richiede richieste di utilizzo di SSL/TLS.

Se desideri specificare il tuo bucket Amazon S3, assicurati che sia configurato seguendo queste best practice:

- Blocca l'accesso pubblico al bucket (impostato suIsPublic). False

- Attiva la registrazione degli accessi di Amazon S3.
- [Consenti solo le richieste SSL al](#) tuo bucket.
- Attiva il controllo delle versioni degli oggetti.
- Usa una chiave AWS Key Management Service (AWS KMS) per crittografare il tuo bucket.

 Important

L'utilizzo di questo runbook potrebbe comportare costi aggiuntivi sul tuo account per la creazione di bucket e oggetti Amazon S3. Consulta [i prezzi di Amazon S3](#) per maggiori dettagli sugli addebiti che potrebbero comportare.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- S3 BucketName

Tipo: AWS::S3::Bucket::Name

Descrizione: (Obbligatorio) Il bucket Amazon S3 nel tuo account in cui caricare il report. Assicurati che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie a parti che

non hanno bisogno di accedere ai log raccolti. Se il bucket specificato non esiste nell'account, l'automazione crea un nuovo bucket nella regione in cui l'automazione viene avviata con il formato del nome, crittografato con una chiave personalizzata. <User-provided-name>-awssupport-YYYY-MM-DD AWS KMS

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

- CustomerManagedKmsKeyArn

Tipo: stringa

Descrizione: (Facoltativo) La AWS KMS chiave personalizzata Amazon Resource Name (ARN) per crittografare il nuovo bucket Amazon S3 che verrà creato se il bucket specificato non esiste nell'account. L'automazione fallisce se si tenta di creare il bucket senza specificare un ARN di chiave AWS KMS personalizzata.

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

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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

Esempio di policy con autorizzazioni IAM minime richieste per eseguire questo runbook:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "Read_Only_Permissions",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeSnapshots",
      "ec2:DescribeVolumes",
      "ssm:DescribeAutomationExecutions"
    ],
    "Resource": ""
  }, {
    "Sid": "KMS_Generate_Permissions",
    "Effect": "Allow",
    "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }, {
    "Sid": "S3_Read_Only_Permissions",
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketAcl",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketPublicAccessBlock",
      "s3:ListBucket"
    ],
  },
```

```
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1",
            "arn:aws:s3:::amzn-s3-demo-bucket2/"
        ]
    }, {
        "Sid": "S3_Create_Permissions",
        "Effect": "Allow",
        "Action": [
            "s3:CreateBucket",
            "s3:PutObject",
            "s3:PutBucketLogging",
            "s3:PutBucketPolicy",
            "s3:PutBucketPublicAccessBlock",
            "s3:PutBucketTagging",
            "s3:PutBucketVersioning",
            "s3:PutEncryptionConfiguration"
        ],
        "Resource": "*"
    }
]
```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Passa a [AWSSupport-AnalyzeEBSResourceUsage](#) nella AWS Systems Manager console.
2. Per i parametri di input, inserisci quanto segue:
 - AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- S3 BucketName (richiesto):

Il bucket Amazon S3 nel tuo account in cui caricare il report.

- CustomerManagedKmsKeyArn(Facoltativo):

La AWS KMS chiave personalizzata Amazon Resource Name (ARN) per crittografare il nuovo bucket Amazon S3 che verrà creato se il bucket specificato non esiste nell'account.

Input parameters

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

Enter the name of an existing S3 Bucket

S3 Bucket
test-bucket-1
Example: s3-bucket-name

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

Select an existing IAM Role

admin-my
arn:aws:iam:::role:

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

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

3. Seleziona Esegui.

4. L'automazione viene avviata.

5. Il runbook di automazione esegue i seguenti passaggi:

- CheckConcurrency:

Assicura che ci sia una sola iniziazione di questo runbook nella regione. Se il runbook rileva un'altra esecuzione in corso, restituisce un errore e termina.

- verifyOrCreateBucket S3:

Verifica se il bucket Amazon S3 esiste. In caso contrario, crea un nuovo bucket Amazon S3 nella regione in cui l'automazione viene avviata con il formato del nome **<User-provided-name>-awssupport-YYYY-MM-DD**, crittografato con una chiave personalizzata. AWS KMS

- gatherAmiDetails:

Le ricerche di AMIs, che non sono utilizzate da nessuna EC2 istanza Amazon, generano il report con il formato **<region>-images.csv** del nome e lo caricano nel bucket Amazon S3.

- gatherVolumeDetails:

Verifica i volumi Amazon EBS nello stato disponibile, genera il report con il formato **<region>-volume.csv** del nome e lo carica in un bucket Amazon S3.

- gatherSnapshotDetails:

Cerca gli snapshot Amazon EBS dei volumi Amazon EBS che sono già stati eliminati, genera il report con il formato **<region>-snapshot.csv** del nome e lo carica nel bucket Amazon S3.

6. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione.

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

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS-ArchiveEBSSnapshots

Descrizione

Il AWS-ArchiveEBSSnapshots runbook ti aiuta ad archiviare le istantanee per i volumi Amazon Elastic Block Store (Amazon EBS) specificando il tag che hai applicato agli snapshot. In alternativa, puoi fornire l'ID di un volume se gli snapshot non sono etichettati.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Descrizione

Tipo: stringa

Descrizione: (Facoltativo) Una descrizione dello snapshot di Amazon EBS.

- DryRun

Tipo: stringa

Valori validi: Sì | No

Descrizione: (Obbligatorio) Verifica se l'utente dispone delle autorizzazioni necessarie per l'azione, senza effettuare effettivamente la richiesta, e fornisce una risposta di errore.

- RetentionCount

Tipo: stringa

Descrizione: (Facoltativo) Il numero di istantanee che desideri archiviare. Non specificate un valore per questo parametro se specificate un valore per `RetentionDays`.

- RetentionDays

Tipo: stringa

Descrizione: (Facoltativo) Il numero di giorni precedenti di istantanee che desideri archiviare. Non specificate un valore per questo parametro se specificate un valore per `RetentionCount`.

- SnapshotWithTag

Tipo: stringa

Valori validi: Sì | No

Descrizione: (Obbligatorio) Specificate se le istantanee che si desidera archiviare sono contrassegnate.

- TagKey

Tipo: stringa

Descrizione: (Facoltativo) La chiave del tag assegnato alle istantanee che desideri archiviare.

- TagValue

Tipo: stringa

Descrizione: (Facoltativo) Il valore del tag assegnato alle istantanee che desideri archiviare.

- VolumeId

Tipo: stringa

Descrizione: (Facoltativo) L'ID del volume di cui desideri archiviare le istantanee. Utilizzate questo parametro se le istantanee non sono contrassegnate.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ec2:ArchiveSnapshots
- ec2:DescribeSnapshots

Fasi del documento

aws:executeScript- Archivia le istantanee utilizzando il tag specificato utilizzando i TagValue parametri TagKey and o il VolumeId parametro.

AWS-AttachEBSVolume

Descrizione

Collega un volume Amazon Elastic Block Store (Amazon EBS) a un'istanza Amazon Elastic Compute Cloud (EC2Amazon).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Dispositivo

Tipo: stringa

Descrizione: (obbligatorio) nome del dispositivo (ad esempio, /dev/sdh o xvdh).

- Instanceld

Tipo: stringa

Descrizione: (obbligatorio) ID dell'istanza in cui si desidera collegare il volume.

- Volumeld

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del volume Amazon EBS. Il volume e l'istanza devono essere nella stessa zona di disponibilità.

AWSsupport-CalculateEBSPerformanceMetrics

Descrizione

Il `AWSSupport-CalculateEBSPerformanceMetrics` runbook aiuta a diagnosticare i problemi di prestazioni di Amazon EBS calcolando e pubblicando i parametri delle prestazioni in un pannello di controllo. CloudWatch Il dashboard mostra gli IOPS e il throughput medi stimati per un volume Amazon EBS di destinazione o tutti i volumi collegati all'istanza Amazon Elastic Compute Cloud (Amazon) di destinazione. EC2 Per EC2 le istanze Amazon, mostra anche gli IOPS e il throughput medi dell'istanza. Il runbook mostra il link alla CloudWatch dashboard appena creata che mostra le metriche calcolate pertinenti. CloudWatch La CloudWatch dashboard viene creata nel tuo account con il nome: `AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>`

Come funziona?

Il runbook esegue i seguenti passaggi:

- Assicura che i timestamp specificati siano validi.
- Verifica se il Resource ID (Amazon EBS Volume o Amazon EC2 Instance) è valido.
- Quando fornisci un Amazon EC2 come ResourceID, viene creato CloudWatch un pannello di controllo con il IOPS/Throughput for that Amazon EC2 instance and Estimated Average IOPS/Throughput grafico Actual Total per tutti i volumi Amazon EBS collegati a un'istanza Amazon. EC2
- Quando fornisci un volume Amazon EBS come resourceID, viene creata una dashboard con CloudWatch un grafico IOPS/throughput medio stimato per quel volume.
- Dopo la generazione del CloudWatch dashboard, se gli IOPS medi stimati o il throughput medio stimato sono rispettivamente superiori a IOPS massimo o Throughput massimo, è possibile il microbursting per il volume o i volumi collegati a un'istanza Amazon. EC2

Note

Per i volumi espandibili (gp2, sc2 e st1), i parametri massimi. IOPS/throughput should be consider, until you have burst balance. After burst balance is completely utilized i.e. it becomes zero, consider baseline IOPS/throughput

Important

La creazione della CloudWatch dashboard potrebbe comportare costi aggiuntivi sul tuo account. Per ulteriori informazioni, consulta la [guida ai CloudWatch prezzi di Amazon](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Politica di esempio

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "cloudwatch:PutDashboard",
      "Resource": "arn:aws:cloudwatch::Account-id:dashboard/*-EBS-Performance-*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
```

```

        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceTypes"
    ],
    "Resource": "*"
}
]
}

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSsupport-CalculateEBSPerformanceMetrics](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ResourceID (obbligatorio):

L'ID dell' EC2 istanza Amazon o del volume Amazon EBS.

- Ora di inizio (obbligatorio):

L'ora di inizio in cui visualizzare i dati CloudWatch. L'ora deve essere nel formato yyyy-mm-ddThh:mm:ss e in UTC.

- Ora di fine (obbligatorio):

L'ora di fine della visualizzazione dei dati CloudWatch. L'ora deve essere nel formato yyyy-mm-ddThh:mm:ss e in UTC.

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. Choose an option	ResourceID (Required) The ID of the EC2 instance or EBS Volume.
StartTime (Required) The start time to view the data in CloudWatch. The time must be in the format "yyyy-mm-ddThh:mm:ss" and in UTC.	EndTime (Required) The end time to view the data in CloudWatch. The time must be in the format "yyyy-mm-ddThh:mm:ss" and in UTC.

4. Seleziona Esegui.
5. L'automazione inizia.
6. Il documento esegue le seguenti operazioni:

- CheckResourceIdAndTimeStamps:

Verifica se l'ora di fine è superiore all'ora di inizio di almeno un minuto e se la risorsa fornita esiste.

- CreateCloudWatchDashboard:

Calcola le prestazioni di Amazon EBS e visualizza un grafico basato sul tuo Resource ID. Se fornisci un Amazon EBS Volume ID per il parametro Resource ID, questo runbook crea una CloudWatch dashboard con IOPS medi stimati e throughput medio stimato per il volume Amazon EBS. Se fornisci un ID di EC2 istanza Amazon per il parametro Resource ID, questo runbook crea una CloudWatch dashboard con IOPS totali medi e throughput totale medio per l'EC2 istanza Amazon e con IOPS medi stimati e throughput medio stimato per tutti i volumi Amazon EBS collegati all'istanza Amazon. EC2

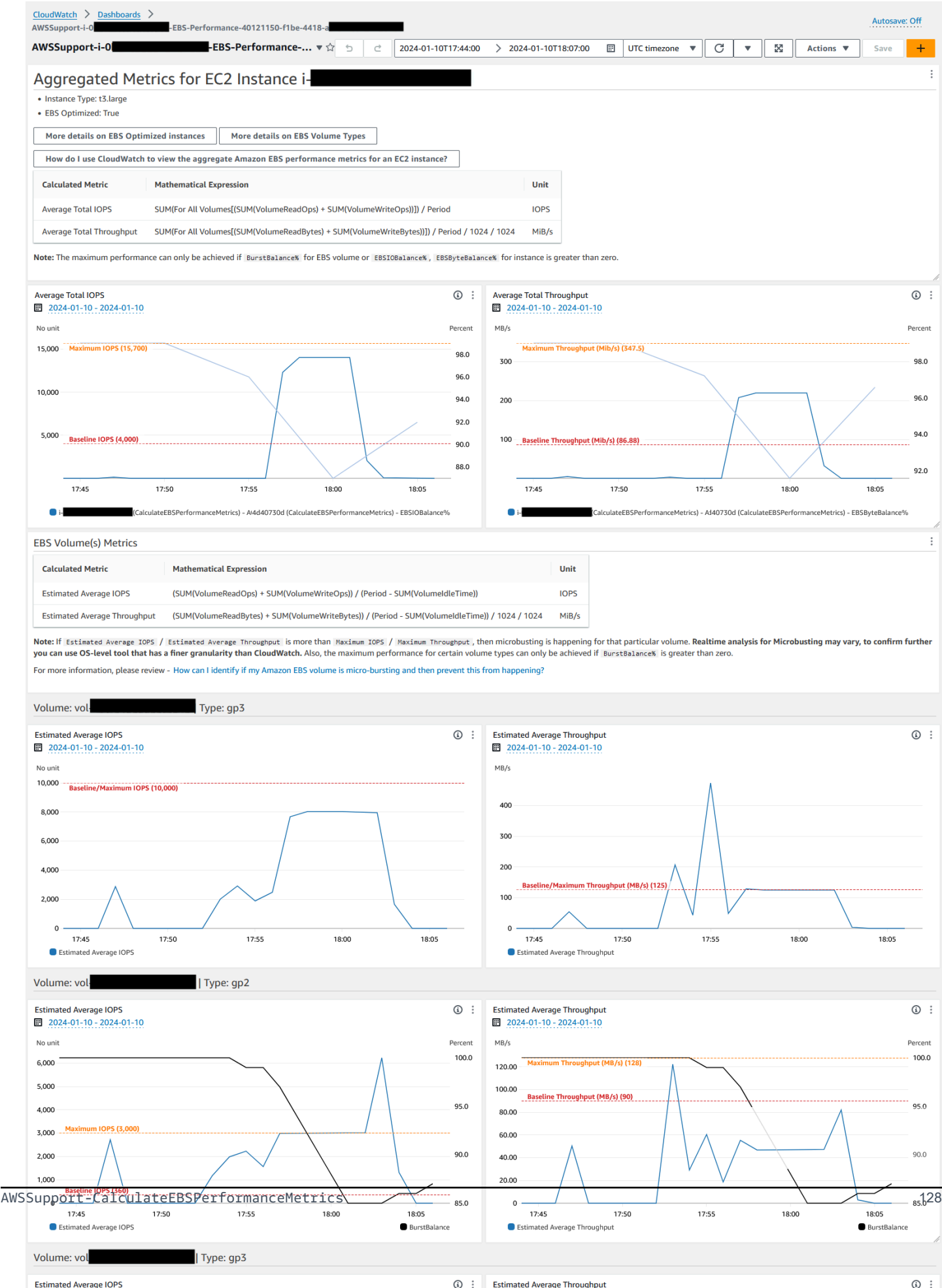
7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

▼ Outputs

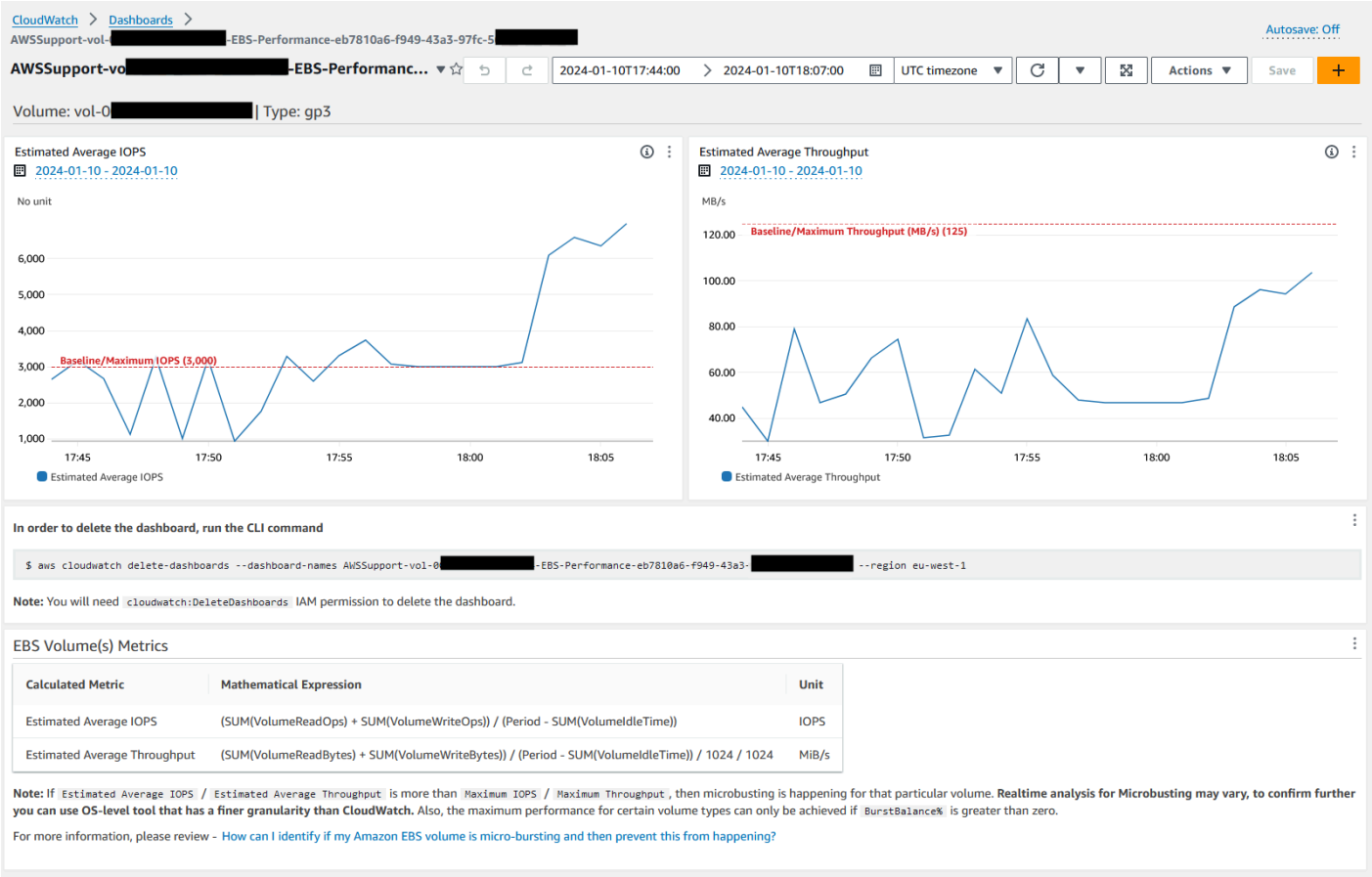
CreateCloudWatchDashboard.CloudWatchDashboardLink
<https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#dashboards:name=AWSSupport-i-██████████:EBS-Performance-443096c1-df23-44ba-96dd-2d005b5ae971>

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

CloudWatch Dashboard di esempio per Resource ID come EC2 istanza Amazon



CloudWatch Dashboard di esempio per Resource ID come ID volume Amazon EBS



Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS documentazione di servizio

- [Come posso identificare se il mio volume Amazon EBS è in fase di microscoppio e quindi evitare che ciò accada?](#)
- [In che modo posso CloudWatch visualizzare i parametri prestazionali aggregati di Amazon EBS per un'istanza? EC2](#)

AWS - CopySnapshot

Descrizione

Copia uno point-in-time snapshot di un volume Amazon Elastic Block Store (Amazon EBS). Puoi copiare lo snapshot all'interno della stessa regione Regione AWS o da una regione all'altra. Le copie degli snapshot crittografati di Amazon EBS rimangono crittografate. Le copie degli snapshot non crittografati rimangono non crittografate. Per copiare uno snapshot crittografato condiviso da un altro account, devi disporre delle autorizzazioni per la chiave KMS utilizzata per crittografare lo snapshot. Gli snapshot creati copiando un altro snapshot sono associati a un ID volume arbitrario che non deve essere utilizzato per nessun motivo.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Descrizione

Tipo: stringa

Descrizione: (Facoltativo) Una descrizione dello snapshot di Amazon EBS.

- SnapshotId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dello snapshot di Amazon EBS da copiare.

- SourceRegion

Tipo: stringa

Descrizione: (obbligatorio) Regione in cui lo snapshot di origine attualmente esiste.

Fasi del documento

CopySnapshot: copia uno snapshot di un volume Amazon EBS.

Output

Copia istantanea. SnapshotId - L'ID della nuova istantanea.

AWS-CreateSnapshot

Descrizione

Crea uno snapshot di un volume Amazon EBS.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Descrizione

Tipo: stringa

Descrizione: (facoltativo) descrizione dello snapshot.

- Volumeld

Tipo: stringa

Descrizione: (obbligatorio) ID del volume.

AWS-DeleteSnapshot

Descrizione

Elimina uno snapshot di un volume Amazon EBS.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- SnapshotId

Tipo: stringa

Descrizione: (obbligatorio) ID dello snapshot EBS.

AWSConfigRemediation-DeleteUnusedEBSVolume

Descrizione

Il AWSConfigRemediation-DeleteUnusedEBSVolume runbook elimina un volume Amazon Elastic Block Store (Amazon EBS) inutilizzato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- CreateSnapshot

Tipo: Booleano

Descrizione: (Facoltativo) Se impostata su `true`, l'automazione crea uno snapshot del volume Amazon EBS prima che venga eliminato.

- `VolumeId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del volume Amazon EBS che desideri eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Verifica che il volume Amazon EBS specificato nel `VolumeId` parametro non sia in uso e crea uno snapshot in base al valore scelto per il parametro. `CreateSnapshot`
- `aws:branch`- Filiali in base al valore scelto per il parametro. `CreateSnapshot`
- `aws:waitForAwsResourceProperty`- Attende il completamento dell'istantanea.
- `aws:executeAwsApi`- Elimina l'istantanea se la creazione dell'istantanea non è riuscita.
- `aws:executeAwsApi`- Elimina il volume Amazon EBS specificato nel `VolumeId` parametro.
- `aws:executeScript`- Verifica che il volume Amazon EBS sia stato eliminato.

AWS-DeregisterAMIs

Descrizione

Il `AWS-DeregisterAMIs` runbook ti aiuta a cancellare la registrazione Amazon Machine Images (AMIs) specificando il tag che hai applicato al tuo. AMIs

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `DryRun`

Tipo: stringa

Valori validi: Sì | No

Descrizione: (Obbligatorio) Verifica se l'utente dispone delle autorizzazioni necessarie per l'azione, senza effettuare effettivamente la richiesta, e fornisce una risposta di errore.

- `RetainNumber`

Tipo: stringa

Descrizione: (Facoltativo) Il numero AMIs che desideri conservare. Non specificate un valore per questo parametro se specificate un valore per `Age`.

- `Età`

Tipo: stringa

Descrizione: (Facoltativo) Il numero di giorni precedenti AMIs che desideri conservare. Non specificate un valore per questo parametro se specificate un valore per `retainNumber`.

- `TagKey`

Tipo: stringa

Descrizione: (Obbligatorio) La chiave del tag assegnato a AMIs cui desideri annullare la registrazione.

- `TagValue`

Tipo: stringa

Descrizione: (Obbligatorio) Il valore del tag assegnato a chi desideri AMIs annullare la registrazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeAwsApi`- Convalida i valori specificati per i parametri di input del runbook.
- `aws:executeAwsApi`- Annulla la registrazione AMIs utilizzando il tag specificato utilizzando i parametri `and. TagKey TagValue`

AWS-DetachEBSVolume

Descrizione

Scollega un volume Amazon EBS da un'istanza Amazon Elastic Compute Cloud (Amazon EC2).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- LambdaAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'ARN del ruolo assunto da Lambda

- VolumeId

Tipo: stringa

Descrizione: (obbligatorio) ID del volume EBS. Il volume e l'istanza devono essere nella stessa zona di disponibilità.

AWSConfigRemediation-EnableEbsEncryptionByDefault

Descrizione

Il **AWSConfigRemediation-EnableEbsEncryptionByDefault** runbook abilita la crittografia su tutti i nuovi volumi Amazon Elastic Block Store (Amazon EBS) nel Account AWS e Regione

AWS dove esegui l'automazione. I volumi creati prima dell'esecuzione dell'automazione non sono crittografati.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- aws:executeAwsApi- Abilita l'impostazione di crittografia predefinita di Amazon EBS nell'account e nella regione correnti.

- `aws:assertAwsResourceProperty`- Verifica che l'impostazione di crittografia predefinita di Amazon EBS sia stata abilitata.

AWS-ExtendEbsVolume

Descrizione

Il `AWS-ExtendEbsVolume` runbook aumenta le dimensioni di un volume Amazon EBS ed estende il file system. Questa automazione supporta i `ext4` file system `xfs` e.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `DriveLetter`

Tipo: stringa

Descrizione: (Facoltativo) La lettera dell'unità di cui si desidera estendere il file system. Questo parametro è obbligatorio per le Windows istanze.

- InstanceId

Tipo: stringa

Descrizione: (Facoltativo) L'ID dell' EC2 istanza Amazon a cui è allegato il volume Amazon EBS che desideri estendere.

- KeepSnapshot

Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Facoltativo) Determina se conservare lo snapshot creato prima di aumentare le dimensioni del volume Amazon EBS.

- MountPoint

Tipo: stringa

Descrizione: (Facoltativo) Il punto di montaggio dell'unità di cui desideri estendere il file system. Questo parametro è obbligatorio per le istanze Linux.

- SizeGib

Tipo: stringa

Descrizione: (Obbligatorio) La dimensione in GiB in cui desideri modificare il volume Amazon EBS.

- VolumeId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del volume EBS che desideri estendere.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

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

Fasi del documento

- `aws:executeScript`- Aumenta la dimensione del volume fino al valore specificato nel `VolumeId` parametro ed estende il file system.

AWSSupport-ModifyEBSSnapshotPermission

Descrizione

Il `AWSSupport-ModifyEBSSnapshotPermission` runbook consente di modificare le autorizzazioni per più snapshot di Amazon Elastic Block Store (Amazon EBS). Usando questo runbook, puoi creare istantanee `Public` o `Private` condividerle con altri. Account AWS Le istantanee crittografate con una chiave KMS predefinita non possono essere condivise con altri account utilizzando questo runbook.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AccountIds

Tipo: StringList

Impostazione predefinita: none

Descrizione: (Facoltativo) Gli IDs account con cui si desidera condividere le istantanee. Questo parametro è obbligatorio se si immette No il valore del Private parametro.

- AccountPermissionOperation

Tipo: stringa

Valori validi: aggiungi | rimuovi

Impostazione predefinita: none

Descrizione: (Facoltativo) Il tipo di operazione da eseguire.

- Privata

Tipo: stringa

Valori validi: Sì | No

Descrizione: (Obbligatorio) Inserisci No il valore se desideri condividere istantanee con account specifici.

- SnapshotIds

Tipo: StringList

Descrizione: (Obbligatorio) Le istantanee IDs di Amazon EBS di cui desideri modificare l'autorizzazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

1. `aws:executeScript`- Verifica le IDs istantanee fornite nel parametro. `SnapshotIds` Dopo aver verificato il IDs, lo script verifica la presenza di istantanee crittografate e genera un elenco, se ne vengono trovate.
2. `aws:branch`- Suddivide l'automazione in base al valore immesso per il parametro. `Private`
3. `aws:executeScript`- Modifica le autorizzazioni delle istantanee specificate per condividerle con gli account specificati.
4. `aws:executeScript`- Modifica le autorizzazioni delle istantanee per cambiarle da a. `Public` `Private`

Output

`ValidateSnapshots.EncryptedSnapshots`

`SharewithOtherAccounts.Risultato`

`MakePrivate.Risultato`

`MakePrivate.Comandi`

AWSConfigRemediation-ModifyEBSVolumeType

Descrizione

Il `AWSConfigRemediation-ModifyEBSVolumeType` runbook modifica il tipo di volume di un volume Amazon Elastic Block Store (Amazon EBS). Dopo la modifica del tipo di volume, il volume entra in uno stato. `optimizing` Per informazioni sul monitoraggio dell'avanzamento delle modifiche

del volume, consulta [Monitorare l'avanzamento delle modifiche del volume](#) nella Amazon EC2 User Guide.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- EbsVolumeld

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del volume Amazon EBS che desideri modificare.

- EbsVolumeType

Tipo: stringa

Valori validi: standard | io1 | io2 | gp2 | gp3 | sc1 | st1

Descrizione: il tipo di volume in cui desideri modificare il volume Amazon EBS. Per informazioni sui tipi di volume Amazon EBS, consulta i tipi di [volume Amazon EBS](#) nella Amazon EC2 User Guide.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:waitForAwsResourceProperty`- Verifica che lo stato del volume sia `available` o `in-use`
- `aws:executeAwsApi`- Modifica il volume Amazon EBS specificato nel `EbsVolumeId` parametro.
- `aws:waitForAwsResourceProperty`- Verifica che il tipo di volume sia stato modificato in base al valore specificato nel parametro. `EbsVolumeType`

Amazon EC2

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic Compute Cloud. I runbook per Amazon Elastic Block Store si trovano nella [Amazon EBS](#) sezione di riferimento del runbook. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

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

- [AWS-SetupJupyter](#)
- [AWS-StartEC2Instance](#)
- [AWS-StopEC2Instance](#)
- [AWS-TerminateEC2Instance](#)
- [AWS-UpdateLinuxAmi](#)
- [AWS-UpdateWindowsAmi](#)
- [AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck](#)
- [AWSConfigRemediation-EnforceEC2InstanceIMDSv2](#)
- [AWSEC2-CloneInstanceAndUpgradeSQLServer](#)
- [AWSEC2-CloneInstanceAndUpgradeWindows](#)
- [AWSEC2-ConfigureSTIG](#)
- [AWSEC2-PatchLoadBalancerInstance](#)
- [AWSEC2-SQLServerDBRestore](#)
- [AWSsupport-ActivateWindowsWithAmazonLicense](#)
- [AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2](#)
- [AWSPremiumSupport-ChangeInstanceTypeIntelToAMD](#)
- [AWSsupport-CheckXenToNitroMigrationRequirements](#)
- [AWSsupport-ConfigureEC2Metadata](#)
- [AWSsupport-ContainEC2Instance](#)
- [AWSsupport-CopyEC2Instance](#)
- [AWSsupport-EnableWindowsEC2SerialConsole](#)
- [AWSsupport-ExecuteEC2Rescue](#)
- [AWSsupport-ListEC2Resources](#)
- [AWSsupport-ManageRDPSettings](#)
- [AWSsupport-ManageWindowsService](#)
- [AWSsupport-MigrateEC2ClassicToVPC](#)
- [AWSsupport-MigrateXenToNitroLinux](#)
- [AWSsupport-ResetAccess](#)

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

AWS-ASGEnterStandby

Descrizione

Modifica lo stato di standby di un'istanza Amazon Elastic Compute Cloud EC2 (Amazon) in un gruppo Auto Scaling.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) ID di un' EC2 istanza Amazon per la quale desideri modificare lo stato di standby all'interno di un gruppo Auto Scaling.

- LambdaRoleArn

Tipo: stringa

Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

AWS-ASGExitStandby

Descrizione

Modifica lo stato di standby di un'istanza Amazon Elastic Compute Cloud EC2 (Amazon) in un gruppo Auto Scaling.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) ID di un' EC2 istanza per la quale si desidera modificare lo stato di standby all'interno di un gruppo Auto Scaling.

- LambdaRoleArn

Tipo: stringa

Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

AWS-CreateImage

Descrizione

Creazione di un nuovo Amazon Machine Image (AMI) da un'istanza Amazon Elastic Compute Cloud (Amazon EC2).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza.

- NoReboot

Tipo: Booleano

Descrizione: (facoltativo) non riavviare l'istanza prima di creare l'immagine.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

```
        "ec2:DescribeImages"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS-DeleteImage

Descrizione

Eliminare un Amazon Machine Image (AMI) e tutte le istantanee associate.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ImageId

Tipo: stringa

Descrizione: (obbligatorio) ID dell'AMI.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DeleteSnapshot",
      "Resource": "arn:aws:ec2:{region}::snapshot/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeImages",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DeregisterImage",
      "Resource": "*"
    }
  ]
}
```

AWS-PatchAsgInstance

Descrizione

Applica patch alle istanze Amazon Elastic Compute Cloud (Amazon EC2) in un gruppo Auto Scaling.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (obbligatorio) ID dell'istanza a cui applicare le patch. Non specificate un ID di istanza configurato per l'esecuzione durante una finestra di manutenzione.

- LambdaRoleArn

Tipo: stringa

Descrizione: (Facoltativo) L'ARN del ruolo che consente alla Lambda creata da Automation di eseguire le azioni per tuo conto. Se non specificato, verrà creato un ruolo transitorio per eseguire la funzione Lambda.

- WaitForInstance

Tipo: stringa

Impostazione predefinita: M PT2

Descrizione: (Facoltativo) Durata della sospensione dell'automazione per consentire all'istanza di tornare in servizio.

- WaitForReboot

Tipo: stringa

Impostazione predefinita: PT5 M

Descrizione: (Facoltativo) Durata della sospensione dell'automazione per consentire il riavvio di un'istanza con patch.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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

Descrizione

Rende un' EC2 istanza conforme alla patch di base applicabile. Ripristina il volume root in caso di errore.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `InstanceId`

Tipo: stringa

Descrizione: (Obbligatorio) EC2 InstanceId a cui applichiamo la patch-baseline.

- `LambdaAssumeRole`

Tipo: stringa

Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

- ReportS3Bucket

Tipo: stringa

Descrizione: (Facoltativo) destinazione Amazon S3 Bucket per il rapporto di conformità generato durante il processo.

Fasi del documento

Numero fase	Nome fase	Operazione di automazione
1	createDocumentStack	aws:createStack
2	IdentifyRootVolume	aws:invokeLambdaFunction
3	PrePatchSnapshot	aws:executeAutomation
4	installMissingUpdates	aws:runCommand
5	SleepThruInstallation	aws:invokeLambdaFunction
6	CheckCompliance	aws:invokeLambdaFunction
7	SaveComplianceReportToS3	aws:invokeLambdaFunction
8	ReportSuccessOrFailure	aws:invokeLambdaFunction
9	RestoreFromSnapshot	aws:invokeLambdaFunction

Numero fase	Nome fase	Operazione di automazione
10	DeleteSnapshot	aws:invokeLambdaFunction
11	deleteCloudFormationModello	aws:deleteStack

Output

IdentifyRootVolume.Carico utile

PrePatchSnapshot.Uscita

SaveComplianceReportToS3. Payload

RestoreFromSnapshot.Carico utile

CheckCompliance.Carico utile

AWS-QuarantineEC2Instance

Descrizione

Con il AWS-QuarantineEC2Instance runbook, puoi assegnare un gruppo di sicurezza a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) che non consente traffico in entrata o in uscita.

Important

Le modifiche alle impostazioni RDP devono essere esaminate attentamente prima di eseguire questo runbook.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (obbligatorio) ID dell'istanza gestita per la quale gestire le impostazioni RDP.

- IsolationSecurityGroup

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del gruppo di sicurezza che si desidera assegnare all'istanza per impedire il traffico in entrata o in uscita.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- autoscaling:DescribeAutoScalingInstances
- autoscaling:DetachInstances
- ec2:CreateSecurityGroup
- ec2:CreateSnapshot
- ec2:DescribeInstances
- ec2:DescribeSecurityGroups

- `ec2:DescribeSnapshots`
- `ec2:ModifyInstanceAttribute`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie dettagli sull'istanza.
- `aws:executeScript`- Verifica che l'istanza non faccia parte di un gruppo Auto Scaling.
- `aws:executeAwsApi`- Crea un'istantanea del volume principale collegato all'istanza.
- `aws:waitForAwsResourceProperty`- Attende che lo stato dell'istantanea sia raggiunto.
`completed`
- `aws:executeAwsApi`- Assegna il gruppo di sicurezza specificato nel
`IsolationSecurityGroup` parametro all'istanza.

Output

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

AWS-ResizeInstance

Descrizione

Cambia il tipo di istanza di un'istanza Amazon Elastic Compute Cloud (Amazon EC2).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (obbligatorio) ID dell'istanza.

- InstanceType

Tipo: stringa

Descrizione: (obbligatorio) tipo di istanza.

AWS-RestartEC2Instance

Descrizione

Riavvia una o più istanze Amazon Elastic Compute Cloud (Amazon EC2).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceIds

Tipo: StringList

Descrizione: (Obbligatorio) Le IDs EC2 istanze Amazon da riavviare.

AWS-SetupJupyter

Descrizione

Il AWS-SetupJupyter runbook ti aiuta a configurare Jupyter Notebook su un'istanza Amazon Elastic Compute Cloud (Amazon). EC2 Puoi specificare un'istanza esistente o fornire un Amazon Machine Image (AMI) ID per l'avvio e la configurazione di una nuova istanza dell'automazione. Prima di iniziare, è necessario creare un SecureString parametro in Parameter Store da utilizzare come password per Jupyter Notebook. Parameter Store è uno strumento in. AWS Systems Manager Per informazioni sulla creazione di parametri, vedere [Creazione di parametri](#) nella Guida AWS Systems Manager per l'utente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Amild

Tipo: stringa

Descrizione: (Facoltativo) L'ID del AMI che desideri utilizzare per avviare una nuova istanza e configurare Jupyter Notebook.

- Instanceld

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza su cui desideri configurare Jupyter Notebook.

- InstanceType

Tipo: stringa

Predefinito: t3.medium

Descrizione: (Facoltativo) Se stai lanciando una nuova istanza per configurare Jupyter Notebook, specifica il tipo di istanza che desideri utilizzare.

- JupyterPasswordSSMKey

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del SecureString parametro in Parameter Store che desiderate utilizzare come password per Jupyter Notebook.

- KeyPairName

Tipo: stringa

Descrizione: (Facoltativo) La coppia di chiavi che desideri associare all'istanza appena lanciata.

- RemoteAccessCidr

Tipo: stringa

Impostazione predefinita: 0.0.0.0/0

Descrizione: (Facoltativo) L'intervallo CIDR da cui desideri consentire il traffico SSH.

- RoleName

Tipo: stringa

Impostazione predefinita: SSMMManaged InstanceProfileRole

Descrizione: (Facoltativo) Il nome del profilo dell'istanza per l'istanza appena lanciata.

- StackName

Tipo: stringa

Impostazione predefinita: CreateManagedInstanceStack {{Automation:execution_id}}

Descrizione: (Facoltativo) Il nome dello AWS CloudFormation stack che desideri venga utilizzato dall'automazione.

- SubnetId

Tipo: stringa

Impostazione predefinita: Default

Descrizione: (Facoltativo) La sottorete da utilizzare per avviare la nuova istanza.

- VpcId

Tipo: stringa

Impostazione predefinita: Default

Descrizione: (Facoltativo) L'ID del cloud privato virtuale (VPC) in cui desideri avviare la nuova istanza.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

- `aws:executeScript`- Configura Jupyter Notebook sull'istanza specificata o su un'istanza appena avviata, utilizzando i valori specificati per i parametri di input del runbook.

AWS-StartEC2Instance

Descrizione

Avvia una o più istanze Amazon Elastic Compute Cloud (Amazon EC2).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceIds

Tipo: StringList

Descrizione: EC2 istanze (obbligatorie) da avviare.

AWS-StopEC2Instance

Descrizione

Arresta una o più istanze Amazon Elastic Compute Cloud (Amazon EC2).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: StringList

Descrizione: EC2 istanze (obbligatorie) da arrestare.

AWS-TerminateEC2Instance

Descrizione

Termina una o più istanze Amazon Elastic Compute Cloud EC2 (Amazon).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceIds

Tipo: StringList

Descrizione: (Obbligatoria) IDs di una o più EC2 istanze da terminare.

AWS-UpdateLinuxAmi

Descrizione

Aggiorna un Amazon Machine Image (AMI) con pacchetti di distribuzione Linux e software Amazon.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ExcludePackages

Tipo: stringa

Impostazione predefinita: none

Descrizione: (facoltativo) nomi dei pacchetti da non aggiornare, in tutte le condizioni. Per impostazione predefinita ("none"), non viene escluso alcun pacchetto.

- IamInstanceProfileName

Tipo: stringa

Impostazione predefinita: ManagedInstanceProfile

Descrizione: (Obbligatorio) Il profilo dell'istanza che consente a Systems Manager di gestire l'istanza.

- IncludePackages

Tipo: stringa

Impostazione predefinita: all

Descrizione: (facoltativo) vengono aggiornati solo i pacchetti specificati. Per impostazione predefinita ("all"), vengono applicati tutti gli aggiornamenti disponibili.

- InstanceType

Tipo: stringa

Impostazione predefinita: t2.micro

Descrizione: (facoltativo) tipo di istanza da avviare come host del workspace. I tipi di istanza variano in base alla regione.

- MetadataOptions

Tipo: StringMap

Predefinito: {» HttpEndpoint «: «enabled», "HttpTokens«: «opzionale"}

Descrizione: (Facoltativo) Le opzioni dei metadati per l'istanza. Per ulteriori informazioni, consulta [InstanceMetadataOptionsRequest](#).

- PostUpdateScript

Tipo: stringa

Impostazione predefinita: none

Descrizione: (facoltativo) URL di uno script da eseguire dopo l'applicazione degli aggiornamenti ai pacchetti. L'impostazione predefinita ("none") non prevede l'esecuzione di uno script.

- PreUpdateScript

Tipo: stringa

Impostazione predefinita: none

Descrizione: (facoltativo) URL di uno script da eseguire prima dell'applicazione degli aggiornamenti ai pacchetti. L'impostazione predefinita ("none") non prevede l'esecuzione di uno script.

- SecurityGroupIds

Tipo: stringa

Descrizione: (Obbligatorio) Un elenco separato da virgole IDs dei gruppi di sicurezza da applicare a AMI.

- SourceAmiId

Tipo: stringa

Descrizione: (obbligatorio) ID AMI (Amazon Machine Image) di origine.

- SubnetId

Tipo: stringa

Descrizione: (Facoltativo) L'ID della sottorete in cui si desidera avviare l'istanza. Se hai eliminato il tuo VPC predefinito, questo parametro è obbligatorio.

- TargetAmiName

Tipo: stringa

Predefinito: UpdateLinuxAmi _from_ {{SourceAmiId}} _on_ {{global:date_time}}

Descrizione: (facoltativo) nome della nuova AMI che verrà creata. L'impostazione predefinita è una stringa generata dall'ID AMI di origine e la data/ora di creazione.

AWS-UpdateWindowsAmi

Descrizione

Aggiorna un Microsoft Windows Amazon Machine Image (AMI). Per impostazione predefinita, questo runbook installa tutti gli aggiornamenti di Windows, il software Amazon e i driver Amazon. Esegue quindi Sysprep per creare una nuova AMI. Supporta Windows Server 2008 R2 o versione successiva.

Important

Se le istanze si connettono AWS Systems Manager tramite endpoint VPC, questo runbook fallirà a meno che non venga utilizzato nella regione us-east-1. Le istanze devono avere TLS 1.2 abilitato per utilizzare questo runbook.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Categories

Tipo: stringa

Descrizione: (facoltativo) specifica una o più categorie di aggiornamento. È possibile filtrare le categorie utilizzando valori separati da virgole. Opzioni: Applicazione, Connettori CriticalUpdates, DefinitionUpdates, DeveloperKits,, DriverFeaturePacks, Guida, Microsoft, SecurityUpdates, ServicePacksUpdateRollups, Strumenti e Aggiornamenti. I formati validi includono una singola voce, per esempio:CriticalUpdates. Oppure puoi specificare un elenco separato da virgole:CriticalUpdates,SecurityUpdates. NOTA: non devono essere presenti spazi tra le virgole.

- ExcludeKbs

Tipo: stringa

Descrizione: (Facoltativo) Specificare uno o più articoli della Microsoft Knowledge Base (KB) IDs da escludere. È possibile escluderne più di IDs uno utilizzando valori separati da virgole. Formati validi: KB9876543 o 9876543.

- IamInstanceProfileName

Tipo: stringa

Predefinito: ManagedInstanceProfile

Descrizione: (Obbligatorio) Il nome del ruolo che consente a Systems Manager di gestire l'istanza.

- IncludeKbs

Tipo: stringa

Descrizione: (Facoltativo) Specificare uno o più articoli della Microsoft Knowledge Base (KB) IDs da includere. È possibile installarne più di IDs uno utilizzando valori separati da virgole. Formati validi: KB9876543 o 9876543.

- InstanceType

Tipo: stringa

Impostazione predefinita: t2.medium

Descrizione: (facoltativo) tipo di istanza da avviare come host del workspace. I tipi di istanza variano in base alla regione. Impostazione predefinita: t2.medium

- MetadataOptions

Tipo: StringMap

Predefinito: {» HttpEndpoint «: «enabled», "HttpTokens«: «opzionale"}

Descrizione: (Facoltativo) Le opzioni dei metadati per l'istanza. Per ulteriori informazioni, consulta [InstanceMetadataOptionsRequest](#).

- PostUpdateScript

Tipo: stringa

Descrizione: (facoltativo) script specificato come stringa. Verrà eseguito dopo l'installazione degli aggiornamenti del sistema operativo.

- PreUpdateScript

Tipo: stringa

Descrizione: (facoltativo) script specificato come stringa. Verrà eseguito prima dell'installazione degli aggiornamenti del sistema operativo.

- PublishedDateAfter

Tipo: stringa

Descrizione: (facoltativo) specifica la data dopo la quale gli aggiornamenti devono essere pubblicati. Ad esempio, se viene specificato 01/01/2017, verranno restituiti tutti gli aggiornamenti rilevati durante la ricerca di Windows Update e la cui pubblicazione è successiva alla data 01/01/2017.

- PublishedDateBefore

Tipo: stringa

Descrizione: (facoltativo) specifica la data prima della quale gli aggiornamenti devono essere pubblicati. Ad esempio, se viene specificato 01/01/2017, verranno restituiti tutti gli aggiornamenti rilevati durante la ricerca di Windows Update e la cui pubblicazione è anteriore alla data 01/01/2017.

- PublishedDaysOld

Tipo: stringa

Descrizione: (facoltativo) specifica il numero di giorni dalla data di pubblicazione degli aggiornamenti. Ad esempio, se si specifica 10, verranno restituiti tutti gli aggiornamenti rilevati durante la ricerca di Windows Update e la cui pubblicazione è avvenuta 10 o più giorni prima.

- SecurityGroupIds

Tipo: stringa

Descrizione: (Obbligatorio) Un elenco separato da virgole IDs dei gruppi di sicurezza da applicare a AMI.

- SeverityLevels

Tipo: stringa

Descrizione: (facoltativo) specifica uno o più livelli di gravità MSRC associati a un aggiornamento. È possibile filtrare i livello di gravità utilizzando valori separati da virgole. Per impostazione predefinita, vengono selezionati tutti i livelli di sicurezza. Se il valore viene specificato, l'elenco di aggiornamenti viene filtrato in base a tali valori. Opzioni: Critical, Important, Low, Moderate o Unspecified. I formati validi includono una singola voce, ad esempio: Critical. In alternativa, è possibile specificare un elenco di valori separati da virgole: Critical,Important,Low.

- SourceAmiId

Tipo: stringa

Descrizione: (Obbligatorio) La fonte AMI ID.

- SubnetId

Tipo: stringa

Descrizione: (Facoltativo) L'ID della sottorete in cui si desidera avviare l'istanza. Se hai eliminato il tuo VPC predefinito, questo parametro è obbligatorio.

- TargetAmiName

Tipo: stringa

Predefinito: UpdateWindowsAmi _from_ {{SourceAmild}} _on_ {{global:date_time}}

Descrizione: (facoltativo) nome della nuova AMI che verrà creata. L'impostazione predefinita è una stringa generata dall'ID AMI di origine e la data/ora di creazione.

AWSConfigRemediation- EnableAutoScalingGroupELBHealthCheck

Descrizione

Il AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck runbook consente controlli di integrità per il gruppo Amazon EC2 Auto Scaling (Auto Scaling) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- **AutoScalingGroupARN**

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del gruppo di auto scaling su cui desideri abilitare i controlli dello stato.

- **HealthCheckGracePeriod**

Tipo: integer

Impostazione predefinita: 300

Descrizione: (Facoltativo) La quantità di tempo, in secondi, che Auto Scaling attende prima di verificare lo stato di integrità di un'istanza Amazon Elastic Compute Cloud (Amazon EC2) entrata in servizio.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Abilita i controlli di integrità sul gruppo Auto Scaling specificato nel `AutoScalingGroupARN` parametro.

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

Descrizione

Il `AWSConfigRemediation-EnforceEC2InstanceIMDSv2` runbook richiede l'istanza Amazon Elastic Compute Cloud EC2 (Amazon) specificata per utilizzare Instance Metadata Service versione 2 (). `IMDSv2`

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon che desideri richiedere di utilizzare IMDSv2.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- HttpPutResponseHopLimit

Tipo: integer

Descrizione: (Facoltativo) Il limite di risposta Hop dal servizio IMDS ritorna al richiedente. Impostato su 2 o superiore per le EC2 istanze che ospitano contenitori. Impostare su 0 per non modificare (impostazione predefinita).

Schema consentito: `^([1-5]?\d|6[0-4])$`

Impostazione predefinita: 0

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

- `aws:executeScript`- Imposta l'`HttpTokens` opzione `required` su sull' EC2 istanza Amazon specificata nel `InstanceId` parametro.
- `aws:assertAwsResourceProperty`- IMDSv2 La verifica è obbligatoria sull' EC2 istanza Amazon.

AWSEC2-CloneInstanceAndUpgradeSQLServer

Descrizione

Crea un AMI da un' EC2 istanza per Windows Server eseguire SQL Server 2008 o versione successiva, quindi aggiornare l'AMI a una versione successiva di SQL Server. Sono supportate solo le versioni in lingua inglese di SQL Server.

Sono supportati i seguenti percorsi di aggiornamento:

- SQL Server 2008 a SQL Server 2017, 2016 o 2014
- SQL Server 2008 R2 a SQL Server 2017, 2016 o 2014
- SQL Server 2012 a SQL Server 2019, 2017, 2016 o 2014
- SQL Server 2014 a SQL Server 2019, 2017 o 2016
- SQL Server 2016 a SQL Server 2019 o 2017

Se si utilizza una versione precedente di Windows Server incompatibile con SQL Server 2019, il documento di automazione deve aggiornare la versione di Windows Server alla 2016.

L'aggiornamento è un processo in più fasi il cui completamento può richiedere 2 ore. L'automazione crea l'AMI dall'istanza e quindi avvia un'istanza temporanea dalla nuova AMI nel campo

specificato SubnetID. I gruppi di sicurezza associati all'istanza originale vengono applicati all'istanza temporanea. L'automazione esegue quindi un aggiornamento TargetSQLVersion sul posto all'istanza temporanea. Dopo l'aggiornamento, l'automazione ne crea una nuova AMI dall'istanza temporanea e quindi termina l'istanza temporanea.

È possibile testare la funzionalità dell'applicazione avviando la nuova AMI nel tuo VPC. Al termine del test e prima di eseguire un altro aggiornamento, pianificare il tempo di inattività dell'applicazione prima passare in modo definitivo all'istanza aggiornata.

Note

Se desideri modificare il nome del computer dell' EC2 istanza lanciata dalla nuova AMI , vedi [Rinominare un computer che ospita un'istanza autonoma di SQL Server](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

Prerequisiti

- Versione TLS 1.2.
- Sono supportate solo le versioni in lingua inglese di SQL Server.
- L' EC2 istanza deve utilizzare una versione di Windows Server questo è Windows Server 2008 R2 (o successivo) e SQL Server 2008 (o successivo).
- Verificare che SSM Agent sia installato nell'istanza. Per ulteriori informazioni, vedere [Installazione e configurazione dell'agente SSM su EC2 istanze](#) per Windows Server.

- Configura l'istanza per utilizzare un ruolo di profilo di istanza AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta [Creazione di un profilo dell'istanza IAM per Systems Manager](#).
- Verificare che l'istanza disponga di 20 GB di spazio sul disco di avvio dell'istanza.
- Per istanze che utilizzano una versione Bring-Your-Own-License (uso di licenze proprie) di SQL Server, si applicano i seguenti prerequisiti aggiuntivi:
 - Fornisci un ID snapshot EBS che includa il supporto di installazione di SQL Server di destinazione. Per farlo:
 1. Verifica che sull' EC2 istanza sia in esecuzione Windows Server 2008 R2 o versione successiva.
 2. Creare un volume EBS da 6 GB nella stessa zona di disponibilità in cui l'istanza è in esecuzione. Collegare il volume all'istanza. Montare il volume, ad esempio come unità D.
 3. Fare clic con il pulsante destro del mouse sull'oggetto ISO e montarlo su un'istanza, ad esempio, sull'unità E.
 4. Copiare il contenuto dell'oggetto ISO dall'unità E:\ all'unità D:\
 5. Creare uno snapshot EBS del volume da 6 GB creato nella fase 2.

Limitazioni

- L'aggiornamento può essere eseguito solo su un'istanza SQL Server che usa l'autenticazione di Windows.
- Verificare che sulle istanze non siano presenti aggiornamenti delle patch di sicurezza in sospeso. Aprire Control Panel (Pannello di controllo), quindi scegliere Check for updates (Verifica disponibilità aggiornamenti).
- Le distribuzioni di SQL Server in modalità HA (High Availability, disponibilità elevata) e mirroring non sono supportate.

Parametri

- `IamInstanceProfile`

Tipo: stringa

Descrizione: (Obbligatorio) Il profilo dell'istanza IAM.

- **InstanceId**

Tipo: stringa

Descrizione: (Obbligatorio) L'istanza in esecuzione Windows Server 2008 R2 (o successivo) e SQL Server 2008 (o successivo).

- **KeepPreUpgradeImageBackUp**

Tipo: stringa

Descrizione: (Facoltativo) Se impostato su `true`, l'automazione non elimina l'AMI creato dall'istanza prima dell'aggiornamento. Se impostato su `true`, è necessario eliminare l'AMI. Per impostazione predefinita, l'AMI viene eliminata.

- **SubnetId**

Tipo: stringa

Descrizione: (obbligatorio) specifica una sottorete per il processo di aggiornamento. Verifica che la sottorete disponga di connettività in uscita ai AWS servizi, Amazon S3 e Microsoft (per scaricare le patch).

- **SQLServerSnapshotId**

Tipo: stringa

Descrizione: ID snapshot (condizionale) per il supporto di installazione di SQL Server di destinazione. Questo parametro è obbligatorio per le istanze che utilizzano una versione BYOL di SQL Server. Questo parametro è facoltativo per le istanze incluse nella licenza di SQL Server (istanze avviate utilizzando un' AWS Amazon Machine Image for Windows Server con Microsoft SQL Server fornita).

- **RebootInstanceBeforeTakingImage**

Tipo: stringa

Descrizione: (Facoltativo) Se impostata su `true`, l'automazione riavvia l'istanza prima di creare un'AMI di pre-aggiornamento. Per impostazione predefinita, l'automazione non si riavvia prima dell'aggiornamento.

- **Obiettivo SQLVersion**

Tipo: stringa

Descrizione: (Facoltativo) Seleziona la versione di destinazione di SQL Server.

Obiettivi possibili:

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

Obiettivo predefinito: SQL Server 2016

Output

AMIID: l'ID dell'AMI creato dall'istanza che è stata aggiornata a una versione successiva di SQL Server.

AWSEC2-CloneInstanceAndUpgradeWindows

Descrizione

Crea un Amazon Machine Image (AMI) da un Windows Server Istanza 2008 R2, 2012 R2, 2016 o 2019, quindi aggiornare AMI in Windows Server 2016, 2019 o 2022. I percorsi di aggiornamento supportati sono i seguenti.

- Windows Server Da 2008 R2 a Windows Server 2016.
- Windows Server Da 2012 R2 a Windows Server 2016.
- Windows Server Da 2012 R2 a Windows Server 2019.
- Windows Server Da 2012 R2 a Windows Server 2022.
- Windows Server Dal 2016 al Windows Server 2019.
- Windows Server Dal 2016 al Windows Server 2022.
- Windows Server Dal 2019 al Windows Server 2022.

L'operazione di aggiornamento è un processo in più fasi il cui completamento può richiedere 2 ore. Ti consigliamo di eseguire un aggiornamento del sistema operativo su istanze con almeno 2 v CPUs e 4 GB di RAM. L'automazione crea un'AMI dall'istanza e quindi avvia un'istanza temporanea dall'AMI appena creato nell'`SubnetId` ambito specificato. I gruppi di sicurezza associati all'istanza

originale vengono applicati all'istanza temporanea. L'automazione esegue quindi un aggiornamento TargetWindowsVersion sul posto all'istanza temporanea. Per aggiornare il tuo Windows Server Istanza 2008 R2 a Windows Server 2016, 2019 o 2022, un aggiornamento sul posto viene eseguito due volte poiché si tratta di un aggiornamento diretto Windows Server 2008 R2 a Windows Server 2016, 2019 o 2022 non sono supportati. L'automazione aggiorna o installa anche i AWS driver richiesti dall'istanza temporanea. Dopo l'aggiornamento, l'automazione crea una nuova AMI dall'istanza temporanea e quindi termina l'istanza temporanea.

Puoi testare la funzionalità dell'applicazione avviando un'istanza di test dall'AMI aggiornata nel tuo Amazon Virtual Private Cloud (Amazon VPC). Al termine del test e prima di eseguire un altro aggiornamento, pianificare il tempo di inattività dell'applicazione prima di passare in modo definitivo all'AMI aggiornata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows Server Edizioni 2008 R2, 2012 R2, 2016 o 2019 Standard e Datacenter

Prerequisiti

- Versione TLS 1.2.
- Verificare che SSM Agent sia installato nell'istanza. Per ulteriori informazioni, consulta [Installazione e configurazione dell'agente SSM su EC2 istanze](#) per Windows Server.
- È necessario installare Windows PowerShell 3.0 o versione successiva sull'istanza.
- Per le istanze che vengono aggiunte a un dominio Microsoft Active Directory, si consiglia di specificare un SubnetId che non dispone di connettività ai controller di dominio per evitare conflitti di nomi host.
- La sottorete dell'istanza deve disporre di connettività in uscita a Internet, che consente l'accesso Servizi AWS ad Amazon S3 e l'accesso al download di patch da Microsoft. Questo requisito è

soddisfatto se la sottorete è una sottorete pubblica e l'istanza ha un indirizzo IP pubblico o se la sottorete è una sottorete privata con un percorso che invia il traffico Internet a un dispositivo NAT pubblico.

- Questa automazione funziona solo con Windows Server Istanze 2008 R2, 2012 R2, 2016 e 2019.
- Configura il Windows Server istanza con un profilo di istanza AWS Identity and Access Management (IAM) che fornisce le autorizzazioni necessarie per Systems Manager. Per ulteriori informazioni, consulta [Creazione di un profilo dell'istanza IAM per Systems Manager](#).
- Verificare che l'istanza disponga di 20 GB di spazio sul disco di avvio.
- Se l'istanza non utilizza una licenza Windows AWS fornita, specifica un ID snapshot Amazon EBS che includa Windows Server Supporti di installazione 2012 R2. Per farlo:
 - Verifica che l' EC2 istanza sia in esecuzione Windows Server 2012 o versioni successive.
 - Creare un volume EBS da 6 GB nella stessa zona di disponibilità in cui l'istanza è in esecuzione. Collegare il volume all'istanza. Montare il volume, ad esempio come unità D.
 - Fare clic con il pulsante destro del mouse sull'oggetto ISO e montarlo su un'istanza, ad esempio, sull'unità E.
 - Copiare il contenuto dell'oggetto ISO dall'unità E:\ all'unità D:\
 - Creare uno snapshot EBS del volume da 6 GB creato nella precedente fase 2.

Limitazioni

Questa automazione non supporta l'aggiornamento di controller di dominio Windows, cluster o sistemi operativi per desktop Windows. Questa automazione inoltre non supporta EC2 le istanze di Windows Server con i seguenti ruoli installati.

- Remote Desktop Session Host (RDSH)
- Remote Desktop Connection Broker (RDCB)
- Remote Desktop Virtualization Host (RDVH)
- Remote Desktop Web Access (RDWA)

Parametri

- AlternativeKeyPairName

Tipo: stringa

Descrizione: (Facoltativo) Il nome di una coppia di key pair alternativa da utilizzare durante il processo di aggiornamento. Ciò è utile in situazioni in cui la coppia di chiavi assegnata all'istanza originale non è disponibile. Se all'istanza originale non è stata assegnata una coppia di key pair, è necessario specificare un valore per questo parametro.

- `BYOLWindowsMediaSnapshotId`

Tipo: stringa

Descrizione: (Facoltativo) L'ID dello snapshot di Amazon EBS da copiare che include i supporti di installazione di Windows Server 2012R2. Obbligatorio solo se si sta eseguendo l'aggiornamento di un'istanza BYOL.

- `IamInstanceProfile`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del profilo dell'istanza IAM che consente a Systems Manager di gestire l'istanza.

- `InstanceId`

Tipo: stringa

Descrizione: (Obbligatorio) L' EC2 istanza in esecuzione Windows Server 2008 R2, 2012 R2, 2016 o 2019.

- `KeepPreUpgradeImageBackUp`

Tipo: stringa

Descrizione: (Facoltativo) Se impostato su True, l'automazione non elimina l'AMI creato dall' EC2 istanza prima dell'aggiornamento. Se impostato su True, è necessario eliminare l'AMI. Per impostazione predefinita, l'AMI viene eliminata.

- `SubnetId`

Tipo: stringa

Descrizione: (Obbligatoria) Questa è la sottorete per il processo di aggiornamento e dove risiede l' EC2 istanza di origine. Verifica che la sottorete disponga di connettività in uscita ai AWS servizi, Amazon S3 e Microsoft (per scaricare le patch).

- `TargetWindowsVersion`

Tipo: stringa

Descrizione: (obbligatorio) selezionare la versione di Windows di destinazione.

Impostazione predefinita: 2022

- RebootInstanceBeforeTakingImage

Tipo: stringa

Descrizione: (facoltativo) se impostato su True, l'automazione riavvia l'istanza prima di creare un'AMI pre-aggiornamento. Per impostazione predefinita, l'automazione non viene riavviata prima dell'aggiornamento.

AWSEC2-ConfigureSTIG

Le guide tecniche di implementazione della sicurezza (STIGs) sono gli standard di rafforzamento della configurazione creati dalla Defense Information Systems Agency (DISA) per proteggere i sistemi informativi e il software. Per la conformità dei propri sistemi agli standard STIG, è necessario installare, configurare e testare una serie di impostazioni di sicurezza.

Amazon EC2 fornisce un documento di comando Systems Manager AWSEC2-ConfigureSTIG, che puoi utilizzare per applicare le impostazioni STIG a un'istanza. Questo documento ti aiuta a creare rapidamente immagini conformi agli standard STIG. Il documento STIG Systems Manager analizza eventuali configurazioni errate ed esegue uno script di correzione. Viene inoltre installato InstallRoot dal Dipartimento della Difesa (DoD) su AMIs Windows per installare e aggiornare i certificati DoD e rimuovere i certificati non necessari per mantenere la conformità STIG. Non ci sono costi aggiuntivi per l'utilizzo del documento STIG Systems Manager.

Note

AWSEC2-ConfigureSTIG è un documento di comando. Per cercare AWSEC2-ConfigureSTIG nella AWS Systems Manager console, seleziona la categoria Documenti di comando.

Questa pagina elenca tutto ciò che STIGs che Amazon EC2 supporta e che i componenti di protezione STIG si applicano alla tua EC2 istanza.

Puoi scegliere quale categoria di conformità STIG applicare.

Livelli di conformità

- Alta (Categoria I)

Il rischio più grave. Include qualsiasi vulnerabilità che può comportare la perdita di riservatezza, disponibilità o integrità.

- Medio (categoria II)

Include qualsiasi vulnerabilità che può comportare la perdita di riservatezza, disponibilità o integrità, ma il rischio può essere mitigato.

- Basso (categoria III)

Include qualsiasi vulnerabilità che degrada le misure di protezione contro la perdita di riservatezza, disponibilità o integrità.

Argomenti

- [Download di componenti di rafforzamento STIG](#)
- [Impostazioni Windows STIG](#)
- [Cronologia delle versioni di Windows STIG](#)
- [Impostazioni Linux STIG](#)
- [Cronologia delle versioni di Linux STIG](#)

Download di componenti di rafforzamento STIG

Amazon raggruppa i componenti di protezione STIG in pacchetti relativi al sistema operativo per ogni versione. I bundle sono file di archivio appropriati per il sistema operativo di destinazione in cui vengono scaricati ed eseguiti. I pacchetti di componenti Linux vengono archiviati come file TAR (estensione.tgz). I pacchetti di componenti Windows vengono archiviati come file ZIP (estensione.zip).

Amazon archivia i pacchetti di componenti nel bucket Image Builder STIG S3 di ciascuno. Regione AWS Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.

Important

Con poche eccezioni, i componenti di protezione STIG scaricati dal documento Systems Manager non installano pacchetti di terze parti. Se sull'istanza sono già installati pacchetti

di terze parti e se ci sono pacchetti correlati STIGs EC2 supportati da Amazon per quel pacchetto, questi STIGs vengono applicati.

I modelli e gli esempi per i percorsi di archiviazione dei componenti e i nomi dei file dei bundle sono i seguenti:

Percorso di archiviazione dei componenti

s3://aws-windows-downloads-*<region>*/STIG/*<bundle file name>*

Variabili del percorso dei componenti

region

Regione AWS (Ogni regione ha il proprio bucket di componenti.)

bundle file name

Il formato è *<os bundle name> _ <YYYY> _Q <quarter> [_<release>]. <file extension>*. Nota che il nome ha caratteri di sottolineatura tra i nodi, non punti.

os bundle name

Il prefisso standard del nome per il pacchetto del sistema operativo è o.

LinuxAWSConfigureSTIG AWSConfigureSTIG Per mantenere la compatibilità con le versioni precedenti, il download per Windows non include un prefisso di piattaforma.

YYYY

L'anno a quattro cifre del rilascio.

quarter

Identifica il trimestre dell'anno: 1, 2, 3 o 4.

release

Numero incrementale che inizia da uno e aumenta di uno per ogni nuova versione. La versione non è inclusa nella prima versione in un trimestre e viene aggiunta solo per le versioni successive.

file extension

Formato di file compresso tgz (Linux) o zip (Windows).

Esempi di nomi di file di bundle

- LinuxAWSConfigureSTIG_2023_Q1_2.tgz
- AWSConfigureSTIG_2022_Q4.zip

Impostazioni Windows STIG

I componenti STIG AMIs e di protezione avanzata di Amazon EC2 Windows sono progettati per server autonomi e applicano criteri di gruppo locali. I componenti conformi a STIG vengono installati InstallRoot dal Dipartimento della Difesa (DoD) su Windows AMIs per scaricare, installare e aggiornare i certificati DoD. Inoltre rimuovono i certificati non necessari per mantenere la conformità STIG. Attualmente, Amazon EC2 supporta le linee di base STIG per le seguenti versioni di Windows Server: 2012 R2, 2016, 2019 e 2022.

Questa sezione elenca le impostazioni STIG correnti EC2 supportate da Amazon per la tua infrastruttura Windows, seguite da un registro della cronologia delle versioni.

Puoi applicare impostazioni STIG basse, medie o alte.

Windows STIG Low (categoria III)

L'elenco seguente contiene le impostazioni STIG EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di protezione STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

[Per un elenco completo di Windows STIGs, consultate la Document Library. STIGs](#) Per informazioni su come visualizzare l'elenco completo, consulta [Strumenti di visualizzazione STIG](#).

- Windows Server 2022 STIG versione 2 versione 2
V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 e V-254481
- Windows Server 2019 STIG versione 3 versione 2
V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 e V-205923
- Windows Server 2016 STIG versione 2 versione 9
V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 e V-225060

- Windows Server 2012 R2 MS STIG versione 3 versione 5

V-225537, V-225536, V-225526, V-225525, V-225514, V-225511, V-225490, V-225489, V-225488, V-225487, V-225485, V-225484, V-225483, V-225482, V-225481, V-225480, V-225479, V-225476, V-225473, V-225468, V-225462, V-225460, V-225459, V-225412, V-225394, V-225392, V-225376, V-225363, V-225362, V-225360, V-225359, V-225358, V-225357, V-225355, V-225343, V-225342, V-225336, V-225335, V-225334, V-225333, V-225332, V-225331, V-225330, V-225328, V-225327, V-225324, V-225319, V-225318 e V-225250

- Microsoft.NET Framework 4.0 STIG Versione 2 Release 2

Nessuna impostazione STIG si applica a Microsoft.NET Framework per le vulnerabilità di categoria III.

- Windows Firewall STIG versione 2 versione 2

V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 e V-242008

- Internet Explorer 11 STIG versione 2 versione 5

V-223016, V-223056 e V-223078

- Microsoft Edge STIG versione 2 versione 2 (solo Windows Server 2022)

V-235727, V-235731, V-235751, V-235752 e V-235765

Windows STIG Medium (categoria II)

L'elenco seguente contiene le impostazioni STIG EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di protezione STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

[Per un elenco completo di Windows STIGs, consultate la Document Library. STIGs](#) Per informazioni su come visualizzare l'elenco completo, consulta [Strumenti di visualizzazione STIG](#).

 Note

La categoria Windows STIG Medium include tutte le impostazioni di protezione STIG elencate che si applicano a Windows STIG low (Categoria III), oltre alle impostazioni di rafforzamento STIG supportate da Amazon EC2 per le vulnerabilità di categoria II.

- Windows Server 2022 STIG versione 2 versione 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-254247, V-254265, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254289, V-254290, V-254291, V-254292, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V-254310, V-254311, V-254312, V-254313, V-254314, V-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254341, V-254342, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254356, V-254358, V-254359, V-254360, V-254361, V-254362, V-254364, V-254366, V-254367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254382, V-254383, V-254384, V-254431, V-254432, V-254433, V-254434, V-254435, V-254436, V-254438, V-254439, V-254442, V-254443, V-254444, V-254445, V-254449, V-254450, V-254451, V-254452, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254476, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254484, V-254485, V-254486, V-254487, V-254488, V-254489, V-254490, V-254493, V-254494, V-254495, V-254497, V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254507, V-254508, V-254509, V-254510, V-254511 e V-254512

- Windows Server 2019 STIG versione 3 versione 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205643, V-205644, V-205648, V-205649, V-205650, V-205651, V-2056651, V-2056652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205678, V-205679, V-205680, V-205681,

V-205682, V-205683, V-205684, V-205685, V-205686, V-205686, V-205686 V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205720, V-205722, V-205729, V-205730, V-205733, V-205747, V-205751, V-205752, V-205754, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205764, V-205765, V-205766, V-205767, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205781, V-205782, V-205783, V-205784, V-205795, V-205796, V-205797, V-792058, V-205788 V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205827, V-205828 V-205830, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838, V-205839, V-205840, V-205841, V-205842, V-205861, V-205863, V-205865, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205924, V-205925, V-236001 e V-257503

- Windows Server 2016 STIG versione 2 versione 9

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224869, V-224870, V-224871, V-224872, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224895, V-224896, V-224897, V-224898, V-224899, V-224900, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224947, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040, V-225041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225058, V-225059, V-225061, V-225062, V-225063, V-225064, V-225065, V-225066, V-225067, V-225068, V-225069, V-225072, V-225073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093, V-236000 e V-257502

- Windows Server 2012 R2 MS STIG versione 3 versione 5

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-225574, V-225573, V-225572, V-225571, V-225570, V-225569, V-225568, V-225567, V-225566, V-225565, V-225564, V-225563, V-225562, V-225561, V-225560, V-225559, V-225558, V-225557, V-225555, V-225554, V-225553, V-225551, V-225550, V-225549, V-225548, V-225546, V-225545, V-225544, V-225543, V-225542, V-225541, V-225540, V-225539, V-225538, V-225535, V-225534, V-225533, V-225532, V-225531, V-225530, V-225529, V-225528, V-225527, V-225524, V-225523, V-225522, V-225521, V-225520, V-225519, V-225518, V-225517, V-225516, V-225515, V-225513, V-225510, V-225509, V-225508, V-225506, V-225504, V-225503, V-225502, V-225501, V-225500, V-225494, V-225486, V-225478, V-225477, V-225475, V-225474, V-225472, V-225471, V-225470, V-225469, V-225464, V-225463, V-225461, V-225461, V-225458, V-225457, V-225456, V-225455, V-225454, V-225453, V-225452, V-225448, V-225443, V-225442, V-225441, V-225415, V-225414, V-225413, V-225411, V-225410, V-225409, V-225408, V-225407, V-225406, V-225405, V-225404, V-225402, V-225401, V-225400, V-225398, V-225397, V-225395, V-225393, V-225391, V-225389, V-225386, V-225385, V-225384, V-225383, V-225382, V-225381, V-225380, V-225379, V-225378, V-225377, V-225375, V-225374, V-225373, V-225372, V-225371, V-225370, V-225369, V-225368, V-225367, V-225356, V-225353, V-225352, V-225351, V-225350, V-225349, V-225348, V-225348, V-225348, V-225352, V-225346, V-225345, V-225344, V-225341, V-225340, V-225339, V-225338, V-225337, V-225329, V-225326, V-225325, V-225317, V-225316, V-225315, V-225314, V-225305, V-225304, V-225303, V-225302, V-225301, V-225300, V-225299, V-225298, V-225297, V-225296, V-225295, V-225294, V-225293, V-225292, V-225291, V-225290, V-225289, V-225288, V-225287, V-225286, V-225285, V-225284, V-225283, V-225282, V-225281, V-225280, V-225279, V-225278, V-225277, V-225276, V-225275, V-225273, V-225272, V-225271, V-225270, V-225269, V-225268, V-225267, V-225266, V-225265, V-225264, V-225263, V-225261, V-225260, V-225259 e V-225239

- Microsoft.NET Framework STIG 4.0 Versione 2 Release 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-225238

- Windows Firewall STIG versione 2 versione 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-241989, V-241990, V-241991, V-241993, V-241993, V-241998, V-241998, V-242003 e V-242003

- Internet Explorer 11 STIG versione 2 versione 5

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-223015, V-223017, V-223018, V-223019, V-223020, V-223021, V-223022, V-223023, V-223024, V-223025, V-223026, V-223027, V-223028, V-223029, V-223030, V-223031, V-223032, V-223033, V-223034, V-223035, V-223036, V-223037, V-223038, V-223039, V-223040, V-223041, V-223042, V-223043, V-223044, V-223045, V-223046, V-223048, V-223049, V-223050, V-223051, V-223052, V-223053, V-223054, V-223055, V-223057, V-223058, V-223059, V-223060, V-223061, V-223062, V-223063, V-223064, V-223065, V-223066, V-223067, V-223068, V-223069, V-223070, V-223071, V-223072, V-223073, V-223074, V-223075, V-223076, V-223077, V-223079, V-223080, V-223081, V-223082, V-223083, V-223084, V-223085, V-223086, V-223087, V-223088, V-223089, V-223090, V-223091, V-223092, V-223093, V-223094, V-223095, V-223096, V-223097, V-223098, V-223099, V-223100, V-223101, V-223102, V-223103, V-223104, V-223105, V-223106, V-223107, V-223108, V-223109, V-223110, V-223111, V-223112, V-223113, V-223114, V-223115, V-223116, V-223117, V-223118, V-223119, V-223120, V-223121, V-223122, V-223123, V-223124, V-223125, V-223126, V-223127, V-223128, V-223129, V-223130, V-223131, V-223132, V-223133, V-223134, V-223135, V-223136, V-223137, V-223138, V-223139, V-223140, V-223141, V-223142, V-223143, V-223144, V-223145, V-223146, V-223147, V-223148, V-223149, V-250540 e V-250541

- Microsoft Edge STIG versione 2 versione 2 (solo Windows Server 2022)

V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774 e V-246736

- Microsoft Defender STIG Versione 2 Release 4

V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465 e V-213466

Windows STIG High (categoria I)

L'elenco seguente contiene le impostazioni STIG EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di protezione STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

[Per un elenco completo di Windows STIGs, consultate la Document Library. STIGs](#) Per informazioni su come visualizzare l'elenco completo, consulta [Strumenti di visualizzazione STIG](#).

Note

La categoria Windows STIG High include tutte le impostazioni di protezione STIG elencate che si applicano alle categorie Windows STIG Medium e Low, oltre alle impostazioni di protezione STIG supportate da Amazon EC2 per le vulnerabilità di categoria I.

- Windows Server 2022 STIG versione 2 versione 2

V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475 e V-254500

- Windows Server 2019 STIG versione 3 versione 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914 e V-205919

- Windows Server 2016 STIG versione 2 versione 9

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054 e V-225079

- Windows Server 2012 R2 MS STIG versione 3 versione 5

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-225556, V-225552, V-225547, V-225507, V-225505, V-225498, V-225497, V-225496, V-225493, V-225492, V-225491, V-225449, V-225444, V-225399, V-225396, V-225390, V-225366, V-225365, V-225364, V-225354 e V-225274

- Microsoft.NET Framework STIG 4.0 Versione 2 Release 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse) per Microsoft.NET Framework. Non si applicano impostazioni STIG aggiuntive per le vulnerabilità di categoria I.

- Windows Firewall STIG versione 2 versione 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-241992, V-241997 e V-242002

- Internet Explorer 11 STIG versione 2 versione 5

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-252910

- Microsoft Edge STIG versione 2 versione 2 (solo Windows Server 2022)

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-235758 e V-235759

- Microsoft Defender STIG Versione 2 Release 4

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-213426, V-213426, V-213452, V-213452, V-213452, V-213453, V-213453 e V-213453

Cronologia delle versioni di Windows STIG

Questa sezione registra la cronologia delle versioni dei componenti di Windows per gli aggiornamenti trimestrali STIG. Per visualizzare le modifiche e le versioni pubblicate per un trimestre, scegliete il titolo per espandere le informazioni.

Modifiche al primo trimestre 2025 - 05/04/2025:

STIGS aggiornato per Internet Explorer 11 STIG versione 2 Release 5 per tutti i componenti STIG per la versione del primo trimestre 2025.

- STIG-Build-Windows-Low versione 2025.1.x
- STIG-Build-Windows-Medium versione 2025.1.x
- STIG-Build-Windows-High versione 2025.1.x

Modifiche al quarto trimestre 2024 - 12/10/2024:

Versioni STIG aggiornate e STIGS applicati per la versione del quarto trimestre 2024 come segue:

STIG-Build-Windows-Low versione 2024.4.0

- Windows Server 2022 STIG versione 2 versione 2
- Windows Server 2019 STIG versione 3 versione 2
- Windows Server 2016 STIG versione 2 versione 9
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 5
- Microsoft Edge STIG versione 2 versione 2 (solo Windows Server 2022)

STIG-Build-Windows-Medium versione 2024.4.0

- Windows Server 2022 STIG versione 2 versione 2
- Windows Server 2019 STIG versione 3 versione 2
- Windows Server 2016 STIG versione 2 versione 9
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5

- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 5
- Microsoft Edge STIG versione 2 versione 2 (solo Windows Server 2022)
- Defender STIG versione 2 versione 4

STIG-Build-Windows-High versione 2024.4.0

- Windows Server 2022 STIG versione 2 versione 2
- Windows Server 2019 STIG versione 3 versione 2
- Windows Server 2016 STIG versione 2 versione 9
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 versione 2
- Internet Explorer 11 STIG versione 2 versione 5
- Microsoft Edge STIG versione 2 versione 2 (solo Windows Server 2022)
- Defender STIG versione 2 versione 4

Modifiche al terzo trimestre 2024 - 10/04/2024 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del terzo trimestre 2024.

Modifiche al secondo trimestre 2024 - 05/10/2024 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del secondo trimestre 2024.

Modifiche al primo trimestre 2024 - 23/02/2024 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del primo trimestre 2024.

Modifiche al quarto trimestre 2023 - 12/07/2023 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del quarto trimestre 2023.

Modifiche al terzo trimestre 2023 - 10/04/2023 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del terzo trimestre 2023.

Modifiche al secondo trimestre 2023 - 05/03/2023 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del secondo trimestre 2023.

Modifiche al 1° trimestre 2023 - 27/03/2023 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del primo trimestre 2023.

Modifiche al quarto trimestre 2022 - 01/02/2023:

Versioni STIG aggiornate e STIGS applicati per la versione del quarto trimestre 2022 come segue:

STIG-Build-Windows-Low versione 2022.4.0

- Windows Server 2022 STIG versione 1 rilascio 1
- Windows Server 2019 STIG versione 2 rilascio 5
- Windows Server 2016 STIG versione 2 rilascio 5
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 2 rilascio 3
- Microsoft Edge STIG versione 1 versione 6 (solo Windows Server 2022)

STIG-Build-Windows-Medium versione 2022.4.0

- Windows Server 2022 STIG versione 1 rilascio 1
- Windows Server 2019 STIG versione 2 rilascio 5
- Windows Server 2016 STIG versione 2 rilascio 5
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2

- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 2 rilascio 3
- Microsoft Edge STIG versione 1 versione 6 (solo Windows Server 2022)
- Defender STIG versione 2 versione 4 (solo Windows Server 2022)

STIG-Build-Windows-High versione 2022.4.0

- Windows Server 2022 STIG versione 1 rilascio 1
- Windows Server 2019 STIG versione 2 rilascio 5
- Windows Server 2016 STIG versione 2 rilascio 5
- Windows Server 2012 R2 MS STIG versione 3 rilascio 5
- Microsoft .NET Framework 4.0 STIG versione 2 rilascio 2
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 2 rilascio 3
- Microsoft Edge STIG versione 1 versione 6 (solo Windows Server 2022)
- Defender STIG versione 2 versione 4 (solo Windows Server 2022)

Modifiche al terzo trimestre 2022 - 30/09/2022 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del terzo trimestre 2022.

Modifiche al secondo trimestre 2022 - 08/02/2022:

Versioni STIG aggiornate e STIGS applicati per la versione del secondo trimestre 2022.

STIG-Build-Windows-Low versione 1.5.0

- Windows Server 2019 STIG versione 2 versione 4
- Windows Server 2016 STIG versione 2 versione 4
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-Medium versione 1.5.0

- Windows Server 2019 STIG versione 2 versione 4
- Windows Server 2016 STIG versione 2 versione 4
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-High versione 1.5.0

- Windows Server 2019 STIG versione 2 versione 4
- Windows Server 2016 STIG versione 2 versione 4
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

Modifiche al 1° trimestre 2022 - 08/02/2022 (nessuna modifica):

Non sono state apportate modifiche al componente Windows STIGS per la versione del primo trimestre 2022.

Modifiche al quarto trimestre 2021 - 20/12/2021:

Versioni STIG aggiornate e STIGS applicato per la versione del quarto trimestre 2021.

STIG-Build-Windows-Low versione 1.5.0

- Windows Server 2019 STIG versione 2 versione 3
- Windows Server 2016 STIG versione 2 versione 3
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-Medium versione 1.5.0

- Windows Server 2019 STIG versione 2 versione 3
- Windows Server 2016 STIG versione 2 versione 3
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-High versione 1.5.0

- Windows Server 2019 STIG versione 2 versione 3
- Windows Server 2016 STIG versione 2 versione 3
- Windows Server 2012 R2 MS STIG versione 3 versione 3
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 1
- Windows Firewall STIG versione 2 rilascio 1
- Internet Explorer 11 STIG versione 1 versione 19

Modifiche al terzo trimestre 2021 - 30/09/2021:

Versioni STIG aggiornate e STIGS applicato per la versione del terzo trimestre 2021.

STIG-Build-Windows-Low versione 1.4.0

- Windows Server 2019 STIG versione 2 versione 2
- Windows Server 2016 STIG versione 2 versione 2
- Windows Server 2012 R2 MS STIG versione 3 versione 2
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 1
- Windows Firewall STIG versione 1 versione 7
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-Medium versione 1.4.0

- Windows Server 2019 STIG versione 2 versione 2

- Windows Server 2016 STIG versione 2 versione 2
- Windows Server 2012 R2 MS STIG versione 3 versione 2
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 1
- Windows Firewall STIG versione 1 versione 7
- Internet Explorer 11 STIG versione 1 versione 19

STIG-Build-Windows-High versione 1.4.0

- Windows Server 2019 STIG versione 2 versione 2
- Windows Server 2016 STIG versione 2 versione 2
- Windows Server 2012 R2 MS STIG versione 3 versione 2
- Microsoft.NET Framework 4.0 STIG Versione 2 Release 1
- Windows Firewall STIG versione 1 versione 7
- Internet Explorer 11 STIG versione 1 versione 19

Impostazioni Linux STIG

Questa sezione contiene informazioni sulle impostazioni di protezione avanzata STIG per Linux EC2 supportate da Amazon, seguite da un registro della cronologia delle versioni. Se la distribuzione Linux non dispone di impostazioni di protezione STIG proprie, Amazon EC2 utilizza le impostazioni RHEL. Le impostazioni di rafforzamento STIG supportate si applicano ad Amazon EC2 Linux AMIs e ai componenti basati sulla distribuzione Linux, come segue:

- Impostazioni STIG di Red Hat Enterprise Linux (RHEL) 7
 - RHEL 7
 - CentOS 7
 - Amazon Linux (2AL2)
- Impostazioni RHEL 8 STIG
 - RHEL 8
 - CentOS 8
 - Amazon Linux 2023 (AL2023)
- Impostazioni RHEL 9 STIG
 - RHEL 9

- CentOS Stream 9

Linux STIG Low (categoria III)

L'elenco seguente contiene le impostazioni STIG EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di protezione STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

[Per un elenco completo, consultate la Document Library STIGs](#) . Per informazioni su come visualizzare l'elenco completo, consulta [Strumenti di visualizzazione STIG](#).

RHEL 7 STIG versione 3 versione 14

- RHEL 7/CentOS 7/ AL2

V-204452, V-204576 e V-204605

RHEL 8 STIG versione 2 versione 2

- RHEL 8/CentOS 8/AL 2023

V-230241, V-230281, V-244527, V-230269, V-230270, V-230285, V-230346, V-230381, V-230395, V-230491, V-230468, V-230469, V-230485, V-230486, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499 e V-230253

RHEL 9 STIG versione 2 Release 3

- RHEL 9/CentOS Stream 9

V-257782, V-257824, V-258138, V-258037, V-257880, V-257795, V-257796, V-258173, V-258069, V-258076, V-258067, V-257946 e V-257947

Ubuntu 18.04 STIG versione 2 versione 15

V-219163, V-219164, V-219165, V-219172, V-219173, V-219174, V-219175, V-219178, V-219180, V-219210, V-219301, V-219327, V-219332 e V-219333

Ubuntu 20.04 STIG versione 2 versione 2

V-238203, V-238202, V-238234, V-238235, V-238237, V-238323, V-238373, V-238221, V-238222, V-238223, V-238224, V-238226, V-238362, V-238357 e V-238308

Ubuntu 22.04 STIG versione 2 versione 3

V-260479, V-260480, V-260481, V-260521, V-260520, V-260476, V-260472, V-260549, V-260550, V-260551, V-260552, V-260581 e V-260596

Ubuntu 24.04 STIG versione 1 versione 1

V-270645, V-270646, V-270664, V-270820, V-270677, V-270690, V-270706, V-270710, V-270695, V-270749, V-270752 e V-270818

Linux STIG Medium (Categoria II)

L'elenco seguente contiene le impostazioni STIG EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di protezione STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

[Per un elenco completo, consultate la Document LibrarySTIGs](#) . Per informazioni su come visualizzare l'elenco completo, consulta [Strumenti di visualizzazione STIG](#).

Note

La categoria Linux STIG Medium include tutte le impostazioni di protezione STIG elencate che si applicano a Linux STIG Low (Categoria III), oltre alle impostazioni di rafforzamento STIG supportate da Amazon EC2 per le vulnerabilità di categoria II.

RHEL 7 STIG versione 3 versione 15

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

- RHEL 7/CentOS 7/ AL2

V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204416, V-204417, V-204418, V-204422, V-204423, V-204426, V-204427, V-204431, V-204434, V-204435, V-204437, V-204449, V-204450, V-204451, V-204457, V-204466, V-204490, V-204491, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204567, V-204568, V-204572, V-204578, V-204579, V-204584, V-204585, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204595, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204619, V-204622, V-204625, V-204630, V-204631, V-204633, V-233307, V-237634, V-237635, V-251703, V-255925, V-255927, V-255928 e V-256970

RHEL 8 STIG versione 2 versione 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

- RHEL 8/CentOS 8/AL 2023

V-230238, V-230239, V-230257, V-230258, V-230259, V-230262, V-230273, V-230275, V-230316, V-230325, V-230366, V-230478, V-230488, V-230489, V-230505, V-230523, V-230550, V-230558, V-230560, V-230561, V-237640, V-244547, V-256974, V-230525, V-244544, V-230248, V-230249, V-230250, V-230245, V-230246, V-230247, V-230397, V-230399, V-230400, V-230401, V-244543, V-230228, V-230298, V-230387, V-230482, V-230231, V-230233, V-230324, V-230365, V-230370, V-230373, V-230378, V-230383, V-230236, V-230314, V-230315, ER-244523, V-257258, V-230266, V-230267, V-230268, V-230280, V-230310, V-230311, V-230312, V-230502, V-230532, MA-230535, V-230536, V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230549, V-244550, V-244551, V-244552, V-244553, V-244554, V-250317, V-251718, V-230237, V-230313, V-230356, V-230357, V-230358, V-230358, V-230358, V-230357, V-230358, V-230358 V-230360, V-230361, V-230362, V-230363, V-230368, V-230369, V-230375, V-230376, V-230377, V-244524, V-244533, V-251713, V-251717, V-251714, V-251715, V-251716, V-23016, V-23030, V-230332, V-230333, V-230335, V-230337, V-230339, V-230341, V-230343, V-230345, V-230240, V-230282, V-250315, V-250316, V-230255, V-230277, V-230278, V-230348, V-230353, V-230386, V-230390, V-230392, V-230394, V-230396, V-230393, V-230398, V-230402, V-230392, V-230392, V-230392, V-230392, V-230392, V-230392, V-230392

V-230398, V-230402, V-230396, V-230398, V-230398, V-230402, V-230392, V-230392, V-230392, V-230392, V-230404, V-230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, V-230418, 230419, V-230421, V-230422, V-230423, V-230423, V-230419, V-230421, V-230423, V-230423, V-230419, V-230421, V-230423, V-230423, V-230419, V-230421, V-230423, V-230423, V-230423, V-23024, V-230425, V-230426, V-230427, V-230428, V-230429, V-230430, V-230431, V-230432, V-230433, 230434, V-230435, V-230436, V-230437, V-230438, V-230439, 230444, V-230446, V-230447, V-230448, V-230449, V-230455, V-230456, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V-230471, V-230472, V-230473, V-230474, V-230480, V-230483, V-244542, V-230503, V-230507, V-244525, V-230244, V-230286, V-230287, V-230288, V-230290, V-230291, V-230296, V-230330, V-230382, V-230526, V-230527, V-230555, V-230556, V-244526, V-244528, V-237642, V-237643 e V-251711

RHEL 9 STIG versione 2 Release 3

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

- RHEL 9/CentOS Stream 9

V-257981, V-257780, V-257825, V-257827, V-257828, V-257829, V-257830, V-257831, V-257832, V-257833, V-257834, V-257836, V-257838, V-257839, V-257840, V-257841, V-257842, V-257882, V-257883, V-257884, V-257885, V-257889, V-257890, V-257891, V-257892, V-257893, V-257894, V-257895, V-257896, V-257897, V-257898, V-257899, V-257900, V-257901, V-257902, V-257903, V-257904, V-257905, V-257906, V-257907, V-257908, V-257909, V-257910, V-257911, V-257912, V-257913, V-257914, V-257915, V-257918, V-257919, V-257920, V-257921, V-257922, V-257923, V-257928, V-257929, V-257930, V-257934, V-257935, V-257943, V-257948, V-257954, V-257978, V-257980, V-258035, V-258041, V-258046, V-258052, V-258063, V-258068, V-258081, V-258082, V-258083, V-258089, V-258120, V-2580124 126, V-258140, V-258141, V-258151, V-258234, V-257886, V-257916, V-257917, V-257952, V-257936, V-257939, V-257940, V-258036, V-258038, V-257887, V-257924, V-257925, V-258145, V-258152, V-258153, V-257887, V-257924, V-257925, V-258145, V-258152, V-258153, V-257887, V-257924, V-257925, V-258145, V-258152, V-258153, V-257887, V-257924, V-257925, V-258145, V-258152, V-258153, V-257887, V-257924, V-257925, V-258145, V-V-258156, V-258157, V-258158, V-258159, V-258160, V-258161, V-258162, V-258163, V-258164, V-258165, V-258166, V-258167, V-258168, V-258169, V-258170, V-258171, V-258172, V-258176, V-258177, V-258178, V-258179, V-258180, V-258181, V-258182, V-258183, V-258184, V-258185, V-258186, V-258187, V-258188, V-258189, V-258190, V-258191, V-258192,

V-258193, V-258194, V-258195, V-258196, V-258197, V-258198, V-258199, V-258200, V-258201, V-258202, V-258203, V-258204, V-258205, V-258206, V-258207, V-258208, V-258209, V-258210, V-258211, V-258212, V-258213, V-258214, V-258215, V-258216, V-258217, V-258219, V-258219, V-2582220, V-258221, V-258222, V-258223, V-258224, V-258225, V-258226, V-258227, V-258228, V-258229, V-257781, V-257783, V-257786, V-257797, V-257798, V-257799, V-257800, V-257801, V-257802, V-257803, V-257809, V-257810, V-257811, V-257812, V-257813, V-257815, V-257816, V-257942, V-257957, V-257958, V-257959, V-257960, V-257961, V-257962, V-257963, V-257964, V-257965, V-257966, V-257967, V-257968, V-257969, V-257970, V-257971, V-257972, V-257973, V-257974, V-257975, V-257976, V-257977, V-258077, V-258128, V V-258129, V-258043, V-258049, V-258071, V-258072, V-258073, V-258074, V-258075, V-258104, V-258105, V-258107, V-258108, V-258109, V-258110, V-258111, V-258117, V-258119, V-257979, V-257982, V-257983, V-257985, V-257987, V-257988, V-257992, V-257993, V-257994, V-257995, V-257996, V-257997, V-257998, V-257999, V-258000, V-258001, V-258002, V-258003, V-258004, V-258005, V-258006, V 258007, V-258008, V-258009, V-258010, V-258011, V-258130, V-257814, V-258054, V-258055, V-258056, V-258057, V-258060, V-258070, V-258080, V-258088, V-258091, V-258092, V-258093, V-258095, V-258095, V-258095, V-258095, V-258091, V-258092, V-258093, V-258095, V-258095, V-258095, V-258091, V-258092, V-258093, V-258095, V-258095, V-258095, V-258091, V-258092, V-258093, V-258095, V-258095, V-258095, V-258091, V-258100, V-258101, V-258102, V-258103, V-258112, V-258113, V-258114, V-258115, V-258116, V-258118, V-258233, V-257951, V-257953, V-258142, V-258144, V-258146, V-258147, V-258148, V-258150, V-258064, V-258065, V-258066, V-258232, V-258237, V-258239, V-258240, V-257788, V-257790, V-257791, V-257792, V-257793, V-257794, V-257817, V-258175, V-257804, V-257805, V-257805, V-257805 6, V-257807, V-257808, V-258034, V-258039, V-257888, V-257926, V-257927, V-257933, V-258084, V-258085, V-257949, V-258040, V-257818, V-257849, V-258122, V-258123, V-258133, V-257944, V-258028, 258079, V-258125 e V-258137

Ubuntu 18.04 STIG versione 2 Release 15

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-219149, V-219155, V-219156, V-219160, V-219166, V-219168, V-219176, V-219181, V-219184, V-219186, V-219188, V-219189, V-219190, V-219191, V-219192, V-219193, V-219194, V-219195, V-219196, V-219197, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219213, V-219214, V-219215, V-219216, V-219217, V-219218, V-219219, V-219220, V-219221, V-219222, V-219223, V-219224, V-219225, V-219226, V-219227, V-219228, V-219229, V-219230, V-219231, V-219232, V-219233, V-219234,

V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243, V-219244, V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267, V-219268, V-219269, V-219270, V-219271, V-219272, V-219273, V-219274, V-219275, V-219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219297, V-219298, V-219299, V-219300, V-219303, V-219304, V-219306, V-219309, V-219310, V-219311, V-219312, V-219315, V-219318, V-219319, V-219323, V-219326, V-219328, V-219330, V-219331, V-219335, V-219336, V-219337, V-219338, V-219339, V-219342, V-219344, V-233779, V-233780 e V- 255906

Ubuntu 20.04 STIG versione 2 Release 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-238200, V-238205, V-238207, V-238231, V-238329, V-238337, V-238339, V-238340, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238350, V-238351, V-238352, V-238371, V-238376, V-238377 V-238378, V-238209, V-238325, V-238330, V-238333, V-238369, V-238230, V-238338, V-238341, V-238342, V-238343, V-238324, V-238353, V-238228, V-238225, V-238227, V-238299, V-238238, V-238239, V-238240, V-238241, V-238241 242, V-238244, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238290, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238300, V-238301, V-238302, V-238304, V-238309, V-238310, V-238315, V-238316, V-238317, V-238318, V-238319, V-238320, V-251505, V-238360, V-238210, V-238211, V-238212, V-238213, V-238220, V-255912, V-238355, V-238236, V-238303, V-238356, V-238359, V-238370, V-238334 e V-238232

Ubuntu 22.04 STIG versione 2 Release 3

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-260546, V-260473, V-260474, V-260478, V-260485, V-260486, V-260487, V-260488, V-260489, V-260490, V-260495, V-260496, V-260496, V-260497, V-260498, V-260499, V-260500, V-260508, V-260513, V-260522, V-260522, V-260522, V-260599 40, V-260542, V-260543, V-260547, V-260554, V-260572, V-260590, V-260475, V-260491, V-260510, V-260511, V-260492, V-260493, V-260494, V-260507, V-260591, V-260594, V-260597, V-260598, V-260505 99, V-260600, V-260601, V-260602, V-260603, V-260604, V-260605, V-260606, V-260607, V-260608, V-260609, V-260610, V-260611, V-260612, V-260613, V-260614, V-260615, V-260616, V-260617, V-260618,

V-260619, V-260620, V-260621, V-260622, V-260623, V-260624, V-260625, V-260626, V-260627, V-260628, V-260629, V-260630, V-260631, V-260632, V-260633, V-260634, V-260635, V-260636, V-260637, V-260638, V-260639, V-260640, V-260641, V-260642, V-260643, V-260644, V-260645, V-260646, V-260647, V-260648, V-260649, V-260471, V-260514, V-260553, V-260576, V-260574, V-260560, V-260561, V-260562, V-260563, V-260564, V-260565, V-260566, V-260567, V-260569, V-260527, V-260528, V-260530, V-260533, V-260534, V-260575, V-260505, V-260506, V-260512, V-260582, V-260584, V-260585, V-260586, V-260477, V-260545, V-260555, V-260556, V-260557, V-260509, V-260588, V-260589, V-260537, V-260538 e V-260535

Ubuntu 24.04 STIG versione 1 versione 1

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria III (bassa), oltre a:

V-270649, V-270651, V-270652, V-270653, V-270654, V-270656, V-270657, V-270659, V-270660, V-270661, V-270662, V-270663, V-270663, V-270669, V-270672, V-270673, V-270674, V-270676, V-270678, V-270679, V-27679, V-2727679, V-2727679, V-27678, V-270679, V-2727679, V-27678, V-270679, V-27679, V-27678, V-270679, V-27679, V-27678, V-270679, V-2727679, V-27678, V-270679, V-27679, V-27678, V-270679, V-27679 0680, V-270681, V-270683, V-270684, V-270685, V-270686, V-270687, V-270688, V-270689, V-270692, V-270693, V-270696, V-270697, V-270698, V-270699, V-270700, V-270701, V-270702, V-270703, V-270703, V-270703 704, V-270705, V-270709, V-270715, V-270716, V-270718, V-270720, V-270721, V-270722, V-270723, V-270724, V-270725, V-270726, V-270727, V-270728, V-270729, V-270730, V-270731, V-270732, V-270733, V-270737, V-270739, V-270740, V-270741, V-270742, V-270743, V-270746, V-270750, V-270753, V-270755, V-270756, V-270757, V-270758, V-270759, V-270760, V-270765, V-270766, V-270767, V-270768, V-270769, V-270770, V-270771, V-270772, V-270773, V-270775, V-270776, V-270777, V-270778, V-270779, V-270780, V-270781, V-270782, V-270783, V-270784, V-270785, V-270786, V-270787 0788, V-270789, V-270790, V-270791, V-270792, V-270793, V-270794, V-270795, V-270796, V-270797, V-270798, V-270799, V-270800, V-270801, V-270802, V-270803, V-270804, V-270805, V-270806, V-270807, V-270808, V-270809, V-270810, V-270811, V-270812, V-270813, V-270814, V-270815, V-270821, V-270822, V-270823, V-270824, V-270825, V-270826, V-270827, V-270828, V-270829, V-270830, V-270831 e V-270832

Linux STIG High (Categoria I)

L'elenco seguente contiene le impostazioni STIG EC2 supportate da Amazon per la tua infrastruttura. Se un'impostazione supportata non è applicabile alla tua infrastruttura, Amazon EC2 ignora tale impostazione e prosegue. Ad esempio, alcune impostazioni di protezione STIG potrebbero non essere applicabili ai server autonomi. Le policy specifiche dell'organizzazione possono inoltre

impedire l'applicazione di alcune impostazioni, come nel caso dell'obbligo per gli amministratori di rivedere le impostazioni dei documenti.

[Per un elenco completo, consultate la Document Library STIGs](#) . Per informazioni su come visualizzare l'elenco completo, consulta [Strumenti di visualizzazione STIG](#).

Note

La categoria Linux STIG High include tutte le impostazioni di protezione STIG elencate che si applicano alle categorie Linux STIG Medium e Low, oltre alle impostazioni di rafforzamento STIG supportate da Amazon EC2 per le vulnerabilità di categoria I.

RHEL 7 STIG versione 3 Release 15

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

- RHEL 7/CentOS 7/ AL2

V-204424, V-204425, V-204442, V-204443, V-204447, V-204448, V-204455, V-204497, V-204502, V-204594, V-204620 e V-204621

RHEL 8 STIG versione 2 versione 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

- RHEL 8/CentOS 8/AL 2023

V-230223, V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533, V-230558 e V-244540

RHEL 9 STIG versione 2 versione 3

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

- RHEL 9/CentOS Stream 9

V-257820, V-257821, V-257826, V-257835, V-257955, V-257956, V-258059, V-258230, V-258238, V-257784, V-257785, V-257984, V-257984, V-257986, V-258078, V-258094 e V-258235

Ubuntu 18.04 STIG versione 2 versione 15

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-219157, V-219158, V-219177, V-219212, V-219308, V-219314, V-219316, V-251507 e V-264388

Ubuntu 20.04 STIG versione 2 versione 2

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-238218, V-238219, V-238201, V-251504, V-238326, V-238327 e V-238380

Ubuntu 22.04 STIG versione 2 versione 3

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-260482, V-260483, V-260523, V-260524, V-260469, V-260526, V-260529, V-260570, V-260571, V-260579 e V-260539

Ubuntu 24.04 STIG versione 1 versione 1

Include tutte le impostazioni di rafforzamento STIG EC2 supportate da Amazon per le vulnerabilità di categoria II e III (medie e basse), oltre a:

V-270647, V-270648, V-270665, V-270666, V-270708, V-270717, V-270711, V-270712, V-270713 e V-270714

Cronologia delle versioni di Linux STIG

Questa sezione registra la cronologia delle versioni dei componenti Linux per gli aggiornamenti trimestrali STIG. Per vedere le modifiche e le versioni pubblicate per un trimestre, scegli il titolo per espandere le informazioni.

Modifiche al primo trimestre 2025 - 11/04/2025:

Sono state aggiornate le seguenti versioni di STIG, applicato STIGS per la versione del primo trimestre 2025 e aggiunto il supporto per Ubuntu 24.04:

STIG-Build-Linux-Low versione 2025.1.x

- RHEL 7 STIG versione 3 versione 15
- RHEL 8 STIG versione 2 versione 2
- RHEL 9 STIG versione 2 versione 3
- Ubuntu 18.04 STIG versione 2 versione 15
- Ubuntu 20.04 STIG versione 2 Release 2
- Ubuntu 22.04 STIG versione 2 Release 3
- Ubuntu 24.04 STIG versione 1 Release 1

STIG-Build-Linux-Medium versione 2025.1.x

- RHEL 7 STIG versione 3 versione 15
- RHEL 8 STIG versione 2 versione 2
- RHEL 9 STIG versione 2 versione 3
- Ubuntu 18.04 STIG versione 2 versione 15
- Ubuntu 20.04 STIG versione 2 Release 2
- Ubuntu 22.04 STIG versione 2 Release 3
- Ubuntu 24.04 STIG versione 1 Release 1

STIG-Build-Linux-High versione 2025.1.x

- RHEL 7 STIG versione 3 versione 15
- RHEL 8 STIG versione 2 versione 2
- RHEL 9 STIG versione 2 versione 3
- Ubuntu 18.04 STIG versione 2 versione 15
- Ubuntu 20.04 STIG versione 2 Release 2
- Ubuntu 22.04 STIG versione 2 Release 3

- Ubuntu 24.04 STIG versione 1 Release 1

Modifiche al quarto trimestre 2024 - 12/10/2024:

Sono state aggiornate le seguenti versioni di STIG, applicato STIGS per la versione del quarto trimestre 2024 e aggiunto informazioni su due nuovi parametri di input per i componenti Linux:

STIG-Build-Linux-Low versione 2024.4.x

- RHEL 7 STIG versione 3 versione 15
- RHEL 8 STIG versione 2 versione 1
- RHEL 9 STIG versione 2 versione 2
- Ubuntu 18.04 STIG versione 2 versione 15
- Ubuntu 20.04 STIG versione 2 Release 1
- Ubuntu 22.04 STIG versione 2 Release 2

STIG-Build-Linux-Medium versione 2024.4.x

- RHEL 7 STIG versione 3 versione 15
- RHEL 8 STIG versione 2 versione 1
- RHEL 9 STIG versione 2 versione 2
- Ubuntu 18.04 STIG versione 2 versione 15
- Ubuntu 20.04 STIG versione 2 Release 1
- Ubuntu 22.04 STIG versione 2 Release 2

STIG-Build-Linux-High versione 2024.4.x

- RHEL 7 STIG versione 3 versione 15
- RHEL 8 STIG versione 2 versione 1
- RHEL 9 STIG versione 2 versione 2
- Ubuntu 18.04 STIG versione 2 versione 15
- Ubuntu 20.04 STIG versione 2 Release 1
- Ubuntu 22.04 STIG versione 2 Release 2

Modifiche al terzo trimestre 2024 - 10/04/2024 (nessuna modifica):

Non sono state apportate modifiche al componente Linux STIGS per la versione del terzo trimestre 2024.

Modifiche al secondo trimestre 2024 - 05/10/2024:

Versioni STIG aggiornate e STIGS applicato per la versione del secondo trimestre 2024. È stato inoltre aggiunto il supporto per RHEL 9, CentOS Stream 9 e Ubuntu 22.04, come segue:

STIG-Build-Linux-Low versione 2024.2.x

- RHEL 7 STIG versione 3 versione 14
- RHEL 8 STIG versione 1 versione 14
- RHEL 9 STIG versione 1 versione 3
- Ubuntu 18.04 STIG versione 2 versione 14
- Ubuntu 20.04 STIG versione 1 versione 12
- Ubuntu 22.04 STIG versione 1 versione 1

STIG-Build-Linux-Medium versione 2024.2.x

- RHEL 7 STIG versione 3 versione 14
- RHEL 8 STIG versione 1 versione 14
- RHEL 9 STIG versione 1 versione 3
- Ubuntu 18.04 STIG versione 2 versione 14
- Ubuntu 20.04 STIG versione 1 versione 12
- Ubuntu 22.04 STIG versione 1 versione 1

STIG-Build-Linux-High versione 2024.2.x

- RHEL 7 STIG versione 3 versione 14
- RHEL 8 STIG versione 1 versione 14
- RHEL 9 STIG versione 1 versione 3
- Ubuntu 18.04 STIG versione 2 versione 14
- Ubuntu 20.04 STIG versione 1 versione 12
- Ubuntu 22.04 STIG versione 1 versione 1

Modifiche al primo trimestre 2024 - 02/06/2024:

Versioni STIG aggiornate e STIGS applicato per la versione del primo trimestre 2024 come segue:

STIG-Build-Linux-Low versione 2024.1.x

- RHEL 7 STIG versione 3 versione 14
- RHEL 8 STIG versione 1 versione 13
- Ubuntu 18.04 STIG versione 2 versione 13
- Ubuntu 20.04 STIG versione 1 versione 11

STIG-Build-Linux-Medium versione 2024.1.x

- RHEL 7 STIG versione 3 versione 14
- RHEL 8 STIG versione 1 versione 13
- Ubuntu 18.04 STIG versione 2 versione 13
- Ubuntu 20.04 STIG versione 1 versione 11

STIG-Build-Linux-High versione 2024.1.x

- RHEL 7 STIG versione 3 versione 14
- RHEL 8 STIG versione 1 versione 13
- Ubuntu 18.04 STIG versione 2 versione 13
- Ubuntu 20.04 STIG versione 1 versione 11

Modifiche al quarto trimestre 2023 - 12/07/2023:

Versioni STIG aggiornate e STIGS applicato per la versione del quarto trimestre 2023 come segue:

STIG-Build-Linux-Low versione 2023.4.x

- RHEL 7 STIG versione 3 versione 13
- RHEL 8 STIG versione 1 versione 12
- Ubuntu 18.04 STIG versione 2 versione 12
- Ubuntu 20.04 STIG versione 1 versione 10

STIG-Build-Linux-Medium versione 2023.4.x

- RHEL 7 STIG versione 3 versione 13
- RHEL 8 STIG versione 1 versione 12
- Ubuntu 18.04 STIG versione 2 versione 12
- Ubuntu 20.04 STIG versione 1 versione 10

STIG-Build-Linux-High versione 2023.4.x

- RHEL 7 STIG versione 3 versione 13
- RHEL 8 STIG versione 1 versione 12
- Ubuntu 18.04 STIG versione 2 versione 12
- Ubuntu 20.04 STIG versione 1 versione 10

Modifiche al terzo trimestre 2023 - 10/04/2023:

Versioni STIG aggiornate e STIGS applicato per la versione del terzo trimestre 2023 come segue:

Linux STIG Low (Categoria III)

- RHEL 7 STIG versione 3 versione 12
- RHEL 8 STIG versione 1 versione 11
- Ubuntu 18.04 STIG versione 2 versione 11
- Ubuntu 20.04 STIG versione 1 versione 9

Linux STIG Medium (Categoria II)

- RHEL 7 STIG versione 3 versione 12
- RHEL 8 STIG versione 1 versione 11
- Ubuntu 18.04 STIG versione 2 versione 11
- Ubuntu 20.04 STIG versione 1 versione 9

Linux STIG High (Categoria I)

- RHEL 7 STIG versione 3 versione 12

- RHEL 8 STIG versione 1 versione 11
- Ubuntu 18.04 STIG versione 2 versione 11
- Ubuntu 20.04 STIG versione 1 versione 9

Modifiche al secondo trimestre 2023 - 05/03/2023:

Versioni STIG aggiornate e STIGS applicato per la versione del secondo trimestre 2023 come segue:

Linux STIG Low (Categoria III)

- RHEL 7 STIG versione 3 versione 11
- RHEL 8 STIG versione 1 versione 10
- Ubuntu 18.04 STIG versione 2 versione 11
- Ubuntu 20.04 STIG versione 1 versione 8

Linux STIG Medium (Categoria II)

- RHEL 7 STIG versione 3 versione 11
- RHEL 8 STIG versione 1 versione 10
- Ubuntu 18.04 STIG versione 2 versione 11
- Ubuntu 20.04 STIG versione 1 versione 8

Linux STIG High (Categoria I)

- RHEL 7 STIG versione 3 versione 11
- RHEL 8 STIG versione 1 versione 10
- Ubuntu 18.04 STIG versione 2 versione 11
- Ubuntu 20.04 STIG versione 1 versione 8

Modifiche al 1° trimestre 2023 - 27/03/2023:

Versioni STIG aggiornate e STIGS applicato per la versione del primo trimestre 2023 come segue:

Linux STIG Low (Categoria III)

- RHEL 7 STIG versione 3 versione 10

- RHEL 8 STIG versione 1 versione 9
- Ubuntu 18.04 STIG versione 2 versione 10
- Ubuntu 20.04 STIG versione 1 versione 7

Linux STIG Medium (Categoria II)

- RHEL 7 STIG versione 3 versione 10
- RHEL 8 STIG versione 1 versione 9
- Ubuntu 18.04 STIG versione 2 versione 10
- Ubuntu 20.04 STIG versione 1 versione 7

Linux STIG High (Categoria I)

- RHEL 7 STIG versione 3 versione 10
- RHEL 8 STIG versione 1 versione 9
- Ubuntu 18.04 STIG versione 2 versione 10
- Ubuntu 20.04 STIG versione 1 versione 7

Modifiche al quarto trimestre 2022 - 02/01/2023:

Versioni STIG aggiornate e STIGS applicato per la versione del quarto trimestre 2022 come segue:

Linux STIG Low (Categoria III)

- RHEL 7 STIG versione 3 versione 9
- RHEL 8 STIG versione 1 versione 8
- Ubuntu 18.04 STIG versione 2 versione 9
- Ubuntu 20.04 STIG versione 1 versione 6

Linux STIG Medium (Categoria II)

- RHEL 7 STIG versione 3 versione 9
- RHEL 8 STIG versione 1 versione 8
- Ubuntu 18.04 STIG versione 2 versione 9

- Ubuntu 20.04 STIG versione 1 versione 6

Linux STIG High (Categoria I)

- RHEL 7 STIG versione 3 versione 9
- RHEL 8 STIG versione 1 versione 8
- Ubuntu 18.04 STIG versione 2 versione 9
- Ubuntu 20.04 STIG versione 1 versione 6

Modifiche al terzo trimestre 2022 - 30/09/2022 (nessuna modifica):

Non ci sono state modifiche per il componente Linux STIGS per la versione del terzo trimestre 2022.

Modifiche al secondo trimestre 2022 - 08/02/2022:

È stato introdotto il supporto per Ubuntu, le versioni STIG aggiornate e STIGS applicato per la versione del secondo trimestre 2022 come segue:

Linux STIG Low (Categoria III)

- RHEL 7 STIG versione 3 Release 7
- RHEL 8 STIG versione 1 versione 6
- Ubuntu 18.04 STIG Versione 2 Release 6 (nuova)
- Ubuntu 20.04 STIG Versione 1 Release 4 (nuova)

Linux STIG Medium (Categoria II)

- RHEL 7 STIG versione 3 versione 7
- RHEL 8 STIG versione 1 versione 6
- Ubuntu 18.04 STIG Versione 2 Release 6 (nuova)
- Ubuntu 20.04 STIG Versione 1 Release 4 (nuova)

Linux STIG High (Categoria I)

- RHEL 7 STIG versione 3 Release 7
- RHEL 8 STIG versione 1 versione 6

- Ubuntu 18.04 STIG Versione 2 Release 6 (nuova)
- Ubuntu 20.04 STIG Versione 1 Release 4 (nuova)

Modifiche al 1° trimestre 2022 - 26/04/2022:

Rifattorizzato per includere un migliore supporto per i contenitori. Combinato lo AL2 script precedente con RHEL 7. Versioni STIG aggiornate e STIGS applicato per la versione del primo trimestre 2022 come segue:

Linux STIG Low (Categoria III)

- RHEL 7 STIG versione 3 versione 6
- RHEL 8 STIG versione 1 versione 5

Linux STIG Medium (categoria II)

- RHEL 7 STIG versione 3 versione 6
- RHEL 8 STIG versione 1 versione 5

Linux STIG High (Categoria I)

- RHEL 7 STIG versione 3 versione 6
- RHEL 8 STIG versione 1 versione 5

Modifiche al quarto trimestre 2021 - 20/12/2021:

Versioni STIG aggiornate e STIGS applicato per la versione del quarto trimestre 2021 come segue:

Linux STIG Low (Categoria III)

- RHEL 7 STIG versione 3 versione 5
- RHEL 8 STIG versione 1 versione 4

Linux STIG Medium (categoria II)

- RHEL 7 STIG versione 3 versione 5
- RHEL 8 STIG versione 1 versione 4

Linux STIG High (Categoria I)

- RHEL 7 STIG versione 3 versione 5
- RHEL 8 STIG versione 1 versione 4

Modifiche al terzo trimestre 2021 - 30/09/2021:

Versioni STIG aggiornate e STIGS applicato per la versione del terzo trimestre 2021 come segue:

Linux STIG Low (Categoria III)

- RHEL 7 STIG versione 3 versione 4
- RHEL 8 STIG versione 1 versione 3

Linux STIG Medium (categoria II)

- RHEL 7 STIG versione 3 versione 4
- RHEL 8 STIG versione 1 versione 3

Linux STIG High (Categoria I)

- RHEL 7 STIG versione 3 versione 4
- RHEL 8 STIG versione 1 versione 3

AWSEC2-PatchLoadBalancerInstance

Descrizione

Aggiorna e applica patch alla versione secondaria di un' EC2 istanza Amazon (Windows o Linux) collegata a qualsiasi sistema di bilanciamento del carico (classico, ALB o NLB). Il tempo di esaurimento della connessione predefinito viene applicato prima della correzione dell'istanza. Puoi ignorare il tempo di attesa inserendo il tempo di drenaggio personalizzato in minuti (1-59) per il parametro. ConnectionDrainTime

Il flusso di lavoro di automazione è il seguente:

1. Viene determinato il sistema di bilanciamento del carico o il gruppo target a cui è collegata l'istanza e l'istanza viene verificata come integra.

2. L'istanza viene rimossa dal sistema di bilanciamento del carico o dal gruppo target.
3. L'automazione attende il periodo di tempo specificato per il periodo di esaurimento della connessione.
4. L'RunPatchBaselineautomazione [AWS](#) viene chiamata per applicare patch all'istanza.
5. L'istanza viene ricollegata al sistema di bilanciamento del carico o al gruppo target.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Prerequisiti

- Verificare che SSM Agent sia installato nell'istanza. Per ulteriori informazioni, consulta [Lavorare con SSM Agent sulle EC2 istanze per Windows Server](#).

Parametri

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) ID dell'istanza da applicare alla patch associata a un sistema di bilanciamento del carico (classico, ALB o NLB).

- ConnectionDrainTime

Tipo: stringa

Descrizione: (Facoltativo) Il tempo di esaurimento della connessione del load balancer, in minuti (-).
1 59

- S3BucketLog

Tipo: stringa

Descrizione: (Facoltativo) Il nome del bucket Amazon S3 da utilizzare per archiviare le risposte di output dei comandi. Puoi specificare un bucket di tua proprietà o un bucket condiviso con te. Se fornisci questo parametro, devi fornire `runCommandAssume` anche `Role`.

- `runCommandAssumeRuolo`

Tipo: stringa

Descrizione: (Facoltativo) L'ARN del ruolo IAM da utilizzare per eseguire il comando sull'istanza. Il ruolo deve avere una relazione di fiducia con il responsabile del **ssm.amazonaws.com** servizio, deve avere la `SSMMManaged InstanceCore` policy di Amazon allegata e deve disporre delle autorizzazioni di scrittura per il bucket Amazon S3 specificato per `S3`. `BucketLog`

AWSEC2-SQLServerDBRestore

Descrizione

Il `AWSEC2-SQLServerDBRestore` runbook ripristina i backup del database Microsoft SQL Server archiviati in Amazon S3 su SQL Server 2017 in esecuzione su un'istanza Linux Amazon Elastic Compute Cloud (). EC2 Puoi fornire la tua EC2 istanza che esegue SQL Server 2017 Linux. Se non viene fornita un' EC2 istanza, l'automazione avvia e configura una nuova EC2 istanza di Ubuntu 16.04 con SQL Server 2017. L'automazione supporta il ripristino dei backup dei log transazionali, differenziali e completi. Questa automazione accetta più file di backup del database e ripristina automaticamente il backup valido più recente di ogni database nei file forniti.

Per automatizzare il backup e il ripristino di un database SQL Server locale su un'EC2 istanza che esegue SQL Server 2017 Linux, puoi utilizzare lo script `-signed`. AWS PowerShell [MigrateSQLServerToEC2Linux](#)

Important

Questo runbook reimposta la password utente dell'amministratore del server SQL Server (SA) ogni volta che viene eseguita l'automazione. Al termine dell'automazione, è necessario impostare nuovamente la propria password utente SA prima di connettersi all'istanza di SQL Server.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Prerequisiti

Per eseguire questa automazione, è necessario soddisfare i seguenti prerequisiti:

- L'utente o il ruolo IAM che esegue questa automazione deve disporre di una policy in linea associata alle autorizzazioni descritte in [Autorizzazioni IAM richieste](#)
- Se fornisci la tua istanza: EC2
 - L' EC2 istanza fornita deve essere un'istanza Linux che esegue Microsoft SQL Server 2017.
 - L' EC2 istanza fornita deve essere configurata con un profilo di istanza AWS Identity and Access Management (IAM) a cui è allegata la policy AmazonSSMManagedInstanceCore gestita. Per ulteriori informazioni, consulta [Creazione di un profilo dell'istanza IAM per Systems Manager](#).
 - L'agente SSM deve essere installato sull' EC2 istanza. Per ulteriori informazioni, consulta [Installazione e configurazione dell'agente SSM su EC2 istanze](#) per Linux.
 - L' EC2 istanza deve disporre di spazio libero su disco sufficiente per scaricare e ripristinare i backup di SQL Server.

Limitazioni

Questa automazione non supporta il ripristino su SQL Server in esecuzione su EC2 istanze di Windows Server. Questa automazione ripristina solo i backup dei database compatibili con SQL Server Linux 2017. Per ulteriori informazioni, consulta [Edizioni e funzionalità supportate di SQL Server 2017 in Linux](#).

Parametri

Questa automazione ha i seguenti parametri:

- DatabaseNames

Tipo: stringa

Descrizione: (facoltativo) elenco separato da virgole con i nomi dei database da ripristinare.

- DataDirectorySize

Tipo: stringa

Descrizione: (Facoltativo) Dimensione del volume desiderata (GiB) della directory SQL Server Data per la nuova EC2 istanza.

Valore predefinito: 100

- KeyPair

Tipo: stringa

Descrizione: (Facoltativo) Coppia di chiavi da utilizzare per la creazione della nuova EC2 istanza.

- IamInstanceProfileName

Tipo: stringa

Descrizione: (Facoltativo) Il profilo dell'istanza IAM da collegare alla nuova EC2 istanza. Al profilo dell'istanza IAM deve essere associata la policy AmazonSSMManagedInstanceCore gestita.

- InstanceId

Tipo: stringa

Descrizione: (facoltativo) l'istanza che esegue SQL Server 2017 in Linux. Se non InstanceId viene fornito alcun valore, l'automazione avvia una nuova EC2 istanza utilizzando l' InstanceType and SQLServer Edition fornita.

- InstanceType

Tipo: stringa

Descrizione: (Facoltativo) Il tipo di EC2 istanza dell'istanza da avviare.

- S3 PresignedUrl

Tipo: stringa

Descrizione: (Facoltativo) Se S3Input è un URL S3 prefirato, indica. yes

Valore predefinito: no

Valori validi: sì | no

- LogDirectorySize

Tipo: stringa

Descrizione: (Facoltativo) Dimensione del volume desiderata (GiB) della directory di log di SQL Server per la nuova EC2 istanza.

Valore predefinito: 100

- Ingresso S3

Tipo: stringa

Descrizione: (obbligatorio) nome del bucket S3, elenco separato da virgole delle chiavi degli oggetti S3 o elenco separato da virgole di S3 prefirato contenente i file di backup SQL da ripristinare. URLs

- SQLServerEdizione

Tipo: stringa

Descrizione: (Facoltativo) L'edizione di SQL Server 2017 da installare sull'istanza appena creata. EC2

Valori validi: Standard | Enterprise | Web | Express

- SubnetId

Tipo: stringa

Descrizione: (Facoltativo) La sottorete in cui avviare la nuova EC2 istanza. La sottorete deve disporre di connettività in uscita ai servizi. AWS Se non SubnetId viene fornito un valore per, l'automazione utilizza la sottorete predefinita.

- TempDbDirectorySize

Tipo: stringa

Descrizione: (Facoltativo) Dimensione del volume desiderata (GiB) della directory TempDB di SQL Server per la nuova istanza. EC2

Valore predefinito: 100

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::ACCOUNTID:role/ROLENAME"
    }
  ]
}
```

Fasi del documento

Per utilizzare questa automazione, segui i passaggi che si applicano al tuo tipo di istanza:

Per le nuove EC2 istanze:

1. `aws:executeAwsApi`- Recupera l'ID AMI per SQL Server 2017 su Ubuntu 16.04.
2. `aws:runInstances`- Avvia una nuova EC2 istanza per Linux.
3. `aws:waitForAwsResourceProperty`- Attendi che l' EC2 istanza appena creata sia pronta.
4. `aws:executeAwsApi`- Riavvia l'istanza se l'istanza non è pronta.
5. `aws:assertAwsResourceProperty`- Verifica che SSM Agent sia installato.
6. `aws:runCommand`- Esegui lo script di ripristino di SQL Server in PowerShell.

Per le EC2 istanze esistenti:

1. `aws:waitForAwsResourceProperty`- Verifica che l' EC2 istanza sia pronta.
2. `aws:executeAwsApi`- Riavvia l'istanza se l'istanza non è pronta.
3. `aws:assertAwsResourceProperty`- Verifica che SSM Agent sia installato.
4. `aws:runCommand`- Esegui lo script di ripristino di SQL Server in PowerShell.

Output

`GetInstance`. `InstanceId`

`restoreToNewIstanza`. `Output`

`restoreToExistingIstanza`. `Output`

AWSsupport-ActivateWindowsWithAmazonLicense

Descrizione

Il `AWSsupport-ActivateWindowsWithAmazonLicense` runbook attiva un'istanza Amazon Elastic Compute Cloud (Amazon EC2) per Windows Server con una licenza fornita da Amazon. L'automazione verifica e configura le impostazioni del sistema operativo del servizio di gestione delle chiavi richieste e i tentativi di attivazione. Ciò include i percorsi del sistema operativo verso i server di gestione delle chiavi di Amazon e le impostazioni del sistema operativo del servizio di gestione delle chiavi. L'impostazione del `AllowOffline` parametro su `true` consente all'automazione di indirizzare correttamente le istanze che non sono gestite da AWS Systems Manager, ma richiede l'arresto e l'avvio dell'istanza.

 Note

Questo runbook non può essere utilizzato sul modello Bring Your Own License (BYOL) Windows Server istanze. Per informazioni su come utilizzare la licenza, consulta la pagina sulle [licenze Microsoft su AWS](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AllowOffline

Tipo: stringa

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (Facoltativo) Impostalo su `true` se consenti una riparazione offline dell'attivazione di Windows nel caso in cui la risoluzione dei problemi online non riesca o se l'istanza fornita non è un'istanza gestita.

 Important

Il metodo offline richiede che l' EC2 istanza fornita venga interrotta e quindi avviata. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico verrà modificato se non si utilizza un IP elastico.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ForceActivation

Tipo: stringa

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (Facoltativo) Impostalo su true se desideri continuare anche se Windows è già attivato.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) ID dell' EC2 istanza gestita per Windows Server.

- SubnetId

Tipo: stringa

Impostazione predefinita: CreateNew VPC

Descrizione: (Facoltativo) Solo offline: l'ID di sottorete dell'istanza EC2 Rescue utilizzato per eseguire la risoluzione dei problemi offline. SelectedInstanceSubnetUtilizzalo per utilizzare la stessa sottorete dell'istanza o CreateNewVPC per creare un nuovo VPC. IMPORTANTE: la sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Consigliamo che l' EC2 istanza che riceve il comando abbia un ruolo IAM con la policy gestita di `SSMManagedInstanceCoreAmazon` Amazon allegata. È necessario disporre almeno di `ssm: StartAutomationExecution` e `ssm: SendCommand` per eseguire l'automazione e inviare il comando all'istanza, più `ssm: GetAutomationExecution` per poter leggere l'output dell'automazione. Per la riparazione offline, consulta le autorizzazioni necessarie da `AWSSupport-StartEC2RescueWorkflow`

Fasi del documento

1. `aws:assertAwsResourceProperty`- Verifica che la piattaforma dell'istanza fornita sia Windows.
2. `aws:assertAwsResourceProperty`- Verifica che l'istanza fornita sia un'istanza gestita:
 - a. (Correzione dell'attivazione online) Se l'istanza di input è un'istanza gestita, esegui `aws:runCommand` per eseguire lo PowerShell script per tentare di correggere l'attivazione di Windows.
 - b. (Correzione dell'attivazione offline) Se l'istanza di input non è un'istanza gestita:
 - i. `aws:assertAwsResourceProperty`- Verifica che il `AllowOffline` flag sia impostato su `true` In tal caso, viene avviata la correzione offline, altrimenti l'automazione termina.
 - ii. `aws:executeAutomation`- Richiama `AWSSupport-StartEC2RescueWorkflow` con lo script di correzione dell'attivazione offline di Windows. Lo script utilizza `EC2 Config` o `EC2 Launch`, a seconda della versione del sistema operativo.
 - iii. `aws:executeAwsApi`- Leggi il risultato da `AWSSupport-StartEC2RescueWorkflow`.

Output

`activateWindows.Output`

`getActivateWindowsOfflineResult.Uscita`

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Descrizione

Il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook analizza la connettività da un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o da un'interfaccia di rete elastica a un endpoint. Servizio AWS IPv6 non è supportato. Il runbook utilizza il valore specificato per il `ServiceEndpoint` parametro per analizzare la connettività a un endpoint. Se non è possibile trovare un AWS PrivateLink endpoint nel tuo VPC, il runbook utilizza un indirizzo IP pubblico per il

servizio corrente. Regione AWS Questa automazione utilizza Reachability Analyzer di Amazon Virtual Private Cloud. Per ulteriori informazioni, consulta [Cos'è Reachability Analyzer?](#) , in Reachability Analyzer.

Questa automazione verifica quanto segue:

- Verifica se il tuo cloud privato virtuale (VPC) è configurato per utilizzare il server DNS fornito da Amazon.
- Verifica se esiste un AWS PrivateLink endpoint nel VPC per quello Servizio AWS specificato. Se viene trovato un endpoint, l'automazione verifica che l'`privateDnsattributo` sia attivato.
- Verifica se l' AWS PrivateLink endpoint utilizza la policy predefinita per gli endpoint.

Considerazioni

- Ti viene addebitato un costo per ogni analisi eseguita tra un'origine e una destinazione. Per ulteriori informazioni, consulta la pagina dei [Prezzi di Amazon VPC](#).
- Durante l'automazione, vengono creati un percorso di analisi della rete e un'analisi delle informazioni di rete. Se l'automazione viene completata correttamente, il runbook elimina queste risorse. Se la fase di pulizia fallisce, il percorso di network Insights non viene eliminato dal runbook e sarà necessario eliminarlo manualmente. Se non elimini manualmente il percorso di network Insights, esso continua a essere conteggiato ai fini della quota prevista per il tuo. Account AWS Per ulteriori informazioni sulle quote per Reachability Analyzer, vedere Quotas for Reachability Analyzer in [Reachability Analyzer](#).
- Le configurazioni a livello di sistema operativo come l'uso di un proxy, un resolver DNS locale o un file hosts possono influire sulla connettività anche se il Reachability Analyzer ritorna. PASS
- Esamina la valutazione di tutti i controlli eseguiti dal Reachability Analyzer. Se uno qualsiasi dei controlli restituisce uno stato di FAIL, ciò potrebbe influire sulla connettività anche se il controllo di raggiungibilità complessivo restituisce uno stato di. PASS

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Origine

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon o dell'interfaccia di rete da cui desideri analizzare la raggiungibilità.

- ServiceEndpoint

Tipo: stringa

Descrizione: (Obbligatorio) Il nome host dell'endpoint del servizio su cui desideri analizzare la raggiungibilità.

- RetainVpcReachabilityAnalysis

Tipo: stringa

Impostazione predefinita: false

Descrizione: (Facoltativo) Determina se il percorso di analisi della rete e la relativa analisi creata vengono conservati. Per impostazione predefinita, le risorse utilizzate per analizzare la raggiungibilità vengono eliminate dopo un'analisi riuscita. Se scegli di conservare l'analisi, il runbook non elimina l'analisi e puoi visualizzarla nella console Amazon VPC. Nell'output dell'automazione è disponibile un collegamento alla console.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

1. `aws:executeScript`: convalida l'endpoint del servizio tentando di risolvere il nome host.
2. `aws:executeScript`: raccoglie dettagli sul VPC e sulla sottorete.
3. `aws:executeScript`: valuta la configurazione DNS del VPC.
4. `aws:executeScript`: valuta i controlli degli endpoint VPC.
5. `aws:executeScript`: individua un gateway Internet per la connessione all'endpoint del servizio pubblico.
6. `aws:executeScript`: determina la destinazione da utilizzare per l'analisi della raggiungibilità.
7. `aws:executeScript`: analizza la raggiungibilità dalla sorgente all'endpoint utilizzando Reachability Analyzer e pulisce le risorse se l'analisi ha esito positivo.

8. `aws:executeScript`: genera un rapporto di valutazione della raggiungibilità.
9. `aws:executeScript`: genera l'output in JSON.

Output

- `generateReport.EvalReport`- I risultati dei controlli eseguiti dall'automazione in formato testo.
- `generateJsonOutput.Output`- Una versione minimale dei risultati in formato JSON.

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

Descrizione

Il `AWSPremiumSupport-ChangeInstanceTypeIntelToAMD` runbook automatizza le migrazioni da istanze Amazon Elastic Compute Cloud (Amazon EC2) con tecnologia Intel ai tipi di istanze equivalenti con tecnologia AMD. Questo runbook supporta istanze generiche (M), burstable generiche (T), ottimizzate per il calcolo (C) e ottimizzate per la memoria (R) basate sul sistema Nitro. Questo runbook può essere utilizzato su istanze non gestite da Systems Manager.

Per ridurre il rischio potenziale di perdita di dati e tempi di inattività, il runbook verifica il comportamento di arresto dell'istanza, se l'istanza fa parte di un gruppo Amazon EC2 Auto Scaling, lo stato dell'istanza e se il tipo di istanza equivalente con tecnologia AMD è disponibile nella stessa zona di disponibilità. Per impostazione predefinita, questo runbook non modifica il tipo di istanza se sono collegati volumi di Instance Store o se l'istanza fa parte di uno stack AWS CloudFormation. Se desideri modificare questo comportamento, specifica uno `yes` dei parametri `AllowInstanceStoreInstances` e `AllowCloudFormationInstances`.

Important

L'accesso ai `AWSPremiumSupport-*` runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, [consulta Confronta Supporto i piani](#).

Considerazioni

- Ti consigliamo di eseguire il backup dell'istanza prima di utilizzare questo runbook.
- La modifica del tipo di istanza richiede che il runbook interrompa l'istanza. Quando un'istanza viene arrestata, tutti i dati memorizzati nella RAM o nei volumi dell'Instance Store vengono persi e l'

IPv4 indirizzo pubblico automatico viene rilasciato. Per ulteriori informazioni, consulta [Arrestare e avviare un'istanza](#).

- Se non si specifica un valore per il `TargetInstanceType` parametro, il runbook tenta di identificare l'istanza AMD equivalente in termini di memoria CPUs e virtuale all'interno della stessa famiglia di istanze. Il runbook termina se non è in grado di identificare un tipo di istanza AMD equivalente.
- Utilizzando l'`DryRun` opzione, è possibile acquisire il tipo di istanza AMD equivalente e convalidare i requisiti senza modificare effettivamente il tipo di istanza.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `Riconoscere`

Tipo: stringa

Descrizione: (Obbligatorio) Inserisci `yes` per confermare che l'istanza di destinazione verrà interrotta se è in esecuzione.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon di cui desideri modificare il tipo.

- TargetInstanceType

Tipo: stringa

Predefinito: automatico

Descrizione: (Facoltativo) Il tipo di istanza AMD in cui desideri modificare l'istanza. Il `automatic` valore predefinito utilizza il tipo di istanza equivalente in termini di memoria CPUs e virtuale. Ad esempio, un `m5.large` verrebbe modificato in `m5a.large`.

- AllowInstanceStoreInstances

Tipo: stringa

Valori validi: no | sì

Impostazione predefinita: no

Descrizione: (Facoltativo) Se si specificayes, il runbook viene eseguito su istanze a cui sono collegati volumi di Instance Store.

- AllowCloudFormationInstances

Tipo: stringa

Valori validi: no | sì

Impostazione predefinita: no

Descrizione: (Facoltativo) Se impostato suyes, il runbook viene eseguito su istanze che fanno parte di uno AWS CloudFormation stack.

- AllowCrossGeneration

Tipo: stringa

Valori validi: no | sì

Descrizione: (Facoltativo) Se impostato su yes, il runbook tenta di trovare il tipo di istanza AMD equivalente più recente all'interno della stessa famiglia di istanze.

- DryRun

Tipo: stringa

Valori validi: no | sì

Impostazione predefinita: no

Descrizione: (Facoltativo) Se impostato su yes, il runbook restituisce il tipo di istanza AMD equivalente e convalida i requisiti di migrazione senza apportare modifiche al tipo di istanza.

- SleepWait

Tipo: stringa

Impostazione predefinita: S PT3

Descrizione: (Facoltativo) Il tempo che il runbook deve attendere prima di iniziare una nuova automazione. Il valore fornito per questo parametro deve corrispondere allo standard ISO 8601.

Per ulteriori informazioni sulla creazione di stringhe ISO 8601, vedere [Formattazione delle stringhe di data e ora per Systems Manager](#).

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

1. `aws:assertAwsResourceProperty`: conferma che lo stato dell' EC2 istanza Amazon di destinazione è `runningpending`, `stopped`, o `stopping`. In caso contrario, l'automazione termina.
2. `aws:executeAwsApi`: raccoglie le proprietà dall' EC2 istanza Amazon di destinazione.
3. `aws:branch`: suddivide l'automazione in base allo stato dell' EC2 istanza Amazon.
 - a. In caso `stopped` o `stopping` affermativo, l'automazione viene eseguita `aws:waitForAwsResourceProperty` fino al completo arresto dell' EC2 istanza Amazon.
 - b. In caso `running pending` affermativo, l'automazione viene eseguita `aws:waitForAwsResourceProperty` fino a quando l' EC2 istanza Amazon non supera i controlli di stato.
4. `aws:assertAwsResourceProperty`: conferma che l' EC2 istanza Amazon non fa parte di un gruppo Auto Scaling controllando se il `aws:autoscaling:groupName` tag è applicato.
5. `aws:executeAwsApi`: raccoglie le proprietà del tipo di istanza corrente per trovare il tipo di istanza AMD equivalente.
6. `aws:assertAwsResourceProperty`: conferma che un codice Marketplace AWS prodotto non è associato all' EC2 istanza Amazon. Alcuni prodotti non sono disponibili per tutti i tipi di istanze.
7. `aws:branch`: suddivide l'automazione a seconda che si desideri che l'automazione controlli se l' EC2 istanza Amazon fa parte di uno AWS CloudFormation stack
 - a. Se il `aws:cloudformation:stack-name` tag viene applicato all'istanza, l'automazione viene eseguita `aws:assertAwsResourceProperty` per confermare che l'istanza non fa parte di uno AWS CloudFormation stack.
8. `aws:branch`: suddivide l'automazione in base al fatto che il tipo di volume root dell'istanza sia Amazon Elastic Block Store (Amazon EBS).
9. `aws:assertAwsResourceProperty`: conferma che il comportamento di chiusura dell'istanza è `stop` corretto e negativo. `terminate`

- 10aws:executeScript: conferma che esiste una sola automazione di questo runbook destinata all'istanza corrente. Se è già in corso un'altra automazione destinata alla stessa istanza, restituisce un errore e termina.
- 11aws:executeAwsApi: restituisce un elenco dei tipi di istanze AMD con la stessa quantità di memoria e v. CPUs
- 12aws:executeScript: verifica se il tipo di istanza corrente è supportato e restituisce il tipo di istanza AMD equivalente. Se non esiste un equivalente, l'automazione termina.
- 13aws:executeScript: conferma che il tipo di istanza AMD è disponibile nella stessa zona di disponibilità e verifica le autorizzazioni IAM fornite.
- 14aws:branch: Suddivide l'automazione in base al fatto che il valore del DryRun parametro sia o meno. yes
- 15aws:branch: Verifica se il tipo di istanza originale e quello di destinazione coincidono. Se sono uguali, l'automazione termina.
- 16aws:executeAwsApi: ottiene lo stato corrente dell'istanza.
- 17aws:changeInstanceState: interrompe l' EC2 istanza Amazon.
- 18aws:changeInstanceState: Forza l'arresto dell'istanza se è bloccata nello stato di arresto.
- 19aws:executeAwsApi: modifica il tipo di istanza nel tipo di istanza AMD di destinazione.
- 20aws:sleep: attende 3 secondi dopo la modifica del tipo di istanza per garantire la coerenza finale.
- 21aws:branch: suddivide l'automazione in base allo stato precedente dell'istanza. In caso affermativorunning, l'istanza viene avviata.
- a. aws:changeInstanceState: avvia l' EC2 istanza Amazon se era in esecuzione prima di cambiare il tipo di istanza.
 - b. aws:waitForAwsResourceProperty: attende che l' EC2 istanza Amazon superi i controlli di stato. Se l'istanza non supera i controlli di stato, torna al tipo di istanza originale.
 - i. aws:changeInstanceState: interrompe l' EC2 istanza Amazon prima di sostituirla con il tipo di istanza originale.
 - ii. aws:changeInstanceState: forza l'interruzione dell' EC2 istanza Amazon prima di cambiarla con il tipo di istanza originale nel caso in cui rimanga bloccata in uno stato di arresto.
 - iii. aws:executeAwsApi: riporta l' EC2 istanza Amazon al tipo originale.
 - iv. aws:sleep: attende 3 secondi dopo la modifica del tipo di istanza per garantire la coerenza finale.

- v. `aws:changeInstanceState`: avvia l' EC2 istanza Amazon se era in esecuzione prima di cambiare il tipo di istanza.
- vi. `aws:waitForAwsResourceProperty`: attende che l' EC2 istanza Amazon superi i controlli di stato.

22.`aws:sleep`: Attende prima di terminare il runbook.

AWSSupport-CheckXenToNitroMigrationRequirements

Descrizione

Il `AWSSupport-CheckXenToNitroMigrationRequirements` runbook verifica che un'istanza Amazon Elastic Compute Cloud (Amazon EC2) soddisfi i prerequisiti per modificare correttamente il tipo di istanza da un'istanza di tipo Xen a un tipo di istanza basata su Nitro. Questa automazione verifica quanto segue:

- Il dispositivo root è un volume Amazon Elastic Block Store (Amazon EBS).
- L'`enaSupport` attributo è abilitato.
- Il modulo ENA è installato sull'istanza.
- Il NVMe modulo è installato sull'istanza. In caso affermativo, il modulo viene installato e uno script verifica che il modulo sia caricato nell'`initramfs` immagine.
- Analizza `/etc/fstab` e cerca i dispositivi a blocchi montati utilizzando i nomi dei dispositivi.
- Determina se il sistema operativo (OS) utilizza nomi di interfaccia di rete prevedibili per impostazione predefinita.

Questo runbook supporta i seguenti sistemi operativi:

- 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

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Impostazione predefinita: false

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon di cui desideri verificare i prerequisiti prima di migrare a un tipo di istanza basato su Nitro.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie dettagli sull'istanza.
- `aws:executeAwsApi`- Raccoglie informazioni sull'hypervisor per l'istanza.
- `aws:branch`- Si ramifica in base al fatto che l'istanza di destinazione stia già eseguendo un tipo di istanza basato su Nitro.
- `aws:branch`- Verifica se il sistema operativo dell'istanza è supportato dalle istanze basate su Nitro.
- `aws:assertAwsResourceProperty`- Verifica che l'istanza specificata sia gestita da Systems Manager e che lo stato sia `Online`.
- `aws:branch`- Filiali in base al fatto che il dispositivo principale dell'istanza sia un volume Amazon EBS.
- `aws:branch`- Filiali in base al fatto che l'attributo ENA sia abilitato per l'istanza.
- `aws:runCommand`- Verifica la presenza di driver ENA sull'istanza.
- `aws:runCommand`- Verifica la presenza di NVMe driver sull'istanza.

- `aws:runCommand`- Verifica la presenza di `fstab` formati non riconosciuti nel file.
- `aws:runCommand`- Verifica la configurazione prevedibile del nome dell'interfaccia sull'istanza.
- `aws:executeScript`- Genera l'output in base ai passaggi precedenti.

Output

`FinalOutput.output` - I risultati dei controlli eseguiti dall'automazione.

AWSSupport-ConfigureEC2Metadata

Descrizione

Questo runbook ti aiuta a configurare le opzioni del servizio di metadata dell'istanza (IMDS) per le istanze Amazon Elastic Compute Cloud (Amazon). EC2 Utilizzando questo runbook, puoi configurare quanto segue:

- Imponi l'uso, ad IMDSv2 esempio, dei metadati.
- Configura il valore. `HttpPutResponseHopLimit`
- Consenti o nega l'accesso ai metadati dell'istanza.

Per ulteriori informazioni sui metadati delle istanze, consulta [Configuring the Instance Metadata Service](#) nella Amazon EC2 User Guide.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Applica IMDSv2

Tipo: stringa

Valori validi: obbligatorio | opzionale

Predefinito: opzionale

Descrizione: (Facoltativo) Applica. IMDSv2 Se lo desideri `required`, verrà utilizzata solo l' EC2 istanza Amazon IMDSv2. Se lo desideri `optional`, puoi scegliere tra IMDSv1 e IMDSv2 per l'accesso ai metadati.

 Important

Se lo applichi IMDSv2, le applicazioni che lo utilizzano IMDSv1 potrebbero non funzionare correttamente. Prima dell'applicazione IMDSv2, assicurati che le applicazioni che utilizzano IMDS siano aggiornate a una versione che supporti. IMDSv2 Per informazioni su Instance Metadata Service versione 2 (IMDSv2), consulta [Configuring the Instance Metadata Service](#) nella Amazon EC2 User Guide.

- HttpPutResponseHopLimit

Tipo: integer

Valori validi: 0-64

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il valore limite dell'hop di risposta HTTP PUT desiderato (1-64), ad esempio le richieste di metadati. Questo valore controlla il numero di hop che la risposta PUT può attraversare. Per evitare che la risposta si sposti all'esterno dell'istanza, specificate il 1 valore del parametro.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon di cui desideri configurare le impostazioni dei metadati.

- MetadataAccess

Tipo: stringa

Valori validi: abilitato | disabilitato

Impostazione predefinita: abilitato

Descrizione: (Facoltativo) Consenti o nega l'accesso ai metadati dell'istanza nell'istanza Amazon EC2 . Se lo specifichi `disabled`, tutti gli altri parametri verranno ignorati e l'accesso ai metadati verrà negato per l'istanza.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

Fasi del documento

1. `branchOnMetadataAccess` - Automazione delle filiali in base al valore del `MetadataAccess` parametro.
2. `disableMetadataAccess` - Richiama l'azione `ModifyInstanceMetadataOptions` API per disabilitare l'accesso agli endpoint dei metadati.
3. `branchOnHttpPutResponseHopLimit` - Automazione delle filiali in base al valore del `HttpPutResponseHopLimit` parametro.
4. `maintainHopLimitAndConfigureImdsVersion` - Se `HttpPutResponseHopLimit` è 0, mantiene il limite di hop corrente e modifica altre opzioni di metadati.

5. `waitBeforeAssertingIMDSv2Stato`: attende 30 secondi prima di affermare IMDSv2 lo stato.
6. `setHopLimitAndConfigureImdsVersion` - Se `HttpPutResponseHopLimit` è maggiore di 0, configura le opzioni dei metadati utilizzando i parametri di input forniti.
7. `waitBeforeAssertingHopLimit` - Attende 30 secondi prima di affermare le opzioni dei metadati.
8. `assertHopLimit` - Asserisce che la `HttpPutResponseHopLimit` proprietà è impostata sul valore specificato.
9. `branchVerificationOnIMDSv2Opzione` - Verifica dei rami in base al valore del `EnforceIMDSv2` parametro.
- 10 `assert IMDSv2IsOptional` : afferma il `HttpTokens` valore impostato su. `optional`
- 11 `assert IMDSv2 IsEnforced` - Asserisce il valore impostato su `HttpTokens`. `required`
- 12 `waitBeforeAssertingMetadataState` - Attende 30 secondi prima di affermare che lo stato dei metadati è disabilitato.
- 13 `assertMetadatalIsDisabilitato`: afferma che i metadati sono. `disabled`
- 14 `describeMetadataOptions` - Ottiene le opzioni relative ai metadati dopo l'applicazione delle modifiche specificate.

Output

`describeMetadataOptions.Stato`

`describeMetadataOptions.MetadataAccess`

`describeMetadataOptions.IMDSv2`

`describeMetadataOptions.HttpPutResponseHopLimit`

AWSSupport-ContainEC2Instance

Descrizione

Il `AWSSupport-ContainEC2Instance` runbook fornisce una soluzione automatizzata per la procedura descritta nell'articolo [How do I isolate the Amazon EC2 Instance di fronte a un'istanza potenzialmente compromessa](#) o sospetta? I rami di automazione dipendono dai valori specificati.

Come funziona?

Questo runbook di automazione `AWSSupport-ContainEC2Instance` esegue il contenimento di rete di un' EC2 istanza Amazon attraverso una serie di passaggi coordinati. Quando viene eseguito in

Contain modalità, convalida innanzitutto i parametri di input e verifica se l'istanza non è terminata. Quindi esegue il backup della configurazione corrente del gruppo di sicurezza in un bucket Amazon S3 per un successivo ripristino. Il runbook crea due gruppi di sicurezza: un gruppo di sicurezza temporaneo «all access» e un gruppo di sicurezza finale «di contenimento». Passa gradualmente le interfacce di rete dell'istanza dai gruppi di sicurezza originali al gruppo di sicurezza con accesso illimitato e infine al gruppo di sicurezza di contenimento. Se specificato, crea sia dati non crittografati che crittografati AMI backup dell'istanza. Per le istanze in un gruppo Auto Scaling, gestisce le modifiche necessarie al gruppo Auto Scaling e porta l'istanza in stato di standby. Quando viene eseguito in Release modalità, ripristina l'istanza alla configurazione di rete originale utilizzando le impostazioni di backup di Amazon S3. Il runbook supporta un DryRun parametro per visualizzare in anteprima le azioni senza apportare modifiche effettive e include meccanismi completi di gestione e segnalazione degli errori in tutti i flussi di lavoro di contenimento e rilascio.

Important

- Questo runbook esegue diverse operazioni che richiedono privilegi elevati, come la modifica dei gruppi di sicurezza, la creazione AMIs e interazione con i gruppi di Auto Scaling. Queste azioni potrebbero potenzialmente portare a un aumento dei privilegi o influire su altri carichi di lavoro del tuo account. È necessario esaminare le autorizzazioni concesse al ruolo specificato dal AutomationAssumeRole parametro e assicurarsi che siano appropriate per il caso d'uso previsto. Puoi fare riferimento alla seguente AWS documentazione per ulteriori informazioni sulle autorizzazioni IAM: [AWS Identity and Access Management \(IAM\) Permissions](#)[AWS Systems Manager Automation Permissions](#)
- Questo runbook esegue azioni mutative che potrebbero potenzialmente causare indisponibilità o interruzione dei carichi di lavoro. In particolare, modifica i gruppi di sicurezza associati all' EC2 istanza Amazon di destinazione, il che potrebbe influire sulla connettività di rete. Inoltre, se l'istanza fa parte di un gruppo Auto Scaling, il runbook può modificare la configurazione del gruppo, influenzando potenzialmente sul suo comportamento di scalabilità.
- Durante il processo di contenimento, questo runbook crea risorse aggiuntive, come gruppi di sicurezza e AMIs. Sebbene queste risorse siano contrassegnate per l'identificazione, è necessario essere consapevoli della loro creazione e garantire una corretta pulizia o gestione dopo il completamento del processo di contenimento.
- Se il Action parametro è impostato suRelease, questo runbook tenta di ripristinare la configurazione dell' EC2 istanza Amazon allo stato originale. Tuttavia, esiste il rischio che

il processo di ripristino non riesca, lasciando l'istanza in uno stato incoerente. Il runbook fornisce istruzioni per il ripristino manuale in caso di tali errori, ma è necessario essere preparati a gestire potenziali problemi durante il processo di ripristino.

Si consiglia di esaminare attentamente il runbook, comprenderne i potenziali impatti e testarlo in un ambiente non di produzione prima di eseguirlo nell'ambiente di produzione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- scalabilità automatica: `CreateOrUpdateTags`
- scalabilità automatica: `DeleteTags`
- scalabilità automatica: `DescribeAutoScalingGroups`
- scalabilità automatica: `DescribeAutoScalingInstances`
- scalabilità automatica: `DescribeTags`
- scalabilità automatica: `EnterStandby`
- scalabilità automatica: `ExitStandby`
- scalabilità automatica: `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
- kms:CreateGrant
- kms:DescribeKey
- kms:GenerateDataKeyWithoutPlaintext
- kms:ReEncryptFrom
- kms: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

Politica di esempio:

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

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-ContainEC2Instance](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - AutomationAssumeRole (Facoltativo):

- **Descrizione:** (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.
- **Tipo:** `AWS::IAM::Role::Arn`
- **Azione (richiesta):**
 - **Descrizione:** (Obbligatorio) Seleziona se Contain isolare l' EC2 istanza Amazon o provare Restore a ripristinare la configurazione originale della configurazione dell' EC2 istanza Amazon da un backup precedente.
 - **Tipo:** stringa
 - **Modello consentito:** `Contain|Restore`
- **DryRun (Opzionale):**
 - **Descrizione:** (Facoltativo) Se impostata su `true`, l'automazione non eseguirà nessuno dei comandi, ma riporterà invece cosa avrebbe tentato di fare, dettagliando ogni passaggio. Valore predefinito: `true`.
 - **Tipo:** Booleano
 - **Valori consentiti:** `true|false`
- **Crea AMIBackup (opzionale):**
 - **Descrizione:** (Facoltativo) Se impostato su `true`, un AMI dell' EC2 istanza Amazon verrà creata prima di eseguire le azioni di contenimento.
 - **Tipo:** Booleano
 - **Valori consentiti:** `true|false`
- **KmsKey (Facoltativo):**
 - **Descrizione:** (Facoltativo) L'ID della AWS KMS chiave che verrà utilizzata per creare un file crittografato AMI dell' EC2 istanza Amazon di destinazione. L'impostazione predefinita è impostata su `alias/aws/ebs`.
 - **Tipo:** stringa
 - **Modello consentito:** `^(((arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}:[0-9]{12}:key/)?([a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}|mrk-[a-f0-9]{32}))|(arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}:[0-9]{12}:)?alias/.{1,}))$`
- **BackupS3 BucketName (condizionale):**

- **Descrizione:** bucket Amazon S3 (condizionale) per caricare la configurazione Action quando Contain è o per ripristinare la configurazione quando lo è. Action Release Nota: se il bucket fornito non esiste nell'account, l'automazione creerà un bucket Amazon S3 per tuo conto.
- **Tipo:** `AWS::S3::Bucket::Name`
- **TagIdentifier (Facoltativo):**
 - **Descrizione:** (Facoltativo) Un tag nel formato `Key=BatchId, Value=78925` che verrà aggiunto alle AWS risorse create o modificate da questo runbook durante il flusso di lavoro di contenimento. Questo tag può essere utilizzato per identificare e gestire le risorse associate durante il processo di contenimento. Durante il flusso di lavoro di ripristino, il tag specificato da questo parametro verrà rimosso dalle risorse. Nota: le chiavi e i valori dei tag fanno distinzione tra maiuscole e minuscole.
 - **Tipo:** stringa
 - **Modello consentito:** `^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{1,128}, [Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{0,128}$`
- **BackupS3 BucketAccess (condizionale):**
 - **Descrizione:** (Condizionale) L'ARN degli utenti o dei ruoli IAM a cui sarà consentito l'accesso al bucket Amazon S3 di backup dopo l'esecuzione delle azioni di contenimento. Questo parametro è obbligatorio quando è. Action Contain L'utente oAutomationAssumeRole, in sua assenza, l'utente nel cui contesto viene eseguita l'automazione viene aggiunto automaticamente all'elenco.
 - **Tipo:** stringa
 - **Modello consentito:** `^[arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\\\/[\\w+\\/=, .@-]+$`
- **IngressTrafficRules (Opzionale):**
 - **Descrizione:** (Facoltativo) Una mappa separata da virgole delle regole di ingresso dei gruppi di sicurezza con Cidr FromPort e ToPort nel formato `[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}]` da applicare all'istanza Amazon EC2. IpProtocol Se non viene fornita alcuna regola, all' EC2 istanza Amazon verrà associato un gruppo di sicurezza senza regole di ingresso, isolandola efficacemente dal traffico in entrata.
 - **Tipo:** MapList

- Modello consentito: `^\\{\\}$|^\\{"Cidr\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"IpProtocol\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"FromPort\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"ToPort\\":\\"[\\x00-\\x7F+]{0,255}\\"}\\$`
- EgressTrafficRules (Opzionale):
 - Descrizione: (Facoltativo) Una mappa separata da virgole delle regole di uscita dei gruppi di sicurezza con Cidr FromPort e ToPort nel formato [{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}] da applicare all'istanza Amazon Amazon EC2 . IpProtocol Se non viene fornita alcuna regola, all' EC2 istanza Amazon verrà associato un gruppo di sicurezza senza regole di uscita, impedendo efficacemente tutto il traffico in uscita.
 - Tipo: MapList
 - Modello consentito: `^\\{\\}$|^\\{"Cidr\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"IpProtocol\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"FromPort\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"ToPort\\":\\"[\\x00-\\x7F+]{0,255}\\"}\\$`
- Backup S3 KeyName (opzionale):
 - Descrizione: (Facoltativo) Se Action impostato suRestore, specifica la chiave Amazon S3 che l'automazione utilizzerà per tentare di ripristinare la configurazione dell'istanza EC2 Amazon di destinazione. La chiave Amazon S3 segue in genere questo formato: {year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json La chiave può essere ottenuta dall'output di una precedente esecuzione di automazione del contenimento.
 - Tipo: stringa
 - Modello consentito: `^[a-zA-Z0-9\\._\\-\\!\\*\\'\\(\\)]{0,1024}$`

4. Seleziona Esegui.

5. L'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- ValidateRequiredInputs

Verifica che siano stati forniti tutti gli input richiesti.

- AssertInstanceIsNotTerminated

Verifica se l' EC2 istanza Amazon di destinazione non è terminata (eliminata).

- GetAutoScalingInstanceInfo

Ottiene il ciclo di vita dell' EC2 istanza Amazon e il nome del gruppo se l' EC2 istanza Amazon di destinazione fa parte di un gruppo Auto Scaling.

- CheckBackupS3BucketName

Verifica se il bucket Amazon S3 di destinazione concede read potenzialmente l'accesso write pubblico ai suoi oggetti. Se il bucket non esiste, viene creato un nuovo bucket Amazon S3BackupS3BucketName.

- BranchOnActionAndMode

Suddivide l'automazione in base ai parametri di input e. Action DryRun

- BranchOnAutoScalingGroupMembership

Suddivide l'automazione in base al fatto che l' EC2 istanza Amazon di destinazione faccia parte del gruppo Auto Scaling e al relativo stato del ciclo di vita.

- DescribeAutoScalingGroups

Ottiene e archivia la configurazione del gruppo Amazon EC2 Auto Scaling associata.

- ModifyAutoScalingGroup

Modifica la configurazione del gruppo Amazon EC2 Auto Scaling associato per le azioni di contenimento, impostando l'istanza EC2 Amazon sullo stato e regolando Standby la capacità del gruppo Auto Scaling. MinSize

- BackupInstanceSecurityGroups

Ottiene e archivia la configurazione dei gruppi di sicurezza Amazon EC2 Instance di destinazione.

- CreateAllAccessSecurityGroup

Crea un gruppo di sicurezza temporaneo che consente tutto il traffico in ingresso che sostituisce i gruppi di sicurezza di Amazon EC2 Instance di destinazione.

- CreateContainmentSecurityGroup

Crea un gruppo di sicurezza di contenimento restrittivo con le regole di ingresso e uscita specificate e sostituisce il gruppo temporaneo ad accesso completo con tale gruppo.

- BranchOnCreateAMIBackup

Suddivide l'automazione in base al parametro di input. CreateAMIBackup

- `AssertSourceInstanceRootVolumeIsEbs`

Verifica se il volume root di Amazon EC2 Instance di destinazione è Amazon EBS.

- `CreateImage`

Crea un AMI dell' EC2 istanza Amazon di destinazione.

- `RestoreInstanceConfiguration`

Ripristina la configurazione Amazon EC2 Instance di destinazione dal backup.

- `ReportContain`

Fornisce i dettagli del dry run per le azioni di contenimento.

- `ReportRestore`

Fornisce i dettagli del funzionamento a secco per le azioni di ripristino.

- `ReportRestoreFailure`

Fornisce istruzioni per ripristinare la configurazione originale di Amazon EC2 Instance di destinazione durante uno scenario di errore del flusso di lavoro di ripristino.

- `ReportContainmentFailure`

Fornisce istruzioni per ripristinare la configurazione originale di Amazon EC2 Instance di destinazione durante uno scenario di errore del flusso di lavoro di contenimento.

- `FinalOutput`

Fornisce i dettagli delle azioni di contenimento.

7. Una volta completata l'esecuzione, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- `FinalOutput.Output`

Restituisce i dettagli delle azioni di contenimento eseguite da questo runbook quando `DryRun` è impostato su `False`.

- `RestoreInstanceConfiguration.Output`

Emette le azioni di ripristino eseguite da questo runbook quando `DryRun` è impostato su `False`.

- `ReportContain.Output`

Restituisce i dettagli delle azioni di contenimento eseguite da questo runbook quando DryRun è impostato su True.

- ReportRestore.Output

Restituisce i dettagli delle azioni di ripristino eseguite da questo runbook quando DryRun è impostato su True.

- ReportContainmentFailure.Output

Fornisce istruzioni per ripristinare la configurazione originale di Amazon EC2 Instance di destinazione durante uno scenario di errore del flusso di lavoro di contenimento.

- ReportRestoreFailure.Output

Fornisce istruzioni per ripristinare la configurazione originale di Amazon EC2 Instance di destinazione durante uno scenario di errore del flusso di lavoro di ripristino.

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esecuzione di un'automazione semplice](#)
- [Configurazione dell'automazione](#)
- [Flussi di lavoro di Support Automation](#)

AWSSupport-CopyEC2Instance

Descrizione

Il AWSSupport-CopyEC2Instance runbook fornisce una soluzione automatizzata per la procedura descritta nell'articolo del Knowledge Center [Come posso spostare la mia EC2 istanza su un'altra sottorete, zona di disponibilità o VPC?](#) I rami di automazione dipendono dai valori specificati per i parametri and. Region SubnetId

Se specificate un valore per il SubnetId parametro ma non un valore per il Region parametro, l'automazione crea un Amazon Machine Image (AMI) dell'istanza di destinazione e avvia una nuova istanza dal AMI nella sottorete specificata.

Se si specifica un valore per il SubnetId parametro e il Region parametro, l'automazione crea un AMI dell'istanza di destinazione, copia il AMI all'indirizzo Regione AWS specificato e avvia una nuova istanza dal AMI nella sottorete specificata.

Se si specifica un valore per il Region parametro ma non un valore per il SubnetId parametro, l'automazione crea un AMI dell'istanza di destinazione, copia il AMI nella regione specificata e avvia una nuova istanza dal AMI nella sottorete predefinita del cloud privato virtuale (VPC) nella regione di destinazione.

Se non viene specificato alcun valore per i SubnetId parametri Region o, l'automazione crea un AMI dell'istanza di destinazione e avvia una nuova istanza dal AMI nella sottorete predefinita del tuo VPC.

Per copiare un AMI in una regione diversa, è necessario fornire un valore per il AutomationAssumeRole parametro. Se l'automazione scade durante la waitForAvailableDestinationAmi fase, AMI potrebbe essere ancora in fase di copia. In tal caso, puoi attendere il completamento della copia e avviare l'istanza manualmente.

Prima di eseguire questa automazione, tieni presente quanto segue:

- AMI sono basati su snapshot di Amazon Elastic Block Store (Amazon EBS). Per file system di grandi dimensioni senza uno snapshot precedente, AMI la creazione può richiedere diverse ore. Per diminuire il AMI ora di creazione, crea uno snapshot Amazon EBS prima di creare il AMI.
- Creare un AMI non crea un'istantanea, ad esempio memorizza i volumi sull'istanza. Per informazioni sul backup dei volumi di Instance Store su Amazon EBS, consulta [Come posso eseguire il backup di un volume di Instance Store sulla mia EC2 istanza Amazon su Amazon EBS?](#)
- La nuova EC2 istanza Amazon ha un indirizzo IPv6 IP pubblico IPv4 o privato diverso. È necessario aggiornare tutti i riferimenti ai vecchi indirizzi IP (ad esempio, nelle voci DNS) con i nuovi indirizzi IP assegnati alla nuova istanza. Se utilizzi un indirizzo IP elastico sulla tua istanza di origine, assicurati di collegarlo alla nuova istanza.
- I problemi di conflitto tra gli identificatori di sicurezza del dominio (SID) possono verificarsi quando la copia viene avviata e tenta di contattare il dominio. Prima di acquisire l'AMI, utilizza Sysprep o rimuovi l'istanza aggiunta al dominio dal dominio per evitare problemi di conflitto. Per ulteriori informazioni, vedere [Come posso usare Sysprep per creare e installare Windows riutilizzabili personalizzati? AMIs](#)

[Esegui questa automazione \(console\)](#)

 Important

Non è consigliabile utilizzare questo runbook per copiare le istanze del controller di dominio Microsoft Active Directory.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza che si desidera copiare.

- KeyPair

Tipo: stringa

Descrizione: (Facoltativo) La coppia di chiavi che desideri associare alla nuova istanza copiata. Se stai copiando l'istanza in una regione diversa, assicurati che la coppia di chiavi esista nella regione specificata.

- Regione

Tipo: stringa

Descrizione: (Facoltativo) La regione in cui vuoi copiare l'istanza. Se si specifica un valore per questo parametro, ma non si specificano valori per i `SecurityGroupIds` parametri `SubnetId` e, l'automazione tenta di avviare l'istanza nel VPC predefinito con il gruppo di sicurezza predefinito. Se EC2 -Classic è abilitato nella regione di destinazione, l'avvio avrà esito negativo.

- SubnetId

Tipo: stringa

Descrizione: (Facoltativo) L'ID della sottorete in cui si desidera copiare l'istanza. Se EC2 -Classic è abilitato nella regione di destinazione, è necessario fornire un valore per questo parametro.

- InstanceType

Tipo: stringa

Descrizione: (Facoltativo) Il tipo di istanza con cui deve essere avviata l'istanza copiata. Se non si specifica un valore per questo parametro, viene utilizzato il tipo di istanza di origine. Se il tipo di istanza di origine non è supportato nella regione in cui viene copiata l'istanza, l'automazione ha esito negativo.

- SecurityGroupIds

Tipo: stringa

Descrizione: (Facoltativo) Un elenco separato da virgole del gruppo di sicurezza IDs che si desidera associare all'istanza copiata. Se non si specifica un valore per questo parametro e l'istanza non viene copiata in un'altra regione, vengono utilizzati i gruppi di sicurezza associati all'istanza di origine. Se stai copiando l'istanza in una regione diversa, viene utilizzato il gruppo di sicurezza predefinito per il VPC predefinito nella regione di destinazione.

- KeepImageSourceRegion

Tipo: Booleano

Valori validi: true | false

Impostazione predefinita: true

Descrizione: (Facoltativo) Se si specifica `true` questo parametro, l'automazione non elimina il AMI dell'istanza di origine. Se si specifica `false` questo parametro, l'automazione annulla la registrazione AMI ed elimina le istantanee associate.

- `KeepImageDestinationRegion`

Tipo: Booleano

Valori validi: `true` | `false`

Impostazione predefinita: `true`

Descrizione: (Facoltativo) Se si specifica `true` questo parametro, l'automazione non elimina il AMI che viene copiato nella regione specificata. Se si specifica `false` questo parametro, l'automazione annulla la registrazione AMI ed elimina le istantanee associate.

- `NoRebootInstanceBeforeTakingImage`

Tipo: Booleano

Valori validi: `true` | `false`

Impostazione predefinita: `false`

Descrizione: (Facoltativo) Se si specifica `true` questo parametro, l'istanza di origine non verrà riavviata prima di aver creato il AMI. Quando si utilizza questa opzione, l'integrità del file system sull'immagine creata non può essere garantita.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

Se stai copiando l'istanza in un'altra regione, avrai bisogno anche delle seguenti autorizzazioni.

- `ec2:CopyImage`

Fasi del documento

- `describeOriginalInstanceDettagli`: raccoglie i dettagli dall'istanza da copiare.
- `assertRootVolumeIsEbs` - Verifica se il tipo di dispositivo del volume principale è `ebs`, in caso contrario, termina l'automazione.
- `evalInputParameters` - Valuta i valori forniti per i parametri di input.
- `createLocalAmi` - Crea un AMI dell'istanza di origine.
- `tagLocalAmi` - Contrassegna il AMI creato nel passaggio precedente.
- `branchAssertRegionIsSame` - Rami in base al fatto che l'istanza venga copiata all'interno della stessa regione o in una regione diversa.
- `branchAssertSameRegionWithKeyPair` - Rami in base al fatto che sia stato fornito un valore per il `KeyPair` parametro per un'istanza che viene copiata all'interno della stessa regione.
- `sameRegionLaunchInstanceWithKeyPair` - Avvia un' EC2 istanza Amazon dal AMI dell'istanza di origine nella stessa sottorete o nella sottorete specificata utilizzando la coppia di chiavi specificata.
- `sameRegionLaunchInstanceWithoutKeyPair` - Avvia un' EC2 istanza Amazon dal AMI dell'istanza di origine nella stessa sottorete o nella sottorete specificata senza una key pair.
- `copyAmiToRegion`: copia il AMI nella regione di destinazione.
- `waitForAvailableDestinationAmi` - Attende la copia AMI stato da diventare `available`
- `destinationRegionLaunchIstanza`: avvia un' EC2 istanza Amazon utilizzando l'istanza copiata AMI.
- `branchAssertDestinationAmiToDelete` - Rami basati sul valore che hai fornito per il `KeepImageDestinationRegion` parametro.
- `deregisterDestinationAmiAndDeleteSnapshots` - Annulla la registrazione del file copiato AMI ed elimina le istantanee associate.
- `branchAssertSourceAmiToDelete` - Rami basati sul valore fornito per il `KeepImageSourceRegion` parametro.
- `deregisterSourceAmiAndDeleteSnapshots` - Annulla la registrazione AMI creato dall'istanza di origine ed elimina le istantanee associate.
- `sleep`: interrompe l'automazione per 2 secondi. Questa è una fase terminale.

Output

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchIstanza. DestinationInstanceIds

AWSSupport-EnableWindowsEC2SerialConsole

Descrizione

Il runbook `AWSSupport-EnableWindowsEC2SerialConsole` aiuta ad abilitare Amazon EC2 Serial Console, Special Admin Console (SAC) e il menu di avvio sulla tua istanza Amazon EC2 Windows. Con la funzionalità Console seriale di Amazon Elastic Compute Cloud (Amazon EC2), hai accesso alla porta seriale dell' EC2 istanza Amazon per risolvere problemi di avvio, configurazione di rete e altri problemi. Il runbook automatizza i passaggi necessari per abilitare la funzionalità sulle istanze in stato di esecuzione e gestite da AWS Systems Manager, nonché su quelle in stato interrotto o non gestite da AWS Systems Manager.

Come funziona?

Il runbook `AWSSupport-EnableWindowsEC2SerialConsole` automazione aiuta ad abilitare SAC e il menu di avvio su EC2 istanze Amazon che eseguono Microsoft Windows Server. Per le istanze in esecuzione e gestite da AWS Systems Manager, il runbook esegue uno PowerShell script `Run Command` per abilitare AWS Systems Manager SAC e il menu di avvio. Per le istanze in stato di arresto o non gestite da AWS Systems Manager, il runbook utilizza il [AWSSupport-StartEC2RescueWorkflow](#) per creare un' EC2 istanza Amazon temporanea per eseguire le modifiche richieste offline.

Per ulteriori informazioni, consulta [Amazon EC2 Serial Console per istanze Windows](#).

Important

- Se abiliti SAC su un'istanza, i EC2 servizi Amazon che si basano sul recupero della password non funzioneranno dalla console Amazon. EC2 Per ulteriori informazioni, consulta [Utilizzo di SAC per risolvere i problemi relativi all'istanza di Windows](#).
- Per configurare l'accesso alla console seriale, devi concedere l'accesso alla console seriale a livello di account e quindi configurare le politiche AWS Identity and Access Management (IAM) per concedere l'accesso ai tuoi utenti. È inoltre necessario configurare un utente con

password su ogni istanza in modo che gli utenti possano utilizzare la console seriale per la risoluzione dei problemi. Per ulteriori informazioni, consulta [Configurare l'accesso alla Amazon EC2 Serial Console](#).

- Per verificare se la console seriale è abilitata sul tuo account, consulta [Visualizza lo stato di accesso dell'account alla console seriale](#).
- L'accesso alla console seriale è supportato solo su istanze virtualizzate basate sul sistema [Nitro](#).

Per ulteriori informazioni, consulta i [prerequisiti](#) di Amazon EC2 Serial Console.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingInstances",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:Describe*",
        "ec2:createTags",
        "ec2:createImage",
        "ssm:DescribeAutomationExecutions",
```

```

        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "iam:GetInstanceProfile",
        "ssm:GetParameters",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
    ],
    "Resource": [
        "arn:${Partition}:ec2:${Region}:${AccountId}:instance/
${InstanceId}",
        "arn:${Partition}:ec2:${Region}:${AccountId}:volume/
${VolumeId}",
        "arn:${Partition}:iam::${AccountId}:instance-profile/
${InstanceProfileName}",
        "arn:${Partition}:ssm:${Region}::parameter/aws/service/*",
        "arn:${Partition}:ssm:${Region}::automation-definition/
AWSSupport-StartEC2RescueWorkflow:*",
        "arn:${Partition}:ssm:${Region}::document/AWS-
ConfigureAWSPackage",
        "arn:${Partition}:ssm:${Region}::document/AWS-
RunPowerShellScript"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack"
    ],
    "Resource": "*",
    "Condition": {

```

```

        "StringLike": {
            "aws:RequestTag/Name": "AWSSupport-EC2Rescue: *"
        },
        "ForAllValues:StringEquals": {
            "aws:TagKeys": [
                "AWSSupport-EC2Rescue-AutomationExecution",
                "Name"
            ]
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "cloudformation:DeleteStack",
            "cloudformation:DescribeStackEvents",
            "cloudformation:DescribeStackResource",
            "cloudformation:DescribeStacks",
            "ec2:AttachVolume",
            "ec2:DetachVolume",
            "ec2:RebootInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances",
            "ssm:SendCommand"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "aws:ResourceTag/Name": "AWSSupport-EC2Rescue: *"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateLaunchTemplate",
            "ec2>DeleteLaunchTemplate",
            "ec2:RunInstances"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:CalledVia": [
                    "cloudformation.amazonaws.com"
                ]
            }
        }
    }
}

```

```

    ]
  }
}
},
{
  "Effect": "Allow",
  "Action": [
    "iam:PassRole"
  ],
  "Resource": "*",
  "Condition": {
    "StringLikeIfExists": {
      "iam:PassedToService": [
        "ssm.amazonaws.com",
        "ec2.amazonaws.com"
      ]
    }
  }
}
]
}
}

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Passa a `AWSSupport-EnableWindowsEC2SerialConsole` nella AWS Systems Manager console.
2. Seleziona `Execute automation` (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:

- `InstanceId`: (Obbligatorio)

L'ID dell' EC2 istanza Amazon a cui desideri abilitare la console EC2 seriale Amazon (SAC) e il menu di avvio.

- `AutomationAssumeRole`: (Facoltativo)

L'Amazon Resource Name (ARN) del ruolo IAM che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `HelperInstanceType`: (Condizionale)

Il tipo di EC2 istanza Amazon fornita dal runbook per configurare la console EC2 seriale Amazon per un'istanza offline.

- **HelperInstanceProfileName:** (Condizionale)

Il nome di un profilo di istanza IAM esistente per l'istanza helper. Se stai abilitando SAC e il menu di avvio su un'istanza che è in stato di arresto o non è gestita da AWS Systems Manager, questo è necessario. Se non viene specificato un profilo di istanza IAM, l'automazione ne crea uno per tuo conto.

- **SubnetId:** (Condizionale)

L'ID di sottorete per un'istanza di supporto. Per impostazione predefinita, utilizza la stessa sottorete in cui risiede l'istanza fornita.

Important

Se si fornisce una sottorete personalizzata, questa deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint Systems Manager. Questo è necessario solo se l'istanza di destinazione è interrotta o non è gestita da AWS Systems Manager

- **CreateInstanceBackupBeforeScriptExecution:** (Facoltativo)

Specificare True per creare un backup Amazon Machine Images (AMI) dell' EC2istanza Amazon prima di abilitare SAC e il menu di avvio. L'AMI verrà conservata dopo il completamento dell'automazione. È responsabilità dell'utente proteggere l'accesso all'AMI o eliminarlo.

- **BackupAmazonMachineImagePrefix:** (Condizionale)

Un prefisso per l'Amazon Machine Image (AMI) che viene creato se il **CreateInstanceBackupBeforeScriptExecution** parametro è impostato True su.

Input parameters	
InstanceId (Required) The ID of Amazon EC2 instance that you want to enable EC2 serial console, Special Admin Console (SAC), and boot menu. Show interactive instance picker i-01234567890abcde0	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. EC2SerialConsole-MinimumRole-AutomationAssumeRole-7noDR7gLLT	HelperInstanceType (Conditional) The type of Amazon EC2 instance that the runbook provisions to configure EC2 serial console for an offline instance. t3.medium
SubnetId (Conditional) The subnet ID for a helper instance. By default, the same subnet where the provided instance resides is used. Important: If you provide a custom subnet, it must be in the same Availability Zone as InstanceId, and it must allow access to the Systems Manager endpoints. This is only required if the target instance is in 'stopped' state or is not managed by AWS Systems Manager. SelectedInstanceSubnet	HelperInstanceProfileName (Conditional) The name of an existing IAM instance profile for the helper instance. If you are enabling SAC and boot menu on an instance that is in 'stopped' state or not managed by AWS Systems Manager, this is required. If an IAM instance profile is not specified, the automation creates one on your behalf. String
CreateInstanceBackupBeforeScriptExecution (Optional) Specify 'True' to create an Amazon Machine Images (AMI) backup of the EC2 instance before enabling SAC and boot menu. The AMI will persist after the automation completes. It is your responsibility to secure access to the AMI, or to delete it. True	BackupAmazonMachineImagePrefix (Conditional) A prefix for the Amazon Machine Image (AMI) that is created if the 'CreateInstanceBackupBeforeScriptExecution' parameter is set to 'True'. AWSsupport

4. Seleziona Esegui.

5. L'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- `CheckIfEc2SerialConsoleAccessEnabled`:

Verifica se l'accesso ad Amazon EC2 Serial Console è abilitato a livello di account. Nota: l'accesso alla console seriale non è disponibile per impostazione predefinita. Per ulteriori informazioni, consulta [Configurare l'accesso alla Amazon EC2 Serial Console](#).

- `CheckIfEc2InstanceIsWindows`:

Indica se la piattaforma dell'istanza di destinazione è Windows.

- `GetInstanceType`:

Recupera il tipo di istanza dell'istanza di destinazione.

- `CheckIfInstanceTypeIsNitro`:

Verifica se l'hypervisor di tipo di istanza è basato su Nitro. Serial Console Access è supportato solo su istanze virtualizzate basate sul sistema Nitro.

- `CheckIfInstanceIsInAutoScalingGroup`:

Verifica se l' EC2 istanza Amazon fa parte di un gruppo Amazon EC2 Auto Scaling chiamando `DescribeAutoScalingInstancesAPI`. Se l'istanza fa parte di un gruppo Amazon EC2 Auto Scaling, garantisce che l'istanza di Porting Assistant for .NET sia in stato di standby del ciclo di vita.

- `WaitForEc2: InstanceStateStablized`

Attende che l'istanza sia in esecuzione o interrotta.

- `GetEc2: InstanceState`

Ottiene lo stato corrente dell'istanza.

- `BranchOnEc2InstanceState`:

Rami basati sullo stato dell'istanza recuperato nel passaggio precedente. Se lo stato dell'istanza è in esecuzione, passa al `CheckIfEc2InstanceIsManagedBySSM` passaggio e, in caso contrario, passa al `CheckIfHelperInstanceProfileIsProvided` passaggio.

- `CheckIfEc2 InstanceIsManagedBy SMS`:

Verifica se l'istanza è gestita da AWS Systems Manager. Se gestito, il runbook abilita SAC e il menu di avvio utilizzando un PowerShell comando Run.

- `BranchOnPreEC2RescueBackup`:

Rami basati sul parametro di `CreateInstanceBackupBeforeScriptExecution` input.

- `CreateAmazonMachineImageBackup`:

Crea un backup AMI dell'istanza.

- `Abilita SACAndBootMenu`:

Abilita SAC e il menu di avvio eseguendo uno script PowerShell Run Command.

- `RebootInstance`:

Riavvia l' EC2 istanza Amazon per applicare la configurazione. Questo è il passaggio finale se l'istanza è online ed è gestita da AWS Systems Manager.

- `CheckIfHelperInstanceProfileIsProvided`:

Verifica se lo `HelperInstanceProfileName` specificato esiste prima di abilitare SAC e il menu di avvio offline utilizzando un' EC2istanza Amazon temporanea.

- `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu`:

Esegue il menu `AWSSupport-StartEC2RescueWorkflow` per abilitare SAC e il menu di avvio quando l'istanza è in stato di arresto o non è gestita da AWS Systems Manager

- `GetExecutionDetails`:

Recupera l'ID dell'immagine del backup e dell'output dello script offline.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- `Abilita SACAnd BootMenu .Output`:

Output dell'esecuzione del comando nel `EnableSACAndBootMenu` passaggio.

- `GetExecutionDetails.OfflineScriptOutput`:

Output dello script offline eseguito nella

`RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` fase.

- `GetExecutionDetails.BackupBeforeScriptExecution`:

ID immagine del backup AMI acquisito se il parametro `CreateInstanceBackupBeforeScriptExecution` di input è `True`.

Output di esecuzione su un'istanza in esecuzione e gestita da AWS Systems Manager

Outputs	
<code>GetExecutionDetails.BackupBeforeScriptExecution</code> No output available yet because the step is not successfully executed <code>EnableSACAndBootMenu.Output</code> The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully.	<code>GetExecutionDetails.OfflineScriptOutput</code> No output available yet because the step is not successfully executed

Output dell'esecuzione su un'istanza interrotta o non gestita da AWS Systems Manager

Outputs	
<code>EnableSACAndBootMenu.Output</code> No output available yet because the step is not successfully executed <code>GetExecutionDetails.OfflineScriptOutput</code> Device xvdf mapped to D Offline Windows installation found in directory D:\Windows Windows Server 2016 Datacenter (10.0.14393.6522) BCD Store found in directory D:\Boot\BCD Detecting installed drivers EC2Rescue environment variables set EC2Rescue script variables set The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully. Volume successfully set offline	<code>GetExecutionDetails.BackupBeforeScriptExecution</code> ami-09c33701932955dde

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWSsupport - ExecuteEC2Rescue

Descrizione

Questo runbook utilizza il EC2Rescue strumento per risolvere e, ove possibile, riparare problemi di connettività comuni con l'istanza Amazon Elastic Compute Cloud (Amazon EC2) specificata per Linux o Windows Server. Le istanze con volumi root crittografati non sono supportate.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EC2RescueInstanceType

Tipo: stringa

Valori validi: t2.small | t2.medium | t2.large

Impostazione predefinita: t2.small

Descrizione: (Obbligatorio) Il tipo di istanza per EC2 EC2Rescue istanza. Dimensioni consigliate: t2.small

- LogDestination

Tipo: stringa

Descrizione: (Facoltativo) nome del bucket Amazon S3 nel tuo account in cui desideri caricare i log di risoluzione dei problemi. Verificare che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie alle parti che non necessitano dell'accesso ai log raccolti.

- SubnetId

Tipo: stringa

Impostazione predefinita: CreateNew VPC

Descrizione: (Facoltativo) L'ID di sottorete per EC2Rescue istanza. Per impostazione predefinita, AWS Systems Manager Automation crea un nuovo VPC. In alternativa, utilizza `SelectedInstanceSubnet` la stessa sottorete dell'istanza o specifica un ID di sottorete personalizzato.

 Important

La sottorete deve trovarsi nella stessa `UnreachableInstanceId` zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

- `UnreachableInstanceId`

Tipo: stringa

Descrizione: (Obbligatorio) ID dell'istanza irraggiungibile. EC2

 Important

Systems Manager Automation interrompe questa istanza e crea un'AMI prima di tentare qualsiasi operazione. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico cambierà se non si utilizza un indirizzo IP elastico.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

È necessario avere almeno `ssm:StartAutomationExecution` ed `ssm:GetAutomationExecution` essere in grado di leggere l'output dell'automazione. Per ulteriori informazioni sulle autorizzazioni richieste, consulta [AWSSupport-StartEC2RescueWorkflow](#).

Fasi del documento

1. `aws:assertAwsResourceProperty`- Afferma se l'istanza fornita è Windows Server:
 - a. (EC2Rescue for Windows Server) Se l'istanza fornita è una Windows Server istanza:
 - i. `aws:executeAutomation`- Invoca `AWSSupport-StartEC2RescueWorkflow` con `Rescue for EC2 Windows Server` script offline.

- ii. `aws:executeAwsApi`- Recupera l'ID AMI di backup dall'automazione annidata.
- iii. `aws:executeAwsApi`- Recupera il riepilogo di EC2 Rescue dall'automazione annidata.
- b. (EC2Rescue per Linux) Se l'istanza fornita è un'istanza Linux:
 - i. `aws:executeAutomation`- Richiama `AWSSupport-StartEC2RescueWorkflow` con gli script offline di EC2 Rescue for Linux
 - ii. `aws:executeAwsApi`- Recupera l'ID AMI di backup dall'automazione annidata.
 - iii. `aws:executeAwsApi`- Recupera il riepilogo di EC2 Rescue dall'automazione annidata.

Output

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

Descrizione

Il `AWSSupport-ListEC2Resources` runbook restituisce informazioni sulle EC2 istanze Amazon e sulle risorse correlate come i volumi Amazon Elastic Block Store (Amazon EBS), gli indirizzi IP elastici e i gruppi Amazon Auto EC2 Scaling dal file specificato. Regioni AWS Per impostazione predefinita, le informazioni vengono raccolte da tutte le regioni e visualizzate nell'output dell'automazione. Facoltativamente, puoi specificare un bucket Amazon Simple Storage Service (Amazon S3) in cui caricare le informazioni come file con valori separati da virgole (.csv).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- BucketName

Tipo: stringa

Descrizione: (Facoltativo) Il nome del bucket S3 in cui vengono caricate le informazioni raccolte.

- DisplayResourceDeletionDocumentation

Tipo: stringa

Impostazione predefinita: true

Descrizione: (Facoltativo) Se impostata su `true`, l'automazione crea collegamenti nell'output alla documentazione relativa all'eliminazione delle risorse.

- RegionsToQuery

Tipo: stringa

Impostazione predefinita: Tutto

Descrizione: (Facoltativo) Le regioni da cui desideri raccogliere informazioni EC2 relative ad Amazon.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRegions`
- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

Inoltre, per caricare correttamente le informazioni raccolte nel bucket S3 specificato, sono necessarie le seguenti azioni:

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

Fasi del documento

- `aws:executeAwsApi`- Raccoglie le regioni abilitate per l'account.
- `aws:executeScript`- Conferma che le regioni abilitate per l'account supportano le regioni specificate nel `RegionsToQuery` parametro.
- `aws:branch`- Se nessuna regione è abilitata per l'account, l'automazione termina.
- `aws:executeScript`- Elenca tutte le EC2 istanze per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutte le Amazon Machine Images (AMI) per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutti i volumi EBS per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutti gli indirizzi IP elastici per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutte le interfacce di rete elastiche per l'account e le regioni specificate.
- `aws:executeScript`- Elenca tutti i gruppi Auto Scaling per l'account e le regioni specificate.

- `aws:executeScript`- Elenca tutti i sistemi di bilanciamento del carico per l'account e le regioni specificate.
- `aws:executeScript`- Carica le informazioni raccolte nel bucket S3 specificato se fornisci un valore per il parametro. Bucket

AWSSupport-ManageRDPSettings

Descrizione

Il `AWSSupport-ManageRDPSettings` runbook consente all'utente di gestire le impostazioni comuni del Remote Desktop Protocol (RDP), come la porta RDP e l'autenticazione a livello di rete (NLA). Per impostazione predefinita, il runbook legge ed emette i valori delle impostazioni.

Important

Le modifiche alle impostazioni RDP devono essere esaminate attentamente prima di eseguire questo runbook.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (obbligatorio) ID dell'istanza gestita per la quale gestire le impostazioni RDP.

- NLASettingAzione

Tipo: stringa

Valori validi: Controlla | Abilita | Disabilita

Impostazione predefinita: Check

Descrizione: (obbligatorio) operazione da eseguire sulle impostazioni NLA: Check, Enable, Disable.

- RDPPort

Tipo: stringa

Impostazione predefinita: 3389

Descrizione: (facoltativo) specifica la nuova porta RDP. Utilizzato solo quando l'operazione è impostata su Modify. Il numero di porta deve essere compreso tra 1025 e 65535. Nota: dopo la modifica della porta il servizio RDP viene riavviato.

- RDPPortAzione

Tipo: stringa

Valori validi: Verifica | Modifica

Impostazione predefinita: Check

Descrizione: (Obbligatoria) Un'azione da applicare alla porta RDP.

- RemoteConnections

Tipo: stringa

Valori validi: Controlla | Abilita | Disabilita

Impostazione predefinita: Check

Descrizione: (Obbligatorio) Un'azione da eseguire sull'impostazione fDeny. TSConnections

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

L' EC2 istanza che riceve il comando deve avere un ruolo IAM con la policy gestita di SSMMangedInstanceCoreAmazon Amazon allegata. L'utente deve avere almeno ssm: SendCommand per inviare il comando all'istanza, più ssm: GetCommandInvocation per poter leggere l'output del comando.

Fasi del documento

aws : runCommand- Esegui lo PowerShell script per modificare o controllare le impostazioni RDP sull'istanza di destinazione.

Output

- gestisci .Output RDPSettings

AWSsupport-ManageWindowsService

Descrizione

Il AWSsupport-ManageWindowsService runbook consente di interrompere, avviare, riavviare, mettere in pausa o disabilitare qualsiasi servizio Windows sull'istanza di destinazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Instanceld

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza gestita di cui gestire i servizi di.

- ServiceAction

Tipo: stringa

Valori validi: Check | Restart | Force-Restart | Start | Stop | Force-Stop | Pause

Impostazione predefinita: Check

Descrizione: (Obbligatorio) Un'azione da applicare al servizio Windows. Tieni presente che Force-Restart e Force-Stop può essere utilizzato per riavviare e interrompere un servizio con servizi dipendenti.

- StartupType

Tipo: stringa

Valori validi: Check | Auto | Demand | Disabled | DelayedAutoStart

Impostazione predefinita: Check

Descrizione: (Obbligatorio) Un tipo di avvio da applicare al servizio Windows.

- WindowsServiceName

Tipo: stringa

Descrizione: (obbligatorio) nome del servizio di Windows valido.

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia che l' EC2 istanza che riceve il comando abbia un ruolo IAM con la policy gestita di `SSMManagedInstanceCoreAmazon` Amazon allegata. L'utente deve disporre almeno di `ssm:StartAutomationExecution` e `ssm:SendCommand` per eseguire l'automazione e inviare il comando all'istanza, più `ssm:GetAutomationExecution` per poter leggere l'output dell'automazione.

Fasi del documento

`aws:runCommand`- Esegui lo PowerShell script per applicare la configurazione desiderata al servizio Windows sull'istanza di destinazione.

Output

`manageWindowsService.Uscita`

AWSSupport-MigrateEC2ClassicToVPC

Descrizione

Il `AWSSupport-MigrateEC2ClassicToVPC` runbook migra un'istanza Amazon Elastic Compute Cloud (Amazon EC2) da EC2 -Classic a un cloud privato virtuale (VPC). Questo runbook supporta la migrazione di EC2 istanze Amazon del tipo di virtualizzazione HVM (Hardware Virtual Machine) con i volumi root di Amazon Elastic Block Store (Amazon EBS).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- Approva IAM

Tipo: StringList

Descrizione: (Facoltativo) I nomi delle risorse Amazon (ARNs) degli utenti IAM che possono approvare o rifiutare l'azione. Questo parametro si applica solo se si specifica il `CutOver` valore del parametro. `MigrationType`

- `DestinationSecurityGroupId`

Tipo: StringList

Descrizione: (Facoltativo) L'ID del gruppo di sicurezza che desideri associare all' EC2 istanza Amazon lanciata nel tuo VPC. Se non specifichi un valore per questo parametro, l'automazione crea un gruppo di sicurezza nel tuo VPC e copia le regole dal gruppo di sicurezza in EC2 -Classic. Se le regole non vengono copiate nel nuovo gruppo di sicurezza, il gruppo di sicurezza predefinito del tuo VPC viene associato all'istanza Amazon EC2 .

- `DestinationSubnetId`

Tipo: stringa

Descrizione: (Facoltativo) L'ID della sottorete verso cui vuoi migrare l' EC2istanza Amazon. Se non si specifica un valore per questo parametro, l'automazione sceglie casualmente una sottorete dal VPC.

- `InstanceId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon che desideri migrare.

- `MigrationType`

Tipo: stringa

Valori validi: `CutOver` | `Test`

Descrizione: (Obbligatorio) Il tipo di migrazione che si desidera eseguire.

L'opzione `CutOver` richiede l'approvazione per interrompere l'EC2 istanza Amazon in esecuzione in EC2 -Classic. Dopo l'approvazione di questa azione, l'EC2 istanza Amazon viene interrotta e l'automazione crea un Amazon Machine Image (AMI). Quando il AMI status è `available`, da questo viene lanciata una nuova EC2 istanza Amazon AMI nel formato `DestinationSubnetId` specificato nel tuo VPC. Se la tua EC2 istanza Amazon in esecuzione in EC2 -Classic ha un indirizzo IP elastico collegato, l'istanza verrà spostata nell'EC2 istanza Amazon appena creata nel tuo VPC. Se l'EC2 istanza Amazon che si avvia nel tuo VPC non viene creata per qualsiasi motivo, viene interrotta e viene richiesta l'approvazione per avviare l'istanza EC2 Amazon in -Classic. EC2

L'opzione `Test` crea un Test AMI della tua EC2 istanza Amazon in esecuzione in EC2 -Classic senza riavvio. Poiché l'EC2 istanza Amazon non si riavvia, non possiamo garantire l'integrità del file system dell'immagine creata. Quando AMI status è `available`, da questo viene lanciata una nuova EC2 istanza Amazon AMI nel formato `DestinationSubnetId` specificato nel tuo VPC. Se la tua EC2 istanza Amazon in esecuzione in EC2 -Classic ha un indirizzo IP elastico collegato, l'automazione verifica che `DestinationSubnetId` quello specificato sia pubblico. Se l'EC2 istanza Amazon che si avvia nel tuo VPC non riesce a creare per qualsiasi motivo, viene interrotta e l'automazione termina.

- `SNSNotificationARNforApprovazione`

Tipo: stringa

Descrizione: (Facoltativo) L'ARN dell'argomento Amazon Simple Notification Service (Amazon SNS) a cui desideri inviare le richieste di approvazione. Questo parametro si applica solo se si specifica il `CutOver` valore per il `MigrationType` parametro.

- `TargetInstanceType`

Tipo: stringa

Impostazione predefinita: `t2.2xlarge`

Descrizione: (Facoltativo) Il tipo di EC2 istanza Amazon che desideri avviare nel tuo VPC. Sono supportati solo i tipi di istanze basate su Xen, come T2, M4 o C4.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie i dettagli sull' EC2 istanza Amazon specificata nel `InstanceId` parametro.
- `aws:assertAwsResourceProperty`- Conferma che il tipo di istanza specificato nel `TargetInstanceType` parametro è basato su Xen.
- `aws:assertAwsResourceProperty`- Conferma che l' EC2 istanza Amazon specificata nel `InstanceId` parametro è del tipo di virtualizzazione HVM.
- `aws:assertAwsResourceProperty`- Conferma che l' EC2 istanza Amazon specificata nel `InstanceId` parametro ha un volume root Amazon EBS.
- `aws:executeScript`- Crea un gruppo di sicurezza in base alle esigenze in base al valore specificato per il `DestinationSecurityGroupId` parametro.
- `aws:branch`- Rami basati sul valore specificato nel `DestinationSubnetId` parametro.
- `aws:executeAwsApi`- Identifica il VPC predefinito nel luogo in cui si Regione AWS esegue questa automazione.
- `aws:executeAwsApi`- Sceglie in modo casuale l'ID di una sottorete situata nel VPC predefinito.
- `aws:createImage`- Crea un AMI senza riavviare l'istanza Amazon EC2.
- `aws:branch`- Rami basati sul valore specificato per il `MigrationType` parametro.
- `aws:branch`- Rami basati sul valore specificato per il `DestinationSubnetId` parametro.
- `aws:runInstances`- Avvia una nuova istanza dal AMI creato senza riavviare l' EC2 istanza Amazon in EC2 -Classic.
- `aws:changeInstanceState`- Termina l' EC2istanza Amazon appena lanciata se il passaggio precedente fallisce per qualsiasi motivo.
- `aws:runInstances`- Avvia una nuova istanza dal AMI creato senza riavviare l' EC2 istanza Amazon in EC2 -Classic se fornito. `DestinationSubnetId`
- `aws:changeInstanceState`- Termina l' EC2istanza Amazon appena lanciata se il passaggio precedente fallisce per qualsiasi motivo.
- `aws:assertAwsResourceProperty`- Conferma il comportamento di arresto per l' EC2 istanza Amazon in esecuzione in EC2 -Classic.
- `aws:approve`- Attende l'approvazione per interrompere l' EC2 istanza Amazon.

- `aws:changeInstanceState`- Interrompe l'esecuzione dell' EC2 istanza Amazon in EC2 - Classic.
- `aws:changeInstanceState`- Se necessario, la forza arresta l' EC2 istanza Amazon in esecuzione in EC2 -Classic.
- `aws:createImage`- Crea un AMI dell' EC2 istanza Amazon dopo l'interruzione.
- `aws:branch`- Rami basati sul valore specificato per il `DestinationSubnetId` parametro.
- `aws:runInstances`- Avvia una nuova istanza dal AMI creato dell' EC2 istanza Amazon interrotta in EC2 -Classic.
- `aws:approve`- Attende l'approvazione per terminare l'istanza appena lanciata e avvia l' EC2 istanza Amazon in EC2 -Classic se il passaggio precedente fallisce per qualsiasi motivo.
- `aws:changeInstanceState`- Termina l' EC2istanza Amazon appena lanciata.
- `aws:runInstances`- Avvia una nuova istanza dal AMI creato dell' EC2 istanza Amazon interrotta in EC2 -Classic dal `DestinationSubnetId` parametro.
- `aws:approve`- Attende l'approvazione per terminare l'istanza appena lanciata e avvia l' EC2 istanza Amazon in EC2 -Classic se il passaggio precedente fallisce per qualsiasi motivo.
- `aws:changeInstanceState`- Termina l' EC2istanza Amazon appena lanciata.
- `aws:changeInstanceState`- Avvia l' EC2 istanza Amazon che è stata interrotta in EC2 -Classic.
- `aws:branch`- Filiali in base al fatto che l' EC2 istanza Amazon abbia un indirizzo IP pubblico.
- `aws:executeAwsApi`- Verifica se l'indirizzo IP pubblico è un indirizzo IP elastico.
- `aws:branch`- Rami basati sul valore specificato nel `MigrationType` parametro.
- `aws:executeAwsApi`- Sposta l'indirizzo IP elastico sul tuo VPC.
- `aws:executeAwsApi`- Raccoglie l'ID di allocazione dell'indirizzo IP elastico che è stato spostato nel tuo VPC.
- `aws:branch`- Filiali in base alla sottorete in cui è stata lanciata l' EC2 istanza Amazon in esecuzione nel tuo VPC.
- `aws:executeAwsApi`- Allega l'indirizzo IP elastico all'istanza appena lanciata nel tuo VPC.
- `aws:executeScript`- Conferma che la sottorete dell' EC2istanza Amazon appena lanciata in esecuzione nel VPC è pubblica.

Output

`getInstanceProperties.virtualizationType` - Il tipo di virtualizzazione dell' EC2 istanza Amazon in esecuzione in EC2 -Classic.

`getInstanceProperties.rootDeviceType`- Il tipo di dispositivo root dell' EC2istanza Amazon in esecuzione in EC2 -Classic.

`createAMIWithoutReboot.ImageId`- L'ID del AMI creato senza riavviare l' EC2 istanza Amazon in esecuzione in EC2 -Classic.

`getDefaultVPC.VpcId`- L'ID del VPC predefinito in cui viene lanciata la nuova EC2 istanza Amazon se non viene fornito un valore per il `DestinationSubnetId` parametro.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`- L'ID della sottorete nel VPC predefinito in cui viene lanciata la nuova istanza EC2 Amazon se non viene fornito un valore per `DestinationSubnetId` il parametro.

`launchTestInstanceDefaultVPC.InstanceIds`- L'ID dell' EC2istanza Amazon appena lanciata nel tuo VPC predefinito durante il tipo di Test migrazione.

`launchTestInstanceProvidedSubnet.InstanceIds`- L'ID dell' EC2 istanza Amazon appena lanciata nel tipo `DestinationSubnetId` di migrazione specificato durante il tipo di Test migrazione.

`createAMIAfterStoppingInstance.ImageId`- L'ID del AMI creato dopo aver interrotto l'esecuzione dell' EC2 istanza Amazon in EC2 -Classic.

`launchCutOverInstanceProvidedSubnet.InstanceIds`- L'ID dell' EC2 istanza Amazon appena lanciata nel tipo `DestinationSubnetId` di migrazione specificato durante il tipo di `CutOver` migrazione.

`launchCutOverInstanceDefaultVPC.InstanceIds`- L'ID dell' EC2 istanza Amazon appena lanciata nel tuo VPC predefinito durante il tipo di `CutOver` migrazione.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`- Se la sottorete scelta dall'automazione nel VPC predefinito è pubblica.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`- Se la sottorete specificata in `DestinationSubnetId` è pubblica.

AWSsupport-MigrateXenToNitroLinux

Descrizione

Il `AWSSupport-MigrateXenToNitroLinux` runbook clona, prepara e migra un'istanza Amazon Elastic Compute Cloud (EC2Amazon) Linux Xen su un [Nitro](#) tipo di istanza. Questo runbook fornisce due opzioni per i tipi di operazioni:

- **Clone&Migrate**— Il flusso di lavoro di questa opzione è costituito da controlli preliminari, test e Clone&Migrate fasi. Il flusso di lavoro viene eseguito utilizzando il `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro` runbook.
- **FullMigration**— Questa opzione esegue il Clone&Migrate flusso di lavoro e quindi esegue il passaggio aggiuntivo di Replace root dei volumi Amazon EBS.

 Important

L'utilizzo di questo runbook comporta costi a carico del tuo account per il tempo di esecuzione delle EC2 istanze Amazon, la creazione di volumi Amazon Elastic Block Store (Amazon EBS) e AMLs. Per ulteriori dettagli, consulta i prezzi di [Amazon e EC2 i prezzi di Amazon EBS](#).

Controlli preliminari

L'automazione esegue i seguenti controlli preliminari prima di continuare con la migrazione. Se uno qualsiasi dei controlli fallisce, l'automazione termina. Questa fase è solo una parte del Clone&Migrate flusso di lavoro.

- Verifica se l'istanza di destinazione è già una Nitro tipo di istanza.
- Verifica se l'opzione di acquisto delle istanze Spot è stata utilizzata per l'istanza di destinazione.
- Verifica se i volumi dell'Instance Store sono collegati all'istanza di destinazione.
- Verifica che il sistema operativo (OS) dell'istanza di destinazione sia Linux.
- Verifica se l'istanza di destinazione fa parte di un gruppo Amazon EC2 Auto Scaling. Se fa parte di un gruppo Auto Scaling, l'automazione verifica che l'istanza sia nello stato. `standby`
- Verifica che l'istanza sia gestita da. AWS Systems Manager

Test in corso

L'automazione crea un Amazon Machine Image (AMI) dall'istanza di destinazione e avvia un'istanza di test dall'istanza appena creata AMI. Questa fase fa parte solo del Clone&Migrate flusso di lavoro.

Se l'istanza di test supera tutti i controlli di stato, l'automazione viene messa in pausa e l'approvazione dei responsabili designati viene richiesta tramite la notifica di Amazon Simple Notification Service (Amazon SNS). Se viene fornita l'approvazione, l'automazione termina l'istanza di test, interrompe l'istanza di destinazione e continua con la migrazione, mentre la nuova istanza viene creata AMI viene annullata la registrazione alla fine del flusso di lavoro. Clone&Migrate

Note

Prima di fornire l'approvazione, consigliamo di verificare che tutte le applicazioni in esecuzione sull'istanza di destinazione siano state chiuse correttamente.

Clona e migra

L'automazione ne crea un'altra AMI dall'istanza di destinazione e avvia una nuova istanza per passare a Nitro tipo di istanza. L'automazione soddisfa i seguenti prerequisiti prima di continuare con la migrazione. Se uno qualsiasi dei controlli fallisce, l'automazione termina. Anche questa fase è solo una parte del Clone&Migrate flusso di lavoro.

- Attiva l'attributo Enhanced Networking (ENA).
- Installa la versione più recente dei driver ENA se non sono già installati o aggiorna la versione dei driver ENA alla versione più recente. Per garantire le massime prestazioni di rete, è necessario l'aggiornamento alla versione più recente del driver ENA se Nitro il tipo di istanza è la sesta generazione.
- Verifica che il NVMe modulo sia installato. Se il modulo è installato, l'automazione verifica che il modulo sia caricato. `initramfs`
- Analizza `/etc/fstab` e sostituisce le voci con i nomi dei dispositivi a blocchi (`/dev/sd*o/dev/xvd*`) con i rispettivi nomi. UUIDs Prima di modificare la configurazione, l'automazione crea un backup del file nel percorso. `/etc/fstab*`
- Disattiva la denominazione prevedibile delle interfacce aggiungendo l'`net.ifnames=0` opzione alla GRUB_CMDLINE_LINUX riga del `/etc/default/grub` file, se esistente, o al kernel in. `/boot/grub/menu.lst`

- Rimuove il `/etc/udev/rules.d/70-persistent-net.rules` file se esiste. Prima di rimuovere il file, l'automazione crea un backup del file nel percorso `/etc/udev/rules.d/`.

Dopo aver verificato tutti i requisiti, il tipo di istanza viene modificato in Nitro tipo di istanza specificato. L'automazione attende che l'istanza appena creata superi tutti i controlli di stato dopo aver iniziato come Nitro tipo di istanza. L'automazione attende quindi l'approvazione dei responsabili designati per creare un AMI di quelli lanciati con successo Nitro istanza. Se l'approvazione viene negata, l'automazione termina, lasciando in esecuzione l'istanza appena creata e l'istanza di destinazione rimane interrotta.

Sostituisci il volume Amazon EBS root

Se scegli `FullMigration` come `OperationType`, l'automazione migra l' EC2 istanza Amazon di destinazione verso Nitro tipo di istanza specificato. L'automazione richiede l'approvazione dei responsabili designati per sostituire il volume Amazon EBS root dell' EC2 istanza Amazon di destinazione con il volume root dell'istanza EC2 Amazon clonata. Una volta completata la migrazione, l' EC2 istanza Amazon clonata viene terminata. Se l'automazione fallisce, il volume root originale di Amazon EBS viene collegato all' EC2 istanza Amazon di destinazione. Se il volume root Amazon EBS collegato all' EC2 istanza Amazon di destinazione presenta tag con il `aws:` prefisso applicato, l'`FullMigration` operazione non è supportata.

Prima di iniziare

L'istanza di destinazione deve disporre di accesso a Internet in uscita. Questo serve per accedere a repository per driver e dipendenze come `kernel-devel`, `gcc`, `patch`, `rpm-build`, `wget`, `dracut`, `make`, `linux-header` e `unzip`. Se necessario, viene utilizzato il gestore di pacchetti.

È necessario un argomento di Amazon SNS per inviare notifiche di approvazioni e aggiornamenti. Per ulteriori informazioni sulla creazione di un argomento Amazon SNS, consulta [Creating an Amazon SNS nella Amazon Simple Notification Service Developer Guide](#).

Questo runbook supporta i seguenti sistemi operativi:

- RHEL 7x - 8,5
- Amazon Linux (2018.03), Amazon Linux 2
- Debian Server
- Ubuntu Server 18.04 LTS, 20.04 LTS e 20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5, SUSE15SP2)

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Riconoscimento

Tipo: stringa

Descrizione: (Obbligatorio) Leggi i dettagli completi delle azioni eseguite da questo runbook di automazione e accedi **Yes, I understand and acknowledge** per procedere con l'utilizzo del runbook.

- Approvatore IAM

Tipo: stringa

Descrizione: (Obbligatorio) ARNs Elenco dei ruoli, degli utenti o dei nomi utente IAM che possono fornire approvazioni all'automazione. Puoi specificare un massimo di 10 approvatori.

- DeleteResourcesOnFailure

Tipo: Booleano

Descrizione: (Facoltativo) Determina se l'istanza appena creata e AMI per la migrazione vengono eliminati se l'automazione fallisce.

Valori validi: True | False

Impostazione predefinita: True

- MinimumRequiredApprovals

Tipo: stringa

Descrizione: (Facoltativo) Il numero minimo di approvazioni necessarie per continuare a eseguire l'automazione quando vengono richieste le approvazioni.

Valori validi: 1-10

Impostazione predefinita: 1

- NitroInstanceType

Tipo: stringa

Descrizione: (Obbligatoria) The Nitro tipo di istanza in cui desideri modificare l'istanza. I tipi di istanza supportati includono M5, M6, C5, C6, R5, R6 e T3.

Impostazione predefinita: m5.xlarge

- OperationType

Tipo: stringa

Descrizione: (Obbligatoria) L'operazione che si desidera eseguire. L'FullMigrationopzione esegue le stesse attività Clone&Migrate e sostituisce inoltre il volume principale dell'istanza di destinazione. Il volume principale dell'istanza di destinazione viene sostituito con il volume principale dell'istanza appena creata dopo il processo di migrazione. L'FullMigrationoperazione non supporta i volumi root definiti da Logical Volume Manager (LVM).

Valori validi: Clone&Migrate | FullMigration

- SNSTopicArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN dell'argomento di Amazon SNS per la notifica di approvazione. L'argomento Amazon SNS viene utilizzato per inviare le notifiche di approvazione richieste durante l'automazione.

- TargetInstanceld

Tipo: stringa

Descrizione: (Obbligatorio) L'ID delle EC2 istanze Amazon da migrare.

Clone&Migrate flusso di lavoro

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

- `startOfPreliminaryChecksBranch`- Si ramifica al flusso di lavoro dei controlli preliminari.
- `getTargetInstanceProperties`- Raccoglie i dettagli dall'istanza di destinazione.
- `checkIfNitroInstanceTypeIsSupportedInAZ`- Determina se il tipo di EC2 istanza Amazon di destinazione è supportato nella stessa zona di disponibilità dell'istanza di destinazione.
- `getXenInstanceDetails`- Raccoglie dettagli sul tipo di istanza di origine.
- `checkIfInstanceHypervisorIsNitroAlready`- Verifica se l'istanza di destinazione è già in esecuzione come Nitro tipo di istanza.
- `checkIfTargetInstanceLifecycleIsSpot`- Verifica se l'opzione di acquisto dell'istanza di destinazione è Spot.
- `checkIfOperatingSystemIsLinux`- Verifica se il sistema operativo dell'istanza di destinazione è Linux.
- `verifySSMConnectivityForTargetInstance`- Verifica che l'istanza di destinazione sia gestita da Systems Manager.
- `checkIfEphemeralVolumeAreSupported`- Verifica se il tipo di istanza corrente dell'istanza di destinazione supporta i volumi dell'Instance Store.
- `verifyIfTargetInstanceHasEphemeralVolumesAttached`- Verifica se all'istanza di destinazione sono collegati volumi di Instance Store.
- `checkIfRootVolumeIsEBS`- Verifica se il tipo di volume principale dell'istanza di destinazione è EBS.

- `checkIfTargetInstanceIsInASG`- Verifica se l'istanza di destinazione fa parte di un gruppo Auto Scaling.
- `endOfPreliminaryChecksBranch`- Fine del ramo dei controlli preliminari.
- `startOfTestBranch`- Succursali del flusso di lavoro di test.
- `createTestImage`- Crea un test AMI dell'istanza di destinazione.
- `launchTestInstanceInSameSubnet`- Avvia un'istanza di test dal test AMI utilizzando la stessa configurazione dell'istanza di destinazione.
- `cleanupTestInstance`- Termina l'istanza di test.
- `endOfTestBranch`- Fine del ramo di test.
- `checkIfTestingBranchSucceeded`- Verifica lo stato del ramo Testing.
- `approvalToStopTargetInstance`- Attende l'approvazione dei responsabili designati per interrompere l'istanza di destinazione.
- `stopTargetEC2Instance`- Arresta l'istanza di destinazione.
- `forceStopTargetEC2Instance`- La forza arresta l'istanza di destinazione solo se il passaggio precedente non riesce a fermare l'istanza.
- `startOfCloneAndMigrateBranch`- Succursali verso Clone&Migrate flusso di lavoro.
- `createBackupImage`- Crea un AMI dell'istanza di destinazione da utilizzare come backup.
- `launchInstanceInSameSubnet`- Avvia una nuova istanza dal backup AMI utilizzando la stessa configurazione dell'istanza di origine.
- `waitForClonedInstanceToPassStatusChecks`- Attende che l'istanza appena creata superi tutti i controlli di stato.
- `verifySSMConnectivityForClonedInstance`- Verifica che l'istanza appena creata sia gestita da Systems Manager.
- `checkAndInstallENADrivers`- Verifica se i driver ENA sono installati sull'istanza appena creata e installa i driver se necessario.
- `checkAndAddNVMeDrivers`- Verifica se NVMe i driver sono installati sull'istanza appena creata e installa i driver se necessario.
- `checkAndModifyFSTABEntries`- Verifica se i nomi dei dispositivi vengono utilizzati `/etc/fstab` e li sostituisce con, UUIDs se necessario.
- `stopClonedInstance`- Arresta l'istanza appena creata.
- `forceStopClonedInstance`- La forza arresta l'istanza appena creata solo se il passaggio precedente non riesce a fermare l'istanza.

- `checkENAAttributeForClonedInstance`- Verifica se l'attributo di rete avanzato è attivato per l'istanza appena creata.
- `setNitroInstanceTypeForClonedInstance`- Cambia il tipo di istanza per l'istanza appena creata in Nitro tipo di istanza specificato.
- `startClonedInstance`- Avvia l'istanza appena creata di cui è stato modificato il tipo di istanza.
- `approvalForCreatingImageAfterDriversInstallation`- Se l'istanza viene avviata correttamente come Nitro tipo di istanza, l'automazione attende l'approvazione dei responsabili richiesti. Se viene fornita l'approvazione, un AMI è stato creato per essere utilizzato come Golden AMI.
- `createImageAfterDriversInstallation`- Crea un AMI da usare come Golden AMI.
- `endOfCloneAndMigrateBranch`- Fine di Clone&Migrate succursale.
- `cleanupTestImage`- Annulla la registrazione AMI creato per essere testato.
- `failureHandling`- Verifica se hai scelto di interrompere le risorse in caso di errore.
- `onFailureTerminateClonedInstance`- Termina l'istanza appena creata se l'automazione fallisce.
- `onFailurecleanupTestImage`- Annulla la registrazione del AMI creato per essere testato.
- `onFailureApprovalToStartTargetInstance`- Se l'automazione fallisce, attende l'approvazione dei responsabili designati per avviare l'istanza di destinazione.
- `onFailureStartTargetInstance`- Se l'automazione fallisce, avvia l'istanza di destinazione.

FullMigration flusso di lavoro

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

Il `FullMigration` flusso di lavoro esegue gli stessi passaggi del `Clone&Migrate` flusso di lavoro e inoltre esegue i seguenti passaggi:

- `checkConcurrency`- Verifica che esista una sola automazione di questo runbook destinata all' EC2 istanza Amazon specificata. Se il runbook rileva un'altra automazione in corso destinata alla stessa istanza, l'automazione termina.

- `getTargetInstanceProperties`- Raccoglie i dettagli dall'istanza di destinazione.
- `checkRootVolumeTags`- Determina se il volume root dell' EC2 istanza Amazon di destinazione contiene tag AWS riservati.
- `cloneTargetInstanceAndMigrateToNitro`- Avvia un'automazione secondaria utilizzando il `AWS-CloneXenInstanceToNitro` runbook.
- `branchOnTheOperationType`- Si ramifica in base al valore specificato per il `OperationType` parametro.
- `getClonedInstanceId`- Recupera l'ID dell'istanza appena avviata dall'automazione secondaria.
- `checkIfRootVolumeIsBasedOnLVM`- Determina se la partizione root è gestita da LVM.
- `branchOnTheRootVolumeLVMStatus`- Se le approvazioni minime richieste vengono ricevute dai principali, l'automazione procede con la sostituzione del volume root.
- `manualInstructionsInCaseOfLVM`- Se il volume root è gestito da LVM, l'automazione invia un output contenente istruzioni su come sostituire manualmente i volumi root.
- `startOfReplaceRootEBSVolumeBranch`- Avvia il flusso di lavoro del ramo `Replace Root EBS Volume`.
- `checkIfTargetInstanceIsManagedByCFN`- Determina se l'istanza di destinazione è gestita da uno AWS CloudFormation stack.
- `branchOnCFNStackStatus`- Filiali in base allo stato dello CloudFormation stack.
- `approvalForRootVolumesReplacement(WithCFN)`- Se l'istanza di destinazione è stata avviata da CloudFormation, l'automazione attende l'approvazione dopo che l'istanza appena avviata è stata avviata con successo come Nitro tipo di istanza. Quando vengono fornite le approvazioni, i volumi Amazon EBS dell'istanza di destinazione vengono sostituiti con i volumi root dell'istanza appena lanciata.
- `approvalForRootVolumesReplacement`- Attende l'approvazione dopo che l'istanza appena lanciata è stata avviata correttamente come Nitro tipo di istanza. Quando vengono fornite le approvazioni, i volumi Amazon EBS dell'istanza di destinazione vengono sostituiti con i volumi root dell'istanza appena lanciata.
- `assertIfTargetEC2InstanceIsStillStopped`- Verifica che l'istanza di destinazione sia in uno `stopped` stato prima di sostituire il volume root.
- `stopTargetInstanceForRootVolumeReplacement`- Se l'istanza di destinazione è in esecuzione, l'automazione interrompe l'istanza prima di sostituire il volume root.
- `forceStopTargetInstanceForRootVolumeReplacement`- Arresta con forza l'istanza di destinazione se il passaggio precedente fallisce.

- `stopClonedInstanceForRootVolumeReplacement`- Arresta l'istanza appena creata prima di sostituire i volumi Amazon EBS.
- `forceStopClonedInstanceForRootVolumeReplacement`- Arresta con forza l'istanza appena creata se il passaggio precedente fallisce.
- `getBlockDeviceMappings`- Recupera le mappature dei dispositivi a blocchi sia per l'istanza di destinazione che per quella appena creata.
- `replaceRootEbsVolumes`- Sostituisce il volume principale dell'istanza di destinazione con il volume principale dell'istanza appena creata.
- `EndOfReplaceRootEBSVolumeBranch`- Fine del flusso di lavoro della filiale Replace Root EBS Volume.
- `checkENAAttributeForTargetInstance`- Verifica se l'attributo Enhanced Networking (ENA) è attivato per l' EC2istanza Amazon di destinazione.
- `enableENAAttributeForTargetInstance`- Attiva l'attributo ENA per l' EC2 istanza Amazon di destinazione, se necessario.
- `setNitroInstanceTypeForTargetInstance`- Cambia l'istanza di destinazione in Nitro tipo di istanza specificato.
- `replicateRootVolumeTags`- Replica i tag sul volume Amazon EBS root dall'istanza Amazon EC2 di destinazione.
- `startTargetInstance`- Avvia l' EC2 istanza Amazon di destinazione dopo aver modificato il tipo di istanza.
- `onFailureStopTargetEC2Instance`- Interrompe l' EC2istanza Amazon di destinazione se non viene avviata come Nitro tipo di istanza.
- `onFailureForceStopTargetEC2Instance`- Arresta con forza l' EC2 istanza Amazon di destinazione se il passaggio precedente fallisce.
- `OnFailureRevertOriginalInstanceType`- Riporta l' EC2istanza Amazon di destinazione al tipo di istanza originale se l'istanza di destinazione non viene avviata come Nitro tipo di istanza.
- `onFailureRollbackRootVolumeReplacement`- Annulla tutte le modifiche apportate al `replaceRootEbsVolumes` passaggio, se necessario.
- `onFailureApprovalToStartTargetInstance`- Attende l'approvazione del responsabile designato per avviare l' EC2 istanza Amazon di destinazione dopo aver ripristinato le modifiche precedenti.
- `onFailureStartTargetInstance`- Avvia l' EC2istanza Amazon di destinazione.

- `terminateClonedEC2Instance`- Termina l'istanza EC2 Amazon clonata dopo aver sostituito il volume Amazon EBS principale.

AWSSupport-ResetAccess

Descrizione

Questo runbook utilizzerà lo strumento EC2 Rescue sull' EC2 istanza specificata per riabilitare la decrittografia delle password utilizzando la EC2 Console (Windows) o per generare e aggiungere una nuova coppia di chiavi SSH (Linux). Se hai perso la tua coppia di chiavi, questa automazione creerà un'AMI con password che potrai utilizzare per avviare una EC2 nuova istanza con una coppia di chiavi di tua proprietà (Windows).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `EC2RescueInstanceType`

Tipo: stringa

Valori validi: t2.small | t2.medium | t2.large

Impostazione predefinita: t2.small

Descrizione: (Obbligatorio) Il tipo di istanza per l' EC2 istanza Rescue. EC2 Dimensioni consigliate: t2.small.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) ID dell' EC2 istanza per cui desideri reimpostare l'accesso.

 Important

Systems Manager Automation interrompe questa istanza e crea un'AMI prima di tentare qualsiasi operazione. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico verrà modificato se non si utilizza un IP elastico.

- SubnetId

Tipo: stringa

Impostazione predefinita: CreateNew VPC

Descrizione: (Facoltativo) L'ID di sottorete per l'istanza EC2 Rescue. Per impostazione predefinita, Systems Manager Automation crea un nuovo VPC. In alternativa, utilizzare SelectedInstanceSubnet per utilizzare la stessa sottorete dell'istanza o specificare un ID di sottorete personalizzato.

 Important

La sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

È necessario disporre almeno di `ssm: StartAutomationExecution`, `ssm: GetParameter` (per recuperare il nome del parametro chiave SSH) e `ssm: GetAutomationExecution` per poter leggere l'output dell'automazione. Per ulteriori informazioni sulle autorizzazioni richieste, consulta [AWS Support - StartEC2RescueWorkflow](#).

Fasi del documento

1. `aws:assertAwsResourceProperty`- Asserisce se l'istanza fornita è Windows.
 - a. (EC2Rescue for Windows) Se l'istanza fornita è Windows:
 - i. `aws:executeAutomation`- Richiama `AWSsupport-StartEC2RescueWorkflow` con lo script di reimpostazione della password offline di EC2 Rescue for Windows
 - ii. `aws:executeAwsApi`- Recupera l'ID AMI di backup dall'automazione annidata
 - iii. `aws:executeAwsApi`- Recupera l'ID AMI abilitato alla password dall'automazione annidata
 - iv. `aws:executeAwsApi`- Recupera il riepilogo di Rescue dall'automazione annidata EC2
 - b. (EC2Rescue for Linux) Se l'istanza fornita è Linux:
 - i. `aws:executeAutomation`- Richiama `AWSsupport-StartEC2RescueWorkflow` con lo script di iniezione di chiavi SSH offline di EC2 Rescue for Linux
 - ii. `aws:executeAwsApi`- Recupera l'ID AMI di backup dall'automazione annidata
 - iii. `aws:executeAwsApi`- Recupera il nome del parametro SSM per la chiave SSH iniettata
 - iv. `aws:executeAwsApi`- Recupera il riepilogo di EC2 Rescue dall'automazione annidata

Output

- ottieni `.Output EC2 RescueForWindowsResult`

`getWindowsBackupAmi`. `ImageId`

`getWindowsPasswordEnabledAmi`. `ImageId`

ottieni `EC2 RescueForLinuxResult` `.Output`

`getLinuxBackupAmi`. `ImageId`

`getLinux Parameter.Name SSHKey`

AWSsupport-ResetLinuxUserPassword

Descrizione

Il `AWSSupport-ResetLinuxUserPassword` runbook consente di reimpostare la password di un utente del sistema operativo locale (OS). Questo runbook è particolarmente utile per gli utenti che devono accedere alle proprie istanze Amazon Elastic Compute Cloud EC2 (Amazon) utilizzando la console seriale. Il runbook crea un' EC2 istanza Amazon temporanea nel tuo ruolo Account AWS e un ruolo AWS Identity and Access Management (IAM) con le autorizzazioni per recuperare un valore AWS Secrets Manager segreto contenente la password.

Il runbook arresta l' EC2 istanza Amazon di destinazione, scollega il volume root Amazon Elastic Block Store (Amazon EBS) e lo collega all'istanza Amazon temporanea. EC2 Utilizzando Run Command, viene eseguito uno script sull'istanza temporanea per impostare la password dell'utente del sistema operativo specificato. Quindi, il volume root di Amazon EBS viene ricollegato all'istanza di destinazione. Il runbook offre anche la possibilità di creare un'istantanea del volume root all'inizio dell'automazione.

Prima di iniziare

Crea un segreto di Secrets Manager con il valore della password che desideri assegnare all'utente del tuo sistema operativo. Il valore deve essere in testo semplice. Per ulteriori informazioni, consulta [Creazione di un segreto AWS Secrets Manager](#) nella Guida per l'utente di AWS Secrets Manager .

Considerazioni

- Ti consigliamo di eseguire il backup dell'istanza prima di utilizzare questo runbook. Considerate di impostare il valore del `CreateSnapshot` parametro come **Yes**
- La modifica della password dell'utente locale richiede che il runbook interrompa l'istanza. Quando un'istanza viene interrotta, tutti i dati archiviati nella memoria o nei volumi dell'Instance Store vengono persi. Inoltre, tutti IPv4 gli indirizzi pubblici assegnati automaticamente vengono rilasciati. Per ulteriori informazioni su cosa succede quando interrompi un'istanza, consulta [Arresta e avvia l'istanza](#) nella Amazon EC2 User Guide.
- Se i volumi Amazon EBS collegati all' EC2 istanza Amazon di destinazione sono crittografati con una chiave gestita dal cliente AWS Key Management Service (AWS KMS), assicurati che la AWS KMS chiave non lo sia `deleted disabled` o l'istanza non si avvierà.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza Amazon EC2 Linux che contiene la password utente del sistema operativo che desideri reimpostare.

- LinuxUserName

Tipo: stringa

Impostazione predefinita: ec2-user

Descrizione: (Facoltativo) L'account utente del sistema operativo di cui desideri reimpostare la password.

- SecretArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del segreto di Secrets Manager contenente la nuova password.

- SecurityGroupId

Tipo: stringa

Descrizione: (Facoltativo) L'ID del gruppo di sicurezza da collegare all' EC2 istanza Amazon temporanea. Se non fornisci un valore per questo parametro, viene utilizzato il gruppo di sicurezza Amazon Virtual Private Cloud (Amazon VPC) predefinito.

- SubnetId

Tipo: stringa

Descrizione: (Facoltativo) L'ID della sottorete in cui desideri avviare l'istanza EC2 temporanea di Amazon. Per impostazione predefinita, l'automazione sceglie la stessa sottorete dell'istanza di destinazione. Se si sceglie di fornire una sottorete diversa, questa deve trovarsi nella stessa zona di disponibilità dell'istanza di destinazione e avere accesso agli endpoint Systems Manager.

- CreateSnapshot

Tipo: stringa

Valori validi: Sì | No

Impostazione predefinita: Sì

Descrizione: (Facoltativo) Determina se viene creata un'istantanea del volume root dell' EC2 istanza Amazon di destinazione prima dell'esecuzione dell'automazione.

- StopConsent

Tipo: stringa

Valori validi: Sì | No

Predefinito: No

Descrizione: inserisci **Yes** per confermare che l' EC2 istanza Amazon di destinazione verrà interrotta durante questa automazione. Quando l' EC2 istanza Amazon viene interrotta, tutti i dati archiviati nella memoria o nei volumi dell'instance store vengono persi e l' IPv4 indirizzo pubblico automatico viene rilasciato. Per ulteriori informazioni, consulta [Stop and start your instance](#) nella Amazon EC2 User Guide.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DescribeInstanceInformation`
- `ssm:ListTagsForResource`
- `ssm:SendCommand`
- `ec2:AttachVolume`
- `ec2:CreateSnapshot`
- `ec2:CreateSnapshots`
- `ec2:CreateVolume`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceState`
- `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`

Fasi del documento

1. `aws:branch`— Succursali a seconda che tu abbia fornito il consenso a interrompere l' EC2 istanza Amazon di destinazione.
2. `aws:assertAwsResourceProperty`— Assicura che lo stato dell' EC2 istanza Amazon sia in uno stopped stato running or. In caso contrario, l'automazione termina.
3. `aws:executeAwsApi`— Ottiene le proprietà dell' EC2 istanza Amazon.
4. `aws:executeAwsApi`— Ottiene le proprietà del volume principale.
5. `aws:branch`— Suddivide l'automazione a seconda che sia stato fornito un ID di sottorete per l' EC2 istanza Amazon temporanea.
6. `aws:assertAwsResourceProperty`— Assicura che la sottorete specificata nel SubnetId parametro si trovi nella stessa zona di disponibilità dell' EC2 istanza Amazon di destinazione.
7. `aws:assertAwsResourceProperty`— Assicura che il volume root dell' EC2istanza Amazon di destinazione sia un volume Amazon EBS.
8. `aws:assertAwsResourceProperty`— Assicura che l'architettura dell' EC2 istanza Amazon sia arm64 o x86_64.
9. `aws:assertAwsResourceProperty`— Assicura che il comportamento di chiusura dell' EC2 istanza Amazon sia corretto stop e non corretto. terminate
10. `aws:branch`— Assicura che l' EC2 istanza Amazon non sia un'istanza Spot. Altrimenti, l'automazione termina.
11. `aws:executeScript`— Assicura che l' EC2 istanza Amazon non faccia parte di un gruppo di auto scaling. Se l'istanza fa parte di un gruppo di auto scaling, l'automazione conferma che l' EC2 istanza Amazon è in uno stato del Standby ciclo di vita.
12. `aws:createStack`— Crea un' EC2 istanza Amazon temporanea che viene utilizzata per reimpostare la password per l'utente del sistema operativo specificato.
13. `aws:waitForAwsResourceProperty`— Attende l'esecuzione dell' EC2 istanza Amazon temporanea appena lanciata.
14. `aws:executeAwsApi`— Ottiene l'ID dell' EC2istanza Amazon temporanea.

- 15 `aws:waitForAwsResourceProperty`— Attende che l' EC2 istanza temporanea di Amazon venga segnalata come gestita da Systems Manager.
- 16 `aws:changeInstanceState`— Arresta l' EC2 istanza Amazon di destinazione.
- 17 `aws:changeInstanceState`— Forza l'interruzione dell' EC2 istanza Amazon di destinazione nel caso in cui rimanga bloccata in uno stato di arresto.
- 18 `aws:branch`— Suddivide l'automazione a seconda che sia stata richiesta un'istantanea del volume root dell' EC2 istanza Amazon di destinazione.
- 19 `aws:executeAwsApi`— Crea uno snapshot del volume Amazon EBS root dell' EC2 istanza Amazon di destinazione.
- 20 `aws:waitForAwsResourceProperty`— Attende che lo snapshot sia in uno stato. `completed`
- 21 `aws:executeAwsApi`— Scollega il volume root di Amazon EBS dall'istanza Amazon EC2 di destinazione.
- 22 `aws:waitForAwsResourceProperty`— Attende che il volume root di Amazon EBS venga scollegato dall'istanza Amazon di destinazione. EC2
- 23 `aws:executeAwsApi`— Collega il volume Amazon EBS root all'istanza Amazon EC2 temporanea.
- 24 `aws:waitForAwsResourceProperty`— Attende che il volume root di Amazon EBS venga collegato all'istanza Amazon EC2 temporanea.
- 25 `aws:runCommand`— Reimposta la password dell'utente di destinazione eseguendo uno script di shell utilizzando Run Command sull' EC2 istanza temporanea di Amazon.
- 26 `aws:executeAwsApi`— Scollega il volume root di Amazon EBS dall'istanza Amazon EC2 temporanea.
- 27 `aws:waitForAwsResourceProperty`— Attende che il volume root di Amazon EBS venga scollegato dall'istanza Amazon temporanea. EC2
- 28 `aws:executeAwsApi`— Scollega il volume root di Amazon EBS dall' EC2 istanza Amazon temporanea dopo un errore.
- 29 `aws:waitForAwsResourceProperty`— Attende che il volume root di Amazon EBS venga scollegato dall' EC2 istanza Amazon temporanea dopo un errore.
- 30 `aws:branch`— Suddivide l'automazione a seconda che sia stata richiesta un'istantanea del volume root per determinare il percorso di ripristino in caso di errore.
- 31 `aws:executeAwsApi`— Ricollega il volume Amazon EBS root all'istanza Amazon di destinazione. EC2

- 32aws:waitForAwsResourceProperty— Attende che il volume root di Amazon EBS venga collegato all'istanza Amazon EC2 .
- 33aws:executeAwsApi— Crea un nuovo volume Amazon EBS dallo snapshot del volume root dell' EC2 istanza Amazon di destinazione.
- 34aws:waitForAwsResourceProperty— Attende che il nuovo volume Amazon EBS sia in uno available stato.
- 35aws:executeAwsApi— Collega il nuovo volume Amazon EBS all'istanza di destinazione come volume root.
- 36aws:waitForAwsResourceProperty— Attende che il volume Amazon EBS si trovi in uno attached stato.
- 37aws:executeAwsApi— Descrive gli eventi AWS CloudFormation dello stack se i runbook non riescono a creare o aggiornare lo stack. AWS CloudFormation
- 38aws:branch— Suddivide l'automazione in base allo stato precedente dell' EC2 istanza Amazon. Se lo stato era running, l'istanza viene avviata. Se era in uno stopped stato, l'automazione continua.
- 39aws:changeInstanceState— Avvia l' EC2 istanza Amazon, se necessario.
- 40aws:waitForAwsResourceProperty— Attende che lo AWS CloudFormation stack assuma lo stato di terminale prima di eliminarlo.
- 41aws:executeAwsApi— Elimina lo AWS CloudFormation stack, inclusa l'istanza Amazon EC2 temporanea.

AWSPremiumSupport-ResizeNitroInstance

Descrizione

Il AWSPremiumSupport-ResizeNitroInstance runbook fornisce una soluzione automatizzata per il ridimensionamento delle istanze Amazon Elastic Compute Cloud (EC2Amazon) basate sul sistema Nitro.

Per ridurre il potenziale rischio di perdita di dati e tempi di inattività, il runbook verifica quanto segue:

- Comportamento di interruzione dell'istanza.
- Se l'istanza fa parte di un gruppo Amazon EC2 Auto Scaling ed è in standby modalità.
- Stato e locazione dell'istanza.

- Il tipo di istanza che desideri modificare supporta il numero di interfacce di rete attualmente collegate all'istanza.
- L'architettura del processore e il tipo di virtualizzazione per il tipo di istanza corrente e quello di destinazione sono gli stessi.
- Se l'istanza è in esecuzione, significa che sta superando tutti i controlli di stato.
- Il tipo di istanza a cui desideri passare è disponibile nella stessa zona di disponibilità.

Se Amazon non EC2 supera i controlli di stato dopo aver cambiato il tipo di istanza, il runbook torna automaticamente al tipo di istanza precedente.

Per impostazione predefinita, questo runbook non modifica il tipo di istanza se è in esecuzione e i volumi dell'Instance Store sono collegati. Inoltre, il runbook non cambierà il tipo di istanza se l'istanza fa parte di uno AWS CloudFormation stack. Se desideri modificare uno di questi comportamenti, specifica `yes` i `AllowInstanceStoreInstances` parametri and `AllowCloudFormationInstances`

Il runbook offre due modi diversi per specificare il tipo di istanza a cui desiderate passare:

- Per le automazioni semplici destinate a una singola istanza, specificate il tipo di istanza in cui desiderate passare utilizzando il parametro. `TargetInstanceTypeFromParameter`
- Per eseguire automazioni su larga scala per modificare il tipo di istanza di più istanze, specifica il tipo di istanza utilizzando il parametro. `TargetInstanceTypeFromTagValue` Per informazioni sull'esecuzione di automazioni su larga scala, consulta [Esegui automazioni](#) su larga scala.

Se non si specifica un valore per nessuno dei due parametri, l'automazione fallisce.

Important

L'accesso ai `AWSPremiumSupport-*` runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, [consulta Confronta Supporto i piani](#).

Considerazioni

- Ti consigliamo di eseguire il backup dell'istanza prima di utilizzare questo runbook.
- Per informazioni sulla compatibilità per la modifica dei tipi di istanza, consulta [Compatibilità per la modifica del tipo di istanza](#).

- Se l'automazione fallisce e torna al tipo di istanza originale, vedi [Risoluzione dei problemi relativi alla modifica del tipo di istanza](#).
- La modifica del tipo di istanza richiede che il runbook interrompa l'istanza. Quando un'istanza viene interrotta, tutti i dati archiviati nella memoria o nei volumi dell'Instance Store vengono persi. Inoltre, tutti IPv4 gli indirizzi pubblici assegnati automaticamente vengono rilasciati. Per ulteriori informazioni su cosa succede quando si arresta un'istanza, consulta [Arrestare e avviare l'istanza](#).
- Utilizzando il `SkipInstancesWithTagKey` parametro, puoi saltare le istanze a cui è applicata una chiave di EC2 tag Amazon specifica.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `Riconoscere`

Tipo: stringa

Descrizione: (Obbligatorio) Inserisci **yes** per confermare che l'istanza verrà interrotta se è attualmente in esecuzione.

- AllowInstanceStoreInstances

Tipo: stringa

Valori validi: no | sì

Impostazione predefinita: no

Descrizione: (Facoltativo) Se lo specifichi `yes`, consenti l'esecuzione del runbook su istanze a cui sono collegati volumi di Instance Store.

- AllowCloudFormationInstances

Tipo: stringa

Valori validi: no | sì

Impostazione predefinita: no

Descrizione: (Facoltativo) Se si specifichi `yes`, il runbook viene eseguito su istanze che fanno parte di uno AWS CloudFormation stack.

- DryRun

Tipo: stringa

Valori validi: no | sì

Impostazione predefinita: no

Descrizione: (Facoltativo) Se si specifichi `yes`, il runbook convalida i requisiti di ridimensionamento senza apportare modifiche al tipo di istanza.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon di cui desideri modificare il tipo.

- SkipInstancesWithTagKey

Tipo: stringa

Descrizione: (Facoltativo) L'automazione salta un'istanza di destinazione se la chiave del tag specificata viene applicata all'istanza.

- SleepTime

Tipo: stringa

Impostazione predefinita: 3

Descrizione: (Facoltativo) Il numero di secondi in cui questo runbook deve rimanere inattivo dopo il completamento.

- TagInstance

Tipo: stringa

Descrizione: (Facoltativo) Etichetta le istanze con la chiave e il valore che preferisci utilizzando il seguente formato: *Key=ChangingType, Value=True*. Questa opzione ti consente di tenere traccia delle istanze che sono state prese di mira da questo runbook. I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole.

- TargetInstanceTypeFromParameter

Tipo: stringa

Descrizione: (Facoltativo) Il tipo di istanza in cui desideri modificare l'istanza. Lascia vuoto questo parametro se desideri utilizzare il valore della chiave del tag fornita nel TargetInstanceTypeFromTagValue parametro.

- TargetInstanceTypeFromTagValue

Tipo: stringa

Descrizione: (Facoltativo) La chiave tag applicata alle istanze di destinazione il cui valore contiene il tipo di istanza a cui desideri passare. Se specificate un valore per il TargetInstanceTypeFromParameter parametro, questo sostituisce qualsiasi valore specificato per questo parametro.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

1. `aws:assertAwsResourceProperty`: assicura che l' EC2 istanza Amazon non sia etichettata con la chiave del tag di risorsa specificata nel `SkipInstancesWithTagKey` parametro. Se la chiave del tag viene trovata applicata all'istanza, il passaggio fallisce e l'automazione termina.
2. `aws:assertAwsResourceProperty`: conferma che lo stato dell' EC2 istanza Amazon di destinazione è `runningpending`, `stopped`, o `stopping`. In caso contrario, l'automazione termina.
3. `aws:executeAwsApi`: raccoglie le proprietà dall' EC2 istanza Amazon.
4. `aws:executeAwsApi`: raccoglie dettagli sull'attuale tipo di EC2 istanza Amazon.
5. `aws:branch`: Verifica se il tipo di istanza corrente e il tipo di istanza specificato nel `TargetInstanceTypeFromParameter` parametro coincidono. Se lo sono, l'automazione termina.
6. `aws:assertAwsResourceProperty`: Assicura che l'istanza sia in esecuzione sul sistema Nitro.
7. `aws:branch`: assicura che il tipo di volume root dell' EC2 istanza Amazon sia un volume Amazon Elastic Block Store (Amazon EBS).
8. `aws:assertAwsResourceProperty`: conferma che il comportamento di chiusura dell'istanza è `stop` corretto e non corretto. `terminate`
9. `aws:branch`: assicura che l' EC2 istanza Amazon non sia un'istanza Spot.

- 10 `aws:branch`: Assicura che la tenancy dell' EC2 istanza Amazon sia predefinita e non sia un host dedicato o un'istanza dedicata.
- 11 `aws:executeScript`: conferma che esiste una sola automazione di questo runbook destinata all'ID dell'istanza corrente. Se è già in corso un'altra automazione destinata alla stessa istanza, l'automazione restituisce un errore e termina.
- 12 `aws:branch`: suddivide l'automazione in base allo stato dell' EC2 istanza Amazon.
- In caso `stopped stopping` affermativo, l'automazione viene eseguita `aws:waitForAwsResourceProperty` fino al completo arresto dell' EC2 istanza Amazon.
 - In caso `running pending` affermativo, l'automazione viene eseguita `aws:waitForAwsResourceProperty` fino a quando l' EC2 istanza Amazon non supera i controlli di stato.
- 13 `aws:assertAwsResourceProperty`: conferma che l' EC2 istanza Amazon non fa parte di un gruppo Auto Scaling chiamando l'operazione `DescribeAutoScalingInstances` API. Se l'istanza fa parte di un gruppo Auto Scaling, assicura che l' EC2 istanza Amazon sia in `standby` modalità.
- 14 `aws:branch`: Suddivide l'automazione a seconda che desideri che l'automazione controlli se l' EC2 istanza Amazon fa parte di uno AWS CloudFormation stack:
- `aws:executeScript` Assicura che l' EC2 istanza Amazon non faccia parte di uno AWS CloudFormation stack chiamando l'operazione `DescribeStackResources` API.
- 15 `aws:executeAwsApi`: restituisce un elenco di tipi di istanza con lo stesso tipo di architettura del processore, tipo di virtualizzazione e che supporta il numero di interfacce di rete attualmente collegate all'istanza di destinazione.
- 16 `aws:executeAwsApi`: ottiene il valore del tipo di istanza di destinazione dalla chiave di tag specificata nel parametro. `TargetInstanceTypeFromTagValue`
- 17 `aws:executeScript`: conferma che i tipi di istanza corrente e di destinazione sono compatibili. Assicura che il tipo di istanza di destinazione sia disponibile nella stessa sottorete. Verifica che il principale che ha avviato il runbook disponga delle autorizzazioni per modificare il tipo di istanza e arrestare e avviare l'istanza se era in esecuzione.
- 18 `aws:branch`: ramifica l'automazione in base al fatto che il valore del `DryRun` parametro sia impostato su. `yes` Seyes, l'automazione termina.
- 19 `aws:branch`: verifica se il tipo di istanza originale e quello di destinazione coincidono. Se sono uguali, l'automazione termina.
- 20 `aws:executeAwsApi`: ottiene lo stato corrente dell'istanza.

21aws:changeInstanceState: interrompe l' EC2 istanza Amazon.

22aws:changeInstanceState: forza l'interruzione dell'istanza se è bloccata nello stopping stato.

23aws:executeAwsApi: modifica il tipo di istanza nel tipo di istanza di destinazione.

24aws:sleep: attende 3 secondi dopo la modifica del tipo di istanza per garantire la coerenza finale.

25aws:branch: suddivide l'automazione in base allo stato precedente dell'istanza. In caso affermativorunning, l'istanza viene avviata.

- a. aws:changeInstanceState: avvia l' EC2 istanza Amazon se era in esecuzione prima di cambiare il tipo di istanza.
- b. aws:waitForAwsResourceProperty: attende che l' EC2 istanza Amazon superi i controlli di stato. Se l'istanza non supera i controlli di stato, torna al tipo di istanza originale.
 - i. aws:changeInstanceState: interrompe l' EC2 istanza Amazon prima di sostituirla con il tipo di istanza originale.
 - ii. aws:changeInstanceState: forza l'interruzione dell' EC2 istanza Amazon prima di cambiarla con il tipo di istanza originale nel caso in cui rimanga bloccata in uno stato di arresto.
 - iii. aws:executeAwsApi: riporta l' EC2 istanza Amazon al tipo originale.
 - iv. aws:sleep: attende 3 secondi dopo aver modificato il tipo di istanza per garantire la coerenza finale.
 - v. aws:changeInstanceState: avvia l' EC2 istanza Amazon se era in esecuzione prima di cambiare il tipo di istanza.
 - vi. aws:waitForAwsResourceProperty: attende che l' EC2 istanza Amazon superi i controlli di stato.

26aws:sleep: Attende prima di terminare il runbook.

AWSSupport-RestoreEC2InstanceFromSnapshot

Descrizione

Il AWSSupport-RestoreEC2InstanceFromSnapshot runbook ti aiuta a identificare e ripristinare un'istanza Amazon Elastic Compute Cloud (Amazon EC2) da uno snapshot Amazon Elastic Block Store (Amazon EBS) funzionante del volume root.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EndDate

Tipo: stringa

Descrizione: (Facoltativo) L'ultima data in cui si desidera che l'automazione cerchi un'istantanea.

- InplaceSwap

Tipo: Booleano

Valori validi: true | false

Descrizione: (Facoltativo) Se il valore di questo parametro è impostato su `true`, il volume appena creato dall'istantanea sostituisce il volume principale esistente collegato all'istanza.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza che desideri ripristinare da un'istantanea.

- LookForInstanceStatusCheck

Tipo: Booleano

Valori validi: true | false

Impostazione predefinita: true

Descrizione: (Facoltativo) Se il valore di questo parametro è impostato su `true`, l'automazione verifica se i controlli dello stato dell'istanza hanno esito negativo sulle istanze di test avviate dalle istantanee.

- `SkipSnapshotsBy`

Tipo: stringa

Descrizione: (Facoltativo) L'intervallo in cui le istantanee vengono saltate durante la ricerca di istantanee per ripristinare l'istanza. Ad esempio, se sono disponibili 100 istantanee e si specifica il valore 2 per questo parametro, viene esaminata ogni terza istantanea.

Impostazione predefinita: 0

- `SnapshotId`

Tipo: stringa

Descrizione: (Facoltativo) L'ID di un'istantanea da cui si desidera ripristinare l'istanza.

- `StartDate`

Tipo: stringa

Descrizione: (Facoltativo) La prima data in cui desideri che l'automazione cerchi un'istantanea.

- `TotalSnapshotsToLook`

Tipo: stringa

Descrizione: (Facoltativo) Il numero di istantanee esaminate dall'automazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

1. `aws:executeAwsApi`- Raccoglie dettagli sull'istanza di destinazione.
2. `aws:assertAwsResourceProperty`- Verifica l'esistenza dell'istanza di destinazione.
3. `aws:assertAwsResourceProperty`- Verifica che il volume root sia un volume Amazon EBS.
4. `aws:assertAwsResourceProperty`- Verifica che non sia già in esecuzione un'altra automazione destinata a questa istanza.
5. `aws:executeAwsApi`- Etichetta l'istanza di destinazione.
6. `aws:executeAwsApi`- Crea un AMI dell'istanza.

7. `aws:executeAwsApi`- Raccoglie dettagli sulla AMI creato nel passaggio precedente.
8. `aws:waitForAwsResourceProperty`- Attende il AMI stato da diventare available prima di procedere.
9. `aws:executeScript`- Avvia una nuova istanza da quella appena creata AMI.
10. `aws:assertAwsResourceProperty`- Verifica che lo stato dell'istanza sia. available
11. `aws:executeAwsApi`- Raccoglie i dettagli sull'istanza appena lanciata.
12. `aws:branch`- Rami in base al fatto che tu abbia fornito un valore per il SnapshotId parametro.
13. `aws:executeScript`- Restituisce un elenco di istantanee entro il periodo di tempo specificato.
14. `aws:executeAwsApi`- Arresta l'istanza.
15. `aws:waitForAwsResourceProperty`- Attende che lo stato del volume sia available raggiunto.
16. `aws:waitForAwsResourceProperty`- Attende che lo stato dell'istanza sia. stopped
17. `aws:executeAwsApi`- Rimuove il volume principale.
18. `aws:waitForAwsResourceProperty`- Attende che il volume principale venga scollegato.
19. `aws:executeAwsApi`- Collega il nuovo volume principale.
20. `aws:waitForAwsResourceProperty`- Attende che il nuovo volume venga allegato.
21. `aws:executeAwsApi`- Avvia l'istanza.
22. `aws:waitForAwsResourceProperty`- Attende che lo stato dell'istanza sia available.
23. `aws:waitForAwsResourceProperty`- Attende che i controlli dello stato del sistema e dell'istanza vengano superati.
24. `aws:executeScript`- Esegue uno script per trovare un'istantanea che può essere utilizzata per creare correttamente un volume.
25. `aws:executeScript`- Esegue uno script per ripristinare l'istanza utilizzando il volume appena creato dall'istantanea identificata dall'automazione o utilizzando il volume creato dall'istantanea specificata nel parametro. SnapshotId
26. `aws:executeScript`- Elimina le risorse create dall'automazione.

Output

`launchCloneInstance.InstanceIds`

`ListSnapshotByDate`. Istanza finali

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.Istantanea funzionante

InstanceRecovery.risultato

AWSSupport - SendLogBundleToS3Bucket

Descrizione

Il `AWSSupport - SendLogBundleToS3Bucket` runbook carica un pacchetto di log generato dallo strumento EC2 Rescue dall'istanza di destinazione al bucket S3 specificato. Il runbook installa la versione di EC2 Rescue specifica per piattaforma basata sulla piattaforma dell'istanza di destinazione. EC2Rescue viene quindi utilizzato per raccogliere tutti i log del sistema operativo (OS) disponibili.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (obbligatorio) ID dell'istanza gestita di Windows o Linux da cui si desidera raccogliere i log.

- S3 BucketName

Tipo: stringa

Descrizione: (obbligatorio) bucket S3 in cui caricare i log.

- S3Path

Tipo: stringa

Predefinito: /AWSsupport-SendLogBundleToS3Bucket

Descrizione: (facoltativo) percorso S3 per i log raccolti.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia che l' EC2 istanza che riceve il comando abbia un ruolo IAM con la policy gestita di `SSMManagedInstanceCoreAmazon Amazon` allegata. L'utente deve disporre almeno di `ssm: StartAutomationExecution` e `ssm: SendCommand` per eseguire l'automazione e inviare il comando all'istanza, più `ssm: GetAutomationExecution` per poter leggere l'output dell'automazione.

Fasi del documento

1. `aws:runCommand`- Installa EC2 Rescue tramite. `AWS-ConfigureAWSPackage`
2. `aws:runCommand`- Esegui lo PowerShell script per raccogliere i registri di risoluzione dei problemi di Windows con EC2 Rescue.
3. `aws:runCommand`- Esegui lo script bash per raccogliere i registri di risoluzione dei problemi di Linux con Rescue. EC2

Output

`collectAndUploadWindowsLogBundle.Uscita`

collectAndUploadLinuxLogBundle.Uscita

AWSSupport-StartEC2RescueWorkflow

Descrizione

Il `AWSSupport-StartEC2RescueWorkflow` runbook esegue lo script con codifica base64 fornito (Bash o Powershell) su un'istanza helper creata per salvare l'istanza. Il volume root dell'istanza è collegato e montato sull'istanza helper, nota anche come istanza Rescue. EC2 Se l'istanza è Windows, specificare uno script Powershell. In caso contrario, utilizzare Bash. Il runbook imposta alcune variabili di ambiente che è possibile utilizzare nello script. Le variabili di ambiente contengono informazioni sull'input fornito, nonché informazioni sul volume root offline. Il volume offline è già montato e pronto all'uso. Ad esempio, è possibile salvare il file di configurazione dello stato desiderato in un volume root di Windows offline o eseguire il comando `chroot` e passare a un volume root di Linux offline ed eseguire la correzione offline.

[Esegui questa automazione \(console\)](#)

Important

EC2 Le istanze Amazon create da Marketplace Amazon Machine Images (AMIs) non sono supportate da questa automazione.

Informazioni aggiuntive

Per applicare la codifica base64 a uno script, è possibile utilizzare Powershell o Bash. Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

Bash:

```
base64 PATH_TO_FILE
```

Ecco un elenco di variabili di ambiente che è possibile utilizzare negli script offline, a seconda del sistema operativo di destinazione.

Windows:

Variabile	Descrizione	Valore di esempio
\$env: RESCUE_ACCOUNT_ID EC2	{{ global:ACCOUNT_ID }}	123456789012
\$env: EC2 RESCUE_DATE	{{ global:DATE }}	2018-09-07
\$env: EC2 RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
\$ env: EC2 RESCUE_RW_DIR EC2	EC2Percorso di installazione di Rescue for Windows	C:\Program Files\ Amazon\ EC2 Rescue
\$ env: EC2 RESCUE_RW_DIR EC2	EC2Percorso di installazione di Rescue for Windows	C:\Program Files\ Amazon\ EC2 Rescue
\$ env: RESCUE_EXECUTION_ID EC2	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
\$ env: EC2 RESCUE_OFFLINE_CURRENT_CONTROL_SET	Percorso dell'insieme di controlli corrente di Windows offline	HKLM:\AWSTempSystem\ControlSet001
\$ env: EC2 RESCUE_OFFLINE_DRIVE	Lettera di unità di Windows offline	D:\
\$ env: EC2 RESCUE_OFFLINE_EBS_DEVICE	Dispositivo EBS del volume root offline	xvdf
\$ env: EC2 RESCUE_OFFLINE_KERNEL_VER	Versione del kernel di Windows offline	6.1.7601.24214
\$env: EC2 RESCUE_OFFLINE_OS_ARCHITECTURE	Architettura di Windows offline	AMD64
\$env: EC2 RESCUE_OFFLINE_OS_CAPTION	Didascalia di Windows offline	Windows Server 2008 R2 Datacenter

Variabile	Descrizione	Valore di esempio
\$env: EC2 RESCUE_OF FLINE_OS_TYPE	Tipo di sistema operativo Windows offline	Server
\$env: EC2 RESCUE_OF FLINE_PROGRAM_FILE S_DIR	Percorso della directory dei file di programma di Windows offline	D:\Program Files
\$ env: EC2 RESCUE_OF FLINE_PROGRAM_FILE S_X86_DIR	Percorso della directory dei file di programma x86 di Windows offline	D:\Program Files (x86)
\$ env: EC2 RESCUE_OF FLINE_REGISTRY_DIR	Percorso della directory del Registro di sistema di Windows offline	D:\Windows\System32\config
\$ env: EC2 RESCUE_OF FLINE_SYSTEM_ROOT	Percorso della directory radice di sistema di Windows offline	D:\Windows
\$env: EC2 RESCUE_REGION	{{ global:REGION }}	us-west-1
\$env: EC2 RESCUE_S3 _BUCKET	{{S3}BucketName }	bucket dimostrativo amzn-s3
\$env: RESCUE_S3_PREFIX EC2	{{ S3Prefix }}	myprefix/
\$env: EC2 RESCUE_SO URCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
\$script: EC2 RESCUE_OF FLINE_WINDOWS_INSTALL	Metadati di installazione di Windows offline	Oggetto Powershell del cliente

Linux:

Variabile	Descrizione	Valore di esempio
EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
EC2DATA DI SALVATAGGIO	{{ global:DATE }}	2018-09-07
EC2DATE_ORA DI SALVATAGGIO	{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_RL_DIR EC2	EC2Percorso di installazione di Rescue for Linux	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2DEVICE_RESCUE_OFFLINE	Nome del dispositivo offline	/dev/xvdf1
EC2DEVICE_RESCUE_OFFLINE_EBS	Dispositivo EBS del volume root offline	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	Punto di montaggio del volume radice offline	/mnt/mount
EC2RESCUE_PYTHON	Versione di Python	python2.7
EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{ S3 }} BucketName	bucket dimostrativo amzn-s3
EC2PREFIXO RESCUE_S3	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AMIPrefix

Tipo: stringa

Impostazione predefinita: `AWSSupport-EC2Rescue`

Descrizione: (facoltativo) prefisso del nome dell'AMI di backup.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- CreatePostEC2RescueBackup

Tipo: stringa

Valori validi: `true` | `false`

Impostazione predefinita: `false`

Descrizione: (Facoltativo) Impostalo `true` per creare un AMI `InstanceId` dopo aver eseguito lo script, prima di avviarlo. L'AMI verrà conservata dopo il completamento dell'automazione. È responsabilità dell'utente proteggere l'accesso all'AMI oppure eliminarla.

- CreatePreEC2RescueBackup

Tipo: stringa

Valori validi: `true` | `false`

Impostazione predefinita: `false`

Descrizione: (Facoltativo) Impostalo `true` per creare un AMI di InstanceId prima dell'esecuzione dello script. L'AMI verrà conservata dopo il completamento dell'automazione. È responsabilità dell'utente proteggere l'accesso all'AMI oppure eliminarla.

- `EC2RescueInstanceType`

Tipo: stringa

Valori validi: `t2.small` | `t2.medium` | `t2.large` | `t3.small` | `t3.medium` | `t3.large` | `i3.large`

Predefinito: `t3.medium`

Descrizione: (Facoltativo) Il tipo di EC2 istanza per l'istanza EC2 Rescue.

- `InstanceId`

Tipo: stringa

Descrizione: (Obbligatorio) ID dell' EC2 istanza. **IMPORTANTE:** AWS Systems Manager l'automazione interrompe questa istanza. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico verrà modificato se non si utilizza un IP elastico.

- `OfflineScript`

Tipo: stringa

Descrizione: (obbligatorio) script con codifica Base64 da eseguire sull'istanza helper. Usa Bash se la tua istanza di origine è Linux e PowerShell se è Windows.

- `S3 BucketName`

Tipo: stringa

Descrizione: (facoltativo) nome del bucket S3 nell'account in cui si desidera caricare i log della risoluzione dei problemi. Verificare che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie alle parti che non necessitano dell'accesso ai log raccolti.

- `S3Prefix`

Tipo: stringa

Impostazione predefinita: `AWSSupport-EC2Rescue`

Descrizione: (facoltativo) prefisso dei log S3.

- SubnetId

Tipo: stringa

Predefinito: SelectedInstanceSubnet

Descrizione: (Facoltativo) L'ID di sottorete per l'istanza EC2 Rescue. Per impostazione predefinita, viene utilizzata la stessa sottorete in cui si trova l'istanza specificata. **IMPORTANTE:** se si fornisce una sottorete personalizzata, questa deve trovarsi nella stessa InstanceId zona di disponibilità dell'utente e deve consentire l'accesso agli endpoint SSM.

- UniqueId

Tipo: stringa

Impostazione predefinita: {{ automation:EXECUTION_ID }}

Descrizione: (Facoltativo) Un identificatore univoco per l'automazione.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia all'utente che esegue l'automazione di allegare la policy gestita di Amazon SSMAutomation Role IAM. Oltre a tale policy l'utente deve disporre di quanto segue:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:*:An-AWS-Account-ID:function:AWSSupport-EC2Rescue-*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
```

```

        "s3:GetObjectVersion"
    ],
    "Resource": [
        "arn:aws:s3:::awssupport-ssm.*/*.template",
        "arn:aws:s3:::awssupport-ssm.*/*.zip"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:PutRolePolicy",
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam>DeleteInstanceProfile"
    ],
    "Resource": [
        "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport-EC2Rescue-*",
        "arn:aws:iam::An-AWS-Account-ID:instance-profile/AWSSupport-
EC2Rescue-*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "lambda:CreateFunction",
        "ec2:CreateVpc",
        "ec2:ModifyVpcAttribute",
        "ec2>DeleteVpc",
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2>DeleteInternetGateway",
        "ec2:CreateSubnet",
        "ec2>DeleteSubnet",
        "ec2:CreateRoute",

```

```

        "ec2:DeleteRoute",
        "ec2:CreateRouteTable",
        "ec2:AssociateRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteRouteTable",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:Describe*"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

Fasi del documento

1. `aws:executeAwsApi`- Descrivi l'istanza fornita
2. `aws:executeAwsApi`- Descrivi il volume principale dell'istanza fornita
3. `aws:assertAwsResourceProperty`- Verifica che il tipo di dispositivo del volume principale sia EBS
4. `aws:assertAwsResourceProperty`- Verifica che il volume root non sia crittografato
5. `aws:assertAwsResourceProperty`- Controlla l'ID di sottorete fornito
 - a. (Usa la sottorete dell'istanza corrente) - Se `* SubnetId = SelectedInstanceSubnet *`, esegui `aws:createStack` per distribuire lo stack Rescue EC2 CloudFormation
 - b. (Crea nuovo VPC) - Se `* SubnetId = CreateNew VPC*`, esegui `aws:createStack` per distribuire lo stack Rescue EC2 CloudFormation
 - c. (Utilizzo della sottorete personalizzata): in tutti gli altri casi:

`aws:assertAwsResourceProperty`- Verifica che la sottorete fornita si trovi nella stessa zona di disponibilità dell'istanza fornita

`aws:createStack`- Implementa lo stack Rescue EC2 CloudFormation

6. `aws:invokeLambdaFunction`- Esegui una convalida aggiuntiva degli input
7. `aws:executeAwsApi`- Aggiorna lo CloudFormation stack EC2 Rescue per creare l'istanza dell'helper EC2 Rescue

8. `aws:waitForAwsResourceProperty`- Attendi il completamento dell'aggiornamento dello CloudFormation stack EC2 Rescue
9. `aws:executeAwsApi`- Descrivi l'output CloudFormation dello stack EC2 Rescue per ottenere l'ID dell'istanza di EC2 Rescue helper
10. `aws:waitForAwsResourceProperty`- Attendi che l'istanza EC2 Rescue helper diventi un'istanza gestita
11. `aws:changeInstanceState`- Arresta l'istanza fornita
12. `aws:changeInstanceState`- Arresta l'istanza fornita
13. `aws:changeInstanceState`- Arresta forzatamente l'istanza fornita
14. `aws:assertAwsResourceProperty`- Controlla il valore `CreatePre EC2 RescueBackup` di input
 - a. (Crea un backup pre- EC2 Rescue) - `I* CreatePre EC2 RescueBackup = true*`
 - b. `aws:executeAwsApi`- Creare un backup AMI dell'istanza fornita
 - c. `aws:createTags`- Etichetta il backup AMI
15. `aws:runCommand`- Installa EC2 Rescue sull'istanza di EC2 Rescue helper
16. `aws:executeAwsApi`- Stacca il volume principale dall'istanza fornita
17. `aws:assertAwsResourceProperty`- Controlla la piattaforma di istanza fornita
 - a. (L'istanza è Windows):

`aws:executeAwsApi`- Collega il volume root all'istanza dell'helper EC2 Rescue come `*xvdf*`

`aws:sleep`- Dormi per 10 secondi

`aws:runCommand`- Esegui lo script offline fornito in Powershell
 - b. (L'istanza è Linux):

`aws:executeAwsApi`- Collega il volume root all'istanza dell'helper EC2 Rescue come `*/dev/sdf*`

`aws:sleep`- Dormi per 10 secondi

`aws:runCommand`- Esegui lo script offline fornito in Bash
18. `aws:changeInstanceState`- Arresta l'istanza dell' EC2helper Rescue
19. `aws:changeInstanceState`- Arresta forzatamente l'istanza EC2 Rescue helper
20. `aws:executeAwsApi`- Scollega il volume root dall'istanza dell'helper EC2 Rescue

21.aws:executeAwsApi- Ricollega il volume root all'istanza fornita

22.aws:assertAwsResourceProperty- Controlla il valore CreatePost EC2 RescueBackup di input

a. (Crea un backup EC2 post-Rescue) - I* CreatePost EC2 RescueBackup = true*

b. aws:executeAwsApi- Creare un backup AMI dell'istanza fornita

c. aws:createTags- Etichetta il backup AMI

23.aws:executeAwsApi- Ripristina l'eliminazione iniziale allo stato di terminazione per il volume principale dell'istanza fornita

24.aws:changeInstanceState- Ripristina lo stato iniziale dell'istanza fornita (in esecuzione/interrotta)

25.aws:deleteStack- Elimina lo stack Rescue EC2 CloudFormation

Output

runScriptForLinux.Output

runScriptForWindows.Output

preScriptBackup.Imageld

postScriptBackup.Imageld

AWSPremiumSupport-TroubleshootEC2DiskUsage

Descrizione

Il AWSPremiumSupport-TroubleshootEC2DiskUsage runbook ti aiuta a indagare e potenzialmente risolvere i problemi relativi all'utilizzo del disco root e non root dell'istanza Amazon Elastic Compute Cloud (Amazon EC2). Se possibile, il runbook tenta di risolvere i problemi estendendo il volume e il relativo file system. Per eseguire queste attività, questo runbook orchestra l'esecuzione di diversi runbook basati sul sistema operativo dell'istanza interessata.

Il primo runbook, AWSPremiumSupport-DiagnoseDiskUsageOnWindows ovveroAWSPremiumSupport-DiagnoseDiskUsageOnLinux, determina se i problemi del disco possono essere mitigati espandendo il volume.

Il secondo runbook, AWSPremiumSupport-ExtendVolumesOnWindows oAWSPremiumSupport-ExtendVolumesOnLinux, utilizza l'output del primo runbook per eseguire codice Python che

modifica il volume. Dopo la modifica del volume, il runbook estende la partizione e il file system dei volumi interessati.

 Important

L'accesso ai `AWSPremiumSupport-*` runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, [consulta Confronta Supporto AWS i piani](#).

Questo documento è stato creato in collaborazione con AWS Managed Services (AMS). AMS ti aiuta a gestire la tua AWS infrastruttura in modo più efficiente e sicuro. AMS offre inoltre flessibilità operativa, maggiore sicurezza e conformità, ottimizzazione della capacità e identificazione dei risparmi sui costi. Per ulteriori informazioni, consulta [AWS Managed Services](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, Windows

Parametri

- InstanceId

Tipo: stringa

Valori consentiti: `^[a-z0-9]{8,17}$`

Descrizione: (obbligatorio) ID della tua EC2 istanza Amazon.

- VolumeExpansionEnabled

Tipo: Booleano

Descrizione: (Facoltativo) Contrassegna per controllare se il documento estenderà i volumi e le partizioni interessati.

Impostazione predefinita: true

- VolumeExpansionUsageTrigger

Tipo: stringa

Descrizione: (Facoltativo) Utilizzo minimo dello spazio di partizione richiesto per attivare l'estensione (in percentuale).

Valori consentiti: ^ [0-9] {1,2} \$

Valore predefinito: 85

- VolumeExpansionCapSize

Tipo: stringa

Descrizione: (Facoltativo) Dimensione massima a cui verrà aumentato il volume Amazon Elastic Block Store (Amazon EBS) (in GiB).

Valori consentiti: ^ [0-9] {1,4} \$

Impostazione predefinita: 2048

- VolumeExpansionGibIncrease

Tipo: stringa

Descrizione: (Facoltativo) Aumento di GiB del volume. VolumeExpansionPercentageIncrease Verrà utilizzato il maggiore aumento netto tra VolumeExpansionGibIncrease e.

Valori consentiti: ^ [0-9] {1,4} \$

Impostazione predefinita: 20

- VolumeExpansionPercentageIncrease

Tipo: stringa

Descrizione: (Facoltativo) Aumento della percentuale del volume.

VolumeExpansionPercentageIncrease Verrà utilizzato il maggiore aumento netto tra VolumeExpansionGibIncrease e.

Valori consentiti: ^ [0-9] {1,2} \$

Impostazione predefinita: 20

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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

Fasi del documento

1. `aws:assertAwsResourceProperty`- Verifica se l'istanza è gestita da Systems Manager
2. `aws:executeAwsApi`- Descrive l'istanza per accedere alla piattaforma.
3. `aws:branch`- Automazione delle filiali basata sulla piattaforma dell'istanza.
 - a. Se l'istanza è Windows:
 - i. `aws:executeAutomation`- Esegui il `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` runbook per diagnosticare i problemi di utilizzo del disco sull'istanza.
 - ii. `aws:executeAwsApi`- Ottiene l'output dell'automazione precedente.
 - iii. `aws:branch`- Filiali in base all'output della diagnostica e se ci sono volumi che possono essere espansi per mitigare l'avviso.
 - A. Non ci sono volumi che devono essere espansi: interrompi l'automazione.
 - B. Ci sono volumi che devono essere espansi:
 - I. `aws:executeAwsApi`- Crea un Amazon Machine Image (AMI) dell'istanza.
 - II. `aws:waitForAwsResourceProperty`- Attende il AMI stato in cui sarà. `available`
 - III. `aws:executeAutomation`- Esegui il `AWSPremiumSupport-ExtendVolumesOnWindows` runbook per eseguire la modifica del volume e i passaggi necessari nel sistema operativo (OS) per rendere disponibile il nuovo spazio.
 - b. (La piattaforma non è Windows) Se l'istanza di input non è Windows:
 - i. `aws:executeAutomation`- Esegui il `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` runbook per diagnosticare i problemi di utilizzo del disco sull'istanza.
 - ii. `aws:executeAwsApi`- Ottiene l'output dell'automazione precedente.
 - iii. `aws:branch`- Filiali in base all'output della diagnostica e se ci sono volumi che possono essere espansi per mitigare l'avviso.
 - A. Non ci sono volumi che devono essere espansi: interrompi l'automazione.
 - B. Ci sono volumi che devono essere espansi:
 - I. `aws:executeAwsApi`- Crea un AMI dell'istanza.
 - II. `aws:waitForAwsResourceProperty`- Aspetta AMI stato che sarà. `available`
 - III. `aws:executeAutomation`- Esegui il `AWSPremiumSupport-ExtendVolumesOnLinux` runbook per eseguire la modifica del volume e i passaggi necessari nel sistema operativo per rendere disponibile il nuovo spazio.

Output

diagnoseDiskUsageAlertOnWindows.Uscita

extendVolumesOnWindows.Output

diagnoseDiskUsageAlertOnLinux.Uscita

extendVolumesOnLinux.Output

BackupAMILinux. Imageld

BackupAMIWindows. Imageld

AWSSupport-TroubleshootEC2InstanceConnect

Descrizione

AWSSupport-TroubleshootEC2InstanceConnect l'automazione aiuta ad analizzare e rilevare gli errori che impediscono la connessione a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) utilizzando [Amazon EC2 Instance Connect](#). Identifica i problemi causati da un'Amazon Machine Image (AMI) non supportata, dall'installazione o dalla configurazione di pacchetti a livello di sistema operativo mancante, da autorizzazioni mancanti AWS Identity and Access Management (IAM) o da problemi di configurazione di rete.

Come funziona?

Il runbook richiede l'ID dell' EC2 istanza Amazon, il nome utente, la modalità di connessione, l'IP CIDR di origine, la porta SSH e Amazon Resource Name (ARN) per il ruolo IAM o l'utente che riscontra problemi con Amazon Instance Connect. EC2 Verifica quindi i [prerequisiti](#) per la connessione a un' EC2 istanza Amazon utilizzando Amazon EC2 Instance Connect:

- L'istanza è in esecuzione ed è integra.
- L'istanza si trova in una AWS regione supportata da Amazon EC2 Instance Connect.
- L'AMI dell'istanza è supportato da Amazon EC2 Instance Connect.
- L'istanza può raggiungere l'Instance Metadata Service (IMDSv2).
- Il pacchetto Amazon EC2 Instance Connect è installato e configurato correttamente a livello di sistema operativo.
- La configurazione di rete (gruppi di sicurezza, ACL di rete e regole della tabella di routing) consente la connessione all'istanza tramite Amazon EC2 Instance Connect.

- Il ruolo o l'utente IAM utilizzato per sfruttare Amazon EC2 Instance Connect ha accesso alle chiavi push per l' EC2 istanza Amazon.

Important

- Per verificare l'AMI dell'istanza, IMDSv2 la raggiungibilità e l'installazione del pacchetto Amazon EC2 Instance Connect, l'istanza deve essere gestita tramite SSM. Altrimenti, salta questi passaggi. Per ulteriori informazioni, consulta [Perché la mia EC2 istanza Amazon non viene visualizzata come nodo gestito](#).
- Il controllo della rete rileverà solo se il gruppo di sicurezza e le regole ACL di rete bloccano il traffico quando SourceIP CIDR viene fornito come parametro di input. Altrimenti, mostrerà solo le regole relative a SSH.
- Le connessioni che utilizzano [Amazon EC2 Instance Connect Endpoint](#) non sono convalidate in questo runbook.
- Per le connessioni private, l'automazione non verifica se il client SSH è installato sulla macchina di origine e se può raggiungere l'indirizzo IP privato dell'istanza.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`

- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`
- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Passa a [AWSSupport-TroubleshootEC2InstanceConnect](#) nella AWS Systems Manager console.

2. Seleziona Execute automation (Esegui automazione).

3. Per i parametri di input, inserisci quanto segue:

- `InstanceId` (Obbligatorio):

L'ID dell' EC2 istanza Amazon di destinazione a cui non sei riuscito a connetterti utilizzando Amazon EC2 Instance Connect.

- `AutomationAssumeRole` (Facoltativo):

L'ARN del ruolo IAM che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `Nome utente` (obbligatorio):

Il nome utente utilizzato per connettersi all' EC2 istanza Amazon tramite Amazon EC2 Instance Connect. Viene utilizzato per valutare se l'accesso IAM è concesso a questo particolare utente.

- `EC2InstanceConnectRoleOrUser`(Obbligatorio):

L'ARN del ruolo o dell'utente IAM che sfrutta Amazon EC2 Instance Connect per inviare le chiavi all'istanza.

- `SSHPort` (Facoltativo):

La porta SSH configurata sull' EC2 istanza Amazon. Il valore predefinito è 22. Il numero di porta deve essere compreso tra 1-65535.

- SourceNetworkType (Facoltativo):

Il metodo di accesso alla rete all' EC2 istanza Amazon:

- Browser: ti connetti dalla console AWS di gestione.
- Pubblica: ti connetti all'istanza situata in una sottorete pubblica su Internet (ad esempio, il computer locale).
- Privato: ti connetti tramite l'indirizzo IP privato dell'istanza.
- SourceNetworkType (opzionale):

Il CIDR di origine che include l'indirizzo IP del dispositivo (ad esempio il computer locale) da cui effettuerai l'accesso utilizzando Amazon EC2 Instance Connect. Esempio: 172.31.48.6/32. Se non viene fornito alcun valore con la modalità di accesso pubblico o privato, il runbook non valuterà se il gruppo di sicurezza dell' EC2 istanza Amazon e le regole ACL di rete consentono il traffico SSH. Visualizzerà invece le regole relative a SSH.

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.
☐ Show interactive instance picker

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

EC2InstanceConnectRoleOrUser
(Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role or user that is being used to leverage EC2 Instance Connect and push keys to the instance.

SourceNetworkType
(Optional) The network access method to the EC2 instance: ****Browser****: you are connecting to the EC2 instance using your browser by clicking the connect button from the console. ****Public****: you are accessing the EC2 instance located in a public subnet over the Internet (example: from your local computer). ****Private****: you are connecting to your instance through its private IP address.

Username
(Required) The username used to connect to the EC2 instance using EC2 Instance Connect. It is used to evaluate if IAM access is granted for this particular user.

SSHPort
(Optional) The SSH port configured on the EC2 instance. Default value is "22". The port number must be between "1-65535".

SourceCIDR
(Optional) The source CIDR that includes the IP address of the device you will be logging from using EC2 Instance Connect (such as your local computer). Example: 172.31.48.0/20.

4. Seleziona Esegui.

5. L'automazione si avvia.

6. Il documento esegue le seguenti operazioni:

- AssertInitialState:

Assicura che lo stato dell' EC2 istanza Amazon sia in esecuzione. In caso contrario, l'automazione termina.

- GetInstanceProperties:

Ottiene le proprietà correnti dell' EC2 istanza Amazon (PlatformDetails PublicIpAddress, VpcId, SubnetId e MetadataHttpEndpoint).

- GatherInstanceInformationFromSSM:

Ottiene lo stato del ping dell'istanza di Systems Manager e i dettagli del sistema operativo se l'istanza è gestita tramite SSM.

- CheckIfAWSRegionSupportato:

Verifica se l' EC2 istanza Amazon si trova in una AWS regione supportata da Amazon EC2 Instance Connect.

- BranchOnIfAWSRegionSupportato:

Continua l'esecuzione se la AWS regione è supportata da Amazon EC2 Instance Connect. Altrimenti, crea l'output ed esce dall'automazione.

- CheckIfInstanceAMIsSupportato:

Verifica se l'AMI associata all'istanza è supportata da Amazon EC2 Instance Connect.

- BranchOnIfInstanceAMIsSupportato:

Se l'AMI dell'istanza è supportata, esegue i controlli a livello di sistema operativo, come la raggiungibilità dei metadati e l'installazione e la configurazione del pacchetto Amazon EC2 Instance Connect. Altrimenti, verifica se i metadati HTTP sono abilitati utilizzando l' AWS API, quindi passa alla fase di controllo della rete.

- Controlla: IMDSReachability FromOs

Esegue uno script Bash sull'istanza Amazon EC2 Linux di destinazione per verificare se è in grado di raggiungere il IMDSv2.

- Controlla l'EICPackageinstallazione:

Esegue uno script Bash sull'istanza Amazon EC2 Linux di destinazione per verificare se il pacchetto Amazon EC2 Instance Connect è installato e configurato correttamente.

- Verifica SSHConfigFromOs:

Esegue uno script Bash sull'istanza Amazon EC2 Linux di destinazione per verificare se la porta SSH configurata corrisponde al parametro di input ` SSHPort `

- CheckMetadataHTTPEndpointIsEnabled:

Verifica se l'endpoint HTTP del servizio di metadati dell'istanza è abilitato.

- Controlla l'accesso EICNetwork:

Verifica se la configurazione di rete (gruppi di sicurezza, ACL di rete e regole della tabella di routing) consente la connessione all'istanza tramite Amazon EC2 Instance Connect.

- Controlla IAMRoleOrUserPermissions:

Verifica se il ruolo o l'utente IAM utilizzato per sfruttare Amazon EC2 Instance Connect ha accesso alle chiavi push per l' EC2 istanza Amazon utilizzando il nome utente fornito.

- MakeFinalOutput:

Consolida l'output di tutti i passaggi precedenti.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

Esecuzione in cui l'istanza di destinazione presenta tutti i prerequisiti richiesti:

```
▼ Outputs

MakeFinalOutput.ExecutionLogs
Starting the check of EC2 Instance Connect pre-requisites for the instance 'i-██████████'.

### Checking if the AWS region is supported by EC2 Instance Connect ###
SUCCESS: The EC2 instance is located in the AWS region 'eu-west-1' which is one of EC2 Instance Connect supported regions

### Checking if the Amazon Machine Image (AMI) associated to the EC2 instance is supported ###
SUCCESS: The instance AMI 'Ubuntu 22.04' is supported by EC2 Instance Connect

### Checking if Instance Metadata service (IMDSv2) is reachable ###
SUCCESS: Instance metadata is reachable.

### Checking if EC2 Instance Connect package is installed and configured on the instance: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-set-up.html ###
SUCCESS: 'ec2-instance-connect' package is installed
SUCCESS: 'ec2-instance-connect' is properly configured

|
### Checking SSH configuration at the OS-level ###
WARNING: If you configured a Firewall in the EC2 instance make sure that it allows SSH traffic from the source ip CIDR
INFO: SSH is configured to listen on port 22.
SUCCESS: The configured SSH port (22) matches the provided input port (22).

### Checking Network configuration requirements to access the instance through EC2 Instance Connect using 'Browser' access mode and port '22' ###
SUCCESS: The instance has a public IPv4 address.
SUCCESS: Subnet subnet-██████████ is public.
SUCCESS: SSH access is allowed by security group id 'sg-██████████'
SUCCESS: 'Inbound' NACL allows connection through EC2 instance connect, using the rule: '100'
SUCCESS: 'Outbound' NACL allows connection through EC2 instance connect, using the rule: '100'
SUCCESS: Network requirements to connect to the instance 'i-██████████' using EC2 Instance Connect are satisfied

### Checking if the required permissions are granted to the IAM identity 'arn:aws:iam:██████████:role/Admin' used to connect to the instance 'i-██████████' through EC2 Instance Connect with the username 'ubuntu' ###
SUCCESS: The IAM identity 'arn:aws:iam:██████████:role/Admin' includes the 'ec2:DescribeInstances' access permission
SUCCESS: The IAM identity 'arn:aws:iam:██████████:role/Admin' includes the 'ec2:SendSSHPublicKey' access permission
```

Esecuzione in cui l'AMI dell'istanza di destinazione non è supportato:

```
▼ Outputs

MakeFinalOutput.ExecutionLogs
Starting the check of EC2 Instance Connect pre-requisites for the instance 'i-██████████'.

### Checking if the AWS region is supported by EC2 Instance Connect ###
SUCCESS: The EC2 instance is located in the AWS region 'eu-west-1' which is one of EC2 Instance Connect supported regions

### Checking if the Amazon Machine Image (AMI) associated to the EC2 instance is supported ###
ERROR: The instance AMI 'SLES 15.5' is not supported by EC2 Instance Connect. Please make sure to use one of the AMIs listed here: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-prerequisites.html#ec2-prereqs-ami
```

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS documentazione di servizio

- [In che modo posso risolvere i problemi di connessione alla mia istanza Amazon utilizzando Amazon EC2 Instance Connect?](#)

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

Descrizione

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs il runbook di automazione viene utilizzato per rilevare errori comuni durante l'installazione degli agenti di replica AWS Application Migration Service (AWS MGN) e AWS Elastic Disaster Recovery (AWS DRS) nei server Linux per migrare i server di origine nel cloud. AWS

Come funziona?

Il runbook utilizza il AWSSupport-TroubleshootLinuxMGNDRSAgentLogs percorso Amazon Simple Storage Service (Amazon S3) in cui il log di installazione AWS MGN o AWS DRS viene caricato come parametro. `aws_replication_agent_installer.log` Quindi, esegue le seguenti attività:

- **Convalida:** verifica se il file di registro fornito è valido e che contenga almeno un'installazione dell'agente.
- **Analisi:** analizza accuratamente l'ultima installazione dell'agente nel file di registro alla ricerca di errori noti di AWS MGN o DRS. AWS
- **Rilevamento e risoluzione degli errori:** in base all'analisi, rileva ed elenca eventuali errori o problemi durante il processo di installazione dell'agente. Per ogni errore rilevato, il runbook fornisce passaggi dettagliati per aiutare a risolvere o mitigare il problema.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `s3:GetObject`
- `s3:ListBucket`

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSsupport-TroubleshootLinuxMGNDRSAgentLogs](#) a Systems Manager nella sezione Documenti.
2. Seleziona `Execute automation` (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - `AutomationAssumeRole` (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `BucketName` (Obbligatorio):

Il nome del bucket Amazon S3 in cui è archiviato il log dell'agente di replica.

- `S3` (richiesto): `ObjectKey`

La chiave dell'oggetto Amazon S3 in cui è archiviato il file di registro del programma di installazione dell'agente di replica. Esempio: se l'URI di Amazon S3 è `s3://bucket_name/path/to/file/aws_replication_agent_installer.log`, allora devi inserire `path/to/file/aws_replication_agent_installer.log`

- **ServiceName** (Obbligatorio):

Il nome del servizio per il quale è installato l'agente di replica. Valori consentiti: `AWS MGN` o `AWS DRS`

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. 	BucketName (Required) The name of the Amazon S3 bucket where the replication agent log is stored. s3bucket-name
S3ObjectKey (Required) The key of S3 object where the replication agent installer log file is stored. Example: if S3 URI is <code>s3://bucket_name/path/to/file/aws_replication_agent_installer.log` then you should provide <code>path/to/file/aws_replication_agent_installer.log` as input.</code> aws_replication_agent_installer.log </code>	ServiceName (Required) The name of the service for which the Replication agent is done: <code>**AWS MGN**</code> : AWS Application Migration Service. <code>**AWS DRS**</code> : AWS Elastic Disaster Recovery. AWS MGN

4. Seleziona Esegui.

5. L'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- **ValidateInput**

Assicura che il file di registro dell'agente di replica sia valido e accessibile utilizzando il nome e il percorso del bucket Amazon S3 forniti all'oggetto, quindi restituisce il numero di byte dell'ultima installazione dell'agente.

- **CheckReplicationAgentLogErrors**

Legge il file di registro dell'agente di replica a partire dal byte di installazione più recente e cerca gli errori noti di MGN o DRS. AWS AWS

- **MakeFinalOutput**

Crea l'output dei controlli precedenti, incluse informazioni sugli errori rilevati e consigli per la risoluzione dei problemi.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

▼ 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:

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWSSupport-TroubleshootRDP

Descrizione

Il AWSSupport-TroubleshootRDP runbook consente all'utente di controllare o modificare le impostazioni comuni sull'istanza di destinazione che possono influire sulle connessioni RDP (Remote Desktop Protocol), come la porta RDP, l'autenticazione a livello di rete (NLA) e i profili Windows Firewall. Facoltativamente, le modifiche possono essere applicate offline arrestando e avviando l'istanza, se l'utente autorizza in modo esplicito la correzione offline. Per impostazione predefinita, il runbook legge ed emette i valori delle impostazioni.

⚠ Important

Le modifiche alle impostazioni RDP, al servizio RDP e ai profili di Windows Firewall devono essere esaminate attentamente prima di utilizzare questo runbook.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- Azione

Tipo: stringa

Valori validi: CheckAll | FixAll | Personalizzato

Impostazione predefinita: Custom

Descrizione: (Facoltativo) [Personalizzato] Utilizza i valori di Firewall RDPServiceStartupType, RDPService RDP Port Action, NLASetting Action e RemoteConnections per gestire le impostazioni. [CheckAll] Leggi i valori delle impostazioni senza modificarli. [FixAll] Ripristina le impostazioni predefinite di RDP e disattiva Windows Firewall.

- AllowOffline

Tipo: stringa

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (facoltativo) solo per la correzione: impostare su True se è abilitata la correzione RDP offline e la risoluzione dei problemi online ha esito negativo oppure se l'istanza specificata non è un'istanza gestita. Nota: per la correzione offline, SSM Automation arresta l'istanza e crea un'AMI prima di provare altre operazioni.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Firewall

Tipo: stringa

Valori validi: Check | Disable

Impostazione predefinita: Check

Descrizione: (facoltativo) controlla o disabilita Windows Firewall (tutti i profili).

- InstanceId

Tipo: stringa

Descrizione: (obbligatorio) ID dell'istanza gestita per la quale risolvere i problemi relativi alle impostazioni RDP.

- NLASettingAzione

Tipo: stringa

Valori validi: Seleziona | Disabilita

Impostazione predefinita: Check

Descrizione: (facoltativo) controlla o disabilita l'autenticazione NLA (Network Layer Authentication).

- RDPPortAzione

Tipo: stringa

Valori validi: Verifica | Modifica

Impostazione predefinita: Check

Descrizione: (facoltativo) controlla la porta corrente utilizzata per le connessioni RDP oppure modifica la porta RDP reimpostandola su 3389 e riavvia il servizio.

- RDPServiceAzione

Tipo: stringa

Valori validi: Check | Start | Restart | Force-Restart

Impostazione predefinita: Check

Descrizione: (Facoltativo) Controlla, avvia, riavvia o forza il riavvio del servizio RDP (). TermService

- RDPServiceStartupType

Tipo: stringa

Valori validi: Check | Auto

Impostazione predefinita: Check

Descrizione: (facoltativo) controlla o imposta l'avvio automatico del servizio RDP all'avvio di Windows.

- RemoteConnections

Tipo: stringa

Valori validi: Verifica | Abilita

Impostazione predefinita: Check

Descrizione: (Facoltativo) Un'azione da eseguire sull'TSConnectionsimpostazione fDeny: Check, Enable.

- S3 BucketName

Tipo: stringa

Descrizione: (facoltativo) solo offline: nome del bucket S3 nell'account in cui si desidera caricare i log della risoluzione dei problemi. Verificare che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie alle parti che non necessitano dell'accesso ai log raccolti.

- SubnetId

Tipo: stringa

Predefinito: SelectedInstanceSubnet

Descrizione: (Facoltativo) Solo offline: l'ID di sottorete per l'istanza EC2 Rescue utilizzata per eseguire la risoluzione dei problemi offline. Se non viene specificato alcun ID di sottorete, AWS Systems Manager Automation creerà un nuovo VPC. **IMPORTANTE:** la sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia che l' EC2 istanza che riceve il comando abbia un ruolo IAM con la policy gestita di `SSMManagedInstanceCoreAmazon` Amazon allegata. Per la riparazione online, l'utente deve disporre almeno di `ssm:DescribeInstanceInformation`, `ssm:StartAutomationExecution` e `ssm:SendCommand` per eseguire l'automazione e inviare il comando all'istanza, più `ssm:GetAutomationExecution` per poter leggere l'output dell'automazione. Per la riparazione offline, l'utente deve disporre almeno di `ssm:`, `ssm:DescribeInstanceInformation`, `ec2:DescribeInstances`, più `ssm:StartAutomationExecution` per poter leggere l'output dell'automazione. `GetAutomationExecution` `AWSSupport-TroubleshootRDP` chiamate `AWSSupport-ExecuteEC2Rescue` per eseguire la riparazione offline: controlla le autorizzazioni per assicurarti di `AWSSupport-ExecuteEC2Rescue` poter eseguire l'automazione con successo.

Fasi del documento

1. `aws:assertAwsResourceProperty`- Controlla se l'istanza è una Windows Server istanza
2. `aws:assertAwsResourceProperty`- Controlla se l'istanza è un'istanza gestita
3. (Risoluzione dei problemi online) Se l'istanza è un'istanza gestita:
 - a. `aws:assertAwsResourceProperty`- Controlla il valore Action fornito
 - b. (Controllo online) Se l'azione = `CheckAll`, allora:

`aws:runPowerShellScript`- Esegue lo PowerShell script per ottenere lo stato dei profili di Windows Firewall.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageWindowsService` per ottenere lo stato del servizio RDP.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageRDPSettings` per ottenere le impostazioni RDP.

c. (Correzione online) Se l'azione = `FixAll`, allora:

`aws:runPowerShellScript`- Esegue lo PowerShell script per disabilitare tutti i profili di Windows Firewall.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageWindowsService` per avviare il servizio RDP.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageRDPSettings` per abilitare le connessioni remote e disabilitare NLA.

d. (Gestione online) Se `Action` = `Custom`:

`aws:runPowerShellScript`- Esegue lo PowerShell script per gestire i profili di Windows Firewall.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageWindowsService` per gestire il servizio RDP.

`aws:executeAutomation`- Chiamate `AWSSupport-ManageRDPSettings` per gestire le impostazioni RDP.

4. (Correzione offline) Se l'istanza non è un'istanza gestita:

a. `aws:assertAwsResourceProperty`- `Assert` = `true AllowOffline`

b. `aws:assertAwsResourceProperty`- Azione assertiva = `FixAll`

c. `aws:assertAwsResourceProperty`- Afferma il valore di `SubnetId`

(Usa la sottorete dell'istanza fornita) If `SubnetId` è `SELECTED_INSTANCE_SUBNET`

`aws:executeAwsApi`- Recupera la sottorete dell'istanza corrente.

`aws:executeAutomation-` Esegui `AWSSupport-ExecuteEC2Rescue` con la sottorete dell'istanza fornita.

d. (Usa la sottorete personalizzata fornita) Se non `SubnetId` è `SELECTED_INSTANCE_SUBNET`

`aws:executeAutomation-` `SubnetId` Esegui con il valore fornito. `AWSSupport-ExecuteEC2Rescue`

Output

`manageFirewallProfiles.Uscita`

`gestire Settings.Output RDPService`

`RDPSettingsgestisci .Output`

`checkFirewallProfiles.Output`

`controlla Impostazioni.Output RDPService`

`seleziona RDPSettings .Output`

`disableFirewallProfiles.Uscita`

Ripristina `RDPService` le impostazioni predefinite. `Output`

Ripristina l'`RDPSettingsoutput` predefinito

risolvere i problemi di `RDPOffline .Output`

risolvere i problemi di `RDPOffline WithSubnetId .Output`

AWSSupport-TroubleshootSSH

Descrizione

Il `AWSSupport-TroubleshootSSH` runbook installa lo strumento Amazon EC2 Rescue per Linux, quindi utilizza lo strumento EC2 Rescue per verificare o tentare di risolvere problemi comuni che impediscono una connessione remota alla macchina Linux tramite SSH. Facoltativamente, le modifiche possono essere applicate offline arrestando e avviando l'istanza, se l'utente autorizza in modo esplicito la correzione offline. Per impostazione predefinita, il runbook funziona in modalità di sola lettura.

[Esegui questa automazione \(console\)](#)

Per informazioni sull'utilizzo del `AWSSupport-TroubleshootSSH` runbook, consulta questo [argomento `AWSSupport-TroubleshootSSH` sulla risoluzione dei problemi](#) di AWS Premium Support.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- Azione

Tipo: stringa

Valori validi: CheckAll | FixAll

Predefinito: CheckAll

Descrizione: (obbligatorio) specifica se individuare la presenza di problemi senza risolverli oppure se individuare e risolvere automaticamente i problemi rilevati.

- AllowOffline

Tipo: stringa

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (facoltativo) solo per la correzione: impostare su True se è abilitata la correzione SSH offline e la risoluzione dei problemi online ha esito negativo oppure se l'istanza specificata non è un'istanza gestita. Nota: per la correzione offline, SSM Automation arresta l'istanza e crea un'AMI prima di provare altre operazioni.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) ID dell' EC2 istanza per Linux.

- S3 BucketName

Tipo: stringa

Descrizione: (facoltativo) solo offline: nome del bucket S3 nell'account in cui si desidera caricare i log della risoluzione dei problemi. Verificare che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie alle parti che non necessitano dell'accesso ai log raccolti.

- SubnetId

Tipo: stringa

Predefinito: SelectedInstanceSubnet

Descrizione: (Facoltativo) Solo offline: l'ID di sottorete per l'istanza EC2 Rescue utilizzata per eseguire la risoluzione dei problemi offline. Se non viene specificato alcun ID di sottorete, AWS Systems Manager Automation creerà un nuovo VPC.

 Important

La sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia che l' EC2 istanza che riceve il comando abbia un ruolo IAM con la policy gestita di `SSMManagedInstanceCoreAmazon` Amazon allegata. Per la riparazione online, l'utente deve disporre almeno di `ssm:DescribeInstanceInformation`, `ssm:StartAutomationExecution` e `ssm:SendCommand` per eseguire l'automazione e inviare il comando all'istanza, più `ssm:GetAutomationExecution` per poter leggere l'output dell'automazione. Per la riparazione offline, l'utente deve disporre almeno di `ssm:`, `ssm:DescribeInstanceInformation`, `ec2:DescribeInstances`, più `ssm:StartAutomationExecution` per poter leggere l'output dell'automazione. `GetAutomationExecution` `AWSSupport-TroubleshootSSH` chiamate `AWSSupport-ExecuteEC2Rescue` per eseguire la riparazione offline: controlla le autorizzazioni per assicurarti di `AWSSupport-ExecuteEC2Rescue` poter eseguire l'automazione con successo.

Fasi del documento

1. `aws:assertAwsResourceProperty`- Controlla se l'istanza è un'istanza gestita
 - a. (Correzione online) Se l'istanza è un'istanza gestita:
 - i. `aws:configurePackage`- Installa EC2 Rescue per Linux tramite `AWS-ConfigureAWSPackage`.
 - ii. `aws:runCommand`- Esegui lo script bash per eseguire EC2 Rescue for Linux.
 - b. (Correzione offline) Se l'istanza non è un'istanza gestita:
 - i. `aws:assertAwsResourceProperty`- Assert = true AllowOffline
 - ii. `aws:assertAwsResourceProperty`- Azione assertiva = FixAll
 - iii. `aws:assertAwsResourceProperty`- Afferma il valore di SubnetId
 - iv. (Usa la sottorete dell'istanza fornita) Se dobbiamo `aws:executeAutomation` eseguire `AWSSupport-ExecuteEC2Rescue` con SubnetId la SelectedInstanceSubnet sottorete dell'istanza fornita.
 - v. (Usa la sottorete personalizzata fornita) If non SubnetId viene SelectedInstanceSubnet utilizzato `aws:executeAutomation` per eseguire `AWSSupport-ExecuteEC2Rescue` con il valore fornito. SubnetId

Output

`troubleshootSSH.Output`

risolvi i problemi SSHOffline di `.Output`

risolvere i problemi di SSHOffline WithSubnetId `.Output`

AWSSupport-TroubleshootSUSERegistration

Descrizione

Il `AWSSupport-TroubleshootSUSERegistration` runbook ti aiuta a capire perché registrare un Amazon Elastic Compute Cloud (Amazon) EC2 SUSE Linux Enterprise Server istanza con SUSE Update Infrastructure non riuscita. L'output di automazione fornisce i passaggi per risolvere o aiuta a risolvere il problema. Se l'istanza supera tutti i controlli durante l'automazione, viene registrata con SUSE Update Infrastructure.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon che desideri risolvere.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:ListCommands`

Fasi del documento

- `aws:assertAwsResourceProperty`- Verifica se l' EC2 istanza Amazon è gestita da AWS Systems Manager.
- `aws:runCommand`- Verifica se la piattaforma di EC2 istanze Amazon è SLES.
- `aws:runCommand`- Verifica se la `cloud-regionsrv-client` versione del pacchetto è superiore o uguale alla versione richiesta 9.0.10.
- `aws:runCommand`- Verifica se il collegamento simbolico per il prodotto di base è interrotto e corregge il collegamento in caso di interruzione.
- `aws:runCommand`- Verifica se il file `hosts (/etc/hosts)` contiene record per. `smt-ec2-suscloud.net` L'automazione rimuove tutte le voci duplicate.
- `aws:runCommand`- Verifica se il `curl` comando è installato.
- `aws:runCommand`- Verifica se l' EC2 istanza Amazon può accedere all'indirizzo IMDS (Instance Metadata Service) 169.254.169.254.
- `aws:runCommand`- Verifica se l' EC2 istanza Amazon ha un codice di fatturazione o un codice Marketplace AWS prodotto.
- `aws:runCommand`- Verifica se l' EC2 istanza Amazon può raggiungere almeno 1 server regionale tramite HTTPS.
- `aws:runCommand`- Verifica se l' EC2 istanza Amazon può raggiungere i server SMT (Subscription Management Tool) tramite HTTP.
- `aws:runCommand`- Verifica se l' EC2 istanza Amazon può raggiungere i server SMT (Subscription Management Tool) tramite HTTPS.

- `aws:runCommand`- Verifica se l' EC2 istanza Amazon può raggiungere l'`smt-ec2.susecloud.net` indirizzo tramite HTTPS.
- `aws:runCommand`- Registra l' EC2 istanza Amazon con SUSE Update Infrastructure.
- `aws:executeScript`- Raccoglie e restituisce l'output di tutti i passaggi precedenti.

AWSSupport-TroubleshootWindowsPerformance

Descrizione

Il runbook `AWSSupport-TroubleshootWindowsPerformance` aiuta a risolvere i problemi di prestazioni in corso sull'istanza Windows di Amazon Elastic Compute Cloud (Amazon EC2). Il runbook acquisisce i log dall'istanza di destinazione e analizza i parametri prestazionali di CPU, memoria, disco e rete. Facoltativamente, l'automazione può acquisire un dump del processo per aiutarti a determinare la potenziale causa del peggioramento delle prestazioni. L'automazione acquisisce anche i registri degli eventi e del sistema utilizzando [EC2Rescue](#) lo strumento più recente, se consenti a questo runbook di installarlo.

Come funziona?

Il runbook esegue i seguenti passaggi:

- Verifica i prerequisiti dell' EC2 istanza Amazon.
- Genera log delle prestazioni nel disco principale dell'istanza Amazon EC2 Windows
- Memorizza i log acquisiti nella cartella `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Se viene fornito un bucket Amazon Simple Storage Service (Amazon S3) e il ruolo di automazione assume le autorizzazioni necessarie, i log acquisiti vengono caricati nel bucket Amazon S3.
- Installa `EC2Rescue` lo strumento più recente sull'istanza di Amazon EC2 Windows per acquisire eventi e log di sistema se scegli di installarlo, ma non analizza il dump del processo e i log acquisiti da `EC2Rescue`

Important

- Per eseguire questo runbook, l'istanza Amazon EC2 Windows deve essere gestita da AWS Systems Manager. Per ulteriori informazioni, consulta [Perché la mia EC2 istanza Amazon non viene visualizzata come nodo gestito](#).

- Per eseguire questo runbook, l'istanza Amazon EC2 Windows deve essere in esecuzione su versioni Windows 8.1 /Windows Server 2012 R2 (6.3) o successive con PowerShell 4.0 o versioni successive. Per ulteriori informazioni, consulta la versione del [sistema operativo Windows](#).
- Per la generazione di registri delle prestazioni, sono necessari almeno 10 GB di spazio libero sul dispositivo root. Se il disco principale è più grande di 100 GB, lo spazio libero deve essere superiore al 10% della dimensione del disco. Se si esegue il dump di un processo durante l'esecuzione, lo spazio libero deve essere superiore a 10 GB più la dimensione totale della memoria consumata dal processo quando il processo consuma più di 10 GB di memoria.
- I log generati sul dispositivo root non vengono eliminati automaticamente.
- Il runbook non disinstalla lo EC2Rescue strumento. Per ulteriori informazioni, consulta [Use EC2Rescue for Windows Server](#).
- È consigliabile eseguire questa automazione durante un impatto sulle prestazioni. È inoltre possibile eseguirla periodicamente utilizzando un'associazione AWS Systems Manager State Manager o pianificando AWS Systems Manager Maintenance Windows.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

(Facoltativo) Il ruolo IAM collegato al profilo dell'istanza o l'utente IAM configurato sull'istanza richiede le seguenti azioni per caricare i log nel bucket Amazon S3 specificato per il parametro: *LogUploadBucketName*

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-TroubleshootWindowsPerformance](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - `AutomationAssumeRole` (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene

specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- **InstanceId (Obbligatorio):**

L'ID dell'istanza Amazon EC2 Windows di destinazione in cui desideri eseguire l'automazione. L'istanza deve essere gestita da Systems Manager per eseguire l'automazione.

- **CaptureProcessDump (Facoltativo):**

Il tipo di dump del processo da acquisire. L'automazione può acquisire un dump del processo che potenzialmente causa l'impatto sulle prestazioni all'inizio dell'automazione. Il volume root dell'istanza richiede almeno 10 GB di spazio libero (più del 10% della dimensione del disco quando la dimensione del volume principale è superiore a 100 GB e 10 GB più la dimensione totale della memoria consumata dal processo quando il processo consuma più di 10 GB di memoria).

- **LogCaptureDuration (Facoltativo):**

Il numero di minuti, tra 1 e 15, durante i quali questa automazione acquisirà i registri mentre il problema è presente. Il valore predefinito è 5.

- **LogUploadBucketName (Facoltativo):**

Il bucket Amazon S3 nel tuo account in cui desideri caricare i log. Il bucket deve essere configurato con la crittografia lato server (SSE) e la policy del bucket non deve concedere autorizzazioni di lettura/scrittura non necessarie a parti che non hanno bisogno di accedere ai log acquisiti. L'istanza Amazon EC2 Windows deve avere accesso al bucket Amazon S3.

- **Installazione EC2 RescueTool (opzionale):**

Impostato per consentire Yes al runbook di installare la versione più recente EC2Rescue dello strumento per acquisire gli eventi di Windows e i registri di sistema. Il valore predefinito è No.

- **Riconoscimento (obbligatorio):**

Leggi i dettagli completi delle azioni eseguite da questo runbook di automazione e, se sei d'accordo, digita. Yes, I understand and acknowledge

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 Windows instance you want to troubleshoot performance issues.

☒ Show interactive instance picker

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

LogCaptureDuration
(Optional) The number of minutes this automation should capture logs while the issue is present. Default is '5' minutes. You can specify a value between '1' and up to '15' minutes.

InstallEC2RescueTool
(Optional) Set it to 'True' if you allow the runbook to install the latest version of the 'EC2Rescue' tool to capture the Windows Events and System logs. Default value 'No'.

CaptureProcessDump
(Optional) The process dump type to capture. The automation can capture one process dump for the process which is potentially causing the performance impact in the beginning of the automation. The instance root volume will require to have at least 10 GB free space (greater than 10% of the disk size when the root volume size is bigger than 100 GB and 10GB plus the total memory size consumed by the process when the process consumes more than 10GB memory).

LogUploadBucketName
(Optional) The Amazon S3 bucket in your account to upload the logs to. Please make sure the bucket is configured with server-side encryption (SSE), and the bucket policy does not grant unnecessary read/write permissions to parties that do not need to access the logs. Also please make sure EC2 Windows instance has necessary access to the S3 Bucket.

Acknowledgement
(Required) Please read the complete details of the actions performed by this automation runbook and write 'Yes, I understand and acknowledge' if you acknowledge the steps.

4. Seleziona Esegui.

5. L'automazione si avvia.

6. Il documento esegue le seguenti operazioni:

- **CheckConcurrency:**

Assicura che esista una sola esecuzione di questo runbook destinata all'istanza. Se il runbook trova un'altra esecuzione destinata alla stessa istanza, restituisce un errore e termina.

- **AssertInstanceIsWindows:**

Afferma che l' EC2 istanza Amazon è in esecuzione sul sistema operativo Windows. Altrimenti, l'automazione termina.

- **AssertInstanceIsManagedInstance:**

Afferma che l' EC2 istanza Amazon è gestita da AWS Systems Manager. Altrimenti l'automazione termina.

- **VerifyPrerequisites:**

Verifica la PowerShell versione sul sistema operativo dell'istanza e assicura che l'istanza possa essere connessa tramite Systems Manager per eseguire PowerShell i comandi. Questa automazione supporta la PowerShell versione 4.0 e successive in esecuzione su versioni Windows 8.1 /Server 2012 R2 (6.3) o successive. Se la versione è precedente, l'automazione fallisce. Quando scegli di caricare i log nel bucket Amazon S3, questa automazione verifica che AWS il modulo Tools PowerShell for sia disponibile. In caso contrario, l'automazione termina.

- **BranchOnProcessDump:**

Le filiali si basano su se è stata impostata per acquisire il dump dei processi che hanno influito sulle prestazioni.

- **CaptureProcessDump:**

Verifica se l'istanza ha spazio sufficiente per eseguire questa automazione (quando scegli Highest CPU/Memoria).

- **CapturePerformanceLogs:**

Controlla nuovamente lo spazio su disco ed esegue lo PowerShell script sull'istanza per creare contatori perfmon e avviare la registrazione di Performance Monitor e Windows Performance Recorder. Lo script si interrompe dopo il raggiungimento del valore definito. LogCaptureDuration

- **SummarizePerformanceLogs:**

Riepiloga il rapporto XML generato nel passaggio precedente CapturePerformanceLogs, per individuare il processo responsabile che consuma più WorkingSet 64 (memoria) e % di tempo del processore (CPU) indicati come output dell'automazione. Genera informazioni simili per l'utilizzo di Interfaccia di rete LogicalDisk TCPv4 IPv4, Memoria UDPv4 e le salva analysis_output.log nella cartella di output.

- **BranchOnInstallEC2Rescue:**

Branches se lo imposti per installare lo EC2Rescue strumento più recente nell' EC2 istanza Amazon.

- **InstallEC2RescueTool:**

Installa lo EC2Rescue strumento nel sistema operativo dell'istanza per acquisire EC2Rescue i log utilizzando. AWS-ConfigureAWSPackage

- **RunEC2RescueTool:**

Esegue lo EC2Rescue strumento nel sistema operativo dell'istanza per acquisire tutti i log necessari. EC2Rescueacquisisce solo i log necessari per risparmiare spazio.

- **BranchOnIfS3BucketProvided:**

I rami si basano sull'input dell'utente LogUploadBucketName per verificare se è disponibile un nome di bucket per caricare i log.

- **GetS3BucketPublicStatus:**

Determina se viene fornito un bucket Amazon S3 e, in tal caso, conferma che il bucket Amazon S3 non è pubblico ed è configurato con SSE.

- **UploadLogResult:**

Carica i log nel bucket Amazon S3 fornito. Se la PowerShell versione è 5.0 o successiva, comprime i log in un archivio ZIP e li carica. Elimina il file ZIP al termine del caricamento. Se la PowerShell versione è inferiore alla 5.0, carica i file direttamente in una cartella.

- **CleanUpLogsOnFailure:**

Pulisce tutti i log generati dal CapturePerformanceLogs passaggio in caso di errore. Il CleanUpLogsOnFailure passaggio potrebbe non riuscire o scadere se SSM Agent non funziona correttamente o il sistema Windows non risponde.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

Esecuzione in cui l'istanza di destinazione presenta tutti i prerequisiti richiesti.

▼ Outputs

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

CapturePerformanceLogs.Output

The instance has enough space to capture performance logs.

WPR capture process is in 'Stopped' state.

Data Collector Set TroubleshootWindowsPerformance_... was not found.

Attempting to create Performance monitor Data Collector Set TroubleshootWindowsPerformance_... created successfully.

Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance_... started successfully.

Data Collector Set TroubleshootWindowsPerformance_... started successfully.

Current CPU usage is '54.73%' and Memory usage is '17.15%'

Not both CPU and Memory usage are over 95% at this moment hence continue to capture WPR log.

Starting Windows Performance Recording (WPR) capture process.

Stopping WPR capture process.

WPR capture process is in 'Stopped' state.

The Data Collector Set TroubleshootWindowsPerformance_... is currently generating logs.

The Data Collector Set TroubleshootWindowsPerformance_... has finished generating logs and is currently in 'Stopped' state.

Attempting to delete Data Collector Set TroubleshootWindowsPerformance_... deleted successfully.

Data Collector Set TroubleshootWindowsPerformance_... deleted successfully.

[PASSED] Performance logs are captured successfully inside the folder: C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\...

The captured log files will not be deleted by this automation, please manually delete it after analysis.

RunEC2RescueTool.Output

[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\..._EC2Rescue_23-05-48.zip'. The latest EC2Rescue tool is installed by this automation and please manually remove it if you don't need it. Its installed path is C:\Program Files\Amazon\EC2Rescue\EC2RescueCmd.exe.

SummarizePerformanceLogs.Output

Top 5 Processes which consumed most CPU in percentage as below. If you see a percentage higher than 100 that means the process is using more than one CPU core.

Process	Counter	Min %	Max %	Avg %
spsvc	Processor	0.00	106.00	9.00
WinPrvSE#2	Processor	0.00	90.00	2.00
MsMpEng	Processor	0.00	38.00	0.75
GenVulObj	Processor	0.00	30.00	0.28
svchost#42	Processor	0.00	29.00	0.17

Top 5 Processes which consumed most WorkingSet64 memory as below (in MB):

Process	Counter	Min MB	Max MB	Avg MB
MsMpEng	WorkingSet	220.00	260.00	236.00
Registry	WorkingSet	78.00	193.00	120.00
powershell	WorkingSet	90.00	92.00	92.00
LogonUI	WorkingSet	43.00	43.00	43.00
dwm	WorkingSet	38.00	38.00	38.00

Esecuzione in cui l'istanza di destinazione si trova sulla piattaforma Linux e l'esecuzione non è riuscita. È necessario selezionare l'ID del passaggio per visualizzare i dettagli dell'errore.

▼ Outputs

CapturePerformanceLogs.Output
No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output
No output available yet because the step is not successfully executed

SummarizePerformanceLogs.Output
No output available yet because the step is not successfully executed

VerifyPrerequisites.Output
No output available yet because the step is not successfully executed

CaptureProcessDump.Output
No output available yet because the step is not successfully executed

RunEC2RescueTool.Output
No output available yet because the step is not successfully executed

UploadLogResult.Output
No output available yet because the step is not successfully executed

Execution status

Overall status
❌ Failed

Failed
1

All executed steps
2

Cancelled
0

Succeeded
1

TimedOut
0

Executed steps (2)

Find Steps

< 1 >

Step ID	Step #	Step name	Action	Status	Start time	End time
	1	CheckConcurrency	aws:executeScript	✔ Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT
	2	AssertInstanceIsWindows	aws:assertAwsResourceProperty	❌ Failed	Tue, 19 Mar 2024 16:15:00 GMT	Tue, 19 Mar 2024 16:15:01 GMT

I dettagli dell'errore della faseAssertInstanceIsWindows.

Failure details

❌ Failure message
Step fails when it is Execute/Canceling action. Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows'].. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

FailureType
Verification

FailureStage
Invocation

VerificationErrorMessage
Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows'].

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWSSupport-TroubleshootWindowsUpdate

Descrizione

Il `AWSSupport-TroubleshootWindowsUpdate` runbook viene utilizzato per identificare problemi che potrebbero fallire negli aggiornamenti di Windows per le istanze Windows di Amazon Elastic Compute Cloud EC2 (Amazon).

Come funziona?

Il runbook esegue i seguenti passaggi:

- Verifica se l' EC2 istanza Amazon di destinazione è gestita da AWS Systems Manager.
- Verifica se le versioni AWS Systems Manager Agent (SSM Agent) e Windows Server sono supportate per le operazioni di patching di Systems Manager.
- Verifica lo spazio disponibile su disco consigliato per gli aggiornamenti di Windows e se è in sospeso un riavvio. Un riavvio in sospeso indica in genere che gli aggiornamenti sono in sospeso ed è necessario un riavvio prima di eseguire aggiornamenti aggiuntivi.
- Configura le impostazioni del proxy a livello di sistema operativo, il che può aiutare a risolvere i problemi di connettività.
- Esegue un test di connettività degli endpoint Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e richiama [GetDeployablePatchSnapshotForInstance](#) l'operazione API per recuperare lo snapshot corrente per la patch baseline utilizzata dal nodo gestito.
- Se la connessione fallisce, offre la possibilità di eseguire il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook per analizzare la connettività dell'istanza agli endpoint Amazon S3.
- Convalida la configurazione degli aggiornamenti di Windows e verifica Windows Server Update Services (WSUS) (se applicabile).

 Important

- I controller di dominio Active Directory non sono supportati.
- La versione 2008 R2 di Windows Server o le versioni precedenti non sono supportate.
- SSM Agent 1.2.371 o versioni precedenti non sono supportate.
- Il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook viene utilizzato [VPC Reachability Analyzer](#) per analizzare la connettività di rete tra un endpoint di origine e un endpoint di servizio. Ti viene addebitato un costo per ogni analisi eseguita tra

un'origine e una destinazione. Per ulteriori dettagli, consulta la pagina dei prezzi di [Amazon VPC](#).

- Il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook non è disponibile in tutte le regioni in cui è supportato Systems Manager.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

Note

[Per eseguire il runbook secondario `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`, aggiungete le autorizzazioni elencate in questo documento.](#)

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-TroubleshootWindowsUpdate](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId (Obbligatorio):

Inserisci l'ID dell' EC2 istanza Amazon in cui l'aggiornamento di Windows non è riuscito.

- RunVpcReachabilityAnalyzer(Facoltativo):

Specificate di `true` eseguire l'`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` automazione se un problema di rete è determinato dai controlli estesi o se l'ID di istanza specificato non è un'istanza gestita. Per ulteriori informazioni su questa automazione secondaria, consulta la [documentazione](#). Il valore predefinito è `false`.

- RetainVpcReachabilityAnalysis(Facoltativo):

Rilevante solo se lo `RunVpcReachabilityAnalyzer` è `true`. `true` Specificare di conservare il percorso di analisi della rete e le relative analisi create da `Reachability Analyzer`. Per impostazione predefinita, tali risorse vengono eliminate dopo un'analisi riuscita. Se scegli di conservare l'analisi, il runbook secondario non elimina l'analisi e puoi visualizzarla nella console Amazon VPC. Il collegamento alla console sarà disponibile nell'output di automazione secondaria. Il valore predefinito è `false`.

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 instance.

☒ Show interactive instance picker

AWS::EC2::Instance::Id

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

RunVpcReachabilityAnalyzer
(Optional) Specify 'true' to run the 'AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2' automation if a network issue is determined by the extended checks, or if the instance ID specified is not a managed instance. For more information on this child automation, please refer to the documentation above. This parameter defaults to 'false'.

false

RetainVpcReachabilityAnalysis
(Optional) Only relevant if 'RunVpcReachabilityAnalyzer' is true. Specify 'true' to retain the network insight path and related analyses created by VPC Reachability Analyzer. By default, those resources are deleted after successful analysis. If you choose to retain the analysis, the child runbook does not delete the analysis and you can visualize it in the VPC console. The console link will be available in the child automation output. This parameter defaults to 'false'.

false

4. Seleziona Esegui.

5. L'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- **getWindowsServerAndSSMAgentVersion:**

Verifica che l'istanza di destinazione sia gestita da AWS Systems Manager e ottiene dettagli sulla versione di SSM Agent e sulla versione Windows.

- **assertIfInstanceIsSsmManaged:**

Assicura che l' EC2 istanza Amazon sia gestita da AWS Systems Manager (SSM), altrimenti l'automazione termina.

- **CheckProxy:**

Verifica la presenza di tutti i tipi di proxy per l'istanza Windows.

- **CheckPrerequisites:**

Ottiene la versione dell'agente SSM e la versione di Windows e determina se si tratta di un controller di dominio Active Directory (DC). Se l'istanza è un DC o la versione SSM Agent o Windows non è supportata, il runbook si interrompe.

- **CheckDiskSpace:**

Recupera e convalida lo spazio su disco disponibile sull'istanza di Windows se è sufficiente per eseguire l'aggiornamento di Windows.

- **CheckPendingReboot:**

Verifica la presenza di eventuali riavvii in sospeso sull'istanza di Windows.

- **CheckS3Connectivity:**

Verifica se l'istanza può raggiungere gli endpoint Amazon S3 per. Patchbaseline

- **branchOnRunVpcReachabilityAnalyzer:**

Se RunVpcReachabilityAnalyzer è vero, allora ramifica l'automazione per eseguire un'analisi più approfondita per il debug della connettività Amazon S3.

- **GenerateEndpoints:**

Genera un endpoint per un controllo esteso della connettività per l'endpoint Amazon S3.

- **analyzeAwsEndpointReachabilityFromEC2:**

Richiama il runbook di automazione,AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2. per verificare la raggiungibilità dell'istanza selezionata verso gli endpoint richiesti.

- **CheckWindowsUpdateServices:**

Verifica lo stato del servizio Windows Update e il tipo di avvio.

- **CheckWindowsUpdateSettings:**

Verifica i criteri di Windows Update configurati sull'istanza di Windows.

- **CheckWSUSSettings:**

Verifica se l'aggiornamento di Windows è configurato con WSUS o Microsoft Update Catalog e verifica la connettività.

- **CheckWUGlobalSettings:**

Verifica le impostazioni globali di Windows Update configurate sull'istanza di Windows.

- **GenerateLogs:**

Scarica i registri di Windows Update e i registri CBS sul desktop dell'istanza e verifica che i registri degli eventi di Windows non presentino errori.

- **FinalReport:**

Genera un report completo di tutti i passaggi.

```

FinalReport.Results
"
=====Prerequisites Check=====
Result: [PASSED]
INFO: The target instance is not an Active Directory Domain Controller.
INFO: The platform 10.0.20348 is supported.
INFO: The SSM Agent version 3.2.1705.0 is supported.

=====Disk Space Check=====
Result: [PASSED]
INFO: Disk space on drive C: is recommended to run Windows updates.

=====Pending Reboot Check=====
Result: [PASSED]
INFO: There is no pending reboot.

=====Amazon S3 Connectivity Check=====
Result: [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

=====AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2=====
Result: [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

=====Windows Update Services Status=====
Result: [PASSED]
Getting Services Status and types for Windows Update...
The service 'Application Identity' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Application Identity'
Service 'Application Identity' started successfully
The service 'Background Intelligent Transfer Service' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Background Intelligent Transfer Service'
Service 'Background Intelligent Transfer Service' started successfully
INFO: The service 'Cryptographic Services' status is currently 'Running'
The service 'Windows Installer' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Windows Installer'
Service 'Windows Installer' started successfully
INFO: The service 'Windows Modules Installer' status is currently 'Running'
INFO: The service 'Windows Update' status is currently 'Running'

=====Windows Proxy Settings=====
Result: [PASSED]
No WinInet Proxy is set on the system
No Winhttp Proxy is set on the system
There is no proxy setting for SSM Agent
System Wide Environment HTTP Proxy is not set.
System Wide Environment HTTPS Proxy is not set.
System Wide Environment NO PROXY is not set.
There is no HTTP Proxy configured at local system account user environment.

=====Windows Update Settings=====
Result: [PASSED]
INFO: Windows Update (Policies): Never check for updates
INFO: To modify this setting is in Computer Configuration\Administrative Template\Windows Component\Windows
Update\Configure Automatic Updates. For more details please check this document: https://learn.microsoft.com/de-
de/security-updates/windowsupdateservices/18127451

=====Windows Update Global Settings=====
Result: [PASSED]
Windows Update Client has no restrictions

=====Copy of Windows Update and CBS logs=====
Result: [PASSED]
No errors found in Microsoft-Windows-WindowsUpdateClient events.
INFO: Logs copied to the C:\Windows\TEMP\c176a507-d074-4402-8a5b-631dd643f33a folder
"

```

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)

- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

Documentazione relativa al servizio AWS

- Per ulteriori informazioni, consulta l'articolo [Troubleshoot Windows Update](#).

AWSSupport-UpgradeWindowsAWSDrivers

Descrizione

Il AWSSupport-UpgradeWindowsAWSDrivers runbook aggiorna o ripara i AWS driver di archiviazione e di rete sull'istanza specificata. EC2 Il runbook tenta di installare le versioni più recenti dei AWS driver online chiamando SSM Agent. Se SSM Agent non è contattabile, il runbook può eseguire un'installazione offline dei driver se richiesto esplicitamente. AWS

Questo runbook supporta i seguenti sistemi operativi:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Note

Sia l'aggiornamento online che quello offline creeranno un'AMI prima di tentare qualsiasi operazione, che persisterà dopo il completamento dell'automazione. È responsabilità dell'utente proteggere l'accesso all'AMI oppure eliminarla. Il metodo online riavvia l'istanza come parte del processo di aggiornamento, mentre il metodo offline richiede l'arresto e l'avvio dell' EC2 istanza fornita.

Important

Se le istanze si connettono AWS Systems Manager tramite endpoint VPC, questo runbook fallirà a meno che non venga utilizzato nella regione us-east-1. Questo runbook fallirà anche

su un controller di dominio. Per aggiornare i driver AWS PV su un controller di dominio, vedere [Aggiornamento di un controller di dominio \(aggiornamento AWS PV\)](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AllowOffline

Tipo: stringa

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (facoltativo) impostare su True se si autorizza l'aggiornamento offline dei driver nel caso in cui risulti impossibile eseguire l'installazione online. Nota: il metodo offline richiede che l'EC2 istanza fornita venga interrotta e quindi avviata. I dati archiviati nei volumi dell'instance store andranno persi. L'indirizzo IP pubblico verrà modificato se non si utilizza un IP elastico.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ForceUpgrade

Tipo: stringa

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (facoltativo) solo offline: impostare su True se si autorizza il proseguimento dell'aggiornamento offline dei driver anche se nell'istanza corrente sono già stati installati i driver più recenti.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) ID dell'istanza per EC2 Windows Server.

- SubnetId

Tipo: stringa

Predefinito: SelectedInstanceSubnet

Descrizione: (Facoltativo) Solo offline: l'ID di sottorete per l'istanza EC2 Rescue utilizzata per eseguire l'aggiornamento dei driver offline. Se non viene specificato alcun ID di sottorete, Systems Manager Automation creerà un nuovo VPC.

 Important

La sottorete deve trovarsi nella stessa InstanceId zona di disponibilità e deve consentire l'accesso agli endpoint SSM.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

L' EC2 istanza che riceve il comando deve avere almeno un ruolo IAM che includa le autorizzazioni per `ssm: StartAutomationExecution` e `ssm: SendCommand` eseguire l'automazione e inviare il comando all'istanza, più `ssm: GetAutomationExecution` per poter leggere l'output dell'automazione. Puoi allegare la politica gestita `AmazonSSMManagedInstanceCore` Amazon al tuo ruolo

IAM per fornire queste autorizzazioni. È tuttavia consigliabile utilizzare il ruolo IAM Automation AmazonSSMAutomationRole per questo scopo. Per ulteriori informazioni, consulta [Utilizzare IAM per configurare i ruoli per l'automazione](#).

Se si sta eseguendo un aggiornamento offline, controlla le autorizzazioni richieste da [AWSSupport-StartEC2RescueWorkflow](#).

Fasi del documento

1. `aws:assertAwsResourceProperty`- Verifica che l'istanza di input sia Windows.
2. `aws:assertAwsResourceProperty`- Verifica che l'istanza di input sia un'istanza gestita. In questo caso, viene avviato l'aggiornamento online. In caso contrario, viene valutato l'aggiornamento offline.
 - a. (Aggiornamento online) Se l'istanza di input è un'istanza gestita:
 - i. `aws:createImage`- Crea un backup AMI.
 - ii. `aws:createTags`- Contrassegna il backup AMI.
 - iii. `aws:runCommand`- Installa il driver di rete ENA tramite `AWS-ConfigureAWSPackage`.
 - iv. `aws:runCommand`- Installa il NVMe driver tramite `AWS-ConfigureAWSPackage`.
 - v. `aws:runCommand`- Installa il driver AWS PV tramite `AWS-ConfigureAWSPackage`.
 - b. (Aggiornamento offline) Se l'istanza di input non è un'istanza gestita:
 - i. `aws:assertAwsResourceProperty`- Verifica che il `AllowOffline` flag sia impostato su `true`. In tal caso, viene avviato l'aggiornamento offline, altrimenti l'automazione termina.
 - ii. `aws:changeInstanceState`- Arresta l'istanza di origine.
 - iii. `aws:changeInstanceState`- Arresta forzatamente l'istanza di origine.
 - iv. `aws:createImage`- Crea un backup AMI dell'istanza di origine.
 - v. `aws:createTags`- Etichetta il backup AMI dell'istanza di origine.
 - vi. `aws:executeAwsApi`- Abilita ENA per l'istanza.
 - vii. `aws:assertAwsResourceProperty`- Afferma la `ForceUpgrade` bandiera.
 - viii. Forza l'aggiornamento offline) Se `ForceUpgrade = true`, `aws:executeAutomation` esegui l'invocazione `AWSSupport-StartEC2RescueWorkflow` con lo script di forzatura dell'aggiornamento del driver. Ciò consente di installare il driver indipendentemente dalla versione corrente installata.

- ix. (Aggiornamento offline) Se `ForceUpgrade = false`, `aws:executeAutomation` esegui l'invocazione `AWSSupport-StartEC2RescueWorkflow` con lo script di aggiornamento dei driver.

Output

`preUpgradeBackup.ImageId`

`preOfflineUpgradeBackup. ImageId`

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

`upgradeDriversOffline.Uscita`

`forceUpgradeDriversOutput offline`

Amazon ECS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic Container Service. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-CollectECSInstanceLogs](#)
- [AWS-InstallAmazonECSAgent](#)
- [AWS-ECSRunTask](#)
- [AWSSupport-TroubleshootECSContainerInstance](#)
- [AWSSupport-TroubleshootECSTaskFailedToStart](#)
- [AWS-UpdateAmazonECSAgent](#)

AWSSupport-CollectECSInstanceLogs

Descrizione

Il `AWSsupport-CollectECSInstanceLogs` runbook raccoglie i file di log relativi al sistema operativo e ad Amazon Elastic Container Service (Amazon ECS) da un'istanza Amazon Elastic Compute Cloud (Amazon) per aiutarti a risolvere i problemi più comuni di EC2 Amazon ECS. Mentre l'automazione raccoglie i file di log associati, vengono apportate modifiche al file system. Queste modifiche includono la creazione di directory temporanee e di una directory di registro, la copia dei file di registro in queste directory e la compressione dei file di registro in un archivio.

Se si specifica un valore per il `LogDestination` parametro, sull'istanza di destinazione deve essere installata la AWS Command Line Interface (AWS CLI) per le istanze Linux o AWS Tools for Windows PowerShell per le istanze Windows. L'automazione valuta lo stato della policy del bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente. Per contribuire alla sicurezza dei log raccolti dalla tua EC2 istanza Amazon, se lo stato della policy `isPublic` è impostato su `o` se l'elenco di controllo degli accessi (ACL) concede `READ|WRITE` le autorizzazioni al gruppo predefinito di `Amazon S3All Users`, i log non vengono caricati. `true` Inoltre, se il bucket fornito non è disponibile nel tuo account, i log non vengono caricati. Per ulteriori informazioni sui gruppi predefiniti di Amazon S3, consulta i [gruppi predefiniti di Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `ECSInstanceid`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza da cui desideri raccogliere i log. L'istanza specificata deve essere gestita da Systems Manager.

- `LogDestination`

Tipo: stringa

Descrizione: (Facoltativo) Il bucket Amazon S3 in cui Account AWS caricare i log archiviati.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`

Consigliamo che l' EC2 istanza Amazon specificata nel `ECSInstanceId` parametro abbia un ruolo IAM con la policy gestita di `AmazonSSMManagedInstanceCore` Amazon allegata. Per caricare l'archivio di log nel bucket Amazon S3 specificato nel `LogDestination` parametro, devi aggiungere le seguenti autorizzazioni:

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

Fasi del documento

- `assertInstanceIsManaged`- Verifica se l'istanza specificata nel `ECSInstanceId` parametro è gestita da Systems Manager.

- `getInstancePlatform`- Ottiene informazioni sulla piattaforma del sistema operativo (OS) dell'istanza specificata nel `ECSInstanceId` parametro.
- `verifyInstancePlatform`- Suddivide l'automazione in base alla piattaforma OS.
- `runLogCollectionScriptOnLinux`- Raccoglie i file di log relativi al sistema operativo e ad Amazon ECS su istanze Linux e crea un file di archivio nella directory. `/var/log/collectECSlogs`
- `runLogCollectionScriptOnWindows`- Raccoglie i file di registro relativi al sistema operativo e ad Amazon ECS sulle istanze di Windows e crea un file di archivio nella directory. `C:\ProgramData\collectECSlogs`
- `verifyIfS3BucketProvided`- Verifica se è stato specificato un valore per il parametro. `LogDestination`
- `runUploadScript`- Suddivide la fase di automazione in base alla piattaforma del sistema operativo.
- `runUploadScriptOnLinux`- Carica l'archivio di log nel bucket Amazon S3 specificato nel parametro ed elimina `LogDestination` il file di registro archiviato dal sistema operativo.
- `runUploadScriptOnWindows`- Carica l'archivio di log nel bucket Amazon S3 specificato nel parametro ed elimina `LogDestination` il file di registro archiviato dal sistema operativo.

AWS-InstallAmazonECSAgent

Descrizione

Il `AWS-InstallAmazonECSAgent` runbook installa l'agente Amazon Elastic Container Service (Amazon ECS) sull'istanza Amazon Elastic Compute Cloud (EC2Amazon) specificata. Questo runbook supporta solo istanze Amazon Linux e Amazon Linux 2.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceIds

Tipo: StringList

Descrizione: (Obbligatorio) Le IDs EC2 istanze Amazon su cui desideri installare l'agente Amazon ECS.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances

Fasi del documento

aws:executeScript- Installa l'agente Amazon ECS sulle EC2 istanze Amazon specificate nel parametro. InstanceIds

Output

InstallAmazonECSAgent. SuccessfulInstances - L'ID dell'istanza in cui l'installazione dell'agente Amazon ECS è riuscita.

InstallAmazonECSAgent. FailedInstances - L'ID dell'istanza in cui l'installazione dell'agente Amazon ECS non è riuscita.

InstallAmazonECSAgent. InProgressInstances - L'ID dell'istanza in cui è in corso l'installazione dell'agente Amazon ECS.

AWS-ECSRunTask

Descrizione

Il AWS-ECSRunTask runbook esegue il task Amazon Elastic Container Service (Amazon ECS) specificato dall'utente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- capacityProviderStrategy

Tipo: stringa

Descrizione: (Facoltativo) La strategia del provider di capacità da utilizzare per l'attività.

- cluster

Tipo: stringa

Descrizione: (Facoltativo) Il nome breve o l'ARN del cluster su cui eseguire l'attività. Se non si specifica un cluster, viene utilizzato il cluster predefinito.

- count

Tipo: stringa

Descrizione: (Facoltativo) Il numero di istanze dell'attività specificata da inserire nel cluster. È possibile specificare fino a 10 attività per ogni richiesta.

- abilita i ECSManaged tag

Tipo: Booleano

Descrizione: (Facoltativo) Specifica se utilizzare i tag gestiti di Amazon ECS per l'attività. Per ulteriori informazioni, consulta la sezione [Tagging delle risorse Amazon ECS](#) nella Guida per gli sviluppatori di Amazon Elastic Container Service.

- enableExecuteCommand

Tipo: Booleano

Descrizione: (Facoltativo) Determina se attivare la funzionalità del comando di esecuzione per i contenitori di questa attività. Se impostato su true, ciò attiva la funzionalità di esecuzione dei comandi su tutti i contenitori dell'attività.

- gruppo

Tipo: stringa

Descrizione: (Facoltativo) Il nome del gruppo di attività da associare all'attività. Il valore predefinito è il cognome della definizione dell'attività. Ad esempio, `family:my-family-name`.

- Tipo di avvio

Tipo: stringa

Valori validi: EC2 | FARGATE | EXTERNAL

Descrizione: (Facoltativo) L'infrastruttura su cui eseguire l'attività autonoma.

- networkConfiguration

Tipo: stringa

Descrizione: (Facoltativo) La configurazione di rete per l'attività. Questo parametro è necessario per le definizioni delle attività che utilizzano la modalità di awsvpc rete per ricevere la propria interfaccia di rete elastica e non è supportato per altre modalità di rete.

- sovrascrive

Tipo: stringa

Descrizione: (Facoltativo) Un elenco di sostituzioni dei contenitori in formato JSON che specificano il nome di un contenitore nella definizione dell'attività specificata e le sostituzioni che deve ricevere. Puoi sovrascrivere il comando predefinito per un contenitore specificato nella definizione dell'attività o nell'immagine Docker con un comando override. Puoi anche sovrascrivere le variabili di ambiente esistenti specificate nella definizione dell'attività o nell'immagine Docker su un contenitore. Inoltre, puoi aggiungere nuove variabili di ambiente con un'override di ambiente.

- Vincoli di posizionamento

Tipo: stringa

Descrizione: (Facoltativo) Una serie di oggetti con vincoli di posizionamento da utilizzare per l'attività. È possibile specificare fino a 10 vincoli per ogni attività, inclusi i vincoli nella definizione dell'attività e quelli specificati in fase di esecuzione.

- Strategia di posizionamento

Tipo: stringa

Descrizione: (Facoltativo) Gli oggetti della strategia di posizionamento da utilizzare per l'attività. È possibile specificare un massimo di 5 regole strategiche per ogni attività.

- platformVersion

Tipo: stringa

Descrizione: (Facoltativo) La versione della piattaforma utilizzata dall'attività. Una versione della piattaforma è specificata solo per le attività ospitate su Fargate. Se non è specificata, di default viene utilizzata la versione della piattaforma LATEST.

- `propagateTags`

Tipo: stringa

Descrizione: (Facoltativo) Determina se i tag si propagano dalla definizione dell'attività all'attività. Se non viene specificato alcun valore, i tag non vengono propagati. I tag possono essere propagati all'attività solo durante la creazione della stessa.

- `referenceId`

Tipo: stringa

Descrizione: (Facoltativo) L'ID di riferimento da utilizzare per l'attività. L'ID di riferimento può avere una lunghezza massima di 1024 caratteri.

- Iniziatore da

Tipo: stringa

Descrizione: (Facoltativo) Un tag opzionale specificato all'avvio di un'attività. Questo ti aiuta a identificare quali attività appartengono a un lavoro specifico filtrando i risultati di un'operazione `ListTasks` API. Sono consentiti fino a 36 lettere (maiuscole e minuscole), numeri, trattini (-) e caratteri di sottolineatura (_).

- `tags`

Tipo: stringa

Descrizione: (Facoltativo) Metadati che desideri applicare all'attività per aiutarti a classificare e organizzare le attività. Ogni tag è costituito da una chiave e da un valore definiti dall'utente.

- Definizione dell'attività

Tipo: stringa

Descrizione: (Facoltativo) L'`familyand revision` (`family:revision`) o l'ARN completo della definizione dell'attività da eseguire. Se non viene specificata una revisione, viene utilizzata la ACTIVE revisione più recente.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ecs:RunTask`

Fasi del documento

`aws:executeScript`- Esegue l'attività Amazon ECS in base ai valori specificati per i parametri di input del runbook.

AWSSupport-TroubleshootECSTaskInstance

Descrizione

Il `AWSSupport-TroubleshootECSTaskInstance` runbook ti aiuta a risolvere i problemi di un'istanza Amazon Elastic Compute Cloud (Amazon EC2) che non riesce a registrarsi con un cluster Amazon ECS. Questa automazione verifica se i dati utente dell'istanza contengono le informazioni corrette sul cluster, se il profilo dell'istanza contiene le autorizzazioni richieste e i problemi di configurazione della rete.

Important

Per eseguire correttamente questa automazione, lo stato dell' EC2 istanza Amazon deve essere `running` e lo stato del cluster Amazon ECS deve essere `ACTIVE` lo stesso.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del cluster Amazon ECS con cui l'istanza non è riuscita a registrarsi.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon per la quale desideri risolvere il problema.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

`AWS:ExecuteScript`: verifica se l' EC2 istanza Amazon soddisfa i prerequisiti necessari per la registrazione con un cluster Amazon ECS.

AWSSupport-TroubleshootECSTaskFailedToStart

Descrizione

Il `AWSSupport-TroubleshootECSTaskFailedToStart` runbook ti aiuta a risolvere il motivo per cui un'attività Amazon Elastic Container Service (Amazon ECS) in un cluster Amazon ECS non è riuscita ad avviarsi. È necessario eseguire questo runbook nello stesso modo in cui l'attività non è Regione AWS stata avviata. Il runbook analizza i seguenti problemi comuni che possono impedire l'avvio di un'attività:

- Connettività di rete al registro dei contenitori configurato
- Autorizzazioni IAM mancanti richieste dal ruolo di esecuzione dell'attività
- Connettività endpoint VPC
- Configurazione delle regole del gruppo di sicurezza
- AWS Secrets Manager riferimenti segreti
- Configurazione della registrazione

Note

Se l'analisi determina che è necessario testare la connettività di rete, nel tuo account vengono creati una funzione Lambda e il ruolo IAM richiesto. Queste risorse vengono utilizzate per simulare la connettività di rete dell'operazione non riuscita. L'automazione elimina queste risorse quando non sono più necessarie. Tuttavia, se l'automazione non riesce a eliminare le risorse, è necessario farlo manualmente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del cluster Amazon ECS in cui l'attività non è stata avviata.

- CloudwatchRetentionPeriod

Tipo: integer

Descrizione: (Facoltativo) Il periodo di conservazione, in giorni, per i log delle funzioni Lambda da archiviare in Amazon Logs. CloudWatch Ciò è necessario solo se l'analisi determina che la connettività di rete deve essere testata.

Valori validi: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

Impostazione predefinita: 30

- TaskId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'operazione non riuscita. Utilizza l'ultima operazione non riuscita.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `cloudtrail:LookupEvents`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ecr:DescribeImages`
- `ecr:GetRepositoryPolicy`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeServices`
- `ecs:DescribeTaskDefinition`
- `ecs:DescribeTasks`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`

- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListRoles`
- `iam:PassRole`
- `iam:SimulateCustomPolicy`
- `iam:SimulatePrincipalPolicy`
- `kms:DescribeKey`
- `lambda:CreateFunction`
- `lambda:DeleteFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:InvokeFunction`
- `lambda:TagResource`
- `logs:DescribeLogGroups`
- `logs:PutRetentionPolicy`
- `secretsmanager:DescribeSecret`
- `ssm:DescribeParameters`
- `sts:GetCallerIdentity`

Fasi del documento

- `aws:executeScript`- Verifica che l'utente o il ruolo che ha avviato l'automazione disponga delle autorizzazioni IAM richieste. Se non disponi di autorizzazioni sufficienti per utilizzare questo runbook, le autorizzazioni richieste mancanti vengono incluse nell'output dell'automazione.
- `aws:branch`- Suddivisione in base alla disponibilità o meno delle autorizzazioni per tutte le azioni richieste per il runbook.
- `aws:executeScript`- Crea una funzione Lambda nel tuo VPC se l'analisi determina che la connettività di rete deve essere testata.
- `aws:branch`- Filiali basate sui risultati del passaggio precedente.
- `aws:executeScript`- Analizza le possibili cause del mancato avvio dell'attività.
- `aws:executeScript`- Elimina le risorse create da questa automazione.

- `aws:executeScript`- Formatta l'output dell'automazione per restituire i risultati dell'analisi alla console. È possibile rivedere l'analisi dopo questo passaggio prima del completamento dell'automazione.
- `aws:branch`- Rami in base al fatto che la funzione Lambda e le risorse associate siano state create e debbano essere eliminate.
- `aws:sleep`- Dorme per 30 minuti in modo che l'interfaccia di rete elastica per la funzione Lambda possa essere eliminata.
- `aws:executeScript`- Elimina l'interfaccia di rete della funzione Lambda.
- `aws:executeScript`- Formatta l'output della fase di eliminazione dell'interfaccia di rete della funzione Lambda.

AWS-UpdateAmazonECSAgent

Descrizione

Il AWS-UpdateAmazonECSAgent runbook aggiorna l'agente Amazon Elastic Container Service (Amazon ECS) sull'istanza Amazon Elastic Compute Cloud (Amazon) specificata. EC2 Questo runbook supporta solo istanze Amazon Linux e Amazon Linux 2.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterARN

Tipo: StringList

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del cluster Amazon ECS in cui sono registrate le istanze di container.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeImage`
- `ec2:DescribeInstance`
- `ec2:DescribeInstanceAttribute`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

Fasi del documento

`aws:executeScript`- Aggiorna l'agente Amazon ECS sul cluster Amazon ECS specificato nei `ClusterARN` parametri.

Output

`UpdateAmazonECSAgent`. `UpdatedContainers` - L'ID dell'istanza in cui l'aggiornamento dell'agente Amazon ECS è riuscito.

UpdateAmazonECSAgent. FailedContainers - L'ID dell'istanza in cui l'aggiornamento dell'agente Amazon ECS non è riuscito.

UpdateAmazonECSAgent. InProgressContainers - L'ID dell'istanza in cui è in corso l'aggiornamento dell'agente Amazon ECS.

Amazon EFS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic File System. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-CheckAndMountEFS](#)

AWSSupport-CheckAndMountEFS

Descrizione

Il AWSSupport-CheckAndMountEFS runbook verifica i prerequisiti per montare il file system Amazon Elastic File System (Amazon EFS) e monta il file system sull'istanza Amazon Elastic Compute Cloud (EC2Amazon) specificata. Questo runbook supporta il montaggio del file system Amazon EFS con il nome DNS o l'utilizzo dell'indirizzo IP del target di montaggio.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Azione

Tipo: stringa

Valori validi: Check | CheckAndMount

Descrizione: (Obbligatorio) Determina se il runbook verifica i prerequisiti oppure verifica i prerequisiti e installa il file system.

- EfsId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del file system che si desidera montare.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon su cui desideri montare il file system.

- MountOptions

Tipo: stringa

Descrizione: (Facoltativo) Le opzioni supportate dall'helper di montaggio di Amazon EFS che desideri utilizzare per il montaggio del file system. Se specifichi l'`tls` opzione, verifica che stunnel sia stato aggiornato sull'istanza di destinazione.

- MountPoint

Tipo: stringa

Descrizione: (Facoltativo) La directory in cui si desidera montare il file system. Se si specifica il `Check` valore per il `Action` parametro, questo parametro non deve essere specificato.

- MountTargetIP

Tipo: stringa

Descrizione: (Facoltativo) L'indirizzo IP del target di montaggio. Il montaggio per indirizzo IP funziona in ambienti in cui il DNS è disabilitato, come i cloud privati virtuali (VPCs) con nomi host DNS disabilitati. Inoltre, puoi utilizzare questa opzione se il tuo ambiente utilizza un provider DNS diverso da Amazon Route 53 (Route 53).

- Regione

Tipo: stringa

Descrizione: (Obbligatorio) La posizione Regione AWS in cui si trovano l' EC2 istanza e il file system di Amazon.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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:*`

Fasi del documento

- `aws:executeScript`- Raccoglie dettagli sull' EC2 istanza Amazon specificata nel `InstanceId` parametro.
- `aws:executeScript`- Raccoglie dettagli sul file system specificato nel `EfsId` parametro.
- `aws:executeScript`- Verifica che il gruppo di sicurezza associato al file system consenta il traffico sulla porta 2049 dall' EC2 istanza Amazon specificata nel `InstanceId` parametro.
- `aws:assertAwsResourceProperty`- Verifica che l' EC2 istanza Amazon specificata nel `InstanceId` parametro sia gestita da Systems Manager e che lo stato sia `Online`.
- `aws:branch`- Filiali in base al valore specificato per il `Action` parametro.
- `aws:runCommand`- Verifica i prerequisiti per il montaggio del file system specificato nel `EfsId` parametro.
- `aws:runCommand`- Verifica i prerequisiti per il montaggio del file system specificato nel `EfsId` parametro e monta il file system sull' EC2 istanza Amazon specificata nel parametro. `InstanceId`

Amazon EKS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Elastic Kubernetes Service. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-CollectEKSIInstanceLogs](#)
- [AWS-CreateEKSClusterWithFargateProfile](#)
- [AWS-CreateEKSClusterWithNodegroup](#)
- [AWS-DeleteEKSCluster](#)
- [AWS-MigrateToNewEKSSelfManagedNodeGroup](#)
- [AWSPremiumSupport-TroubleshootEKSCluster](#)

- [AWSSupport-TroubleshootEKSWorkerNode](#)
- [AWS-UpdateEKSCluster](#)
- [AWS-UpdateEKSMangedNodeGroup](#)
- [AWS-UpdateEKSSelfManagedLinuxNodeGroups](#)
- [AWSSupport-SetupK8sApiProxyForEKS](#)
- [AWSSupport-TroubleshootEbsCsiDriversForEks](#)

AWSSupport-CollectEKSIInstanceLogs

Descrizione

Il `AWSSupport-CollectEKSIInstanceLogs` runbook raccoglie i file di log relativi al sistema operativo e ad Amazon Elastic Kubernetes Service (Amazon EKS) da un'istanza Amazon Elastic Compute Cloud EC2 (Amazon) per aiutarti a risolvere i problemi più comuni. Mentre l'automazione raccoglie i file di registro associati, vengono apportate modifiche alla struttura del file system, tra cui la creazione di directory temporanee, la copia dei file di registro nelle directory temporanee e la compressione dei file di registro in un archivio. Questa attività può comportare un aumento dell'istanzaCPUUtilization. EC2 Per ulteriori informazioniCPUUtilization, consulta le [metriche delle istanze](#) nella Amazon CloudWatch User Guide.

Se specifichi un valore per il `LogDestination` parametro, l'automazione valuta lo stato della policy del bucket Amazon Simple Storage Service (Amazon S3) che hai specificato. Per contribuire alla sicurezza dei log raccolti dall' EC2 istanza, se lo stato della policy `isPublic` è impostato su `o` se l'elenco di controllo degli accessi (ACL) concede `READ|WRITE` le autorizzazioni al gruppo predefinito di Amazon `S3A11 Users`, i log non vengono caricati. `true` Per ulteriori informazioni sui gruppi predefiniti di Amazon S3, consulta i gruppi predefiniti di [Amazon S3 nella Guida per l'utente](#) di Amazon Simple Storage Service.

Note

Questa automazione richiede almeno il 10% dello spazio su disco disponibile sul volume root Amazon Elastic Block Store (Amazon EBS) collegato all'istanza. EC2 Se lo spazio su disco disponibile sul volume principale non è sufficiente, l'automazione si interrompe.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EKSInstanceId

Tipo: stringa

Descrizione: (obbligatorio) ID dell' EC2 istanza Amazon EKS da cui desideri raccogliere i log.

- LogDestination

Tipo: stringa

Descrizione: (Facoltativo) Il bucket S3 nel tuo account in cui caricare i log archiviati.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:SendCommand

Consigliamo che l' EC2 istanza che riceve il comando abbia un ruolo IAM con la policy gestita di `SSMManagedInstanceCoreAmazon` Amazon allegata. Per caricare l'archivio di log nel bucket S3 specificato nel `LogDestination` parametro, devi aggiungere l'`s3:PutObject` autorizzazione.

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che il sistema operativo del valore specificato nel `EKSInstanceId` parametro è Linux.
- `aws:runCommand`- Raccoglie i file di log relativi al sistema operativo e ad Amazon EKS, comprimendoli in un archivio nella `/var/log` directory.
- `aws:branch`- Conferma se è stato specificato un valore per il `LogDestination` parametro.
- `aws:runCommand`- Carica l'archivio di log nel bucket S3 specificato nel parametro. `LogDestination`

AWS-CreateEKSClusterWithFargateProfile

Descrizione

Il `AWS-CreateEKSClusterWithFargateProfile` runbook crea un cluster Amazon Elastic Kubernetes Service (Amazon EKS) utilizzando un. AWS Fargate

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `ClusterName`

Tipo: stringa

Descrizione: (Obbligatorio) Un nome univoco per il cluster.

- `ClusterRoleArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo IAM che fornisce le autorizzazioni al piano di controllo Kubernetes per effettuare chiamate alle AWS operazioni API per tuo conto.

- `FargateProfileName`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del profilo Fargate.

- `FargateProfileRoleArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo IAM di esecuzione di Amazon EKS Pod.

- `FargateProfileSelectors`

Tipo: stringa

Descrizione: (Obbligatorio) I selettori per abbinare i pod al profilo Fargate.

- `SubnetIds`

Tipo: `StringList`

Descrizione: (Obbligatorio) Le IDs sottoreti che desideri utilizzare per il tuo cluster Amazon EKS. Amazon EKS crea interfacce di rete elastiche in queste sottoreti per la comunicazione tra i nodi e il piano di controllo Kubernetes. È necessario specificare almeno due sottoreti. IDs

- `EKSEndpointPrivateAccess`

Tipo: Booleano

Impostazione predefinita: True

Descrizione: (Facoltativo) Imposta questo valore True per consentire l'accesso privato all'endpoint del server API Kubernetes del cluster. Se abiliti l'accesso privato, le richieste API Kubernetes che provengono dal VPC del cluster utilizzano l'endpoint VPC privato. Se disabiliti l'accesso privato e hai nodi o AWS Fargate pod nel cluster, assicurati di `publicAccessCidrs` includere i blocchi CIDR necessari per la comunicazione con i nodi o i pod Fargate.

- `EKSEndpointPublicAccess`

Tipo: Booleano

Impostazione predefinita: False

Descrizione: (Facoltativo) Imposta questo valore per disabilitare l'accesso pubblico False all'endpoint del server dell'API Kubernetes del cluster. Se disabiliti l'accesso pubblico, il server API Kubernetes del tuo cluster può ricevere richieste solo dall'interno del VPC in cui è stato avviato.

- `PublicAccessCIDRs`

Tipo: StringList

Descrizione: (Facoltativo) I blocchi CIDR a cui è consentito l'accesso all'endpoint pubblico del server API Kubernetes del cluster. La comunicazione all'endpoint da indirizzi esterni ai blocchi CIDR specificati è negata. Se hai disabilitato l'accesso privato agli endpoint e hai nodi o pod Fargate nel cluster, assicurati di specificare i blocchi CIDR necessari.

- `SecurityGroupIds`

Tipo: StringList

Descrizione: (Facoltativo) Specificare uno o più gruppi di sicurezza da associare alle interfacce di rete elastiche create nel tuo account da Amazon EKS.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

- `Create EKSCluster (aws:executeAwsApi)` - Crea un cluster Amazon EKS.
- `Verify EKSCluster IsActive (aws: waitForAwsResourceProperty)` - Verifica che lo stato del cluster sia `ACTIVE`.
- `CreateFargateProfile (aws:executeAwsApi)` - Crea un Fargate per il cluster.
- `VerifyFargateProfileIsActive (aws: waitForAwsResourceProperty)` - Verifica che lo stato del profilo Fargate sia. `ACTIVE`

Output

`CreateEKSCluster.CreateClusterResponse`

Descrizione: risposta ricevuta dalla chiamata `CreateCluster` API.

`CreateFargateProfile.CreateFargateProfileResponse`

Descrizione: risposta ricevuta dalla chiamata `CreateFargateProfile` API.

AWS-CreateEKSClusterWithNodegroup

Descrizione

Il `AWS-CreateEKSClusterWithNodegroup` runbook crea un cluster Amazon Elastic Kubernetes Service (Amazon EKS) utilizzando un gruppo di nodi per la capacità.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `ClusterName`

Tipo: stringa

Descrizione: (Obbligatorio) Un nome univoco per il cluster.

- `ClusterRoleArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo IAM che fornisce le autorizzazioni al piano di controllo Kubernetes per effettuare chiamate alle AWS operazioni API per tuo conto.

- `NodegroupName`

Tipo: stringa

Descrizione: (Obbligatorio) Un nome univoco per il gruppo di nodi.

- `NodegroupRoleArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo IAM da associare al gruppo di nodi. Il daemon kubelet del nodo di lavoro Amazon EKS effettua chiamate per AWS APIs tuo conto. I nodi ricevono le autorizzazioni per queste chiamate API attraverso un profilo dell'istanza IAM e le policy associate. Prima di avviare i nodi e registrarli in un cluster, devi creare un ruolo IAM che i nodi possano utilizzare all'avvio.

- `SubnetIds`

Tipo: `StringList`

Descrizione: (Obbligatorio) Le IDs sottoreti che desideri utilizzare per il tuo cluster Amazon EKS. Amazon EKS crea interfacce di rete elastiche in queste sottoreti per la comunicazione tra i nodi e il piano di controllo Kubernetes. È necessario specificare almeno due sottoreti. IDs

- `EKSEndpointPrivateAccess`

Tipo: Booleano

Impostazione predefinita: `True`

Descrizione: (Facoltativo) Imposta questo valore `True` per consentire l'accesso privato all'endpoint del server API Kubernetes del cluster. Se abiliti l'accesso privato, le richieste API Kubernetes che provengono dal VPC del cluster utilizzano l'endpoint VPC privato. Se disabiliti l'accesso privato e hai nodi o AWS Fargate pod nel cluster, assicurati di `publicAccessCidrs` includere i blocchi CIDR necessari per la comunicazione con i nodi o i pod Fargate.

- `EKSEndpointPublicAccess`

Tipo: Booleano

Impostazione predefinita: `False`

Descrizione: (Facoltativo) Imposta questo valore per disabilitare l'accesso pubblico `False` all'endpoint del server dell'API Kubernetes del cluster. Se disabiliti l'accesso pubblico, il server API Kubernetes del tuo cluster può ricevere richieste solo dall'interno del VPC in cui è stato avviato.

- `PublicAccessCIDRs`

Tipo: `StringList`

Descrizione: (Facoltativo) I blocchi CIDR a cui è consentito l'accesso all'endpoint pubblico del server API Kubernetes del cluster. La comunicazione all'endpoint da indirizzi esterni ai blocchi CIDR specificati è negata. Se hai disabilitato l'accesso privato agli endpoint e hai nodi o pod Fargate nel cluster, assicurati di specificare i blocchi CIDR necessari.

- `SecurityGroupIds`

Tipo: `StringList`

Descrizione: (Facoltativo) Specificare uno o più gruppi di sicurezza da associare alle interfacce di rete elastiche create nel tuo account da Amazon EKS.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

Fasi del documento

- `Create EKSCluster (aws:executeAwsApi)` - Crea un cluster Amazon EKS.
- `Verify EKSCluster IsActive (aws: waitForAwsResourceProperty)` - Verifica che lo stato del cluster sia `ACTIVE`.

- `CreateNodegroup` (`aws:executeAwsApi`) - Crea un gruppo di nodi per il cluster.
- `VerifyNodegroupsActive` (`aws:waitForAwsResourceProperty`) - Verifica che lo stato del gruppo di nodi sia `ACTIVE`.

Output

- `CreateEKSCluster.CreateClusterResponse`: Risposta ricevuta dalla chiamata `CreateCluster` API.
- `CreateNodegroup.CreateNodegroupResponse`: Risposta ricevuta dalla chiamata `CreateNodegroup` API.

AWS-DeleteEKSCluster

Descrizione

Questo runbook elimina le risorse associate a un cluster Amazon EKS, inclusi i gruppi di nodi e i profili Fargate. Facoltativamente, puoi scegliere di eliminare tutti i nodi autogestiti, gli AWS CloudFormation stack utilizzati per creare i nodi e lo stack VPC CloudFormation per il tuo cluster. Per ulteriori informazioni sull'eliminazione di un cluster, consulta [Eliminazione di un cluster](#) nella Amazon EKS User Guide.

Note

Se nel cluster sono presenti servizi attivi associati a un sistema di bilanciamento del carico, è necessario eliminare tali servizi prima di eliminare il cluster. In caso contrario, il sistema non può eliminare i sistemi di bilanciamento del carico. Utilizzare la procedura seguente per trovare ed eliminare i servizi prima di eseguire il `AWS-DeleteEKSCluster` runbook.

Per individuare ed eliminare i servizi nel cluster

1. Installa l'utilità da riga di comando Kubernetes, `kubectl`. Per ulteriori informazioni, consulta [Installazione di kubectl](#) nella Guida per l'utente di Amazon EKS.
2. Esegui il comando seguente per elencare tutti i servizi in esecuzione nel cluster.

```
kubectl get svc --all-namespaces
```

3. Esegui il comando seguente per eliminare tutti i servizi a cui è associato un valore EXTERNAL-IP. Questi servizi sono gestiti da un sistema di bilanciamento del carico ed è necessario eliminarli in Kubernetes per consentire il corretto rilascio del sistema di bilanciamento del carico e delle risorse associate.

```
kubectl delete svc  
service-name
```

Ora puoi eseguire il runbook. `AWS-DeleteEKSCluster`

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EKSClusterNome

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del cluster Amazon EKS da eliminare.

- `VPCCloudFormationStack`

Tipo: stringa

Descrizione: (Facoltativo) nome AWS CloudFormation dello stack per il VPC per il cluster EKS da eliminare. Questo elimina lo AWS CloudFormation stack per il VPC e tutte le risorse create dallo stack.

- `VPCCloudFormationStackRole`

Tipo: stringa

Descrizione: (Facoltativo) L'ARN di un ruolo IAM che AWS CloudFormation presuppone l'eliminazione dello stack VPC. CloudFormation AWS CloudFormation utilizza le credenziali del ruolo per effettuare chiamate per tuo conto.

- `SelfManagedNodeStacks`

Tipo: stringa

Descrizione: (Facoltativo) Elenco separato da virgole di nomi di AWS CloudFormation stack per i nodi autogestiti. Questo eliminerà gli stack per i nodi autogestiti. AWS CloudFormation

- `SelfManagedNodeStacksRole`

Tipo: stringa

Descrizione: (Facoltativo) L'ARN di un ruolo IAM che AWS CloudFormation presuppone l'eliminazione degli stack di nodi autogestiti. AWS CloudFormation utilizza le credenziali del ruolo per effettuare chiamate per tuo conto.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `sts:AssumeRole`
- `eks:ListNodegroups`
- `eks:DeleteNodegroup`
- `eks:ListFargateProfiles`
- `eks:DeleteFargateProfile`

- `eks:DeleteCluster`
- `cfn:DescribeStacks`
- `cfn>DeleteStack`

Fasi del documento

- `aws:executeScript- DeleteNodeGroups`: Trova ed elimina tutti i gruppi di nodi nel cluster EKS.
- `aws:executeScript- DeleteFargateProfiles`: Trova ed elimina tutti i profili Fargate nel cluster EKS.
- `aws:executeScript- DeleteSelfManagedNodes`: Elimina tutti i nodi autogestiti e gli CloudFormation stack utilizzati per creare i nodi.
- `aws:executeScript- EliminaEKSCluster`: elimina il cluster EKS.
- `aws:executeScript- Elimina VPCCloudFormationStack`: elimina lo stack VPC. CloudFormation

AWS-MigrateToNewEKSSelfManagedNodeGroup

Descrizione

Il `AWS-MigrateToNewEKSSelfManagedNodeGroup` runbook ti aiuta a creare un nuovo gruppo di nodi Linux Amazon Elastic Kubernetes Service (Amazon EKS) su cui migrare l'applicazione esistente. Per ulteriori informazioni, consulta [Migrazione a un nuovo gruppo di nodi](#) nella Amazon EKS User Guide.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- OldStackName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome o l'ID dello stack esistente. AWS CloudFormation

- NewStackName

Tipo: stringa

Descrizione: (Facoltativo) Il nome del nuovo AWS CloudFormation stack creato per il nuovo gruppo di nodi. Se non specificate un valore per questo parametro, il nome dello stack viene creato utilizzando il formato: `NewNodeGroup-ClusterName-AutomationExecutionID`

- ClusterControlPlaneSecurityGroup

Tipo: stringa

Descrizione: (Facoltativo) L'ID del gruppo di sicurezza che desideri che i nodi utilizzino per comunicare con il piano di controllo di Amazon EKS. Se non specifichi un valore per questo parametro, viene utilizzato il gruppo di sicurezza specificato nello AWS CloudFormation stack esistente.

- NodeInstanceType

Tipo: stringa

Descrizione: (Facoltativo) Il tipo di istanza che desideri utilizzare per il nuovo gruppo di nodi. Se non specificate un valore per questo parametro, viene utilizzato il tipo di istanza specificato nello AWS CloudFormation stack esistente.

- NodeGroupName

Tipo: stringa

Descrizione: (Facoltativo) Il nome del nuovo gruppo di nodi. Se non si specifica un valore per questo parametro, viene utilizzato il nome del gruppo di nodi specificato nello AWS CloudFormation stack esistente.

- NodeAutoScalingGroupDesiredCapacity

Tipo: stringa

Descrizione: (Facoltativo) Il numero desiderato di nodi su cui scalare quando viene creato il nuovo stack. Questo numero deve essere maggiore o uguale al NodeAutoScalingGroupMinSize valore e minore o uguale a. NodeAutoScalingGroupMaxSize Se non si specifica un valore per questo parametro, viene utilizzata la capacità desiderata del gruppo di nodi specificata nello AWS CloudFormation stack esistente.

- NodeAutoScalingGroupMaxSize

Tipo: stringa

Descrizione: (Facoltativo) Il numero massimo di nodi fino a cui il gruppo di nodi può essere scalato orizzontalmente. Se non specifichi un valore per questo parametro, viene utilizzata la dimensione massima del gruppo di nodi specificata nello AWS CloudFormation stack esistente.

- NodeAutoScalingGroupMinSize

Tipo: stringa

Descrizione: (Facoltativo) Il numero minimo di nodi fino a cui il gruppo di nodi può scalare. Se non specifichi un valore per questo parametro, viene utilizzata la dimensione minima del gruppo di nodi specificata nello AWS CloudFormation stack esistente.

- NodeImageId

Tipo: stringa

Descrizione: (Facoltativo) L'ID del Amazon Machine Image (AMI) che desideri venga utilizzato dal gruppo di nodi.

- NodeImageIdSSMParam

Tipo: stringa

Descrizione: (Facoltativo) Il parametro pubblico di Systems Manager AMI che si desidera venga utilizzato dal gruppo di nodi.

- NodeVolumeSize

Tipo: stringa

Descrizione: (Facoltativo) La dimensione del volume root per i nodi in GiB. Se non si specifica un valore per questo parametro, viene utilizzata la dimensione del volume del nodo specificata nello AWS CloudFormation stack esistente.

- NodeVolumeType

Tipo: stringa

Descrizione: (Facoltativo) Il tipo di volume Amazon EBS che desideri utilizzare per il volume root dei tuoi nodi. Se non specifichi un valore per questo parametro, viene utilizzato il tipo di volume specificato nello AWS CloudFormation stack esistente.

- KeyName

Tipo: stringa

Descrizione: (Facoltativo) La coppia di chiavi che desideri assegnare ai tuoi nodi. Se non si specifica un valore per questo parametro, viene utilizzata la coppia di chiavi specificata nello AWS CloudFormation stack esistente.

- Sottoreti

Tipo: StringList

Descrizione: (Facoltativo) Un elenco separato da virgole della sottorete IDs che desiderate utilizzare per il nuovo gruppo di nodi. Se non specificate un valore per questo parametro, vengono utilizzate le sottoreti specificate nello stack esistente. AWS CloudFormation

- Disabilita IMDSv1

Tipo: Booleano

Descrizione: (Facoltativo) `true` Specificare la disattivazione del servizio di metadati dell'istanza versione 1 (IMDSv1). Per impostazione predefinita, i nodi supportano IMDSv1 e IMDSv2.

- BootstrapArguments

Tipo: stringa

Descrizione: (Facoltativo) Argomenti aggiuntivi da passare allo script di bootstrap del nodo.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

- `DetermineParameterValuesForNewNodeGroup` (`aws:ExecuteScript`) - Raccoglie i valori dei parametri da utilizzare per il nuovo gruppo di nodi.
- `CreateStack` (`aws:CreateStack`) - Crea lo stack per il nuovo gruppo di nodi. AWS CloudFormation
- `GetNewStackNodeInstanceRole` (`aws:executeAwsApi`) - Ottiene il ruolo dell'istanza del nodo.
- `GetNewStackSecurityGroup` (`aws:executeAwsApi`) - Il passaggio ottiene il gruppo di sicurezza del nodo.
- `AddIngressRulesToNewNodeSecurityGroup` (`aws:executeAwsApi`) - Aggiunge regole di ingresso al gruppo di sicurezza appena creato in modo che possa accettare il traffico proveniente da quello assegnato al gruppo di nodi precedente.

- `AddIngressRulesToOldNodeSecurityGroup` (`aws:executeAwsApi`) - Aggiunge regole di ingresso al gruppo di sicurezza precedente in modo che possa accettare il traffico proveniente da quello assegnato al gruppo di nodi appena creato.
- `VerifyStackComplete` (`aws:assertAwsResource Property`) - Verifica che il nuovo stato dello stack sia `CREATE_COMPLETE`

Output

`DetermineParameterValuesForNewNodeGroup`. `NewStackParameters` - I parametri utilizzati per creare il nuovo stack.

`GetNewStackNodeInstanceRole`. `NewNodeInstanceRole` - Il ruolo dell'istanza del nodo per il nuovo gruppo di nodi.

`GetNewStackSecurityGroup`. `NewNodeSecurityGroup` - L'ID del gruppo di sicurezza per il nuovo gruppo di nodi.

`DetermineParameterValuesForNewNodeGroup`. `NewStackName` - Il nome AWS CloudFormation dello stack per il nuovo gruppo di nodi.

`CreateStack`. `StackId` - L'ID AWS CloudFormation dello stack per il nuovo gruppo di nodi.

AWSPremiumSupport-TroubleshootEKSCluster

Descrizione

Il `AWSPremiumSupport-TroubleshootEKSCluster` runbook diagnostica i problemi più comuni relativi a un cluster Amazon Elastic Kubernetes Service (Amazon EKS), all'infrastruttura sottostante e fornisce i passaggi di correzione consigliati.

Important

L'accesso ai `AWSPremiumSupport-*` runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, [consulta Compare AWS Support Plans](#).

Se specifichi un valore per il `S3BucketName` parametro, l'automazione valuta lo stato della policy del bucket Amazon Simple Storage Service (Amazon S3) che hai specificato. Per contribuire alla sicurezza dei log raccolti dall' EC2 istanza, se lo stato della policy `isPublic` è impostato su `o` se l'elenco di controllo degli accessi (ACL) concede `READ|WRITE` le autorizzazioni al gruppo predefinito

di Amazon S3. All Users, i log non vengono caricati. true Per ulteriori informazioni sui gruppi predefiniti di Amazon S3, consulta i gruppi predefiniti di [Amazon S3 nella Guida per l'utente](#) di Amazon Simple Storage Service.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del cluster Amazon EKS di cui desideri risolvere i problemi.

- S3 BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket privato Amazon S3 in cui caricare il report generato dal runbook.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Inoltre, la policy AWS Identity and Access Management (IAM) associata all'utente o al ruolo che avvia l'automazione deve consentire il `ssm:GetParameter` funzionamento dei seguenti AWS Systems Manager parametri pubblici per ottenere la versione più recente di Amazon EKS Amazon Machine Image (AMI) consigliata per i nodi di lavoro.

- `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`

Per caricare il report generato dal runbook in un bucket Amazon S3, sono necessarie le seguenti autorizzazioni per il bucket Amazon S3 specificato.

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

Fasi del documento

- `aws:executeAwsApi`- Raccoglie i dettagli per il cluster Amazon EKS specificato.
- `aws:executeScript`- Raccoglie i dettagli delle istanze Amazon Elastic Compute Cloud EC2 (Amazon), dei gruppi di Auto Scaling e dei tipi di istanze AMI grafiche Amazon EC2 GPU.
- `aws:executeScript`- Raccoglie i dettagli del cloud privato virtuale (VPC), delle sottoreti, dei gateway NAT (Network Address Translation), dei percorsi di sottorete, dei gruppi di sicurezza e delle liste di controllo degli accessi alla rete (ACLs) del cluster Amazon EKS.
- `aws:executeScript`- Raccoglie i dettagli dei profili delle istanze IAM allegate e delle politiche dei ruoli.
- `aws:executeScript`- Raccoglie i dettagli del bucket Amazon S3 specificato nel parametro. `S3BucketName`
- `aws:executeScript`- Classifica le sottoreti Amazon VPC come pubbliche o private.
- `aws:executeScript`- Verifica la presenza di tag nelle sottoreti Amazon VPC per individuare i tag necessari come parte di un cluster Amazon EKS.
- `aws:executeScript`- Controlla le sottoreti Amazon VPC per i tag necessari per le sottoreti Elastic Load Balancing.
- `aws:executeScript`- Verifica se le EC2 istanze Amazon del nodo di lavoro utilizzano le ultime versioni ottimizzate per AMI Amazon EKS
- `aws:executeScript`- Verifica se i gruppi di sicurezza Amazon VPC sono collegati ai nodi di lavoro per i tag richiesti.

- `aws:executeScript`- Verifica le regole del gruppo di sicurezza Amazon EKS e del nodo di lavoro Amazon VPC per le regole di ingresso consigliate nel cluster Amazon EKS.
- `aws:executeScript`- Verifica le regole del gruppo di sicurezza Amazon VPC del cluster Amazon EKS e del nodo di lavoro per verificare le regole di uscita consigliate dal cluster Amazon EKS.
- `aws:executeScript`- Verifica la configurazione ACL di rete delle sottoreti Amazon VPC.
- `aws:executeScript`- Verifica se le EC2 istanze Amazon del nodo di lavoro dispongono delle politiche gestite richieste.
- `aws:executeScript`- Verifica se i gruppi Auto Scaling dispongono dei tag necessari per la scalabilità automatica del cluster.
- `aws:executeScript`- Verifica se le EC2 istanze Amazon del nodo di lavoro sono connesse a Internet.
- `aws:executeScript`- Genera un rapporto basato sugli output dei passaggi precedenti. Se viene specificato un valore per il `S3BucketName` parametro, il report generato viene caricato nel bucket Amazon S3.

AWSSupport-TroubleshootEKSTWorkerNode

Descrizione

Il `AWSSupport-TroubleshootEKSTWorkerNode` runbook analizza un nodo di lavoro Amazon Elastic Compute Cloud (Amazon EC2) e un cluster Amazon Elastic Kubernetes Service (Amazon EKS) per aiutarti a identificare e risolvere le cause più comuni che impediscono ai nodi di lavoro di entrare a far parte di un cluster. Il runbook fornisce indicazioni per aiutarti a risolvere eventuali problemi identificati.

Important

Per eseguire correttamente questa automazione, lo stato del nodo di EC2 lavoro Amazon deve essere `running` e lo stato del cluster Amazon EKS deve essere `lo stessoACTIVE`.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del cluster Amazon EKS.

- WorkerID

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del nodo di EC2 lavoro Amazon che non è riuscito a entrare a far parte del cluster.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che il cluster Amazon EKS specificato nel `ClusterName` parametro esiste e si trova in uno `ACTIVE` stato.
- `aws:assertAwsResourceProperty`- Conferma che il EC2 nodo di lavoro Amazon specificato nel `WorkerID` parametro esiste e si trova in uno `running` stato.
- `aws:executeScript`- Esegue uno script Python che aiuta a identificare le possibili cause del mancato ingresso del nodo di lavoro nel cluster.

AWS-UpdateEKSCluster

Descrizione

Il `AWS-UpdateEKSCluster` runbook ti aiuta ad aggiornare il cluster Amazon Elastic Kubernetes Service (Amazon EKS) alla versione Kubernetes che desideri utilizzare.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del tuo cluster Amazon EKS.

- Versione

Tipo: stringa

Descrizione: (Obbligatoria) La versione di Kubernetes a cui desideri aggiornare il cluster.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- eks:DescribeUpdate

- `eks:UpdateClusterVersion`

Fasi del documento

- `aws:executeAwsApi`- Aggiorna la versione di Kubernetes utilizzata dal tuo cluster Amazon EKS.
- `aws:waitForAwsResourceProperty`- Attende che lo stato dell'aggiornamento sia. `Successful`

AWS-UpdateEKSMangedNodeGroup

Descrizione

Il AWS-UpdateEKSMangedNodeGroup runbook ti aiuta ad aggiornare un gruppo di nodi gestiti di Amazon Elastic Kubernetes Service (Amazon EKS). Puoi scegliere o aggiornare. `Version Configuration`

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- **ClusterName**

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del cluster di cui si desidera aggiornare il gruppo di nodi.

- **NodeGroupName**

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del gruppo di nodi da aggiornare.

- **UpdateType**

Tipo: stringa

Valori validi: Aggiorna la versione del gruppo di nodi | Aggiorna le configurazioni del gruppo di nodi

Impostazione predefinita: aggiorna la versione del gruppo di nodi

Descrizione: (Obbligatorio) Il tipo di aggiornamento che si desidera eseguire sul gruppo di nodi.

I seguenti parametri si applicano solo al tipo di `Version` aggiornamento:

- **AMIReleaseVersion**

Tipo: stringa

Descrizione: (Facoltativa) La versione ottimizzata di Amazon EKS AMI che desideri utilizzare. Per impostazione predefinita viene utilizzata la versione più recente.

- **ForceUpgrade**

Tipo: Booleano

Descrizione: (Facoltativo) Se impostato su `true`, l'aggiornamento non avrà esito negativo in caso di violazione del budget relativo all'interruzione del pod.

- **KubernetesVersion**

Tipo: stringa

Descrizione: (Facoltativo) La versione di Kubernetes a cui aggiornare il gruppo di nodi.

Tipo: stringa

Descrizione: (Facoltativo) L'ID del modello di lancio.

- LaunchTemplateName

Tipo: stringa

Descrizione: (Facoltativo) Il nome del modello di lancio.

- LaunchTemplateVersion

Tipo: stringa

Descrizione: (Facoltativo) La versione del modello di lancio di Amazon Elastic Compute Cloud (Amazon EC2). Questo parametro è valido solo se un gruppo di nodi è stato creato da un modello di lancio.

I seguenti parametri si applicano solo al tipo di Configuration aggiornamento:

- AddOrUpdateNodeGroupLabels

Tipo: StringMap

Descrizione: (Facoltativo) Etichette Kubernetes che desideri aggiungere o aggiornare.

- AddOrUpdateKubernetesTaintsEffect

Tipo: StringList

Descrizione: (Facoltativo) I taint Kubernetes che desideri aggiungere o aggiornare.

- MaxUnavailableNodeGroups

Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero massimo di nodi che non sono disponibili contemporaneamente durante un aggiornamento della versione.

- MaxUnavailablePercentageNodeGroup

Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) La percentuale di nodi che non sono disponibili durante un aggiornamento della versione.

- NodeGroupDesiredSize

Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero di nodi che il gruppo di nodi gestiti deve mantenere.

- NodeGroupMaxSize

Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero massimo di nodi fino a cui il gruppo di nodi gestiti può scalare orizzontalmente.

- NodeGroupMinSize

Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero minimo di nodi in cui il gruppo di nodi gestiti può scalare.

- RemoveKubernetesTaintsEffect

Tipo: StringList

Descrizione: (Facoltativo) Le macchie Kubernetes che desideri rimuovere.

- RemoveNodeGroupLabels

Tipo: StringList

Descrizione: (Facoltativo) Un elenco di etichette separate da virgole che desideri rimuovere.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

Fasi del documento

- `aws:executeScript`- Aggiorna un gruppo di nodi del cluster Amazon EKS in base ai valori specificati per i parametri di input del runbook.
- `aws:waitForAwsResourceProperty`- Attende che lo stato di aggiornamento del cluster sia raggiunto. `Successful`

AWS-UpdateEKSSelfManagedLinuxNodeGroups

Descrizione

Il `AWS-UpdateEKSSelfManagedLinuxNodeGroups` runbook aggiorna i gruppi di nodi autogestiti nel cluster Amazon Elastic Kubernetes Service (Amazon EKS) utilizzando uno stack AWS CloudFormation

Se il tuo cluster utilizza la scalabilità automatica, ti consigliamo di ridimensionare la distribuzione fino a due repliche prima di utilizzare questo runbook.

Per scalare una distribuzione a due repliche

1. Installa l'utilità della riga di comando Kubernetes, `kubectl` Per ulteriori informazioni, consulta la pagina relativa all'[installazione di kubectl](#) nella Guida per l'utente di Amazon EKS.
2. Esegui il comando seguente.

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. Esegui il runbook. `AWS-UpdateEKSSelfManagedLinuxNodeGroups`
4. Ridimensiona la distribuzione al numero di repliche desiderato eseguendo il comando seguente.

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del cluster Amazon EKS.

- NodeGroupName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del gruppo di nodi gestiti.

- ClusterControlPlaneSecurityGroup

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza del piano di controllo.

- Disabilita IMDSv1

Tipo: Booleano

Descrizione: (Facoltativo) Determina se si desidera consentire Instance Metadata Service versione 1 (IMDSv1) e IMDSv2.

- KeyName

Tipo: stringa

Descrizione: (Facoltativo) Il nome chiave per le istanze.

- NodeAutoScalingGroupDesiredCapacity

Tipo: stringa

Descrizione: (Facoltativo) Il numero di nodi che il gruppo di nodi deve mantenere.

- NodeAutoScalingGroupMaxSize

Tipo: stringa

Descrizione: (Facoltativo) Il numero massimo di nodi fino a cui il gruppo di nodi può scalare orizzontalmente.

- NodeAutoScalingGroupMinSize

Tipo: stringa

Descrizione: (Facoltativo) Il numero minimo di nodi in cui il gruppo di nodi può scalare.

- NodeInstanceType

Tipo: stringa

Impostazione predefinita: t3.large

Descrizione: (Facoltativo) Il tipo di istanza che desideri utilizzare per il gruppo di nodi.

- NodeImageId

Tipo: stringa

Descrizione: (Facoltativo) L'ID del Amazon Machine Image (AMI) che desiderate venga utilizzato dal gruppo di nodi.

- NodeImageIdSSMParam

Tipo: stringa

Predefinito: `/aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id`

Descrizione: (Facoltativo) Il parametro pubblico di Systems Manager AMI che si desidera venga utilizzato dal gruppo di nodi.

- `StackName`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome dello AWS CloudFormation stack utilizzato per aggiornare il gruppo di nodi.

- `Sottoreti`

Tipo: stringa

Descrizione: (Obbligatorio) Un elenco separato da virgole delle IDs sottoreti che desideri vengano utilizzate dal cluster.

- `VpcId`

Tipo: stringa

Impostazione predefinita: Default

Descrizione: (Obbligatorio) Il cloud privato virtuale (VPC) in cui viene distribuito il cluster.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks>DeleteNodegroup`
- `eks>DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`

- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

Fasi del documento

- `aws:executeScript`- Aggiorna un gruppo di nodi del cluster Amazon EKS in base ai valori specificati per i parametri di input del runbook.
- `aws:waitForAwsResourceProperty`- Attende che venga restituito lo stato di aggiornamento dello AWS CloudFormation stack.

AWSSupport-SetupK8sApiProxyForEKS

Descrizione

Il runbook di automazione AWSSupport-SetupK8sApiProxy ForEks offre un modo per creare una AWS Lambda funzione che funge da proxy per effettuare chiamate API del piano di controllo all'endpoint del cluster Amazon Elastic Kubernetes Service. Funge da elemento costitutivo per i runbook che richiedono l'esecuzione di chiamate API del piano di controllo per automatizzare le attività e risolvere i problemi con un cluster Amazon EKS.

Important

Tutte le risorse create da questa automazione sono contrassegnate in modo che possano essere trovate facilmente. I tag utilizzati sono:

- `AWSSupport-SetupK8sApiProxyForEKS: true`

Note

- L'automazione è un runbook di supporto e non può essere eseguita come runbook autonomo. Viene richiamata come automazione secondaria per i runbook che richiedono chiamate API del piano di controllo al cluster Amazon EKS.
- Assicurati di eseguire l'Cleanupoperazione dopo l'uso per evitare di incorrere in costi indesiderati.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del cluster Amazon Elastic Kubernetes Service.

- Operazione

Tipo: stringa

Descrizione: (Obbligatoria) Operazione da eseguire: esegue il Setup provisioning della funzione Lambda nell'account, Cleanup disattiverà le risorse create durante la fase di configurazione.

Valori consentiti: | Setup Cleanup

Predefinito: Configurazione

- LambdaRoleArn

Tipo: stringa

Descrizione: (Facoltativo) L'ARN del ruolo IAM che consente alla AWS Lambda funzione di accedere ai servizi e alle risorse AWS richiesti. Se non viene specificato alcun ruolo, questa Systems Manager Automation creerà un ruolo IAM per Lambda nel tuo account con il nome `Automation-K8sProxy-Role-<ExecutionId>` che include le politiche gestite: `AWSLambdaBasicExecutionRole` e `AWSLambdaVPCLambdaAccessExecutionRole`

Come funziona?

Il runbook esegue i seguenti passaggi:

- Verifica che l'automazione sia in esecuzione come esecuzione secondaria. Il runbook non funzionerà se richiamato come runbook autonomo poiché non esegue alcun lavoro significativo da solo.
- Verifica AWS CloudFormation lo stack esistente per la funzione proxy Lambda per il cluster specificato.
 - Se lo stack esiste, l'infrastruttura esistente viene riutilizzata anziché ricrearla.
 - Un contatore di riferimento viene gestito utilizzando tag per garantire che un runbook non elimini l'infrastruttura se viene riutilizzata da un altro runbook per lo stesso cluster.
- Esegui il tipo di operazione (Setup/Cleanup) specificato per la chiamata:
 - Configurazione: crea o descrive le risorse esistenti.

Pulizia: rimuove le risorse assegnate, se l'infrastruttura non viene utilizzata da nessun altro runbook.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede che le seguenti autorizzazioni non vengano passate `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`

Quando `LambdaRoleArn` viene fornita, non è necessario che l'automazione crei il ruolo e possono essere escluse le seguenti autorizzazioni:

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

Di seguito è riportato un esempio di policy che dimostra le autorizzazioni richieste `AutomationAssumeRole` quando non `LambdaRoleArn` vengono concesse:

```
{
  "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:<partition>:iam::<account-id>:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "AllowCreateRoleWithRequiredTag"
  },
  {
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
      }
    },
    "Action": [
      "iam:DeleteRole",
      "iam:TagRole",
      "iam:UntagRole"
    ],
    "Resource": [
      "arn:<partition>:iam::<account-id>:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "IAMActions"
  },
  {
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
      },
      "StringLike": {
        "iam:PolicyARN": [
          "arn:<partition>:iam::<partition>:policy/service-role/
AWSLambdaBasicExecutionRole",
          "arn:<partition>:iam::<partition>:policy/service-role/
AWSLambdaVPCLAccessExecutionRole"

```

```

    ]
  }
},
"Action": [
  "iam:AttachRolePolicy",
  "iam:DetachRolePolicy"
],
"Resource": [
  "arn:<partition>:iam::<account-id>::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:<partition>:lambda::<region-id>::<account-id>::function:Automation-K8sProxy*",
  "Effect": "Allow",
  "Sid": "LambdaActions"
},
{
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
    }
  },
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:<partition>:cloudformation::<region-id>::<account-id>::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:<partition>:logs::<region-id>::<account-id>:log-group:/aws/lambda/Automation-K8sProxy*",
      "arn:<partition>:logs::<region-id>::<account-id>:log-group:/aws/lambda/Automation-K8sProxy*:*"
    ],
    "Effect": "Allow",
    "Sid": "LogsActions"
  },
  {
    "Condition": {
      "StringLikeIfExists": {
        "iam:PassedToService": "lambda.amazonaws.com"
      }
    },
    "Action": [
      "iam:PassRole"
    ],
    "Resource": [
      "arn:<partition>:iam::<account-id>:role/Automation-K8sProxy-Role*"
    ],
    "Effect": "Allow",
    "Sid": "PassRoleToLambda"
  }
]
}

```

Nel caso in cui `LambdaRoleArn` venga approvata, assicurati che sia associata una [AWSLambdaBasicExecutionRole](#) policy per i cluster pubblici e, in aggiunta, [AWSLambdaVPCLambdaAccessExecutionRole](#) per i cluster privati.

Risorse create

Le seguenti risorse vengono create durante il Setup funzionamento:

1. AWS Lambda funzione
2. Ruolo IAM: ruolo di esecuzione Lambda, se non fornito.
3. CloudWatch Gruppo di log (Lambda Logs)

La funzione Lambda e il ruolo di esecuzione vengono mantenuti fino all'esecuzione *Cleanup* dell'operazione. Il gruppo di log Lambda verrà conservato per 30 giorni o fino all'eliminazione manuale.

Istruzioni

Il runbook è un'utilità di supporto progettata per essere eseguita da altri runbook come automazione secondaria. Facilita la creazione di un'infrastruttura che consente al runbook principale di effettuare chiamate API del piano di controllo Amazon EKS K8s. Per utilizzare il runbook, puoi seguire i passaggi seguenti dal contesto dell'automazione principale.

1. Fase di configurazione: richiama l'automazione utilizzando l'operazione di `aws:executeAutomation` azione dal runbook che desidera effettuare chiamate API del piano di controllo Amazon EKS K8s con l'operazione impostata su. Setup

Esempio di parametri di input:

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Setup"
}
```

L'output del `aws:executeAutomation` passaggio conterrà l'ARN della funzione proxy Lambda.

2. Utilizzo del proxy Lambda: richiama la funzione Lambda all'interno dell'`aws:executeScriptazione` utilizzando `boto3's Lambda.Client.invoke(...)` con un elenco di percorsi di chiamata API e token bearer. La funzione Lambda eseguirà GET

chiamate HTTP al percorso specificato passando il token bearer come parte dell'intestazione di autorizzazione.

Esempio di evento invoke Lambda:

```
{
  "ApiCalls": ["/api/v1/pods/", ...],
  "BearerToken": "..."
```

Note

Il token bearer deve essere generato come parte dello script di automazione principale. Devi assicurarti che il principale che esegue il runbook principale disponga dell'autorizzazione di sola lettura per il cluster Amazon EKS specificato.

3. Fase di pulizia: richiama l'automazione utilizzando l'operazione di `aws:executeAutomation` azione dal runbook che desidera effettuare chiamate API del piano di controllo Amazon EKS K8s con l'operazione impostata su. `Cleanup`

Esempio di parametri di input:

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Cleanup"
}
```

Fasi di automazione

1. ValidateExecution

- Verifica che l'automazione non sia in esecuzione come esecuzione autonoma.

2. CheckForExistingStack

- Verifica se è già stato fornito uno AWS CloudFormation stack per il nome del cluster specificato.
- Restituisce lo stato di esistenza dello stack e se è sicuro eliminarlo.

3. BranchOnIsStackExists

- Fase decisionale che si ramifica in base all'esistenza dello stack.

- Percorsi per aggiornare il nome dello stack esistente o procedere con la ramificazione dell'operazione.

4. UpdateStackName

- Aggiorna la StackName variabile con il nome dello stack esistente.
- Eseguito solo se lo stack esiste già.

5. BranchOnOperation

- Instrada l'automazione in base al Operation parametro (Setup/Cleanup).
- PerSetup: percorsi per creare un nuovo stack o descrivere risorse esistenti.
- PerCleanup: procede all'eliminazione dello stack se l'eliminazione è sicura.

6. GetClusterNetworkConfig

- Descrive il cluster Amazon EKS per ottenere la configurazione VPC.
- Recupera endpoint, ID VPC, sottorete IDs, ID del gruppo di sicurezza e dati CA.

7. ProvisionResources

- Crea uno AWS CloudFormation stack con le risorse richieste.
- Fornisce la funzione Lambda con la configurazione di rete necessaria.
- Contrassegna tutte le risorse per il monitoraggio e la gestione.

8. DescribeStackResources

- Recupera informazioni sullo stack creato/esistente.
- Ottiene l'ARN della funzione Lambda fornita.

9. BranchOnIsLambdaDeploymentRequired

- Determina se è necessaria la distribuzione del codice Lambda.
- Procede solo alla distribuzione degli stack appena creati.

10. DeployLambdaFunctionCode

- Distribuisce il codice della funzione Lambda utilizzando il pacchetto di distribuzione.
- Aggiorna la funzione con l'implementazione del proxy.

11. AssertLambdaAvailable

- Verifica che l'aggiornamento del codice della funzione Lambda abbia avuto successo.
- Attende che la funzione sia attiva. Successful

12. PerformStackCleanup

- Elimina lo AWS CloudFormation stack e le risorse associate.

- Eseguito durante il Cleanup funzionamento o in caso di fallimento dell' Setupoperazione.

Output

LambdaFunctionArn: ARN della funzione proxy Lambda

Riferimenti

Systems Manager Automation

- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Flussi di lavoro di Support Automation](#)

AWSSupport-TroubleshootEbsCsiDriversForEks

Descrizione

Il AWSSupport-TroubleshootEbsCsiDriversForEks runbook aiuta a risolvere i problemi relativi ai montaggi di volumi Amazon Elastic Block Store nei driver Amazon Elastic Kubernetes Service (Amazon EKS) e Amazon EBS Container Storage Interface (CSI)

Important

Attualmente il driver Amazon EBS CSI su cui è in esecuzione non AWS Fargate è supportato.

Come funziona?

Il runbook AWSSupport-TroubleshootEbsCsiDriversForEks esegue i seguenti passaggi di alto livello:

- Verifica se il cluster Amazon EKS di destinazione esiste ed è in stato attivo.
- Implementa le risorse di autenticazione necessarie per effettuare chiamate all'API Kubernetes a seconda che l'addon sia gestito da Amazon EKS o autogestito.
- Esegue controlli e diagnostiche dello stato del controller Amazon EBS CSI.
- Esegue controlli delle autorizzazioni IAM sui ruoli dei nodi e sui ruoli degli account di servizio.
- Diagnostica i problemi persistenti di creazione di volumi per il pod dell'applicazione specificato.

- Controlla la node-to-pod pianificazione ed esamina gli eventi del pod.
- Raccoglie i log pertinenti di Kubernetes e delle applicazioni, caricandoli nel bucket Amazon S3 specificato.
- Esegue controlli dello stato dei nodi e verifica la connettività con gli EC2 endpoint Amazon.
- Verifica lo stato di montaggio e gli allegati dei dispositivi a blocchi di volume persistenti.
- Pulisce l'infrastruttura di autenticazione creata durante la risoluzione dei problemi.
- Genera un rapporto completo sulla risoluzione dei problemi che combina tutti i risultati diagnostici.

Note

- La modalità di autenticazione del cluster Amazon EKS deve essere impostata su API oAPI_AND_CONFIG_MAP. Ti consigliamo di utilizzare Amazon EKS Access entry. Il runbook richiede le autorizzazioni RBAC (Kubernetes Role-based Access Control) per eseguire le chiamate API necessarie.
- Se non specifichi un ruolo IAM per la funzione Lambda (`LambdaRoleArn` parametro), l'automazione crea un ruolo denominato `Automation-K8sProxy-Role-<ExecutionId>` nel tuo account. Questo ruolo include le politiche gestite `AWSLambdaBasicExecutionRole` e `AWSLambdaVPCLambdaAccessExecutionRole`.
- Alcuni passaggi diagnostici richiedono che i nodi di lavoro di Amazon EKS siano istanze gestite da Systems Manager. Se i nodi non sono istanze gestite da Systems Manager, i passaggi che richiedono l'accesso a Systems Manager vengono ignorati, ma gli altri controlli continuano.
- L'automazione include una fase di pulizia che rimuove le risorse dell'infrastruttura di autenticazione. Questa fase di pulizia viene eseguita anche quando i passaggi precedenti falliscono, il che aiuta a evitare che le risorse rimangano orfane nell'account. AWS

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Crea un ruolo di automazione SSM `TroubleshootEbsCsiDriversForEks-SSM-Role` nel tuo account. Verifica che la relazione di trust includa la policy seguente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Allega la seguente policy al ruolo IAM per concedere le autorizzazioni necessarie per eseguire le azioni specificate sulle risorse specificate.

- Se prevedi di caricare i log di esecuzione e delle risorse nel bucket Amazon S3 nella AWS stessa regione, `arn:{partition}:s3:::BUCKET_NAME/*` sostituiscili con i tuoi. `OptionalRestrictPutObjects`
- Il bucket Amazon S3 dovrebbe puntare al bucket Amazon S3 corretto se si seleziona l'esecuzione SSM. `S3BucketName`
- Questa autorizzazione è facoltativa se non lo specifichi `S3BucketName`
- Il bucket Amazon S3 deve essere privato e nella stessa AWS regione in cui si esegue l'automazione SSM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OptionalRestrictPutObjects",
      "Effect": "Allow",
      "Action": ["s3:PutObject"],
      "Resource": ["arn:{partition}:s3:::BUCKET_NAME/*"]
    }
  ]
}
```



```

    },
    {
      "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:*:iam::*:role/TroubleshootEbsCsiDriversForEks-SSM-Role",
        "arn:*: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. Concedi le autorizzazioni richieste per il cluster Amazon EKS RBAC (Role-Based Access Control). L'approccio consigliato consiste nel creare un Access Entry nel cluster Amazon EKS.

Nella console Amazon EKS, accedi al tuo cluster. Per le voci di accesso ad Amazon EKS, verifica che la configurazione di accesso sia impostata su API_AND_CONFIG_MAP o API. Per i passaggi per configurare la modalità di autenticazione per le voci di accesso, consulta [Configurazione delle voci di accesso](#).

Seleziona Crea voce di accesso.

- Per l'ARN principale IAM, seleziona il ruolo IAM che hai creato per l'automazione SSM nel passaggio precedente.
- Per Tipo, seleziona. Standard

4. Aggiungi una politica di accesso:

- Per Ambito di accesso, selezionare `Cluster`.
- Per Nome della politica, selezionare `AmazonEKSAAdminViewPolicy`.

Scegli Aggiungi policy.

Se non utilizzi le voci di accesso per gestire le autorizzazioni dell'API Kubernetes, devi aggiornare `aws-auth ConfigMap` e creare un'associazione di ruolo tra l'utente o il ruolo IAM. Assicurati che la tua entità IAM disponga delle seguenti autorizzazioni API Kubernetes di sola lettura:

- `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. [Esegui l'automazione \(console\) AWSsupport-TroubleshootEbsCsiDriversForEks](#)

6. Seleziona `Execute automation` (Esegui automazione).

7. Per i parametri di input, inserisci quanto segue:

- `AutomationAssumeRole` (Facoltativo):
 - Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a SSM Automation di eseguire le azioni per tuo conto. Il ruolo deve essere aggiunto alla voce di accesso al cluster Amazon EKS o all'autorizzazione RBAC per consentire le chiamate API Kubernetes.
 - Tipo: `AWS::IAM::Role::Arn`
 - Esempio: `TroubleshootEbsCsiDriversForEks-SSM-Role`
- `EksClusterName`:
 - Descrizione: il nome del cluster Amazon Elastic Kubernetes Service (Amazon EKS) di destinazione.
 - Tipo: `String`
- `ApplicationPodName`:

- **Descrizione:** il nome del pod dell'applicazione Kubernetes che presenta problemi con il driver CSI di Amazon EBS.
- **Tipo:** String
- **ApplicationNamespace:**
 - **Descrizione:** lo spazio dei nomi Kubernetes per il pod dell'applicazione presenta problemi con il driver CSI di Amazon EBS.
 - **Tipo:** String
- **EbsCsiControllerDeploymentName (Facoltativo):**
 - **Descrizione:** (Facoltativo) Il nome di distribuzione per il pod controller CSI di Amazon EBS.
 - **Tipo:** String
 - **Impostazione predefinita:** `ebs-csi-controller`
- **EbsCsiControllerNamespace (Facoltativo):**
 - **Descrizione:** (Facoltativo) Lo spazio dei nomi Kubernetes per il controller pod Amazon EBS CSI.
 - **Tipo:** String
 - **Impostazione predefinita:** `kube-system`
- **BucketName S3 (opzionale):**
 - **Descrizione:** (Facoltativo) Il nome del bucket Amazon S3 di destinazione in cui verranno caricati i log di risoluzione dei problemi.
 - **Tipo:** `AWS::S3::Bucket::Name`
- **LambdaRoleArn (Facoltativo):**
 - **Descrizione:** (Facoltativo) L'ARN del ruolo IAM che consente alla AWS Lambda funzione di accedere ai AWS servizi e alle risorse richiesti.
 - **Tipo:** `AWS::IAM::Role::Arn`

Seleziona Esegui.

8. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione.

Riferimenti

Systems Manager Automation

- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Flussi di lavoro di Support Automation](#)

Per ulteriori informazioni su Amazon EBS CSI Driver, consulta [Amazon EBS CSI Driver](#).

Elastic Beanstalk

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Elastic Beanstalk
Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-CollectElasticBeanstalkLogs](#)
- [AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming](#)
- [AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications](#)
- [AWSSupport-TroubleshootElasticBeanstalk](#)

AWSSupport-CollectElasticBeanstalkLogs

Descrizione

Il AWSSupport-CollectElasticBeanstalkLogs runbook raccoglie i file di log AWS Elastic Beanstalk correlati da un'Windows Serveristanza Amazon Elastic Compute Cloud (Amazon EC2) lanciata da Elastic Beanstalk per aiutarti a risolvere i problemi più comuni. Mentre l'automazione raccoglie i file di log associati, vengono apportate modifiche alla struttura del file system, tra cui la creazione di directory temporanee, la copia dei file di registro nelle directory temporanee e la compressione dei file di registro in un archivio. Questa attività può comportare un aumento CPUUtilization sull' EC2 istanza Amazon. Per ulteriori informazioniCPUUtilization, consulta le [metriche delle istanze](#) nella Amazon CloudWatch User Guide.

Se specifichi un valore per il S3BucketName parametro, l'automazione valuta lo stato della policy del bucket Amazon Simple Storage Service (Amazon S3) che hai specificato. Per contribuire alla sicurezza dei log raccolti dalla tua EC2 istanza Amazon, se lo stato della policy isPublic è impostato su o se l'elenco di controllo degli accessi (ACL) concede READ|WRITE le autorizzazioni al gruppo predefinito di Amazon S3A11 Users, i log non vengono caricati. true Per ulteriori

informazioni sui gruppi predefiniti di Amazon S3, consulta i gruppi predefiniti di [Amazon S3 nella Guida per l'utente](#) di Amazon Simple Storage Service.

Se non specifichi un valore per il `S3BucketName` parametro, l'automazione carica il pacchetto di log nel bucket Elastic Beanstalk Amazon S3 predefinito nel punto in cui esegui l'automazione. Regione AWS La directory viene denominata in base alla seguente struttura,. `elasticbeanstalk-region - accountId accountId` I valori `region` and differiranno in base alla regione in Account AWS cui viene eseguita l'automazione. Il pacchetto di log verrà salvato nella `resources/environments/logs/bundle/ environmentID / instanceID` directory. `instanceID` I valori `environmentID` and differiranno in base al tuo ambiente Elastic Beanstalk e all'istanza Amazon da cui stai raccogliendo EC2 i log.

Per impostazione predefinita, il profilo dell'istanza AWS Identity and Access Management (IAM) collegato alle EC2 istanze Amazon dell'ambiente Elastic Beanstalk dispone delle autorizzazioni necessarie per caricare il pacchetto nel bucket Elastic Beanstalk Amazon S3 predefinito per il tuo ambiente. Se specifichi un valore per il `S3BucketName` parametro, il profilo dell'istanza collegato all' EC2istanza Amazon deve consentire le `s3:PutObject` azioni `s3:GetBucketAcl`, `s3:GetBucketPolicies` `s3:GetBucketPolicyStatus`, e per il bucket e il percorso Amazon S3 specificati.

Note

Questa automazione richiede almeno 500 MB di spazio su disco disponibile sul volume root Amazon Elastic Block Store (Amazon EBS) collegato alla tua istanza Amazon. EC2 Se lo spazio su disco disponibile sul volume principale non è sufficiente, l'automazione si interrompe.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EnvironmentId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ambiente Elastic Beanstalk da cui desideri raccogliere il pacchetto di log.

- InstanceId

Tipo: stringa

(Obbligatorio) L'ID dell' EC2 istanza Amazon nell'ambiente Elastic Beanstalk da cui desideri raccogliere il pacchetto di log.

- S3 BucketName

Tipo: stringa

(Facoltativo) Il bucket Amazon S3 in cui desideri caricare i log archiviati.

- S3 BucketPath

Tipo: stringa

(Facoltativo) Il percorso del bucket di Amazon S3 in cui desideri caricare il pacchetto di log. Questo parametro viene ignorato se non si specifica un valore per il parametro. S3BucketName

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che l' EC2 istanza Amazon specificata nel `InstanceId` parametro è gestita da AWS Systems Manager.
- `aws:assertAwsResourceProperty`- Conferma che l' EC2 istanza Amazon specificata nel `InstanceId` parametro è un'Windows Serveristanza.
- `aws:runCommand`- Verifica se l'istanza fa parte di un ambiente Elastic Beanstalk, se c'è spazio su disco sufficiente per raggruppare i log e se il bucket Amazon S3 in cui verranno caricati i log è pubblico.
- `aws:runCommand`- Raccoglie i file di log e carica l'archivio nel bucket Amazon S3 specificato nel parametro o nel bucket predefinito per `S3BucketName` l'ambiente Elastic Beanstalk se non viene specificato un valore.

AWSConfigRemediation- EnableElasticBeanstalkEnvironmentLogStreaming

Descrizione

Il `AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming` runbook consente la registrazione sull'ambiente AWS Elastic Beanstalk (Elastic Beanstalk) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- EnvironmentId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ambiente Elastic Beanstalk a cui desideri abilitare l'accesso.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

Fasi del documento

- aws:executeAwsApi- Abilita la registrazione sull'ambiente Elastic Beanstalk specificato nel parametro. EnvironmentId
- aws:waitForAwsResourceProperty- Attende che lo stato dell'ambiente cambi a. Ready
- aws:executeScript- Verifica che la registrazione sia stata abilitata nell'ambiente Elastic Beanstalk.

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

Descrizione

Il AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications runbook abilita le notifiche per l'ambiente AWS Elastic Beanstalk (Elastic Beanstalk) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- EnvironmentId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ambiente Elastic Beanstalk per cui desideri abilitare le notifiche.

- TopicArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN dell'argomento Amazon Simple Notification Service (Amazon SNS) a cui desideri inviare le notifiche.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Fasi del documento

- `aws:executeAwsApi`- Abilita le notifiche per l'ambiente Elastic Beanstalk specificato nel parametro. `EnvironmentId`
- `aws:waitForAwsResourceProperty`- Attende che lo stato dell'ambiente cambi a. `Ready`
- `aws:executeScript`- Verifica che le notifiche siano state abilitate per l'ambiente Elastic Beanstalk.

AWSSupport-TroubleshootElasticBeanstalk

Descrizione

Il `AWSSupport-TroubleshootElasticBeanstalk` runbook ti aiuta a risolvere i potenziali motivi per cui l'ambiente si trova in uno stato o. `AWS Elastic Beanstalk Degraded Severe` Questa automazione controlla le seguenti AWS risorse associate all'ambiente Elastic Beanstalk:

- Dettagli di configurazione per un sistema di bilanciamento del carico, uno `AWS CloudFormation` stack, un gruppo `Amazon Auto EC2 Scaling`, istanze `Amazon Elastic Compute Cloud` (`EC2Amazon`) e cloud privato virtuale (`VPC`).
- Problemi di configurazione della rete con le regole dei gruppi di sicurezza associati, le tabelle di routing e le liste di controllo dell'accesso alla rete (`ACLs`) associate alle sottoreti.

- Verifica la connettività agli endpoint Elastic Beanstalk e l'accesso pubblico a Internet.
- Verifica lo stato del load balancer.
- Verifica lo stato delle EC2 istanze Amazon.
- Recupera un pacchetto di log dall'ambiente Elastic Beanstalk e, facoltativamente, carica i file in. Supporto

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ApplicationName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome dell'applicazione Elastic Beanstalk.

- EnvironmentName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome dell'ambiente Elastic Beanstalk.

- `AWSS3UploaderLink`

Tipo: stringa

Descrizione: (Facoltativo) Un URL che ti è stato fornito da Supporto per caricare il pacchetto di log dal tuo ambiente Elastic Beanstalk su. Questa opzione è disponibile solo per i clienti che hanno acquistato un Supporto piano e hanno aperto una richiesta di assistenza.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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*`

Fasi del documento

- `aws:executeScript`- Verifica che il principale AWS Identity and Access Management (IAM) che ha avviato l'automazione disponga delle autorizzazioni necessarie per eseguire tutte le azioni definite nel runbook.
- `aws:branch`- Suddivide il flusso di lavoro in base ai risultati del passaggio precedente.
- `aws:executeScript`- Raccoglie informazioni sull'ambiente Elastic Beanstalk, tra cui il load balancer AWS CloudFormation , lo stack, il gruppo Auto Scaling, le istanze Amazon e la configurazione VPC. EC2
- `aws:executeScript`- Verifica la presenza di problemi di connettività di rete con le tabelle di ACLs routing e associati alle sottoreti nel tuo VPC.
- `aws:executeScript`- Verifica la presenza di problemi di connettività di rete con le regole del gruppo di sicurezza associate alle tue EC2 istanze Amazon.
- `aws:executeScript`- Verifica i controlli di stato per le EC2 istanze Amazon.
- `aws:executeScript`- Genera un link per un pacchetto di log del tuo ambiente Elastic Beanstalk.
- `aws:executeScript`- Carica il pacchetto di log su. Supporto
- `aws:executeScript`- Genera un rapporto sulle azioni da intraprendere per aiutarti a risolvere i problemi che potrebbero influire sullo stato del tuo ambiente Elastic Beanstalk.

Sistema di bilanciamento del carico elastico

AWS Systems Manager L'automazione fornisce runbook predefiniti per Elastic Load Balancing. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSConfigRemediation-DropInvalidHeadersForALB](#)
- [AWS-EnableCLBAccessLogs](#)
- [AWS-EnableCLBConnectionDraining](#)
- [AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing](#)
- [AWSConfigRemediation-EnableELBDeletionProtection](#)

- [AWSConfigRemediation-EnableLoggingForALBAndCLB](#)
- [AWSSupport-TroubleshootCLBConnectivity](#)
- [AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing](#)
- [AWS-UpdateALBDesyncMitigationMode](#)
- [AWS-UpdateCLBDesyncMitigationMode](#)

AWSConfigRemediation-DropInvalidHeadersForALB

Descrizione

Il `AWSConfigRemediation-DropInvalidHeadersForALB` runbook consente all'application load balancer specificato di rimuovere le intestazioni HTTP con intestazioni non valide.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `LoadBalancerArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del load balancer da cui desideri eliminare le intestazioni non valide.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeAwsApi`- Abilita l'impostazione `drop invalid header` per il load balancer specificato nel parametro. `LoadBalancerArn`
- `aws:executeScript`- Verifica che l'impostazione `drop invalid headers` sia stata abilitata sul load balancer specificato nel parametro. `LoadBalancerArn`

AWS-EnableCLBAccessLogs

Descrizione

Il `AWS-EnableCLBAccessLogs` runbook abilita i log di accesso per un Classic Load Balancer.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EmitInterval

Tipo: integer

Valori validi: 5 | 60

Impostazione predefinita: 60

Descrizione: (Facoltativo) L'intervallo per la pubblicazione dei log di accesso in minuti.

- LoadBalancerNames

Tipo: stringa

Descrizione: (Obbligatorio) Un elenco separato da virgole di Classic Load Balancer per cui si desidera abilitare i log di accesso.

- S3 BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon Simple Storage Service (Amazon S3) in cui sono archiviati i log di accesso.

- S3 BucketPrefix

Tipo: stringa

Descrizione: (Facoltativo) La gerarchia logica che hai creato per il tuo bucket Amazon S3, ad esempio. my-bucket-prefix/prod Se il prefisso non è fornito, il log viene posizionato al livello root del bucket.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeAwsApi`- Abilita i log di accesso per i Classic Load Balancer specificati nel parametro. `LoadBalancerNames`

Output

Abilita i registri. `CLBAccess SuccessesLoadBalancers` - Elenco dei nomi dei sistemi di bilanciamento del carico in cui i log di accesso sono stati abilitati correttamente.

Abilita `CLBAccess` i registri. `FailedLoadBalancers` - `MapList` dei nomi dei sistemi di bilanciamento del carico in cui l'attivazione dei log di accesso non è riuscita e il motivo dell'errore.

AWS-EnableCLBConnectionDraining

Descrizione

Il `AWS-EnableCLBConnectionDraining` runbook consente il drenaggio della connessione su un Classic Load Balancer (CLB) fino al valore di timeout specificato. Il drenaggio delle connessioni consente al CLB di completare le richieste in corso inoltrate alle istanze che stanno annullando la registrazione o che non sono funzionanti, con il timeout specificato che indica il momento in cui mantiene attive le connessioni prima di segnalare l'annullamento della registrazione dell'istanza. Per ulteriori informazioni sull'esaurimento della connessione su CLB, consulta [Configurare il drenaggio della connessione per Classic Load Balancer](#) nella Guida utente per Classic Load Balancer.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- LoadBalancerName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del sistema di bilanciamento del carico su cui si desidera abilitare il drenaggio della connessione.

- ConnectionTimeout

Tipo: integer

Valori validi: 1-3600

Impostazione predefinita: 300

Descrizione: (Obbligatorio) Il valore di timeout della connessione per il sistema di bilanciamento del carico. Il valore di timeout può essere impostato tra 1 e 3600 secondi.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

Fasi del documento

- `ModifyLoadBalancerConnectionDraining` (aws:executeAwsApi): Abilita il drenaggio della connessione e imposta il valore di timeout specificato per il sistema di bilanciamento del carico specificato.
- `VerifyLoadBalancerConnectionDrainingEnabled`(aws: assertAwsResource Property): verifica che il drenaggio della connessione sia abilitato per il load balancer.
- `VerifyLoadBalancerConnectionDrainingTimeout`(aws: assertAwsResource Property): verifica che il valore di timeout della connessione per il sistema di bilanciamento del carico corrisponda al valore specificato.

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

Descrizione

Il `AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` runbook consente il bilanciamento del carico tra zone per il Classic Load Balancer (CLB) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- **LoadBalancerName**

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del CLB su cui desideri abilitare il bilanciamento del carico tra zone.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeAwsApi`- Abilita il bilanciamento del carico tra zone per il CLB specificato nel parametro. `LoadBalancerName`
- `aws:assertAwsResourceProperty`- Verifica che il bilanciamento del carico tra zone sia stato abilitato sul CLB.

AWSConfigRemediation-EnableELBDeletionProtection

Descrizione

Il `AWSConfigRemediation-EnableELBDeletionProtection` runbook abilita la protezione dall'eliminazione per l'elastic load balancer (ELB) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- LoadBalancerArn

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) dell'ELB su cui desideri abilitare la protezione da eliminazione.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:ModifyLoadBalancerAttributes

Fasi del documento

- aws:executeScript- Abilita la protezione da eliminazione sull'ELB specificato nel LoadBalancerArn parametro.

AWSConfigRemediation-EnableLoggingForALBAndCLB

Descrizione

Il AWSConfigRemediation-EnableLoggingForALBAndCLB runbook consente la registrazione per l' AWS Application Load Balancer o un Classic Load Balancer (CLB) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- LoadBalancerId

Tipo: stringa

Descrizione: (Obbligatorio) Il nome Classic Load Balancer o l'Application Load Balancer ARN.

- S3 BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3.

- S3 BucketPrefix

Tipo: stringa

Descrizione: (Facoltativo) La gerarchia logica che hai creato per il tuo bucket Amazon Simple Storage Service (Amazon S3), ad esempio. `my-bucket-prefix/prod` Se il prefisso non è fornito, il log viene posizionato al livello root del bucket.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeScript`- Abilita e verifica la registrazione per Classic Load Balancer o Application Load Balancer.

AWSSupport-TroubleshootCLBConnectivity

Descrizione

Il `AWSSupport-TroubleshootCLBConnectivity` runbook ti aiuta a risolvere i problemi di connettività tra istanze Classic Load Balancer (CLB) e Amazon Elastic Compute Cloud (Amazon) EC2. Inoltre, vengono esaminati i problemi di connettività tra un client e il CLB. Questo runbook esamina anche i controlli sanitari del CLB, verifica che vengano seguite le migliori pratiche e crea una dashboard per la risoluzione dei problemi. Facoltativamente, puoi caricare l'output di automazione in un bucket Amazon Simple Storage Service (Amazon S3). Tuttavia, questo runbook non supporta il caricamento dell'output su bucket S3 accessibili al pubblico. Ti consigliamo di creare un bucket S3 temporaneo per questa automazione.

Important

L'utilizzo di questo runbook potrebbe comportare costi per la dashboard creata. Per ulteriori informazioni, consulta la pagina [CloudWatch dei prezzi di Amazon](#)

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InvestigationType

Tipo: stringa

Valori validi: Best practice | Problemi di connettività | Dashboard per la risoluzione dei problemi

Descrizione: (Obbligatorio) Le operazioni che si desidera vengano eseguite dal runbook.

- LoadBalancerName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del CLB.

- S3Location

Tipo: stringa

Descrizione: (Facoltativo) Il nome del bucket S3 a cui desideri inviare i risultati dell'automazione. I bucket accessibili pubblicamente non sono supportati. Se il bucket S3 utilizza la crittografia lato

server, l'utente o il ruolo che esegue questa automazione deve disporre `kms:GenerateDataKey` delle autorizzazioni per la chiave. AWS KMS

- `S3 LocationPrefix`

Tipo: stringa

Descrizione: (Facoltativo) Il prefisso chiave di Amazon S3 (sottocartella) in cui desideri caricare l'output dell'automazione. Il formato di output è memorizzato nel seguente formato: `amzn-s3-demo-bucket/S3LocationPrefix/{{}} _ {{automation:}} .txt. InvestigationType EXECUTION_ID`

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

- `aws:executeScript`- Verifica che il CLB specificato nel parametro esista. `LoadBalancerName`
- `aws:branch`- Rami basati sul valore specificato per il `InvestigationType` parametro.
- `aws:executeScript`- Esegue controlli di connettività al CLB.
- `aws:executeScript`- Verifica che la configurazione CLB sia conforme alle best practice di Elastic Load Balancing.
- `aws:executeScript`- Crea una CloudWatch dashboard Amazon per il tuo CLB.
- `aws:executeScript`- Crea un file di testo con i risultati dell'automazione e lo carica nel bucket Amazon S3 specificato nel parametro. `S3Location`

Output

`RunBestPractices.Riepilogo`

`RunConnectivityChecks.Riepilogo`

`CreateTroubleshootingDashboard.Uscita`

`UploadOutputToS3. Uscita`

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

Descrizione

Il `AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` runbook abilita il bilanciamento del carico tra zone per il sistema di bilanciamento del carico di rete (NLB) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `LoadBalancerArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) dell'NLB su cui desideri abilitare il bilanciamento del carico tra zone.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `aws:executeAwsApi`- Abilita il bilanciamento del carico tra zone per l'NLB specificato nel parametro. `LoadBalancerArn`
- `aws:executeScript`- Verifica che il bilanciamento del carico tra zone sia stato abilitato sull'NLB.

AWS-UpdateALBDesyncMitigationMode

Descrizione

Il `AWS-UpdateALBDesyncMitigationMode` runbook aggiornerà la modalità di mitigazione della desincronizzazione su un Application Load Balancer (ALB) alla modalità di mitigazione specificata. La modalità di mitigazione della sincronizzazione determina il modo in cui il load balancer gestisce le richieste che potrebbero rappresentare un rischio per la sicurezza dell'applicazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `LoadBalancerArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) dell'ALB di cui desideri modificare la modalità di mitigazione del desync.

- `DesyncMitigationMode`

Tipo: stringa

Valori validi: monitor | defensive | strictest

Descrizione: (Obbligatoria) La modalità di mitigazione che si desidera utilizzare con ALB. Per informazioni sulle modalità di mitigazione della desincronizzazione, consulta la modalità di mitigazione di [Desync nella Guida utente per Application Load Balancers](#).

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `VerifyLoadBalancerType` (aws: assertAwsResource Property): verifica che il valore specificato per il parametro di `LoadBalancerArn` input sia per un sistema di bilanciamento del carico delle applicazioni prima di procedere al passaggio successivo.
- `ModifyLoadBalancerDesyncMode` (aws:executeAwsApi) - Aggiorna l'ALB per utilizzare quanto specificato. `DesyncMitigationMode`
- `VerifyLoadBalancerDesyncMitigationMode` (aws:ExecuteScript) - Verifica che la modalità di mitigazione della desincronizzazione sia stata aggiornata per l'ALB di destinazione.

Output

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Caricamento del messaggio dello script che verifica la modifica al tuo ALB.

AWS-UpdateCLBDesyncMitigationMode

Descrizione

Il AWS-UpdateCLBDesyncMitigationMode runbook aggiornerà la modalità di mitigazione della desincronizzazione su un Classic Load Balancer (CLB) alla modalità di mitigazione specificata. La modalità di mitigazione della sincronizzazione determina il modo in cui il load balancer gestisce le richieste che potrebbero rappresentare un rischio per la sicurezza dell'applicazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- LoadBalancerName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del CLB di cui si desidera modificare la modalità di mitigazione della desincronizzazione.

- `DesyncMitigationMode`

Tipo: stringa

Valori validi: `monitor` | `defensive` | `strictest`

Descrizione: (Obbligatoria) La modalità di mitigazione che desideri venga utilizzata dal CLB. Per informazioni sulle modalità di mitigazione della desincronizzazione, consultate la modalità di mitigazione di [Desync nella Guida utente per Application Load Balancers](#).

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Fasi del documento

- `ModifyLoadBalancerDesyncMode` (`aws:executeAwsApi`) - Aggiorna il CLB per utilizzare quanto specificato. `DesyncMitigationMode`
- `VerifyLoadBalancerDesyncMitigationMode` (`aws:ExecuteScript`) - Verifica che la modalità di mitigazione della desincronizzazione sia stata aggiornata per il CLB di destinazione.

Output

`VerifyLoadBalancerDesyncMitigationMode`. `ModificationResult` - Caricamento del messaggio dello script che verifica la modifica al CLB.

Amazon EMR

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon EMR. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-AnalyzeEMRLogs](#)
- [AWSSupport-DiagnoseEMRLogsWithAthena](#)

AWSSupport - AnalyzeEMRLogs

Descrizione

Questo runbook aiuta a identificare gli errori durante l'esecuzione di un job su un cluster Amazon EMR. Il runbook analizza un elenco di log definiti sul file system e cerca un elenco di parole chiave predefinite. Queste voci di registro vengono utilizzate per creare CloudWatch eventi Amazon Events in modo da poter intraprendere tutte le azioni necessarie in base agli eventi. Facoltativamente, il runbook pubblica le voci di registro nel gruppo di log Amazon CloudWatch Logs di tua scelta. Questo runbook attualmente cerca i seguenti errori e modelli nei file di registro:

- `container_out_of_memory` — Il contenitore YARN ha esaurito la memoria, l'esecuzione del processo potrebbe non riuscire.
- `yarn_nodemanager_health`: il nodo CORE o TASK sta esaurendo lo spazio su disco e non sarà in grado di eseguire attività.
- `node_state_change`: il nodo CORE o TASK non è raggiungibile dal nodo MASTER.
- `step_failure`: Un passaggio EMR non è riuscito.
- `no_core_nodes_running`: Nessun nodo CORE è attualmente in esecuzione, il cluster non è integro.
- `hdfs_missing_blocks`: Mancano blocchi HDFS che potrebbero portare alla perdita di dati.
- `hdfs_high_util`: L'utilizzo di HDFS è elevato, il che può influire sui job e sullo stato del cluster.
- `instance_controller_restart`: il processo Instance-Controller è stato riavviato. Questo processo è essenziale per l'integrità del cluster.
- `instance_controller_restart_legacy`: il processo Instance-Controller è stato riavviato. Questo processo è essenziale per l'integrità del cluster.

- `high_load`: rilevata una media di carico elevata, può influire sulla segnalazione dello stato dei nodi o causare timeout o rallentamenti.
- `yarn_node_blacklisted`: il nodo CORE o TASK è stato inserito nella lista nera da YARN per impedire l'esecuzione delle attività.
- `yarn_node_lost`: il nodo CORE o TASK è stato contrassegnato come LOST da YARN, possibili problemi di connettività.

Le istanze associate a quello `ClusterID` specificato devono essere gestite da AWS Systems Manager. È possibile eseguire questa automazione una sola volta, pianificare l'automazione in modo che venga eseguita a un intervallo di tempo specifico o rimuovere una pianificazione creata in precedenza da un'automazione. Questo runbook supporta le versioni di Amazon EMR dalla 5.20 alla 6.30.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `ClusterID`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del cluster di cui si desidera analizzare i log dei nodi.

- Operazione

Tipo: stringa

Valori validi: Run Once | Schedule | Remove Schedule

Descrizione: (Obbligatoria) L'operazione da eseguire sul cluster.

- IntervalTime

Tipo: stringa

Valori validi: 5 minuti | 10 minuti | 15 minuti

Descrizione: (Facoltativo) L'intervallo di tempo che intercorre tra l'esecuzione dell'automazione. Questo parametro è applicabile solo se viene specificato Schedule per il Operation parametro.

- LogToCloudWatchLogs

Tipo: stringa

Valori validi: sì | no

Descrizione: (Facoltativo) Se si specifica yes il valore di questo parametro, l'automazione crea un gruppo di log CloudWatch Logs con il nome specificato nel CloudWatchLogGroup parametro per memorizzare tutte le voci di registro corrispondenti.

- CloudWatchLogGroup

Tipo: stringa

Descrizione: (Facoltativo) Il nome del gruppo di log CloudWatch Logs in cui si desidera memorizzare tutte le voci di registro corrispondenti. Questo parametro è applicabile solo se viene specificato yes per il LogToCloudWatchLogs parametro.

- CreateLogInsightsDashboard

Tipo: stringa

Valori validi: sì | no

Descrizione: (Facoltativo) Se si specificayes, la CloudWatch dashboard viene creata se non esiste già. Questo parametro è applicabile solo se viene specificato yes per il LogToCloudWatchLogs parametro.

- CreateMetricFilters

Tipo: stringa

Valori validi: sì | no

Descrizione: (Facoltativo) Specificate yes se desiderate creare filtri metrici per il gruppo di log CloudWatch Logs. Questo parametro è applicabile solo se si specifica yes per il LogToCloudWatchLogs parametro.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie informazioni sul cluster Amazon EMR specificato nel `ClusterID` parametro.
- `aws:branch`- Filiali basate sull'input.
 - Se l'operazione fornita è `Run Once` o `Schedule`:
 - `aws:assertAwsResourceProperty`- Verifica che il cluster sia disponibile.
 - `aws:executeAwsApi`- Raccoglie tutte le istanze in esecuzione nel cluster. IDs
 - `aws:assertAwsResourceProperty`- Verifica che l'agente SSM sia in esecuzione su tutte le istanze del cluster.
 - `aws:branch`- Filiali a seconda che tu abbia specificato di eseguire l'automazione una sola volta o in base a una pianificazione.
 - Se l'operazione fornita è `Run Once`:
 - `aws:branch`- Rami basati sul valore specificato nel `LogToCloudWatchLogs` parametro.
 - Se `LogToCloudWatchLogs` il valore è `yes`:

- `aws:executeScript`- Verifica se esiste CloudWatchLogGroup già un gruppo di log CloudWatch Logs con il nome specificato nel parametro. In caso contrario, il gruppo viene creato con il nome specificato.
- `aws:branch`- Rami basati sul valore specificato nel `CreateMetricFilters` parametro.
 - Se `CreateMetricFilters` il valore è `yes`:
 - `aws:executeAwsApi`- Vengono eseguiti 12 passaggi per ogni filtro metrico
 - `aws:branch`- Rami basati sul valore specificato nel `CreateLogInsightsDashboard` parametro.
 - Se `CreateLogInsightsDashboard` il valore è `yes`:
 - `aws:executeAwsApi`- Crea una CloudWatch dashboard con lo stesso nome specificato nel `CloudWatchLogGroup` parametro, se non esiste già.
 - Se `CreateLogInsightsDashboard` il valore è `no`:
 - `aws:runCommand`- Esegue uno script di shell per trovare modelli di registro su ogni istanza del cluster.
 - Se `CreateMetricFilters` il valore è `no`:
 - `aws:branch`- Rami basati sul valore specificato nel `CreateLogInsightsDashboard` parametro.
 - Se `CreateLogInsightsDashboard` il valore è `yes`:
 - `aws:executeAwsApi`- Crea una CloudWatch dashboard con lo stesso nome specificato nel `CloudWatchLogGroup` parametro, se non esiste già.
 - Se `CreateLogInsightsDashboard` il valore è `no`:
 - `aws:runCommand`- Esegue uno script di shell per trovare modelli di registro su ogni istanza del cluster.
 - Se `LogToCloudWatchLogs` il valore è `no`:
 - `aws:executeAwsApi`- Esegue uno script di shell per trovare modelli di registro su ogni istanza del cluster.
 - Se l'operazione fornita è `Schedule`:
 - `aws:createStack`- Crea un EventBridge evento Amazon destinato a questo runbook.
 - Se l'operazione fornita è `Remove Schedule`:
 - `aws:executeAwsApi`- Verifica l'esistenza di una pianificazione per il cluster.
 - `aws:deleteStack`- Elimina la pianificazione.

Output

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstances.Istanza IDs

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists.uscita

FindLogPatternOnEMRNode.CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

Descrizione

Il `AWSSupport-DiagnoseEMRLogsWithAthena` runbook aiuta a diagnosticare i log di Amazon EMR utilizzando Amazon Athena in integrazione con Data Catalog. AWS Glue Amazon Athena viene utilizzato per interrogare i file di log di Amazon EMR per contenitori, log dei nodi o entrambi, con parametri opzionali per intervalli di date specifici o ricerche basate su parole chiave.

Il runbook può recuperare automaticamente la posizione di log di Amazon EMR per un cluster esistente oppure puoi specificare la posizione di log di Amazon S3. Per analizzare i log, il runbook:

- Crea un AWS Glue database ed esegue query Amazon Athena Data Definition Language (DDL) sulla posizione di log Amazon EMR Amazon S3 per creare tabelle per i log del cluster e un elenco di problemi noti.
- Esegue query DML (Data Manipulation Language) per cercare modelli di problemi noti nei log di Amazon EMR. Le query restituiscono un elenco di problemi rilevati, il relativo numero di occorrenze e il numero di parole chiave corrispondenti in base al percorso del file Amazon S3.
- I risultati vengono caricati in un bucket Amazon S3 specificato sotto il prefisso.
`saw_diagnose_EMR_known_issues`
- Il runbook restituisce i risultati delle query di Amazon Athena, evidenziando risultati, consigli e riferimenti agli articoli di Amazon Knowledge Center (KC) provenienti da un sottoinsieme predefinito.
- In caso di completamento o errore, il AWS Glue database e i file dei problemi noti caricati nel bucket Amazon S3 vengono eliminati.

Come funziona?

AWSsupport-DiagnoseEMRLogsWithAthena esegui l'analisi dei log di Amazon EMR utilizzando Amazon Athena per rilevare errori ed evidenziare risultati, consigli e articoli pertinenti del Knowledge Center.

Il runbook esegue i seguenti passaggi:

- Ottieni la posizione del log del cluster Amazon EMR utilizzando l'ID del cluster o inserisci la posizione Amazon S3 per recuperare la posizione e le dimensioni del log.
- Fornisci una stima dei costi di Athena in base alla dimensione della posizione del registro.
- Ottieni l'approvazione per procedere richiedendo l'approvazione ai responsabili IAM designati prima di eseguire le query Athena e continuare con i passaggi successivi.
- Carica i problemi noti nel bucket Amazon S3 specificato, crea un AWS Glue database e tabelle.
- Esegui le query Athena sui dati dei log di Amazon EMR. Le query possono essere eseguite per intervallo di date, parole chiave, entrambi i criteri oppure essere eseguite senza filtri in base agli input forniti.
- Analizza i risultati per evidenziare i risultati, i consigli e gli articoli KC pertinenti.
- Link di output per i risultati delle query DML di Amazon Athena.
- Pulisci l'ambiente rimuovendo il database creato, le tabelle e i problemi noti caricati.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Il **AutomationAssumeRole** parametro richiede le seguenti azioni per utilizzare correttamente il runbook:

- atena: GetQueryExecution
- atena: StartQueryExecution
- atena: GetPreparedStatement

- atena: CreatePreparedStatement
- colla: GetDatabase
- colla: CreateDatabase
- colla: DeleteDatabase
- colla: CreateTable
- colla: GetTable
- colla: DeleteTable
- riduzione elastica della mappa: DescribeCluster
- s3: ListBucket
- s3: GetBucketVersioning
- s3: ListBucketVersions
- s3: GetBucketPublicAccessBlock
- s3: GetBucketPolicyStatus
- s3: GetObject
- s3: GetBucketLocation
- prezzi: GetProducts
- prezzi: GetAttributeValues
- prezzi: DescribeServices
- prezzi: ListPriceLists

 Important

Per limitare l'accesso solo alle risorse necessarie a questa automazione, collega la seguente policy al ruolo IAM che si fida del servizio SSM. Sostituisci Partition, Region e Account con i valori appropriati per la partizione, la regione e il numero di account in cui viene eseguito il runbook.

```
{
  "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:{Partition}:s3::*/*/results/*",
        "arn:{partition}:s3::*/*/saw_diagnose_emr_known_issues/*"
    ]
},
{
    "Sid": "RestrictDeleteAccess",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
    ],
    "Resource": [
        "arn:{Partition}:s3::*/*/saw_diagnose_emr_known_issues/*"
    ]
},

```

```

{
  "Effect": "Allow",
  "Action": [
    "glue:GetDatabase",
    "glue:CreateDatabase",
    "glue>DeleteDatabase"
  ],
  "Resource": [
    "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
    "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/**",
    "arn:{Partition}:glue:{Region}:{Account}:userDefinedFunction/
saw_diagnose_emr_database_*/**",
    "arn:{Partition}:glue:{Region}:{Account}:catalog"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "glue:CreateTable",
    "glue:GetTable",
    "glue>DeleteTable"
  ],
  "Resource": [
    "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
saw_diagnose_emr_known_issues",
    "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
saw_diagnose_emr_logs_table",
    "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
j_**",
    "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
    "arn:{Partition}:glue:{Region}:{Account}:catalog"
  ]
}
]
}

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Naviga [AWSSupport-DiagnoseEMRLogsWithAthena](#) nella AWS Systems Manager sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).

3. Per i parametri di input, inserisci quanto segue:

- AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterId (obbligatorio):

L'ID del cluster Amazon EMR.

- S3 LogLocation (opzionale):

La posizione del log Amazon S3 Amazon EMR. Inserisci la posizione Amazon S3 dell'URL in stile Path, ad esempio: `s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/`. Fornisci questo parametro se il cluster Amazon EMR è stato chiuso per più di giorni. 30

- S3 BucketName (richiesto):

Il nome del bucket Amazon S3 per caricare un elenco di problemi noti e l'output delle query Amazon Athena. Il bucket deve avere l'opzione [Block Public Access abilitata](#) e trovarsi nella stessa AWS regione e nello stesso account del cluster Amazon EMR.

- Approvatori (obbligatori):

L'elenco dei responsabili AWS autenticati che sono in grado di approvare o rifiutare l'azione. Puoi specificare i principali utilizzando uno dei seguenti formati: nome utente, ARN utente, ruolo IAM ARN o IAM assume il ruolo ARN. Il numero massimo di approvatori è 10.

- FetchNodeLogsOnly (Facoltativo):

Se impostato su `true`, l'automazione diagnostica i log dei contenitori delle applicazioni Amazon EMR. Il valore predefinito è `false`.

- FetchContainersLogsOnly (Facoltativo):

Se impostato su `true`, l'automazione diagnostica i log dei contenitori Amazon EMR. Il valore predefinito è `false`.

- EndSearchDate (Facoltativo):

La data di fine delle ricerche nei log. Se fornito, l'automazione cercherà esclusivamente i log generati fino alla data specificata nel formato YYYY-MM-DD (ad esempio: 2024-12-30).

- **DaysToCheck (Facoltativo):**

Quando `EndSearchDate` viene fornito, questo parametro è necessario per determinare il numero di giorni in cui cercare in modo retrospettivo i log tra quelli specificati. `EndSearchDate` Il valore massimo è in giorni. 30 Il valore predefinito è 1.

- **SearchKeywords (Facoltativo):**

L'elenco delle parole chiave da cercare nei log, separate da virgole. Le parole chiave non possono contenere virgolette singole o doppie.

Input parameters

AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. SSMAutomation	ClusterID (Required) The Amazon EMR cluster ID. j-1K4BX00000HCB
S3LogLocation (Optional) The Amazon S3 URL that contains the Amazon EMR logs. Provide this parameter if the Amazon EMR cluster has been terminated for more than 30 days. Provide the full Amazon S3 path prefix for the EMR logs. Example <code>s3://mybucket/infolder/j-1K4BX00000HCB/</code>. String	S3BucketName (Required) The Amazon S3 bucket name to upload a list of known issues, and the output of Amazon Athena queries. The bucket should have [Block Public Access Enabled](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html) and be in the same AWS region as the Amazon EMR cluster provided. String
Approvers (Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats: 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN. arn:aws:iam::[redacted]:role/Approver	FetchNodeLogsOnly (Optional) If set to "true", the automation diagnoses the Amazon EMR node logs. false
FetchContainersLogsOnly (Optional) If set to "true", the automation diagnoses the Amazon EMR containers logs related to applications on the cluster. false	EndSearchDate (Optional) The end date for log searches. If provided, the automation will exclusively search for logs generated up to the specified date in the format YYYY-MM-DD (for example: "2024-12-30"). String
DaysToCheck (Optional) When "EndSearchDate" is provided, this parameter is required to determine the number of days to retrospectively search for logs from the specified "EndSearchDate". The maximum value is "30" days. 1	SearchKeywords (Optional) The list of keywords to search in the logs, separated by commas. The keywords cannot contain single or double quotes. StringList

4. Seleziona Esegui.

5. L'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- **getLogLocation:**

Recupera la posizione del log di Amazon S3 interrogando l'ID cluster Amazon EMR specificato. Se l'automazione non è in grado di interrogare la posizione del log dall'ID del cluster Amazon EMR, il runbook utilizza il `S3LogLocation` parametro di input.

- **branchOnValidRegistro:**

Verifica la posizione dei log di Amazon EMR. Se la posizione è valida, procedi a stimare i costi potenziali di Amazon Athena durante l'esecuzione di query sui log di Amazon EMR.

- **estimateAthenaCosts:**

Determina la dimensione dei log di Amazon EMR e fornisce una stima dei costi per l'esecuzione delle scansioni Athena sul set di dati di log. Per le regioni non commerciali (non AWS partizioni), questo passaggio fornisce semplicemente la dimensione del log senza stimare i costi. I costi

possono essere calcolati utilizzando la documentazione sui prezzi di Athena nella regione specificata.

- Approva l'automazione:

Attende l'approvazione dei responsabili IAM designati per procedere con i passaggi successivi dell'automazione. La notifica di approvazione contiene il costo stimato della scansione di Amazon Athena sui log di Amazon EMR e dettagli sulle risorse fornite dall'automazione.

- `uploadKnownIssuesExecuteAthenaQueries`:

Carica i problemi noti predefiniti nel bucket Amazon S3 specificato nel parametro.

`S3BucketName` Crea database e tabelle AWS Glue . Esegue le query di Amazon Athena nel database in base AWS Glue ai parametri di input.

- `getQueryExecutionStato`:

Attende che l'esecuzione della query di Amazon Athena sia SUCCEEDED in corso. La query DML di Amazon Athena cerca errori ed eccezioni nei log del cluster Amazon EMR.

- `analyzeAthenaResults`:

Analizza i risultati di Amazon Athena per fornire risultati, consigli e articoli del Knowledge Center (KC) provenienti da un set predefinito di mappature.

- `getAnalyzeResultsQuery 1: ExecutionStatus`

Attende che l'esecuzione della query sia in corso. SUCCEEDED La query DML di Amazon Athena analizza i risultati della precedente query DML. Questa query di analisi restituirà eccezioni corrispondenti con risoluzioni e articoli KC

- `getAnalyzeResultsExecutionStatusQuery 2:`

Attende che l'esecuzione della query sia in corso. SUCCEEDED La query DML di Amazon Athena analizza i risultati della precedente query DML. Questa query di analisi restituirà un elenco di eccezioni/errori rilevati in ogni percorso di log di Amazon S3.

- `printAthenaQueriesMessaggio`:

Stampa i link per i risultati delle query DML di Amazon Athena.

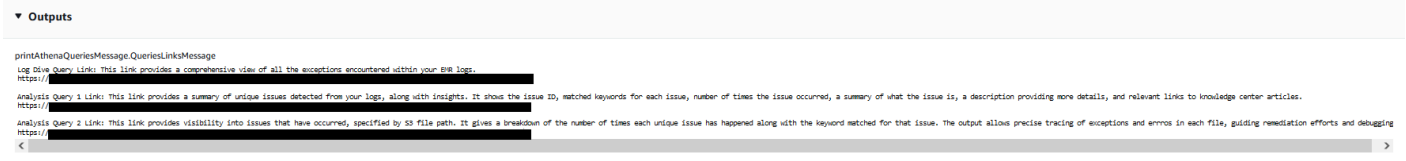
- Risorse di pulizia:

Pulisce le risorse eliminando il AWS Glue database creato ed eliminando i file con problemi noti creati nel bucket di log di Amazon EMR.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

L'output fornisce tre collegamenti per i risultati delle query Athena:

- Elenco di tutti gli errori e le eccezioni ricorrenti presenti nei log del cluster Amazon EMR, insieme alle posizioni dei log corrispondenti (prefisso Amazon S3).
- Riepilogo delle eccezioni note uniche riportate nei log di Amazon EMR, insieme alle risoluzioni consigliate e agli articoli KC per facilitare la risoluzione dei problemi.
- Dettagli su dove compaiono errori ed eccezioni specifici nei percorsi di log di Amazon S3, per supportare ulteriori diagnosi.



Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS documentazione di servizio

- Per ulteriori informazioni, consulta la sezione [Risoluzione dei problemi dei cluster Amazon EMR](#)

OpenSearch Servizio Amazon

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon OpenSearch Service. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSConfigRemediation-DeleteOpenSearchDomain](#)
- [AWSConfigRemediation-EnforceHTTPSONOpenSearchDomain](#)

- [AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups](#)
- [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#)
- [AWSSupport-TroubleshootOpenSearchHighCPU](#)

AWSConfigRemediation-DeleteOpenSearchDomain

Descrizione

Il `AWSConfigRemediation-DeleteOpenSearchDomain` runbook elimina il dominio Amazon OpenSearch Service specificato utilizzando l'[DeleteDomain](#) API.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `DomainName`

Tipo: stringa

Valori consentiti: `(\ d {12}/)? [a-z] {1} [a-z0-9-] {2,28}`

Descrizione: (Obbligatorio) Il nome del dominio Amazon OpenSearch Service che desideri eliminare.

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es>DeleteDomain`
- `es:DescribeDomain`

Fasi del documento

- `aws:executeScript`- Accetta il nome OpenSearch di dominio Amazon Service come input, lo elimina e verifica l'eliminazione.

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

Descrizione

Il `AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain` runbook si abilita `EnforceHTTPS` su un determinato dominio Amazon OpenSearch Service utilizzando l'[UpdateDomainConfig](#) API.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `DomainName`

Tipo: stringa

Valori consentiti: (\ d {12}/)? [a-z] {1} [a-z0-9-] {2,28}

Descrizione: (Obbligatorio) Il nome del dominio Amazon OpenSearch Service che desideri utilizzare per applicare HTTPS.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

Fasi del documento

- aws:executeScript- Abilita l'opzione EnforceHTTPS endpoint sul dominio Amazon OpenSearch Service specificato nel DomainName parametro.

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

Descrizione

Il AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups runbook aggiorna la configurazione del gruppo di sicurezza su un determinato dominio Amazon OpenSearch Service utilizzando l'[UpdateDomainConfig](#) API.

 Note

AWS I gruppi di sicurezza possono essere applicati solo ai domini Amazon OpenSearch Service configurati per Amazon Virtual Private Cloud (VPC) Access e non ai domini Amazon OpenSearch Service configurati per l'accesso pubblico.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- DomainName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del dominio Amazon OpenSearch Service che desideri utilizzare per aggiornare i gruppi di sicurezza.

- SecurityGroupList

Tipo: StringList

Descrizione: (Obbligatorio) Il gruppo di sicurezza IDs che desideri assegnare al dominio Amazon OpenSearch Service.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Fasi del documento

- `aws:executeScript`- Aggiorna la configurazione del gruppo di sicurezza sul dominio Amazon OpenSearch Service specificato nel `DomainName` parametro.

AWSSupport-TroubleshootOpenSearchRedYellowCluster

Descrizione

`AWSSupport-TroubleshootOpenSearchRedYellowCluster` il runbook di automazione viene utilizzato per identificare la causa dello stato di salute del cluster [rosso](#) o [giallo](#) e guidarti nella modifica del cluster in verde.

Come funziona?

Il runbook `AWSSupport-TroubleshootOpenSearchRedYellowCluster` aiuta a risolvere la causa del cluster rosso o giallo e fornisce i passaggi successivi per risolvere questo problema analizzando la configurazione del cluster e l'utilizzo delle risorse.

Il runbook esegue i seguenti passaggi:

- Richiama l'[DescribeDomain](#) API sul dominio di destinazione per ottenere la configurazione del cluster.
- Verifica se il dominio del OpenSearch servizio è basato su Internet (pubblico) o [Amazon Virtual Private Cloud](#) (VPC).
- Crea una AWS Lambda funzione pubblica o [basata su Amazon VPC](#) a seconda della configurazione del cluster. Nota: la funzione Lambda contiene il codice di risoluzione dei problemi

che esegue il OpenSearch servizio APIs sul cluster per determinare il motivo per cui il cluster è in rosso o giallo.

- Elimina la funzione Lambda.
- Visualizza i controlli eseguiti e i passaggi successivi consigliati per risolvere il problema del cluster rosso o giallo.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Il `LambdaExecutionRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook:

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`

Panoramica della `LambdaExecutionRole` politica:

Di seguito è riportato un esempio di ruolo di esecuzione di una funzione Lambda (ruolo AWS Identity and Access Management (IAM)) che concede alla funzione il permesso di accedere ai AWS servizi e alle risorse richiesti da questo runbook. Per ulteriori informazioni, consulta [Ruolo di esecuzione Lambda](#).

Note

I `ec2:DescribeNetworkInterfaces` `ec2:CreateNetworkInterface`, e `ec2>DeleteNetworkInterface` sono necessari solo se il cluster di OpenSearch servizi è [basato su Amazon VPC](#) per consentire alla funzione Lambda di creare e gestire le interfacce di rete Amazon VPC. Per ulteriori informazioni, consulta [Connessione della rete in uscita alle risorse in un ruolo di esecuzione Amazon VPC](#) e [Lambda](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "es:ESHttpGet",
      "Resource": [
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-
name>/",
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cluster/health",
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cat/indices",
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cat/allocation",
        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cluster/allocation/explain"
      ]
    },
    {
      "Condition": {
        "ArnLikeIfExists": {
          "ec2:Vpc": "arn:<partition>:ec2:<region>:<account-id>:vpc/
<vpc_id>"
        }
      },
      "Action": [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Passa a [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#) nella AWS Systems Manager console.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:

- AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- LambdaExecutionRole (Obbligatorio):

L'ARN del ruolo IAM che Lambda utilizzerà per firmare le richieste al tuo cluster Amazon Service. OpenSearch

- DomainName (Obbligatorio):

Il nome del dominio del OpenSearch servizio con lo stato di integrità del cluster rosso o giallo.

- UtilizationThreshold (Facoltativo):

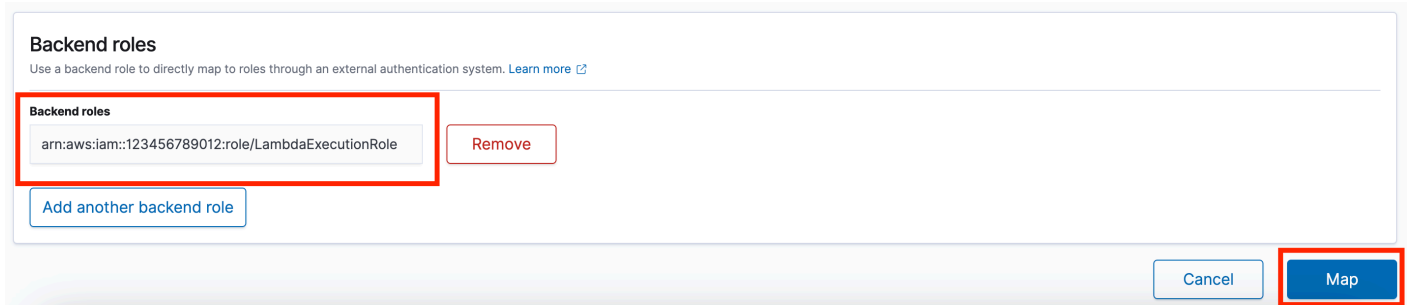
La percentuale della soglia di utilizzo utilizzata per confrontare le metriche di JVMMemory pressione CPUUtilization e di pressione. Il valore predefinito è 80.

The screenshot shows the 'Input parameters' section of the AWS Systems Manager console. It contains four input fields:

- AutomationAssumeRole**: (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. The dropdown menu shows 'Select an existing IAM Role' and a search bar with 'arn:aws:iam::[redacted]:role/AutomationAssumeRole'.
- LambdaExecutionRole**: (Required) The ARN of the IAM role that the AWS Lambda will use to sign requests to your Amazon OpenSearch Service cluster. The dropdown menu shows 'Select an existing IAM Role' and a search bar with 'arn:aws:iam::[redacted]:role/LambdaExecutionRole'.
- DomainName**: (Required) The name of the Amazon OpenSearch Service domain is red or yellow status. The text input field contains 'opensearch-red-yellow-sample'.
- UtilizationThreshold**: (Optional) The utilization threshold in percentage used to compare the 'CPUUtilization' and 'JVMMemoryPressure' metrics. Default value is '80'. The text input field contains '80'.

4. Se hai abilitato il [controllo granulare degli accessi](#) su un cluster di OpenSearch servizi, assicurati che il LambdaExecutionRole ruolo arn sia mappato a un ruolo con almeno l'autorizzazione. `cluster_monitor`

The screenshot shows the 'Permissions' section of the AWS Systems Manager console. It contains a 'Mapped users' section with a 'Cluster permissions (1)' section. The 'Cluster permissions (1)' section shows a list of permissions, with 'cluster_monitor' selected.



5. Seleziona Esegui.

6. L'automazione inizia.

7. Il runbook di automazione esegue i seguenti passaggi:

- GetClusterConfiguration:

Recupera la configurazione del cluster OpenSearch di servizio.

- Crea AWSLambdaFunctionStack:

Crea una funzione Lambda temporanea nel tuo account utilizzando. AWS CloudFormation La funzione Lambda viene utilizzata per eseguire il OpenSearch servizio. APIs

- WaitForAWSLambdaFunctionStack:

Attende il completamento dello CloudFormation stack.

- GetClusterMetricsFromCloudWatch:

Ottiene le metriche relative al cluster Amazon CloudWatch ClusterStatus e JVMMemory Pressure OpenSearch Service e la relativa data di creazione. CPUUtilization

- RunOpenSearchAPIs:

Utilizza la funzione Lambda per chiamare il OpenSearch servizio APIs e analizzare i dati delle metriche del cluster per diagnosticare la causa dello stato rosso o giallo del cluster.

- Elimina: AWSLambda FunctionStack

Elimina la funzione Lambda creata da questa automazione nel tuo account.

8. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione.

- RootCause:

Fornisce una panoramica della causa identificata dello stato di salute del cluster in rosso o giallo.

- **IssueDescription:**

Fornisce dettagli sul motivo per cui il cluster è in rosso o giallo e sui possibili passaggi per riportare il cluster allo stato verde.

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS documentazione di servizio

- Per ulteriori informazioni, consulta la sezione [Risoluzione dei problemi di Amazon OpenSearch Service](#)

AWSSupport-TroubleshootOpenSearchHighCPU

Descrizione

Il AWSSupport-TroubleshootOpenSearchHighCPU runbook fornisce una soluzione automatizzata per raccogliere dati diagnostici da un dominio Amazon OpenSearch Service per risolvere problemi [elevati](#) di CPU.

Come funziona?

Il AWSSupport-TroubleshootOpenSearchHighCPU runbook aiuta a risolvere i problemi di utilizzo elevato della CPU nel dominio Amazon Service. OpenSearch

Il runbook esegue i seguenti passaggi:

- Esegue l'[DescribeDomain](#) API sul dominio Amazon OpenSearch Service fornito per ottenere i metadati del cluster.
- Verifica se il dominio Amazon OpenSearch Service è pubblico o basato su Amazon VPC e, con l'aiuto di AWS CloudFormation, crea una funzione pubblica o basata su [Amazon AWS Lambda VPC](#).

- La funzione Lambda recupera i dati diagnostici dai domini di Amazon OpenSearch Service.
- Utilizza una macchina a AWS Step Functions stati per orchestrare più esecuzioni di funzioni Lambda per raccogliere dati più completi.
- Per impostazione predefinita, archivia i dati raccolti in un gruppo di CloudWatch log Amazon per 24 ore.
- Elimina le risorse create, ad eccezione del gruppo di CloudWatch log.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Il `LambdaExecutionRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook:

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`

- `ec2:DescribeNetworkInterfaces`
- `ec2:DeleteNetworkInterface`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Il ruolo di esecuzione Lambda concede alla funzione l'autorizzazione ad accedere ai AWS servizi e alle risorse richiesti da questo runbook. Per ulteriori informazioni, consulta [Ruolo di esecuzione Lambda](#).

Note

I `ec2:DescribeNetworkInterfaces` e `ec2:CreateNetworkInterface`, e `ec2:DeleteNetworkInterface` sono necessari solo se il cluster di OpenSearch servizi è [basato su Amazon VPC](#) per consentire alla funzione Lambda di creare e gestire le interfacce di rete Amazon VPC. Per ulteriori informazioni, consulta [Connessione della rete in uscita alle risorse in un ruolo di esecuzione Amazon VPC](#) e [Lambda](#).

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Passa a [AWSsupport-TroubleshootOpenSearchHighCPU](#) nella AWS Systems Manager console.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:
 - `AutomationAssumeRole` (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `DomainName` (Obbligatorio):

Il nome del dominio Amazon OpenSearch Service che desideri risolvere per problemi elevati di CPU.

- `LambdaExecutionRoleForOpenSearch` (Obbligatorio):

L'ARN del ruolo IAM da collegare alla funzione Lambda. La funzione Lambda utilizza le credenziali di questo ruolo per firmare le richieste al dominio Amazon OpenSearch Service. Se il controllo granulare degli accessi è abilitato sul dominio Amazon OpenSearch Service, devi mappare questo ruolo a un ruolo di backend di OpenSearch Service Dashboards con un minimo di autorizzazione «cluster_monitor».

- DataRetentionDays (Facoltativo):

Il numero di giorni per conservare i dati diagnostici raccolti dal dominio Amazon OpenSearch Service. Per impostazione predefinita, i dati vengono conservati per 24 ore (un giorno). Puoi scegliere di conservare i dati per un massimo di 30 giorni.

- NumberOfDataSamples (Facoltativo):

Il numero di campioni di dati da raccogliere dal dominio Amazon OpenSearch Service. Per impostazione predefinita, vengono raccolti 5 campioni di dati. È possibile raccogliere fino a 10 campioni e la funzione Lambda verrà richiamata per ogni raccolta di campioni.

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. 	DomainName (Required) The name of the Amazon OpenSearch domain that you want to troubleshoot for high CPU issues. String
LambdaExecutionRoleForOpenSearch (Required) The ARN of the IAM role to attach to the Lambda function. The Lambda function uses the credentials from this role sign requests to your AOS domain. If Fine-grained access control (FGAC) is enabled on your AOS domain, you must map this role to a OpenSearch dashboards backend role with minimum of "cluster_monitor" permission. 	DataRetentionDays (Optional) The number of days to retain the diagnostic data collected from the AOS domain. By default, the data retained for 24 hours (1 day). You can choose to retain the data for maximum of 7 days period. 1
NumberOfDataSamples (Optional) The number of data samples to collect from the AOS domain. By default, 5 data sample are collected by the automation. You can collect up to 10 samples and the Lambda function will be invoked for each sample collection. 5	

- Se hai abilitato il [controllo granulare degli accessi](#) su un cluster di OpenSearch servizi, assicurati che il LambdaExecutionRole ruolo arn sia mappato a un ruolo con almeno l'autorizzazione. cluster_monitor

Permissions	Mapped users
Cluster permissions (1) Cluster permissions specify how users in this role can access the cluster. You can specify permissions using both action groups or single permissions. An action group is a list of single permissions. Learn more > • cluster_monitor	

Backend roles
Use a backend role to directly map to roles through an external authentication system. [Learn more](#)

Backend roles

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

[Add another backend role](#)

Cancel Map

5. Seleziona Esegui.

6. L'automazione inizia.

7. Il runbook di automazione esegue i seguenti passaggi:

- CheckConcurrency:

Assicura che esista una sola esecuzione di questo runbook destinata al dominio Amazon OpenSearch Service specificato. Se il runbook trova un'altra esecuzione indirizzata allo stesso nome di dominio, restituisce un errore e termina.

- getDomainConfig:

Ottiene i dettagli di configurazione per il dominio di OpenSearch servizio di destinazione.

- Risorse di fornitura:

Fornisce le risorse per la raccolta dei dati utilizzando AWS CloudFormation

- waitForStackCreazione:

Attende il completamento dello AWS CloudFormation stack.

- describeStackResources:

Descrive lo AWS CloudFormation stack e ottiene l'ARN della macchina a stati.

- runStateMachine:

Richiama la funzione Lambda del raccogliitore di dati una o più volte eseguendo una macchina a stati Step Functions.

- describeErrorsFromStackEvents:

Descrive gli errori presenti nella pila per individuare eventuali errori. AWS CloudFormation

- unstageOpenSearchAltoCPUAutomation:

- `describeErrorsFromStackDeletion`:

Descrive gli errori riscontrati durante l'eliminazione dello stack. AWS CloudFormation

- Stato finale:

Restituisce l'output finale del runbook. `AWSsupport-TroubleshootOpenSearchHighCPU`

8. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione.

- Stato finale. `FinalOutput`:

Fornisce il gruppo di CloudWatch log in cui sono archiviati i dati diagnostici.

▼ Outputs
<code>finalStatus.FinalOutput</code> Hot thread data collection completed. Please check the custom CloudWatch log group <code>/aws/lambda/AWSsupport-HighCPU-df52ba5d-8773-4038-a908-b67ecd9c9d11</code> for more information.

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS documentazione di servizio

- Per ulteriori informazioni, consulta la sezione [Risoluzione dei problemi di Amazon OpenSearch Service](#)

EventBridge

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. EventBridge

Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-AddOpsItemDedupStringToEventBridgeRule](#)
- [AWS-DisableEventBridgeRule](#)

AWS-AddOpsItemDedupStringToEventBridgeRule

Descrizione

Il `AWS-AddOpsItemDedupStringToEventBridgeRule` runbook aggiunge una stringa di deduplicazione per tutti coloro che sono AWS Systems Manager OpsItems associati a una regola Amazon EventBridge. Il runbook non aggiunge una stringa di deduplicazione alla regola se ne è già stata applicata una. Per ulteriori informazioni sulle stringhe di deduplicazione e OpsItems, vedere [Reducing duplicate](#) nella Guida per l'utente. OpsItems AWS Systems Manager

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DedupString

Tipo: stringa

Descrizione: (Obbligatoria) La stringa di deduplicazione che si desidera aggiungere alla regola.

- RuleName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della regola a cui si desidera aggiungere la stringa di deduplicazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

Fasi del documento

- `aws:executeScript`- Aggiunge una stringa di deduplicazione alla EventBridge regola specificata nel parametro. `RuleName`

AWS-DisableEventBridgeRule

Descrizione

Il *AWS-DisableEventBridgeRule* runbook disabilita la EventBridge regola Amazon specificata. Per ulteriori informazioni sulle regole EventBridge , consulta le regole di Amazon [EventBridge nella Amazon User Guide](#). EventBridge

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EventBusName

Tipo: stringa

Impostazione predefinita: impostazione predefinita

Descrizione: (Facoltativo) Il bus degli eventi associato alla regola che desideri disabilitare.

- RuleName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della regola che desideri disabilitare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- events:DisableRule

Fasi del documento

- aws:executeAwsApi- Disattiva la EventBridge regola specificata nel RuleName parametro.

AWS Glue

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Glue Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-TroubleshootGlueConnection](#)

AWSSupport-TroubleshootGlueConnection

Descrizione

Il AWSSupport-TroubleshootGlueConnectionsrunbook aiuta a risolvere i problemi di connessione. AWS Glue La destinazione della connessione testata deve essere raggiunta tramite una connessione JDBC e può essere un cluster/istanza Amazon Relational Database Service (Amazon RDS), un cluster Amazon Redshift o qualsiasi altra destinazione accessibile tramite JDBC. Nei primi due casi, lo strumento Reachability Analyzer viene utilizzato per determinare se la connettività tra l'origine AWS Glue() e la destinazione (Amazon RDS o Amazon Redshift) è garantita.

Se la destinazione della connessione non è Amazon RDS o Amazon Redshift, la connettività viene comunque testata creando AWS Lambda una funzione nella stessa sottorete della connessione (un punto di presenza di rete) e verificando se il nome della destinazione è risolvibile e se è raggiungibile nella porta di destinazione. AWS Glue

Important

Per eseguire i controlli [Reachability](#) Analyzer, [verranno create interfacce di rete elastiche](#) in ciascuna delle sottoreti di origine dati della connessione. Assicurati di avere abbastanza spazio libero IPs su quelle sottoreti e che il consumo di un IP non influisca sul tuo carico di lavoro prima di eseguire questa automazione.

Important

Tutte le risorse create da questa automazione sono contrassegnate in modo che possano essere trovate facilmente. I tag utilizzati sono:

- `AWSSupport-TroubleshootGlueConnection`: true
- `AutomationExecutionId`: *Amazon EC2 Systems Manager Execution Id*

Come funziona?

Il runbook esegue i seguenti passaggi:

- Descrive la AWS Glue connessione per ottenere le informazioni di origine (sottorete e gruppi di sicurezza) per i controlli di connettività.
- Recupera le informazioni di destinazione (sottorete e gruppi di sicurezza) dall'origine dati a cui si fa riferimento nell'URL JDBC o dai parametri and, se presenti. `DatasourceSecurityGroups` `DatasourceSubnets`
- Se l'origine dati presente nell'URL JDBC è un'istanza o un cluster Amazon RDS o un cluster Amazon Redshift, questa automazione crea ENIs utilizzando sia le informazioni di origine che quelle di destinazione raccolte nei passaggi precedenti e utilizza Reachability Analyzer per eseguire un controllo di connettività tra di loro.
- Una funzione Lambda (punto di presenza della rete, nel contesto di questa automazione) viene utilizzata per eseguire controlli di connettività L4 e risoluzione dei nomi.
- La stessa funzione Lambda viene utilizzata per eseguire i controlli sull'endpoint Amazon S3.
- Policy Simulator viene utilizzato per determinare se il ruolo IAM utilizzato nella connessione dispone delle autorizzazioni necessarie.
- L'automazione verifica se il gruppo di sicurezza utilizzato dalla connessione ha la configurazione prevista.
- Viene generato un rapporto contenente le possibili cause dell'errore nell'operazione di test di connessione e/o anche i test eseguiti con successo.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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

Oltre alle azioni sopra menzionate, `AutomationAssumeRole` dovrebbero avere [Amazon VPCReachability AnalyzerFullAccessPolicy](#) come [policy gestita allegata](#) in modo che i test [Reachability](#) Analyzer vengano eseguiti correttamente.

Ecco un esempio di politica che potrebbe essere concessa per: `AutomationAssumeRole`

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

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSsupport-TroubleshootGlueConnection](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- TestConnectionRole (Obbligatorio)

L'Amazon Resource Name (ARN) del ruolo IAM utilizzato durante il test di connessione.

- ConnectionName (Obbligatorio)

AWS Glue nome della connessione di test fallita che desideri risolvere.

- **PersistReachabilityAnalyzerResults(Facoltativo)**

Il flag che indica se i risultati dell'esecuzione del Reachability Analyzer devono essere conservati o meno. Impostazione predefinita: `false`.

- **PointOfPresenceLogRetentionPeriod(Facoltativo)**

Il numero di giorni per cui verranno archiviati i log per il punto di presenza Lambda. Default: 7.

- **DatasourceSubnets (Facoltativo)**

Se l'origine dati originale non è disponibile, utilizzate questo parametro per fornire le sottoreti utilizzate in modo che i test di connettività vengano comunque eseguiti. Deve essere usato con. `DatasourceSecurityGroups` Esempio: `subnet-1, subnet-2`.

- **DatasourceSecurityGroups (Facoltativo)**

Se l'origine dati originale non è disponibile, utilizzate questo parametro per fornire i gruppi di sicurezza utilizzati in modo che i test di connettività vengano comunque eseguiti. Deve essere usato con. `DatasourceSubnets` Esempio: `sg-1, sg-2`.

Input parameters

AutomationAssumeRole

(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

TestConnectionRole

(Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that is used during the connection test.

PointOfPresenceLogRetentionPeriod

(Optional) The amount of days the logs for the point of presence AWS Lambda will be stored for. Default: 7.

DatasourceSecurityGroups

(Optional) If the original datasource is not available, use this parameter to provide the security groups it used so that the connectivity tests are still performed. ****Must**** be used with ``DatasourceSubnets``. Example: `sg-1,sg-2`.

ConnectionName

(Required) The name of the AWS Glue Connection you want to troubleshoot the failed test connection attempt.

PersistReachabilityAnalyzerResults

(Optional) The flag informing if the results of the VPC Reachability Analyzer execution should be kept or not. Default: false.

DatasourceSubnets

(Optional) If the original datasource is not available, use this parameter to provide the subnets that it used so that the connectivity tests are still performed. ****Must**** be used with ``DatasourceSecurityGroups``. Example: `subnet-1,subnet-2`.

4. Seleziona Esegui.

5. L'automazione si avvia.

6. Il runbook di automazione esegue i seguenti passaggi:

- **ParseInputs:**

Questo passaggio convalida la combinazione di input. Se `DatasourceSubnets` vengono forniti entrambi `DatasourceSecurityGroups`, sono validi e restituiti così come sono. Se non ne viene fornito nessuno, vengono restituiti due elenchi vuoti. Se viene fornito solo uno di essi, il passaggio genera un `ValueException`.

- `GetConnectionDetails`:

Questo passaggio restituisce i dettagli della AWS Glue connessione fornita.

- `ParseSecurityGroupList`:

Questo passaggio viene utilizzato per concatenare le informazioni per un utilizzo `String` futuro `SecurityGroupIdList` in questa automazione.

- `GetConnectionData`:

Determina, in base all'URL JDBC, il tipo di connessione tra:, e. `RedShift RdsInstance RdsCluster Other` Inoltre, restituisce il dominio e la porta utilizzati nella connessione JDBC, Amazon VPC della connessione e i relativi server dei nomi di dominio.

- `GetNetworkDetails`:

Ottiene le informazioni sulla sottorete e sul gruppo di sicurezza dal target Amazon RDS o Amazon Redshift.

- Crea: `ENITemplate`

Genera il AWS CloudFormation modello utilizzato per creare le interfacce di rete utilizzate per testare la connettività. Ciò è necessario per eseguire lo strumento `Reachability Analyzer`.

- Crea: `ENIStack`

Crea lo AWS CloudFormation stack dal modello creato nel passaggio precedente.

- `GetStackDetails`:

Descrive lo AWS CloudFormation stack creato nello stack precedente e recupera le informazioni. `SourceNetworkInterface TargetNetworkInterfaces`

- `RunSourceToTargetCheck`:

Esegue i controlli tra l'origine e la destinazione ENIs creati nel passaggio precedente utilizzando lo strumento `Reachability Analyzer`.

- Elimina: `ENIStack`

Elimina lo AWS CloudFormation stack che crea le interfacce di rete

- `CreateNetworkPointOfPresence`:

AWS CloudFormation crea la funzione Lambda utilizzata come punto di presenza di rete.

- `GetFunctionName`:

Esegue una chiamata API AWS CloudFormation `describe stack` per recuperare il nome della funzione Lambda creata nel passaggio precedente.

- `RunEndpointChecks`:

Utilizza il punto di presenza della rete per determinare se l'endpoint presente nella connessione JDBC è risolvibile e raggiungibile nella porta dichiarata.

- Verifica la connettività S3:

Verifica la connettività di rete dalla AWS Glue connessione al servizio Amazon S3.

- `DeletePointOfPresence`:

Elimina lo AWS CloudFormation stack che crea il punto di presenza della rete Lambda.

- Autorizzazioni di test: `IAMRole`

Verifica se il ruolo IAM utilizzato per il test dispone delle autorizzazioni necessarie per eseguirlo.

- `CheckConnectionSecurityGroupReferencingRule`:

Verifica se il gruppo di sicurezza utilizzato nella AWS Glue connessione consente tutto il traffico in ingresso da se stesso. Restituirà un elenco dei gruppi di sicurezza senza questa regola, se presente.

- `GenerateReport`:

Genera un rapporto contenente un elenco di risultati (possibili motivi dell'errore nel test di connessione) e i passaggi successivi (tentativi di risolvere l'errore del test di connessione).

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- Risultati di automazione

In questa sezione, troverai gli scenari che descrivono le possibili cause del fallimento dell'operazione di connessione di test (risultati) e come risolverle (passaggi successivi). Se l'automazione non riesce a trovare la causa dell'errore del test, ne verrà data notizia anche in

questa sezione.

- Test riusciti

In questa sezione, troverai scenari che informano su ciò che è stato testato con successo da questa automazione. I test eseguiti con successo sono utili nel caso in cui l'automazione non sia in grado di identificare la causa dell'errore della connessione di test, in quanto riducono l'ambito dell'indagine informando gli elementi che non contribuiscono al problema.

- Errori di automazione

In questa sezione, troverai scenari che descrivono i problemi che si sono verificati durante l'automazione, che potrebbero aver limitato il numero di test che l'automazione poteva eseguire. La descrizione dello scenario indicherà quale passaggio non è riuscito.

```
TroubleshootGlueConnection

Automation Results
Below are possible causes for the issue being troubleshoot and their fixes.

-----

# Scenario: AWS Glue connection's VPC using Amazon Provided DNS
🔍 Findings:
- The JDBC URL's endpoint dummy-instance.c3c3tj8ogvmj.us-east-1.rds.amazonaws.com could not be resolved from the AWS Glue connection's subnet subnet-
- Glue connection's VPC (vpc-██████████) is using AWS DNS Resolver but no issue could be found.
➔ Next steps:
- Please check the following links for further DNS troubleshooting:
- https://repost.aws/knowledge-center/vpc-find-cause-of-failed-dns-queries
- https://repost.aws/knowledge-center/vpc-peering-troubleshoot-dns-resolution
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-support

# Scenario: Checking AWS Glue connection IAM role trust relationship
🔍 Findings:
- The IAM role arn:aws:iam::██████████:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi used for the AWS Glue connection test has no trust relationship with the AWS Glue service.
➔ Next steps:
- Please add the AWS Glue service to the arn:aws:iam::██████████:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi trust relationship. More details on the following link:
- https://docs.aws.amazon.com/directoryservice/latest/admin-guide/edit_trust.html

# Scenario: Glue test connection role IAM check
🔍 Findings:
- The IAM role (arn:aws:iam::██████████:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi) used to test the connection is not allowed to perform 'glue:TestConnection'.
➔ Next steps:
- Please add the 'glue:TestConnection' action to the role used for the AWS Glue connection test: arn:aws:iam::██████████:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi.

-----

✓ Successful Tests
Below are the successful tests performed by the automation, for further troubleshooting.

-----

# Scenario: Datasource security group
✓ The target's security group(s) allow(s) inbound connections from the Glue connection.

# Scenario: Checking connection security group self referencing rule
✓ The AWS Glue connection has a self referencing inbound rule allowing all traffic.
```

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)

- [Pagina iniziale Support Automation Workflows](#)

Amazon FSx

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon FSx. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta [Visualizza il contenuto del runbook](#).

Argomenti

- [AWSSupport-ValidateFSxWindowsADConfig](#)

AWSSupport-ValidateFSxWindowsADConfig

Descrizione

Il `AWSSupport-ValidateFSxWindowsADConfig` runbook viene utilizzato per convalidare la configurazione autogestita di Active Directory (AD) di un file server Amazon FSx per Windows.

Come funziona?

Il runbook `AWSSupport-ValidateFSxWindowsADConfig` esegue lo script di FSx convalida di Amazon sull'istanza temporanea di Amazon Elastic Compute Cloud (Amazon EC2) Windows lanciata dal runbook nella sottorete Amazon FSx. Lo script esegue più controlli per convalidare la connettività di rete ai server AD/DNS autogestiti e le autorizzazioni dell'account di servizio Amazon FSx. Il runbook può convalidare un file server FSx Amazon for Windows fallito o configurato in modo errato o creare un nuovo FSx Amazon for Windows File Server con AD autogestito.

Per impostazione predefinita, il runbook crea l'istanza Amazon EC2 Windows, il gruppo di sicurezza per l'accesso AWS Systems Manager (SSM), il ruolo AWS Identity and Access Management (IAM) e la policy utilizzando nella AWS CloudFormation sottorete Amazon FSx. Se desideri eseguire lo script su un'EC2 istanza Amazon esistente, fornisci l'ID nel parametro `InstanceId`. In caso di esecuzione riuscita, elimina le CloudFormation risorse. Tuttavia, per conservare le risorse, impostate il `RetainCloudFormationStack` parametro su `true`.

Il CloudFormation modello crea un ruolo IAM per tuo conto con le autorizzazioni necessarie per il collegamento all'EC2 istanza Amazon per eseguire lo script di FSx convalida di Amazon. Per specificare un profilo di istanza IAM esistente per l'istanza temporanea, utilizza

il `InstanceProfileName` parametro. Il ruolo IAM associato deve contenere le seguenti autorizzazioni:

- `ec2:DescribeSubnet` e `ec2:DescribeVpcs` autorizzazioni e `AmazonManagedPolicyAmazonSSMManagedInstanceCore`.
- Autorizzazioni per ottenere il nome utente e la password dell'account del FSx servizio Amazon da Systems Manager chiamando `GetSecretValueAPI`.
- Autorizzazioni per inserire l'oggetto nel bucket Amazon Simple Storage Service (Amazon S3) per l'output dello script.

Prerequisiti

La sottorete in cui viene creata l' EC2 istanza Amazon temporanea (o l'istanza esistente fornita nel `InstanceId` parametro) deve consentire l'accesso agli endpoint e Amazon S3 per eseguire `AmazonFSxADValidation` lo script utilizzando SSM Run Command. AWS Systems Manager AWS Secrets Manager

AWS Secrets Manager configurazione

Lo script di convalida si connette al dominio Microsoft AD recuperando il nome utente e la password dell'account del FSx servizio Amazon con una chiamata di runtime a Secrets Manager. Segui i passaggi descritti in [Creare un AWS Secrets Manager segreto](#) per creare un nuovo segreto di Secrets Manager. Assicurati che il nome utente e la password siano archiviati utilizzando una coppia chiave/valore nel formato. `{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}` Per informazioni sulla protezione dell'[accesso ai segreti, consulta Autenticazione e controllo](#) degli accessi. AWS Secrets Manager

Per ulteriori informazioni sullo strumento, consulta i `README.md` file `TROUBLESHOOTING.md` and nel FSx ADValidation file [Amazon](#).

Esecuzione del runbook

Esegui il runbook con i parametri Amazon FSx ID o AD. Di seguito è riportato il flusso di lavoro del runbook:

- Ottiene i parametri dall' FSx ID Amazon o utilizza i parametri AD di input.
- Crea l'istanza Amazon EC2 Windows di convalida temporanea sulla FSx sottorete Amazon, il gruppo di sicurezza per l'accesso SSM, il ruolo e la policy IAM (condizionale) utilizzando. CloudFormation Se il `InstanceId` parametro è specificato, viene utilizzato.

- Scarica ed esegue lo script di convalida sull' EC2 istanza Amazon di destinazione nella sottorete FSx principale di Amazon.
- Fornisce il codice dei risultati della convalida AD nell'output dell'automazione. Inoltre, l'output completo dello script viene caricato nel bucket Amazon S3.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Esempio di politica IAM per l'automazione Assume Role

```
{
  "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"
                ]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:GetEncryptionConfiguration",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
        ],
        "Resource": "*"
    }
]
}

```


Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-ValidateFSxWindowsADConfig](#) Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per convalidare AD autogestito con un FSx Amazon esistente fallito o configurato in modo errato, inserisci i seguenti parametri:

- AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- FSxId (condizionale):

L'ID del file server Amazon FSx per Windows. Ciò è necessario per convalidare Amazon esistente con errori o configurazioni errate. FSx

- SecretArn (Obbligatorio):

L'ARN del segreto di Secrets Manager contenente il nome utente e la password dell'account del FSx servizio Amazon. Assicurati che il nome utente e la password siano memorizzati utilizzando una coppia chiave/valore nel formato. {"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"} Lo CloudFormation stack crea l'istanza di convalida con le autorizzazioni per l'esecuzione su GetSecretValue questo ARN.

- FSxSecurityGroupId (Obbligatorio):

L'ID del gruppo di sicurezza per Amazon FSx for Windows File Server.

- BucketName (Obbligatorio):

Il bucket Amazon S3 su cui caricare i risultati della convalida. Assicurati che il bucket sia configurato con la crittografia lato server (SSE) e che la policy del bucket non conceda autorizzazioni di lettura/scrittura non necessarie a parti che non hanno bisogno di accedere ai log. Assicurati inoltre che l'istanza Amazon EC2 Windows disponga dell'accesso necessario al bucket Amazon S3.

Input parameters

InstanceId
(Optional) The ID of an existing AWS Systems Manager managed Windows Server Amazon EC2 instance where you intend to run the validation script. The instance requires the [AWS Tools for PowerShell](https://docs.aws.amazon.com/powershell/) to be installed. ****Caution**:** The script will temporarily modify the DNS configuration of the instance, which may result in loss of network connectivity. To avoid disruptions, ****do not use a production instance****. Ensure the selected instance is designated for testing purposes only. Please ensure that access to the contents of the instance's volume is not exposed to parties that do not need to access the logs.

☐ Show interactive instance picker

AWS::EC2::Instance::Id

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

fsx-test

BucketName
(Required) The Amazon S3 bucket to upload the validation results to. Please make sure the bucket is configured with server-side encryption (SSE), and the bucket policy does not grant unnecessary read/write permissions to parties that do not need to access the logs. Also please make sure EC2 Windows instance has necessary access to the S3 Bucket.

test-for-customer

RetainCloudFormationStack
(Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

false

SecretArn
(Required) The ARN of your AWS Secrets Manager secret containing the FSx service account username and password. Make sure that the username and password are stored using a key/value pair in the format `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`.

arn:aws:secretsmanager:us-west-2:123456789012:secret:fsx-test

FSxSecurityGroupId
(Required) The security group ID of the Amazon FSx for Windows File Server.

sg-examplesg1234

FSxId
(Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.

fs-abcdef123456789

4. Per convalidare la configurazione AD autogestita per una nuova FSx creazione Amazon, inserisci i seguenti parametri:

- AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- SecretArn (Obbligatorio):

L'ARN del segreto di Secrets Manager contenente il nome utente e la password dell'account del FSx servizio Amazon. Assicurati che il nome utente e la password siano memorizzati utilizzando una coppia chiave/valore nel formato. `{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}` Lo CloudFormation stack crea l'istanza di convalida con le autorizzazioni per l'esecuzione su `GetSecretValue` questo ARN.

- FSxSecurityGroupId (Obbligatorio):

L'ID del gruppo di sicurezza per Amazon FSx for Windows File Server.

- BucketName (Obbligatorio):

Il bucket Amazon S3 su cui caricare i risultati della convalida. Assicurati che il bucket sia configurato con la crittografia lato server (SSE) e che la policy del bucket non conceda

autorizzazioni di lettura/scrittura non necessarie a parti che non hanno bisogno di accedere ai log. Assicurati inoltre che l'istanza Amazon EC2 Windows disponga dell'accesso necessario al bucket Amazon S3.

- **FSxPreferredSubnetId(Condizionale):**

La sottorete preferita di Amazon FSx for Windows File Server.

- **DomainName (Condizionale):**

Il nome di dominio completo del tuo dominio Microsoft AD autogestito.

- **DnsIpAddresses (Condizionale):**

Un elenco di un massimo di due indirizzi IP del server DNS o del controller di dominio nel dominio AD autogestito. Per un massimo di due IPs, inseriscili separati da una virgola.

- **FSxAdminsGroup (Condizionale):**

Il gruppo FSx di amministratori di file system delegati di Amazon for Windows File Server. Per impostazione predefinita, questo è `Domain Admins`.

- **FSxOrganizationalUnit(Condizionale):**

L'unità organizzativa (OU) all'interno della quale si desidera inserire il file system. Fornire il nome del percorso distinto dell'unità organizzativa. Esempio: `OU=org,DC=example,DC=com`.

RetainCloudFormationStack

(Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

false

TestServiceAccountPermissions

(Optional) Enable service account permission validation. This validation will create test Active Directory computer objects in the Microsoft Active Directory Organizational Unit. The resources are cleaned up by the script unless delete permissions are not properly configured on the provided service account in which case manual cleanup may be necessary.

true

DnsIpAddresses

(Conditional) A list of up to two DNS server or domain controller IP addresses in your self-managed AD domain. Required if the `FSxId` parameter is not specified. For up to two IPs, enter them separated by a comma.

10.0.1.10

FSxSecondarySubnetId

(Conditional) The Amazon FSx for Windows File Server secondary subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Optional if the `FSxId` parameter is not specified.

String

FSxOrganizationalUnit

(Conditional) The Organizational Unit (OU) within which you want to join your file system. Provide the distinguished path name of the OU. Example: `OU=org,DC=example,DC=com`. Optional if the `FSxId` parameter is not specified.

OU=testou,DC=example,DC=com

FSxId

(Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.

String

DomainName

(Conditional) The fully qualified domain name of your self-managed Microsoft Active Directory domain. Required if the `FSxId` parameter is not specified.

example.com

FSxPreferredSubnetId

(Conditional) The Amazon FSx for Windows File Server preferred subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Required if the `FSxId` parameter is not specified.

subnet-test1234example

FSxAdminsGroup

(Conditional) The Amazon FSx for Windows File Server delegated file system administrators group. Optional if the `FSxId` parameter is not specified. By default, this is `Domain Admins`.

Domain Admins

InstanceKeyPairName

(Conditional) An existing Amazon EC2 key pair you want to associate to the temporary Amazon EC2 instance. Optional when the `InstanceId` parameter is not specified.

String

5. Seleziona Esegui.

6. L'automazione si avvia.

7. Il documento esegue le seguenti operazioni:

- `CheckBucketPublicStatus(AWS: ExecuteScript)`:

Verifica se il bucket Amazon S3 di destinazione concede potenzialmente l'accesso pubblico in lettura e/o scrittura ai suoi oggetti.

- `BranchOnInputParameters(aws:branch)`:

Rami sui parametri di input forniti come Amazon FSx ID o FSx parametri Amazon.

- `AssertFileSystemTypelsWindows(aws: assertAwsResource Proprietà)`:

Se viene fornito un FSx ID Amazon, verifica che il tipo di file system sia Amazon FSx for Windows File Server.

- `GetValidationInputs(AWS: ExecuteScript)`:

Restituisce la configurazione Microsoft AD autogestita richiesta dal CloudFormation modello per creare l' EC2 istanza Amazon.

- `BranchOnInstanceId (aws:branch)`:

Rami sull'ingresso fornito. `InstanceId` Se `InstanceId` fornito, lo script di convalida viene eseguito sull' EC2 istanza Amazon di destinazione dall'automazione `step:RunValidationScript`.

- `Crea EC2 InstanceStack (aws:CreateStack)`:

Crea l' EC2 istanza Amazon nella sottorete preferita utilizzando AWS CloudFormation dove verrà `AmazonFSxADValidation` eseguito lo strumento

- `DescribeStackResources(aws:executeAwsApi)`:

Descrive lo CloudFormation stack per ottenere l'ID temporaneo dell' EC2 istanza Amazon.

- `WaitForEC2InstanceToBeManaged(leggi: waitForAwsResourceProperty)`:

Attende che l' EC2 istanza Amazon venga gestita da Systems Manager per eseguire lo script di convalida utilizzando SSM Run Command.

- `GetAmazonFSxADValidationAllegato (aws): executeAwsApi`

Ottiene l'URL `AmazonFSxADValidation` dello strumento dagli allegati del runbook.

Esegue lo AmazonFSxADValidation strumento sull' EC2istanza Amazon temporanea e archivia il risultato nel bucket Amazon S3 specificato nel parametro. BucketName

- DescribeErrorsFromStackEvents(AWS: ExecuteScript):

Descrive gli eventi CloudFormation dello stack se i runbook non riescono a creare lo stack.

- BranchOnRetainCloudFormationStack(aws:branch):

Rami RetainCloudFormationStack e InstanceId parametri per determinare se lo CloudFormation stack deve essere eliminato.

- DeleteCloudFormationStack(AWS: deleteStack):

Elimina lo stack. AWS CloudFormation

8. Al termine, consulta la sezione Output per i risultati dell'esecuzione:

```
▼ Outputs

DescribeInstanceAndSubnet.InstanceId
i-06: [REDACTED]

CreateEC2InstanceStack.CloudFormationStackId
arn:aws:cloudformation:us-east-1:3[REDACTED]:stack/AWSSupport-ValidateFSxWindowsADConfig-3428bd96-f8ca-4c8d-9b02-57d81560bac8/67c23cc0-3585-11ef-868f-0efb7b77b54b

RunValidationScript.Output
AmazonFSxADValidation tool downloaded and extracted successfully.
RSAT-AD-PowerShell installed successfully.

Running Test-FSxADConfiguration with parameters:
DomainDNSRoot: self.msfc.com
DnsIpAddresses: 10.10.1.191
SubnetIds: subnet-0[REDACTED]
TestServiceAccountPermissions: True
TranscriptDirectory: C:\ProgramData\Amazon\AmazonFSxADValidation\3428bd96-f8ca-4c8d-9b02-57d81560bac8
AdminGroup: Domain Admins
OrganizationalUnit:

=====
The validation details and logs can be found in the bucket test-for-customer.

ERRORS: 1
- InvalidCredentials

WARNINGS: 0

For detailed information about a given warning or error, see C:\ProgramData\Amazon\AmazonFSxADValidation\AmazonFSxADValidation\TROUBLESHOOTING.md.

=====
The local DNS configuration has been reset successfully.
```

Il runbook caricherà i risultati dell'esecuzione dello script di convalida nel bucket Amazon S3.

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)

- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS documentazione di servizio

- [Cos'è Amazon FSx per Windows File Server?](#)
- [Convalida della configurazione AD autogestita FSx per Amazon for Windows File Server](#)

GuardDuty

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. GuardDuty Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSConfigRemediation-CreateGuardDutyDetector](#)

AWSConfigRemediation-CreateGuardDutyDetector

Descrizione

Il AWSConfigRemediation-CreateGuardDutyDetector runbook crea un rilevatore Amazon GuardDuty (GuardDuty) nel luogo in Regione AWS cui esegui l'automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- guardduty:CreateDetector
- guardduty:GetDetector

Fasi del documento

- aws:executeAwsApi- Crea un GuardDuty rilevatore.
- aws:assertAwsResourceProperty- Verifica lo stato Status del rilevatore. ENABLED

IAM

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Identity and Access Management Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [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-TroubleshootIAMAccessDeniedEvents

Descrizione

Il runbook di AWSSupport-TroubleshootIAMAccessDeniedEvents automazione aiuta a risolvere i problemi di accesso negato AWS Identity and Access Management (IAM). Il runbook interroga gli eventi CloudTrail recenti di accesso negato relativi all'entità IAM specificata e all'origine degli eventi del AWS servizio. Analizza gli eventi all'interno di una finestra temporale configurabile fino a 24 ore, elaborando fino a 10 eventi per esecuzione. Ogni evento di accesso negato identificato viene esaminato per aiutare a comprendere il contesto del rifiuto e delle azioni tentate. L'automazione analizza sia le politiche IAM basate sull'identità che quelle basate sulle risorse. Per quanto riguarda le politiche basate sull'identità, esamina le politiche in linea e gestite collegate all'entità IAM. Per le politiche basate sulle risorse, valuta le politiche su più servizi AWS tra cui Amazon Simple Storage Service (Amazon S3), (), Amazon Simple Notification Service (Amazon SNS AWS Key Management Service)AWS KMS, AWS Lambda Amazon Elastic Container Registry (Amazon ECR), Amazon API Gateway, Amazon Elastic File System (Amazon EFS), Amazon API Gateway, Amazon Elastic File System (Amazon EFS), CodeArtifact Amazon Simple Queue Service (Amazon SQS), Amazon Service, Signer e. AWS Cloud9 OpenSearch AWS AWS Serverless Application Repository AWS Secrets Manager

Il runbook utilizza le funzionalità di simulazione delle policy IAM per valutare queste policy rispetto alle azioni negate riscontrate negli CloudTrail eventi. Il runbook sfrutta le funzionalità di simulazione delle policy di IAM sia [SimulatePrincipalPolicy](#) per gli utenti IAM che per i ruoli IAM [SimulateCustomPolicy](#) per valutare queste policy rispetto alle azioni negate riscontrate negli eventi.

CloudTrail L'automazione genera un report che aiuta a identificare le azioni specifiche che sono state negate, distingue tra negazioni implicite ed esplicite, elenca le politiche responsabili dei dinieghi di accesso e fornisce spiegazioni per ogni rifiuto. Il rapporto suggerisce anche possibili soluzioni, come l'identificazione delle dichiarazioni di autorizzazione mancanti o delle dichiarazioni di rifiuto in conflitto.

Come funziona?

Il runbook esegue i seguenti passaggi:

- Descrive e convalida `RequesterARN` (ruolo o utente) per ottenere informazioni come il tipo di entità IAM e l'ID IAM.
- Recupera CloudTrail gli eventi associati a `RequesterARNEventSource`, e `ResourceARN` se fornito.
- Analizza CloudTrail gli eventi per ottenere l'azione eseguita quando è stato restituito l'errore `Access Denied`, quindi esamina tutte le policy IAM, ad esempio le politiche in linea e gestite collegate all'entità IAM, nonché le politiche basate sulle risorse. Quindi simula queste politiche rispetto alle azioni rilevate negli errori di accesso negato derivanti dagli CloudTrail eventi in questione per determinare la causa dell'errore.
- Emette un rapporto che determina il tipo di errore di accesso negato, le politiche responsabili degli errori e fornisce suggerimenti per una potenziale soluzione all'errore.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Politica di esempio:

```

{
  "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:GetFileSystemPolicy",
        "sqs:GetQueueAttributes",
        "cloud9:GetEnvironment",
        "es:DescribeDomain",
        "signer:GetSigningProfile",
        "serverlessrepo:GetApplication",
        "secretsmanager:GetResourcePolicy"
      ],

```

```

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

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSsupport-TroubleshootIAMAccessDeniedEvents](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - AutomationAssumeRole (Facoltativo):
 - Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a SSM Automation di eseguire le azioni per tuo conto. Il ruolo deve essere aggiunto alla voce di accesso al cluster Amazon EKS o all'autorizzazione RBAC per consentire le chiamate API Kubernetes.
 - Tipo: `AWS::IAM::Role::Arn`
 - RequesterARN (obbligatorio):
 - Descrizione: (Obbligatorio) L'ARN dell'utente o del ruolo IAM per il quale desideri esaminare le autorizzazioni di accesso su una risorsa specifica. AWS
 - Tipo: stringa
 - Pattern consentito: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:[0-9]{12}:(role|user)\\/[\\w+\\/=,.-]+$`
 - ResourceArn (opzionale):
 - Descrizione: (Facoltativo) L'ARN della risorsa per AWS la quale viene valutato l'accesso negato. La risorsa AWS di destinazione deve trovarsi nella stessa regione in cui viene eseguito il runbook di automazione.
 - Tipo: stringa
 - Pattern consentito: `^$|^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 (Obbligatorio):**
 - Descrizione: (Obbligatorio) L'endpoint dell'API Amazon da cui ha avuto origine l' CloudTrail evento. Ad esempio: `s3.amazonaws.com`.
 - Tipo: stringa
 - Pattern consentito: `^[a-zA-Z0-9.-]+\.\.amazonaws\.\.com$`
- **EventName (Facoltativo):**
 - Descrizione: (Facoltativo) Il nome dell'azione dell'API Amazon associato all' CloudTrail evento. Ad esempio: `s3:CreateBucket`.
 - Tipo: stringa
 - Pattern di autorizzazione: `^[a-zA-Z0-9]+:[A-Za-z0-9]+$`
- **LookBackHours (Facoltativo):**
 - Descrizione: (Facoltativo) Il numero di ore per esaminare gli CloudTrail eventi durante la ricerca di Access Denied eventi. Intervallo valido: 1 da 1 a 24 4 ore.
 - Tipo: integer
 - Pattern consentito: `^[1-9]|1[0-9]|2[0-4]$`
 - Valore predefinito: 12
- **MaxEvents (Facoltativo):**
 - Descrizione: (Facoltativo) Il numero massimo di CloudTrail Access Denied eventi restituiti durante la ricerca di eventi. Intervallo valido: 1 fino agli 5 eventi.
 - Tipo: integer
 - Pattern consentito: `^[1-9]|1[0-9]|2[0-4]$`
 - Impostazione predefinita: 3
- **UseContextEntries (Facoltativo):**
 - Descrizione: (Facoltativo) Se lo specifichi `true`, l'automazione estrae i dettagli sul contesto della richiesta API dall' CloudTrail evento e li include per la simulazione della policy IAM.
 - Tipo: Booleano
 - Pattern di consenso: `^[1-9]|1[0-9]|2[0-4]$`
 - Impostazione predefinita: 3

4. Seleziona Esegui.

5. L'automazione si avvia.

6. Il documento esegue le seguenti operazioni:

- `ValidateRequesterArn`

Convalida e decostruisce l'`RequesterArn`ARN, recuperando informazioni sull'utente o sul ruolo IAM di destinazione.

- `GetCloudTrailEventsWithAccessDeniedError`

Interroga gli CloudTrail eventi per gli `Access Denied` eventi recenti relativi all'entità e al servizio IAM specificati. `AWS EventSource`

- Valuta le politiche `IAMRequester`

Valuta le autorizzazioni IAM dell'entità IAM richiedente rispetto alle azioni degli eventi. CloudTrail Questa valutazione include l'analisi delle politiche basate sull'identità e sulle risorse associate al richiedente. L'automazione utilizza le funzionalità di simulazione delle politiche di IAM per valutare queste politiche nel contesto delle azioni negate identificate negli eventi. CloudTrail

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- `PermissionEvaluationResults`

Genera un rapporto che aiuta a identificare le azioni specifiche che sono state negate, distinguendo tra negazioni implicite ed esplicite. Elenca inoltre le politiche responsabili dei dinieghi di accesso e fornisce spiegazioni per ogni rifiuto. Il rapporto suggerisce anche possibili soluzioni, come l'identificazione delle dichiarazioni di autorizzazione mancanti o delle dichiarazioni di rifiuto contrastanti

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS-AttachIAMToInstance

Descrizione

Associa un ruolo AWS Identity and Access Management (IAM) a un'istanza gestita.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ForceReplace

Tipo: Booleano

Descrizione: (Facoltativo) Contrassegno per specificare se sostituire o meno il profilo IAM esistente.

Impostazione predefinita: true

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza a cui desideri assegnare un ruolo IAM.

- RoleName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del ruolo IAM da aggiungere all'istanza gestita.

Fasi del documento

1. `aws:executeAwsApi- DescribeInstanceProfile` - Trova il profilo dell'istanza IAM collegato all' EC2 istanza.
2. `aws:branch- CheckInstanceProfileAssociations` - Controlla il profilo dell'istanza IAM collegato all' EC2 istanza.
 - a. Se un profilo di istanza IAM è collegato ed `ForceReplace` è impostato su `true`:
 - i. `aws:executeAwsApi- DisassociateIamInstanceProfile` - Dissocia il profilo dell'istanza IAM dall' EC2 istanza.
 - b. `aws:executeAwsApi- ListInstanceProfilesForRole` - Elenca i profili di istanza per il ruolo IAM fornito.
 - c. `aws:branch- CheckInstanceProfileCreated` - Verifica se il ruolo IAM fornito ha un profilo di istanza associato.
 - i. Se il ruolo IAM ha un profilo di istanza associato:
 - A. `aws:executeAwsApi IAMProfileToInstance` - Allega: collega il ruolo del profilo dell'istanza IAM all' EC2 istanza.
 - i. Se al ruolo IAM non è associato un profilo di istanza:
 - A. `aws:executeAwsApi- CreateInstanceProfileForRole` - Crea un ruolo di profilo di istanza per il ruolo IAM specificato.
 - B. `aws:executeAwsApi- AddRoleToInstanceProfile` - Associa il ruolo del profilo dell'istanza al ruolo IAM specificato.
 - C. `aws:executeAwsApi- GetInstanceProfile` - Ottieni i dati del profilo dell'istanza per il ruolo IAM specificato.
 - D. `aws:executeAwsApi IAMProfileToInstanceWithRetry` - Allega: collega il ruolo del profilo dell'istanza IAM all' EC2 istanza.

Output

`Allega IAMProfileToInstanceWithRetry. AssociationId`

`GetInstanceProfile.InstanceProfileName`

`GetInstanceProfile.InstanceProfileArn`

`Allega IAMProfileToInstance. AssociationId`

ListInstanceProfilesForRole.InstanceProfileName

ListInstanceProfilesForRole.InstanceProfileArn

AWS-DeleteIAMInlinePolicy

Descrizione

Il AWS-DeleteIAMInlinePolicy runbook elimina tutte le policy in linea AWS Identity and Access Management (IAM) allegate alle identità IAM specificate.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- IamArns

Tipo: stringa

Descrizione: (Obbligatorio) Un elenco separato da virgole delle ARNs identità IAM da cui si desidera eliminare le politiche in linea. Questo elenco può includere utenti, gruppi o ruoli IAM.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

Fasi del documento

- `aws:executeScript`- Elimina le policy IAM in linea collegate alle identità IAM mirate.

AWSConfigRemediation-DeleteIAMRole

Descrizione

Il `AWSConfigRemediation-DeleteIAMRole` runbook elimina il ruolo AWS Identity and Access Management (IAM) specificato. Questa automazione non elimina i profili di istanza associati al ruolo IAM o i ruoli collegati ai servizi.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- IAMRoleID

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del ruolo IAM che desideri eliminare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam>DeleteRole
- iam>DeleteRolePolicy
- iam:GetRole
- iam>ListAttachedRolePolicies
- iam>ListInstanceProfilesForRole
- iam>ListRolePolicies
- iam>ListRoles
- iam:RemoveRoleFromInstanceProfile

Fasi del documento

- aws:executeScript- Raccoglie il nome del ruolo IAM specificato nel IAMRoleID parametro.
- aws:executeScript- Raccoglie le politiche e i profili di istanza associati al ruolo IAM.
- aws:executeScript- Elimina le politiche allegate.
- aws:executeScript- Elimina il ruolo IAM e verifica che il ruolo sia stato eliminato.

AWSConfigRemediation-DeleteIAMUser

Descrizione

Il `AWSConfigRemediation-DeleteIAMUser` runbook elimina l'utente AWS Identity and Access Management (IAM) specificato. Questa automazione elimina o scollega le seguenti risorse associate all'utente IAM:

- Chiavi di accesso
- Politiche gestite allegate
- Credenziali Git
- Appartenenze al gruppo IAM
- Password utente IAM
- Policy inline
- Dispositivi di autenticazione a più fattori (MFA)
- Certificati di firma
- Chiavi pubbliche SSH

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- IAMUserId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'utente IAM che desideri eliminare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

- `aws:executeScript`- Raccoglie il nome utente dell'utente IAM specificato nel `IAMUserId` parametro.
- `aws:executeScript`- Raccoglie chiavi di accesso, certificati, credenziali, dispositivi MFA e chiavi SSH associati all'utente IAM.
- `aws:executeScript`- Raccoglie le appartenenze ai gruppi e le politiche per l'utente IAM.
- `aws:executeScript`- Elimina chiavi di accesso, certificati, credenziali, dispositivi MFA e chiavi SSH associati all'utente IAM.
- `aws:executeScript`- Elimina le appartenenze ai gruppi e le politiche per l'utente IAM.
- `aws:executeScript`- Elimina l'utente IAM e verifica che l'utente sia stato eliminato.

AWSConfigRemediation-DeleteUnusedIAMGroup

Descrizione

Il `AWSConfigRemediation-DeleteUnusedIAMGroup` runbook elimina un gruppo IAM che non contiene utenti.

Il `AWSConfigRemediation-DeleteUnusedIAMGroup` runbook elimina un gruppo IAM che non contiene utenti.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- GroupName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del gruppo IAM che desideri eliminare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam>DeleteGroup
- iam>DeleteGroupPolicy
- iam:DetachGroupPolicy

Fasi del documento

- aws:executeScript- Rimuove le policy IAM gestite e in linea collegate al gruppo IAM di destinazione, quindi elimina il gruppo IAM.

AWSConfigRemediation-DeleteUnusedIAMPolicy

Descrizione

Il `AWSConfigRemediation-DeleteUnusedIAMPolicy` runbook elimina una policy AWS Identity and Access Management (IAM) che non è associata a nessun utente, gruppo o ruolo.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `IAMResourceId`

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa della policy IAM che desideri eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

- `config:ListDiscoveredResources`
- `iam>DeletePolicy`
- `iam>DeletePolicyVersion`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`
- `iam:ListPolicyVersions`

Fasi del documento

- `aws:executeScript`- Elimina la politica specificata nel `IAMResourceId` parametro e verifica che la politica sia stata eliminata.

AWSConfigRemediation-DetachIAMPolicy

Descrizione

Il `AWSConfigRemediation-DetachIAMPolicy` runbook rimuove la policy AWS Identity and Access Management (IAM) specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- IAMResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della policy IAM che desideri scollegare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DetachGroupPolicy
- iam:DetachRolePolicy
- iam:DetachUserPolicy
- iam:GetPolicy
- iam:ListEntitiesForPolicy

Fasi del documento

- aws:executeScript- Scollega la policy IAM da tutte le risorse.

AWSConfigRemediation-EnableAccountAccessAnalyzer

Descrizione

Il AWSConfigRemediation-EnableAccountAccessAnalyzer runbook crea un AWS Identity and Access Management (IAM) Access Analyzer nel tuo Account AWS. Per informazioni su Access Analyzer, consulta [Using AWS IAM Access Analyzer](#) nella IAM User Guide.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AnalyzerName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome dell'analizzatore da creare.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- access-analyzer:CreateAnalyzer
- access-analyzer:GetAnalyzer

Fasi del documento

- `aws:executeAwsApi`- Crea un analizzatore di accesso per il tuo account.
- `aws:waitForAwsResourceProperty`- Attende che sia lo stato dell'analizzatore di accesso. `ACTIVE`
- `aws:assertAwsResourceProperty`- Conferma che lo stato dell'analizzatore di accesso è. `ACTIVE`

AWSSupport-GrantPermissionsToIAMUser

Descrizione

Questo runbook concede le autorizzazioni specificate a un gruppo IAM (nuovo o esistente) e vi aggiunge l'utente IAM esistente. Le policy valide disponibili sono: [Billing \(Fatturazione\)](#) o [Support \(Supporto\)](#). Per abilitare l'accesso al servizio di fatturazione per IAM, ricorda di attivare anche [l'accesso utente IAM e l'accesso utente federato alle pagine di fatturazione e gestione costi](#).

Important

Se si specifica un gruppo di IAM esistente, a tutti gli utenti IAM correnti inclusi nel gruppo verranno assegnate le nuove autorizzazioni.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- IAMGroupName

Tipo: stringa

Impostazione predefinita: ExampleSupportAndBillingGroup

Descrizione: (obbligatorio) può essere un gruppo nuovo o esistente. Deve essere conforme ai [limiti per i nomi delle entità IAM](#).

- IAMUserName

Tipo: stringa

Predefinito: ExampleUser

Descrizione: (obbligatorio) deve essere un utente esistente.

- LambdaAssumeRole

Tipo: stringa

Descrizione: (facoltativo) ARN del ruolo presunto da Lambda.

- Autorizzazioni

Tipo: stringa

Valori validi: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

Predefinito: SupportAndBillingFullAccess

Descrizione: (Obbligatorio) Scegli una delle seguenti opzioni: `SupportFullAccess` garantisce l'accesso completo al Support center. `BillingFullAccess` concede l'accesso completo alla dashboard di fatturazione. `SupportAndBillingFullAccess` garantisce l'accesso completo sia al Support center che alla dashboard di fatturazione. Ulteriori informazioni sulle policy sono disponibili nei dettagli del documento.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Le autorizzazioni richieste dipendono dalla modalità `AWSSupport-GrantPermissionsToIAMUser` di esecuzione.

In esecuzione come utente o ruolo attualmente connesso

Si consiglia di allegare la policy gestita di `AmazonSSMAutomationRole` Amazon e le seguenti autorizzazioni aggiuntive per poter creare la funzione Lambda e il ruolo IAM da passare a Lambda:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "lambda:InvokeFunction",
                "lambda:CreateFunction",
                "lambda>DeleteFunction",
                "lambda:GetFunction"
            ],
            "Resource":
                "arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
            "Effect": "Allow"
        },
        {
            "Effect" : "Allow",
            "Action" : [
                "iam:CreateGroup",
                "iam:AddUserToGroup",
                "iam:ListAttachedGroupPolicies",
                "iam:GetGroup",
                "iam:GetUser"
            ],
            "Resource" : [
                "arn:aws:iam:*:user/*",
                "arn:aws:iam:*:group/*"
            ]
        },
        {
            "Effect" : "Allow",
            "Action" : [
                "iam:AttachGroupPolicy"
            ]
        }
    ]
}
```

```

    ],
    "Resource": "*",
    "Condition": {
        "ArnEquals": {
            "iam:PolicyArn": [
                "arn:aws:iam::aws:policy/job-function/Billing",
                "arn:aws:iam::aws:policy/AWSSupportAccess"
            ]
        }
    }
},
{
    "Effect" : "Allow",
    "Action" : [
        "iam:ListAccountAliases",
        "iam:GetAccountSummary"
    ],
    "Resource" : "*"
}
]
}

```

Utilizzo di AutomationAssumeRole e LambdaAssumeRole

L'utente deve disporre dei `StartAutomationExecution` permessi `ssm:` sul runbook e `iam: PassRole` sui ruoli IAM passati come `and. AutomationAssumeRoleLambdaAssumeRole`. Di seguito sono riportate le autorizzazioni richieste da ciascun ruolo IAM:

AutomationAssumeRole

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "lambda:InvokeFunction",
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction"
            ],
            "Resource":
                "arn:aws:lambda*:ACCOUNTID:function:AWSSupport-*",
            "Effect": "Allow"
        }
    ]
}

```

```

    }
  ]
}

```

LambdaAssumeRole

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateGroup",
        "iam:AddUserToGroup",
        "iam:ListAttachedGroupPolicies",
        "iam:GetGroup",
        "iam:GetUser"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/*",
        "arn:aws:iam::*:group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachGroupPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "iam:PolicyArn": [
            "arn:aws:iam::aws:policy/job-function/Billing",
            "arn:aws:iam::aws:policy/AWSSupportAccess"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",

```



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

Fasi del documento

1. `aws:createStack`- Esegui AWS CloudFormation Template per creare una funzione Lambda.
2. `aws:invokeLambdaFunction`- Esegui Lambda per impostare le autorizzazioni IAM.
3. `aws:deleteStack`- Elimina CloudFormation modello.

Output

`configureIAM.Payload`

AWSConfigRemediation-RemoveUserPolicies

Descrizione

Il `AWSConfigRemediation-RemoveUserPolicies` runbook elimina le policy in linea AWS Identity and Access Management (IAM) e rimuove tutte le policy gestite collegate all'utente specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- IAMUserID

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'utente da cui desideri rimuovere le politiche.

- PolicyType

Tipo: stringa

Valori validi: Tutti | In linea | Gestiti

Predefinito: Tutti

Descrizione: (Obbligatorio) Il tipo di policy IAM che desideri rimuovere dall'utente.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam>DeleteUserPolicy
- iam:DetachUserPolicy
- iam:ListAttachedUserPolicies
- iam:ListUserPolicies
- iam:ListUsers

Fasi del documento

- aws:executeScript- Elimina e scollega le policy IAM dall'utente specificato nel parametro. IAMUserID

AWSConfigRemediation-ReplaceIAMInlinePolicy

Descrizione

Il `AWSConfigRemediation-ReplaceIAMInlinePolicy` runbook sostituisce una policy in linea AWS Identity and Access Management (IAM) con una policy IAM gestita replicata. Per una policy in linea associata a un utente, gruppo o ruolo, le autorizzazioni della policy in linea vengono clonate in una policy IAM gestita. La policy IAM gestita viene aggiunta alla risorsa e la policy in linea viene rimossa. AWS Config deve essere abilitata nel Regione AWS luogo in cui si esegue questa automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- InlinePolicyName

Tipo: StringList

Descrizione: (Obbligatoria) La policy IAM in linea che desideri sostituire.

- ResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'utente, del gruppo o del ruolo IAM di cui desideri sostituire la politica in linea.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

- `aws:executeScript`- Sostituisci la policy IAM in linea con una policy AWS replicata sulla risorsa specificata.

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

Descrizione

Il `AWSConfigRemediation-RevokeUnusedIAMUserCredentials` runbook revoca le password non utilizzate AWS Identity and Access Management (IAM) e le chiavi di accesso attive. Questo runbook disattiva anche le chiavi di accesso scadute ed elimina i profili di accesso scaduti. AWS Config deve essere abilitato nel luogo in cui si esegue questa automazione Regione AWS .

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `IAMResourceId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della risorsa IAM da cui desideri revocare le credenziali non utilizzate.

- `MaxCredentialUsageAge`

Tipo: stringa

Impostazione predefinita: 90

Descrizione: (Obbligatorio) Il numero di giorni entro i quali la credenziale deve essere stata utilizzata.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:ListDiscoveredResources`
- `iam:DeleteAccessKey`
- `iam:DeleteLoginProfile`
- `iam:GetAccessKeyLastUsed`
- `iam:GetLoginProfile`
- `iam:GetUser`
- `iam:ListAccessKeys`
- `iam:UpdateAccessKey`

Fasi del documento

- `aws:executeScript`- Revoca le credenziali IAM per l'utente specificato nel parametro. `IAMResourceId` Le chiavi di accesso scadute vengono disattivate e i profili di accesso scaduti vengono eliminati.

Note

Assicurati di configurare il `MaxCredentialUsageAge` parametro di questa azione di riparazione in modo che corrisponda al `maxAccessKeyAge` parametro della AWS Config regola utilizzata per attivare questa azione: [access-keys-rotated](#)

AWSConfigRemediation-SetIAMPasswordPolicy

Descrizione

Il `AWSConfigRemediation-SetIAMPasswordPolicy` runbook imposta la politica delle password utente AWS Identity and Access Management (IAM) per il tuo Account AWS.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- AllowUsersToChangePassword

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se impostato su `true`, tutti gli utenti IAM del tuo account Account AWS possono utilizzare il AWS Management Console per modificare le proprie password.

- HardExpiry

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se impostato su `true`, agli utenti IAM viene impedito di reimpostare le password dopo la scadenza della password.

- MaxPasswordAge

Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero di giorni di validità della password di un utente IAM.

- `MinimumPasswordLength`

Tipo: integer

Valore predefinito: 6

Descrizione: (Facoltativo) Il numero minimo di caratteri che può contenere la password di un utente IAM.

- `PasswordReusePrevention`

Tipo: integer

Impostazione predefinita: 0

Descrizione: (Facoltativo) Il numero di password precedenti che un utente IAM non può riutilizzare.

- `RequireLowercaseCharacters`

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se impostata su `true`, la password di un utente IAM deve contenere un carattere minuscolo dell'alfabeto latino di base ISO (dalla a alla z).

- `RequireNumbers`

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se impostata su `true`, la password di un utente IAM deve contenere un carattere numerico (0-9).

- `RequireSymbols`

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se impostata su `true`, la password di un utente IAM deve contenere un carattere non alfanumerico (! @ # \$ % ^ * () _ + - = [] { } | ').

- `RequireUppercaseCharacters`

Tipo: Booleano

Impostazione predefinita: `false`

Descrizione: (Facoltativo) Se impostata su `true`, la password di un utente IAM deve contenere un carattere maiuscolo dell'alfabeto latino di base ISO (dalla A alla Z).

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

Fasi del documento

- `aws:executeScript`- Imposta la politica delle password utente IAM in base ai valori specificati per i parametri del runbook per il tuo Account AWS

AWSSupport-ContainIAMPrincipal

Descrizione

In caso di incidente di sicurezza o di sospetta compromissione di un utente/ruolo AWS Identity and Access Management (IAM) o di un utente dell' AWS Identity Center (IDC), è fondamentale isolare rapidamente l'identità interessata, preservandone al contempo la configurazione per le indagini. Il `AWSSupport-ContainIAMPrincipal` runbook fornisce un approccio strutturato e reversibile per contenere le identità IAM o IDC compromesse, bloccando efficacemente il loro accesso alle risorse e prevenendo la potenziale diffusione della compromissione. AWS

Questo processo automatizzato consente l'indagine senza alterazioni permanenti della configurazione dell'identità, consentendo il ripristino del normale accesso quando ritenuto appropriato. Il processo di contenimento mantiene l'utente o il ruolo all'interno di IAM o l'utente all'interno di IDC, isolandolo efficacemente da tutte le attività di rete. Questo isolamento impedisce alla risorsa di identità contenuta di comunicare con le risorse all'interno del tuo Amazon Virtual Private Cloud o di accedere alle risorse Internet. Il contenimento è progettato per essere reversibile e consentire il ripristino del normale accesso quando ritenuto appropriato.

Come funziona?

Il `AWSSupport-ContainIAMPrincipal` runbook implementa un processo di contenimento completo per gli utenti, i ruoli e gli utenti di Identity Center di IAM. Quando viene eseguito in `Contain` modalità, prima convalida tutti i parametri di input ed esegue controlli di sicurezza sul bucket Amazon S3 specificato. Quindi raccoglie informazioni dettagliate sul principale IAM di destinazione e applica le misure di contenimento appropriate in base al tipo principale. Per gli utenti IAM, disabilita le chiavi di accesso, rimuove l'accesso alla console e applica una politica di negazione. Per i ruoli IAM, allega una policy di negazione che revoca le autorizzazioni per le sessioni create prima del contenimento. Per gli utenti di Identity Center, rimuove i set di autorizzazioni, le appartenenze ai gruppi e applica una politica di negazione. Durante tutto il processo, il runbook esegue il backup della configurazione originale in un bucket Amazon S3 per un potenziale ripristino. Quando viene eseguito in `Restore` modalità, tenta di riportare il file principale allo stato di precontenimento utilizzando la configurazione di backup. Il runbook include un'`DryRun` opzione per visualizzare in anteprima le modifiche senza applicarle e fornisce report completi sia sulle operazioni riuscite che sugli scenari di errore.

Important

- **Uso di privilegi elevati:** questo documento SSM esegue diverse operazioni che richiedono privilegi elevati, come la modifica delle policy di identità IAM e IDC e l'applicazione di configurazioni di quarantena. Queste azioni potrebbero potenzialmente portare a un aumento dei privilegi o avere un impatto su altri carichi di lavoro che dipendono dalle identità di destinazione. È necessario esaminare le autorizzazioni concesse al ruolo specificato dal `AutomationAssumeRole` parametro e assicurarsi che siano appropriate per il caso d'uso previsto. Puoi fare riferimento alla seguente AWS documentazione per ulteriori informazioni sulle autorizzazioni IAM:
 - [Autorizzazioni di Identity and Access Management \(IAM\)](#)
 - [AWS Autorizzazioni di automazione di Systems Manager](#)

- **Rischi di indisponibilità del carico di lavoro:** questo documento Systems Manager esegue azioni di isolamento che potrebbero potenzialmente causare indisponibilità o interruzioni dei carichi di lavoro. Se eseguito durante un evento di sicurezza, limiterà l'accesso alla risorsa interessata revocando le autorizzazioni AWS API alle identità IAM e IDC specificate, impedendo loro di effettuare chiamate o azioni API. AWS Ciò potrebbe influire su tutte le applicazioni o i servizi che dipendono da queste identità.
- **Creazione di risorse aggiuntive:** il documento di automazione può creare in modo condizionale risorse aggiuntive, come un bucket Amazon Simple Storage Service (Amazon S3) e oggetti Amazon S3 in essi memorizzati, a seconda dei parametri di esecuzione. Queste risorse comporteranno costi aggiuntivi in base all'utilizzo. AWS
- **Rischi di ripristino:** se il parametro Action è impostato suRestore, questo documento SSM tenta di ripristinare la configurazione dell'identità IAM o IDC allo stato originale. Tuttavia, esiste il rischio che il processo di ripristino possa fallire, lasciando l'identità IAM o IDC in uno stato incoerente. Il documento fornisce istruzioni per il ripristino manuale in caso di tali errori, ma è necessario essere preparati a gestire potenziali problemi durante il processo di ripristino.

Si consiglia di esaminare attentamente il runbook, comprenderne i potenziali impatti e testarlo in un ambiente non di produzione prima di eseguirlo nell'ambiente di produzione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti autorizzazioni per utilizzare correttamente il runbook:

- s3: GetBucketLocation
- s3: GetBucket
- s3: ListBucket
- s3: GetBucketPublicAccessBlocks
- s3: GetAccountPublicAccessBlocks
- s3: GetBucketPolicyStatus
- s3: GetBucketAcl
- s3: GetObject
- s3: CreateBucket
- s3: PutObject
- obiettivo: GetUser
- Io sono: GetUserPolicy
- Io sono: GetRole
- Io sono: ListUserPolicies
- Io sono: ListAttachedUserPolicies
- Io sono: ListAccessKeys
- Io sono: ListMfaDevices
- Io sono: ListVirtual MFADevices
- Io sono: GetLoginProfile
- Io sono: GetPolicy
- Io sono: GetRolePolicy
- Io sono: ListPolicies
- Io sono: ListAttachedRolePolicies
- Io sono: ListRolePolicies
- Io sono: UpdateAccessKey
- Io sono: CreateAccessKey
- Io sono: DeleteLoginProfile
- Io sono: DeleteAccessKey
- Io sono: PutUserPolicy
- Io sono: DeleteUserPolicy

- IAM: disattiva MFADevice
- sono: AttachRolePolicy
- lo sono: AttachUserPolicy
- lo sono: DeleteRolePolicy
- iam: tag MFADevice
- Sono: PutRolePolicy
- lo sono: TagPolicy
- lo sono: TagRole
- lo sono: TagUser
- lo sono: UntagUser
- lo sono: UntagRole
- organizzazioni: ListAccounts
- quindi: ListPermissionSetsProvisionedToAccount
- sso: GetInlinePolicyForPermissionSet
- sso: ListInstances
- cartella sso: SearchUsers
- sso: ListPermissionSets
- sso: ListAccountAssignments
- cartella sso: DescribeUser
- archivio di identità: ListUsers
- archivio di identità: ListGroups
- archivio di identità: IsMemberInGroups
- archivio di identità: ListGroupMemberships
- gestore dei segreti: CreateSecret
- gestore dei segreti: DeleteSecret
- quindi: DeleteAccountAssignment
- sso: PutInlinePolicyToPermissionSet
- sso: CreateAccountAssignment
- sso: DeleteInlinePolicyFromPermissionSet
- sso: TagResource

- sso: UntagResource
- archivio di identità: DeleteGroupMembership
- archivio di identità: CreateGroupMembership

Ecco un esempio di policy IAM che concede le autorizzazioni necessarie per:
AutomationAssumeRole

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucket",
        "s3:ListBucket",
        "s3:GetBucketPublicAccessBlocks",
        "s3:GetAccountPublicAccessBlocks",
        "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": "*"
}
]
}
```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-ContainIAMPrincipal](#) alla console AWS Systems Manager.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:
 - AutomationAssumeRole (Facoltativo):
 - Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le

azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Tipo: `AWS::IAM::Role::Arn`
- PrincipalType (Obbligatorio):
 - Descrizione: (Obbligatorio) Il AWS tipo principale IAM: utente IAM, ruolo IAM o utente Identity Center.
 - Tipo: stringa
 - Valori consentiti: `IAM user|IAM role|Identity Center user`
- PrincipalName (Obbligatorio):
 - Descrizione: (Obbligatorio) Il nome del principale IAM. Per gli utenti di Identity Center, fornisci il nome utente.
 - Tipo: stringa
 - Modello consentito: `^[a-zA-Z0-9\\.\_-\\\\!*'() /+=, @]{1,1024}$`
- Azione (richiesta):
 - Descrizione: (Obbligatorio) Seleziona se `Contain` isolare il principale IAM di destinazione o provare `Restore` a ripristinare il principale IAM alla sua configurazione originale da un backup precedente.
 - Tipo: stringa
 - Valori consentiti: `Contain|Restore`
- DryRun (Facoltativo):
 - Descrizione: (Facoltativo) Se impostata su `true`, l'automazione non apporterà alcuna modifica al principale IAM di destinazione, ma genererà risultati su ciò che avrebbe tentato di modificare, specificando in dettaglio ogni passaggio. Valore predefinito: `true`.
 - Tipo: Booleano
 - Valori consentiti: `true|false`
- ActivateDisabledKeys (Condizionale):
 - Descrizione: (Condizionale) Se il parametro di input `Action` è impostato su `Restore` e l'utente IAM `PrincipalType` è impostato su, questa opzione determina se questa automazione deve provare ad attivare le chiavi di accesso associate se disattivata. Tieni presente che l'integrità di una chiave di accesso compromessa non può essere verificata. AWS sconsiglia vivamente di riattivare una chiave compromessa. Si consiglia invece di generare nuove chiavi. Valore predefinito: `false`.

- Tipo: Booleano
- Valori consentiti: `true` | `false`
- BackupS3 BucketName (condizionale):
 - Descrizione: (Condizionale) Il bucket Amazon Amazon S3 per il backup della configurazione principale IAM quando l'Action è impostata su `Contain` per ripristinare la configurazione da quando l'Action è impostata. Restore Tieni presente che se l'azione specificata è `Contain` e il runbook non è in grado di accedere al bucket o non viene fornito un valore, nel tuo account viene creato un nuovo bucket con il nome. `awssupport-containiamprincipal-
<random-string>` Se `DryRun` è impostato su `true` questo parametro è obbligatorio.
 - Tipo: `AWS::S3::Bucket::Name`
- BackupS3 KeyName (condizionale):
 - Descrizione: (Condizionale) Se Action è impostato su `Restore`, specifica la chiave Amazon Amazon S3 che l'automazione utilizzerà per tentare di ripristinare la configurazione principale IAM. La chiave Amazon S3 segue in genere questo formato: `{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json` La chiave può essere ottenuta dall'output di una precedente esecuzione di automazione del contenimento.
 - Tipo: stringa
 - Modello consentito: `^[a-zA-Z0-9\\.\_\-\!\*'()]/]{0,1024}$`
- BackupS3 BucketAccess (condizionale):
 - Descrizione: (Condizionale) L'ARN degli utenti o dei ruoli IAM a cui sarà consentito l'accesso al bucket Amazon Amazon S3 di backup dopo l'esecuzione delle azioni di contenimento. Questo parametro è obbligatorio quando Action è. `Contain` L'utente o `AutomationAssumeRole`, in sua assenza, l'utente nel cui contesto viene eseguita l'automazione viene aggiunto automaticamente all'elenco.
 - Tipo: `StringList`
 - Modello consentito: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:[0-9]{12}:(role|user)\\/[\\w+\\/=, .@-]+$`
- TagIdentifier (Opzionale):
 - Descrizione: (Facoltativo) Etichetta il principale IAM con un tag a tua scelta utilizzando il seguente formato: `Key=<EXAMPLE_KEY>, Value=<EXAMPLE_VALUE>`. Questa opzione ti consente di tenere traccia dei principali IAM che sono stati presi di mira da questo runbook. Nota: le chiavi e i valori dei tag fanno distinzione tra maiuscole e minuscole.
 - Tipo: stringa

- Modello consentito: `^$|^([Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{0,128})$`

4. Seleziona Esegui.

5. L'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- `ValidateRequiredInputs`

Convalida i parametri di input di automazione richiesti in base a `Action` quanto specificato.

- `CheckBackupS3BucketName`

Verifica se il bucket Amazon Amazon S3 di destinazione concede `read` potenzialmente l'accesso `write` pubblico ai suoi oggetti. In caso di flusso di lavoro di contenimento, viene creato un nuovo bucket Amazon Amazon S3 se `BackupS3BucketName` il bucket non esiste.

- `BranchOnAction`

Suddivide l'automazione in base al valore specificato. `Action`

- `BranchOnPrincipalTypeAndDryRun`

Suddivide l'automazione in base al tipo di principale IAM (utente IAM, ruolo IAM o utente Identity Center) e se è in esecuzione in `DryRun` modalità.

- `BranchOnPrincipalTypeForContain`

Suddivide l'automazione in base `Contain` all'azione e al tipo principale IAM (utente IAM, ruolo IAM o utente Identity Center) specificato nell'input.

- `Ottieni IAMUser`

Ottiene l'ora di creazione e il nome utente dell'utente IAM di destinazione.

- `Ottieni IAMUser dettagli`

Ottiene e archivia la configurazione dell'utente IAM di destinazione, incluse le policy in linea, le policy gestite, le chiavi di accesso, i dispositivi MFA e il profilo di accesso.

- `Aggiornamenti 3 KeyForUser`

Aggiorna la variabile di automazione `'S3Key'` dall'output del passaggio. `GetIAMUserDetails`

- `Ottieni IAMRole`

Ottiene l'ora di creazione, il nome del ruolo e il percorso del ruolo IAM di destinazione.

- Ottieni IAMRole dettagli

Ottiene e archivia la configurazione del ruolo IAM di destinazione, incluse le policy in linea e le policy gestite associate al ruolo.

- Aggiornamenti 3 KeyForRole

Aggiorna la variabile di automazione 'S3Key' dall'output del passaggio. `GetIAMRoleDetails`

- `GetIdentityStoreId`

Ottiene l'ID dell'istanza AWS IAM Identity Center associata all' AWS account.

- Ottieni IDCUser

Ottiene l'ID utente dell'utente di Identity Center di destinazione utilizzando l'ID Identity Store.

- Raccogli IDCUser dettagli

Ottiene e archivia la configurazione dell'utente dell'Identity Center di destinazione, incluse le assegnazioni degli account, i set di autorizzazioni associati e le politiche in linea.

- Aggiornamenti 3 KeyFor IDCUser

Aggiorna la variabile di automazione 'S3Key' dall'output del passaggio.

`GatherIDCUserDetails`

- `BranchOnIdentityContain`

Suddivide l'automazione in base al valore `DryRun` e al tipo principale IAM dell'Contenazione.

- `BranchOnDisableAccessKeys`

Suddivide l'automazione in base al fatto che l'utente IAM disponga di chiavi di accesso che devono essere disabilitate.

- `DisableAccessKeys`

Disattiva le chiavi di accesso utente IAM attive.

- `BranchOnDisableConsoleAccess`

Filiali a seconda che l'utente IAM abbia abilitato o meno l'accesso alla Console di AWS gestione.

- `DisableConsoleAccess`

Rimuove l'accesso basato su password dell'utente IAM alla console di gestione. AWS

- `AttachInlineDenyPolicyToUser`

Allega una politica di negazione all'utente IAM per revocare le autorizzazioni per i token di sessione precedenti.

- `AttachInlineDenyPolicyToRole`

Allega una politica di negazione al ruolo IAM per revocare le autorizzazioni per i token di sessione precedenti.

- `RemovePermissionSets`

Rimuove i set di autorizzazioni associati all'utente di Identity Center.

- `Rimuovi IDCUser da IDCGroups`

Rimuove l'utente di Identity Center dai gruppi di Identity Center.

- `AttachInlineDenyPolicyToPermissionSet`

Allega una politica di rifiuto ai set di autorizzazioni associati all'utente di Identity Center.

- `BranchOnReactivateKeys`

Suddivide l'automazione in base al `ActivateDisabledKeys` parametro durante il processo di ripristino.

- `DetachInlineDenyPolicy`

Rimuove la politica di rifiuto associata al ruolo IAM durante il processo di contenimento.

- `DetachInlineDenyPolicyFromPermissionSet`

Rimuove la politica di negazione allegata ai set di autorizzazioni durante il processo di contenimento.

- `ReportContain`

Fornisce informazioni dettagliate sulle azioni di contenimento che verrebbero eseguite quando `DryRun` è impostato su `True`

- `ReportRestore`

Fornisce informazioni dettagliate sulle azioni di ripristino che verrebbero eseguite quando

`DryRun` è impostato su `True`

- **ReportContainFailure**

Fornisce istruzioni complete per ripristinare manualmente la configurazione originale del principale IAM durante uno scenario di errore del flusso di lavoro di contenimento.

- **ReportRestoreFailure**

Fornisce istruzioni dettagliate per completare manualmente il ripristino della configurazione originale del principale IAM durante uno scenario di errore del workflow di ripristino.

7. Una volta completata l'esecuzione, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- **Contiene.Output IAMPrincipal**

Fornisce informazioni dettagliate sulle azioni di contenimento eseguite quando Action è impostato su Contain ed DryRun è impostato su False. Include informazioni sulla posizione di backup, sulle politiche di negazione applicate e sulle configurazioni modificate.

- **Ripristina .Output IAMPrincipal**

Fornisce informazioni dettagliate sulle azioni di ripristino eseguite quando Action è impostato su Restore ed DryRun è impostato su False. Include informazioni sulle configurazioni ripristinate e sugli eventuali problemi riscontrati durante il ripristino.

- **ReportContain.Output**

Fornisce informazioni dettagliate sulle azioni di contenimento che verrebbero eseguite quando Action è impostato su Contain ed DryRun è impostato su True. Include un confronto tra le configurazioni attuali e successive al contenimento.

- **ReportRestore.Output**

Fornisce informazioni dettagliate sulle azioni di ripristino che verrebbero eseguite quando Action è impostato su Restore ed DryRun è impostato su True. Mostra la configurazione corrente e la configurazione originale che verrebbe ripristinata.

- **ReportContainFailure.Uscita**

Fornisce istruzioni complete per ripristinare manualmente la configurazione originale del principale IAM durante uno scenario di errore del flusso di lavoro di contenimento.

- **ReportRestoreFailure.Output**

Fornisce istruzioni dettagliate per completare manualmente il ripristino della configurazione originale del principale IAM durante uno scenario di errore del workflow di ripristino.

Output

Una volta completata l'esecuzione, consulta la sezione Output per i risultati dettagliati:

- Contenere .Output IAMPrincipal

Fornisce informazioni dettagliate sulle azioni di contenimento eseguite quando Action è impostato su Contain ed DryRun è impostato su False. Include informazioni sulla posizione di backup, sulle politiche di negazione applicate e sulle configurazioni modificate.

- Ripristina .Output IAMPrincipal

Fornisce informazioni dettagliate sulle azioni di ripristino eseguite quando Action è impostato su Restore ed DryRun è impostato su False. Include informazioni sulle configurazioni ripristinate e sugli eventuali problemi riscontrati durante il ripristino.

- ReportContain.Output

Fornisce informazioni dettagliate sulle azioni di contenimento che verrebbero eseguite quando Action è impostato su Contain ed DryRun è impostato su True. Include un confronto tra le configurazioni attuali e successive al contenimento.

- ReportRestore.Output

Fornisce informazioni dettagliate sulle azioni di ripristino che verrebbero eseguite quando Action è impostato su Restore ed DryRun è impostato su True. Mostra la configurazione corrente e la configurazione originale che verrebbe ripristinata.

- ReportContainFailure.Uscita

Fornisce istruzioni complete per ripristinare manualmente la configurazione originale del principale IAM durante uno scenario di errore del flusso di lavoro di contenimento.

- ReportRestoreFailure.Output

Fornisce istruzioni dettagliate per completare manualmente il ripristino della configurazione originale del principale IAM durante uno scenario di errore del workflow di ripristino.

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esecuzione di un'automazione semplice](#)
- [Configurazione dell'automazione](#)
- [Flussi di lavoro di Support Automation](#)

Flusso di dati Amazon Kinesis

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Kinesis Data Streams. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-EnableKinesisStreamEncryption](#)

AWS-EnableKinesisStreamEncryption

Descrizione

Il AWS-EnableKinesisStreamEncryption runbook abilita la crittografia su un Amazon Kinesis Data Streams (Kinesis Data Streams). Le applicazioni Producer che scrivono su uno stream crittografato riscontreranno errori se non hanno accesso alla chiave (). AWS Key Management Service AWS KMS

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- KinesisStreamName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome dello stream su cui si desidera abilitare la crittografia.

- KeyId

Tipo: stringa

Impostazione predefinita: alias/aws/kinesis

Descrizione: (Obbligatoria) La AWS KMS chiave gestita dal cliente che desideri utilizzare per la crittografia. Questo valore può essere un identificatore univoco globale, un ARN per un alias o una chiave o un nome alias preceduto da «alias/». È inoltre possibile utilizzare la chiave AWS gestita utilizzando il valore predefinito per il parametro.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- kinesis:DescribeStream
- kinesis:StartStreamEncryption
- kms:DescribeKey

Fasi del documento

- `VerifyKinesisStreamStatus (aws:waitForAwsResourceProperty)` - Verifica lo stato di Kinesis Data Streams.
- `EnableKinesisStreamEncryption (aws:executeAwsApi)` - Abilita la crittografia per Kinesis Data Streams.
- `VerifyKinesisStreamUpdateComplete (aws:waitForAwsResourceProperty)` - Attende che lo stato di Kinesis Data Streams ritorni a. ACTIVE
- `VerifyKinesisStreamEncryption (aws:assertAwsResourceProperty)` - Verifica che la crittografia sia abilitata per Kinesis Data Streams.

AWS KMS

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Key Management Service Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSConfigRemediation-CancelKeyDeletion](#)
- [AWSConfigRemediation-EnableKeyRotation](#)

AWSConfigRemediation-CancelKeyDeletion

Descrizione

Il `AWSConfigRemediation-CancelKeyDeletion` runbook annulla l'eliminazione della chiave gestita dal cliente AWS Key Management Service (AWS KMS) specificata dall'utente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- KeyId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della chiave gestita dal cliente di cui desideri annullare l'eliminazione.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:CancelKeyDeletion
- kms:DescribeKey

Fasi del documento

- aws:executeAwsApi- Annulla l'eliminazione della chiave gestita dal cliente specificata nel KeyId parametro.
- aws:assertAwsResourceProperty- Conferma che l'eliminazione della chiave è disabilitata nella chiave gestita dal cliente.

AWSConfigRemediation-EnableKeyRotation

Descrizione

Il `AWSConfigRemediation-EnableKeyRotation` runbook consente la rotazione automatica delle chiavi per la chiave simmetrica AWS Key Management Service (AWS KMS) gestita dal cliente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `KeyId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della chiave gestita dal cliente su cui desideri abilitare la rotazione automatica delle chiavi.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

Fasi del documento

- `aws:executeAwsApi`- Abilita la rotazione automatica delle chiavi sulla chiave gestita dal cliente specificata nel `KeyId` parametro.
- `aws:assertAwsResourceProperty`- Conferma che la rotazione automatica delle chiavi è abilitata sulla chiave gestita dal cliente.

Lambda

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Lambda Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing](#)
- [AWSConfigRemediation-DeleteLambdaFunction](#)
- [AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK](#)
- [AWSConfigRemediation-MoveLambdaToVPC](#)
- [AWSSupport-RemediateLambdaS3Event](#)
- [AWSSupport-TroubleshootLambdaInternetAccess](#)
- [AWSSupport-TroubleshootLambdaS3Event](#)

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

Descrizione

Il `AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing` runbook abilita il AWS X-Ray live tracing sulla AWS Lambda funzione specificata nel parametro. `FunctionName`

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- FunctionName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome o l'ARN della funzione Lambda su cui abilitare la traccia.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `lambda:UpdateFunctionConfiguration`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Fasi del documento

- `aws:executeAwsApi`- Abilita il tracciamento X-Ray sulla funzione Lambda specificata nel parametro. FunctionName
- `aws:assertAwsResourceProperty`- Verifica che il tracciamento X-Ray sia stato abilitato sulla funzione Lambda.

Output

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Risposta dalla chiamata UpdateFunctionConfiguration API.

AWSConfigRemediation-DeleteLambdaFunction

Descrizione

Il AWSConfigRemediation-DeleteLambdaFunction runbook elimina la AWS Lambda funzione specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- LambdaFunctionName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della funzione Lambda che desideri eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

Fasi del documento

- `aws:executeAwsApi`- Elimina la funzione Lambda specificata nel `LambdaFunctionName` parametro.
- `aws:executeScript`- Verifica che la funzione Lambda sia stata eliminata.

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

Descrizione

Il `AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` runbook crittografa, a riposo, le variabili di ambiente per la funzione (AWS Lambda Lambda) specificata utilizzando una chiave AWS Key Management Service (AWS KMS) gestita dal cliente. Questo runbook deve essere usato solo come base per garantire che le variabili di ambiente della funzione Lambda siano crittografate secondo le migliori pratiche di sicurezza minime consigliate. Consigliamo di crittografare più funzioni con diverse chiavi gestite dal cliente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- FunctionName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome o l'ARN della funzione Lambda di cui si desidera crittografare le variabili di ambiente.

- KMSKeyArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN della chiave gestita AWS KMS dal cliente che desideri utilizzare per crittografare le variabili di ambiente della funzione Lambda.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

Fasi del documento

- aws:waitForAwsResourceProperty- Attende che la LastUpdateStatus proprietà sia. Successful

- `aws:executeAwsApi`- Crittografa le variabili di ambiente per la funzione Lambda specificata nel parametro utilizzando `FunctionName` AWS KMS la chiave gestita dal cliente specificata nel `KMSKeyArn` parametro.
- `aws:assertAwsResourceProperty`- Conferma che la crittografia è abilitata sulle variabili di ambiente per la funzione Lambda.

AWSConfigRemediation-MoveLambdaToVPC

Descrizione

Il `AWSConfigRemediation-MoveLambdaToVPC` runbook sposta una funzione AWS Lambda (Lambda) su un Amazon Virtual Private Cloud (Amazon VPC).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `FunctionName`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della funzione Lambda da passare a un Amazon VPC.

- `SecurityGroupIds`

Tipo: stringa

Descrizione: (Obbligatorio) Il gruppo di sicurezza che IDs desideri assegnare alle interfacce di rete elastiche (ENIs) associate alla funzione Lambda.

- `SubnetIds`

Tipo: stringa

Descrizione: (Obbligatoria) La IDs sottorete in cui si desidera creare le interfacce di rete elastiche (ENIs) associate alla funzione Lambda.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Fasi del documento

- `aws:executeAwsApi`- Aggiorna la configurazione Amazon VPC per la funzione Lambda specificata nel parametro. `FunctionName`
- `aws:waitForAwsResourceProperty`- Attende che la `LastUpdateStatus` funzione Lambda sia attiva. `successful`
- `aws:executeScript`- Verifica che la configurazione Amazon VPC della funzione Lambda sia stata aggiornata correttamente.

AWSSupport-RemediateLambdaS3Event

Descrizione

Il `AWSSupport-TroubleshootLambdaS3Event` runbook fornisce una soluzione automatizzata per le procedure descritte negli articoli del AWS Knowledge Center [Perché la notifica degli eventi di Amazon S3 non attiva la mia funzione Lambda?](#) e [perché ricevo l'errore «Impossibile convalidare le seguenti configurazioni di destinazione» quando creo una notifica di evento Amazon S3 per attivare la mia](#) funzione Lambda? Questo runbook ti aiuta a identificare e correggere il motivo per cui una notifica di evento di Amazon Simple Storage Service (Amazon S3) non è riuscita ad attivare la funzione specificata. AWS Lambda [Se l'output del runbook suggerisce di convalidare e configurare la concorrenza della funzione Lambda, consulta Invocazione asincrona e scalabilità delle funzioni.](#)[AWS Lambda](#)

Note

Gli errori «Impossibile convalidare le seguenti configurazioni di destinazione» possono verificarsi anche a causa di configurazioni errate degli eventi Amazon Simple Notification Service (Amazon SNS) e Amazon Simple Queue Service (Amazon SQS) Amazon S3. Questo runbook controlla solo le configurazioni delle funzioni Lambda. Se dopo aver utilizzato il runbook continui a ricevere l'errore «Impossibile convalidare le seguenti configurazioni di destinazione», esamina eventuali configurazioni di eventi Amazon SNS e Amazon SQS Amazon S3 esistenti.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- LambdaFunctionArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN della funzione Lambda.

- S3 BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 le cui notifiche di eventi attivano la funzione Lambda.

- Azione

Tipo: stringa

Valori validi: Risoluzione dei problemi | Rimedia

Descrizione: (Obbligatoria) L'azione che desideri venga eseguita dal runbook.

L'Troubleshootopzione consente di identificare eventuali problemi, ma non esegue alcuna azione mutante per risolverli. L'Remediateopzione consente di identificare e tentare di risolvere i problemi al posto tuo.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetDocument
- ssm:ListDocuments
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution

- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

Fasi del documento

- `aws:branch`- Rami basati sull'input specificato per il `Action` parametro.

Se il valore specificato è `Troubleshoot`:

- `aws:executeAutomation`- Esegue il `AWSSupport-TroubleshootLambdaS3Event` runbook.
- `aws:executeAwsApi`- Controlla l'output del `AWSSupport-TroubleshootLambdaS3Event` runbook eseguito nel passaggio precedente.

Se il valore specificato è `Remediate`:

- `aws:executeScript`- Esegue uno script per risolvere i problemi descritti nella sezione [Perché la notifica degli eventi di Amazon S3 non attiva la mia funzione Lambda?](#) e [perché ricevo l'errore «Impossibile convalidare le seguenti configurazioni di destinazione» quando creo una notifica di evento Amazon S3 per attivare la mia](#) funzione Lambda? Articoli del Knowledge Center.

Output

`CheckOutput.Output`

`Risolvi Lambdas3Event.Output`

AWSSupport-TroubleshootLambdaInternetAccess

Descrizione

Il `AWSSupport-TroubleshootLambdaInternetAccess` runbook ti aiuta a risolvere i problemi di accesso a Internet per una AWS Lambda funzione che è stata lanciata in Amazon Virtual Private Cloud (Amazon VPC). Risorse come i percorsi di sottorete, le regole dei gruppi di sicurezza e le regole della lista di controllo degli accessi alla rete (ACL) vengono esaminate per confermare che l'accesso a Internet in uscita è consentito.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- FunctionName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome della funzione Lambda per la quale desideri risolvere i problemi di accesso a Internet.

- destinationIp

Tipo: stringa

Descrizione: (Obbligatorio) L'indirizzo IP di destinazione a cui desideri stabilire una connessione in uscita.

- destinationPort

Tipo: stringa

Impostazione predefinita: 443

Descrizione: (Facoltativo) La porta di destinazione su cui si desidera stabilire una connessione in uscita.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

Fasi del documento

- `aws:executeScript`- Verifica la configurazione di varie risorse nel tuo VPC in cui è stata lanciata la funzione Lambda.
- `aws:branch`- Rami in base al fatto che la funzione Lambda specificata si trovi o meno in un VPC.
- `aws:executeScript`- Esamina le route della tabella di routing per la sottorete in cui è stata lanciata la funzione Lambda e verifica che siano presenti le route verso un gateway NAT (Network Address Translation) e un gateway Internet. Conferma che la funzione Lambda non si trova in una sottorete pubblica.
- `aws:executeScript`- Verifica che il gruppo di sicurezza associato alla funzione Lambda consenta l'accesso a Internet in uscita in base ai valori specificati per `destinationIp` i parametri `and. destinationPort`
- `aws:executeScript`- Verifica che le regole ACL associate alle sottoreti della funzione Lambda e il gateway NAT consentano l'accesso a Internet in uscita in base ai valori specificati per i parametri `and. destinationIp destinationPort`

Output

`checkVPC.vpc`: l'ID del VPC in cui è stata lanciata la funzione Lambda.

`checkVPC.Subnet` - La IDs delle sottoreti in cui è stata lanciata la funzione Lambda.

`checkVPC.SecurityGroups` - Gruppi di sicurezza associati alla funzione Lambda.

`CheckNACL.NACL` - Messaggio di analisi con nomi di risorse. `LambdaIpsi` riferisce all'indirizzo IP privato dell'interfaccia elastic network per la funzione Lambda. L'`LambdaIpRule` soggetto viene

generato solo per le sottoreti che hanno un percorso verso un gateway NAT. Il seguente contenuto è un esempio di output.

```
{
  "subnet-1234567890":{
    "NACL":"acl-1234567890",
    "destinationIp_Egress":"Allowed",
    "destinationIp_Ingress":"notAllowed",
    "Analysis":"This NACL has an allow rule for Egress traffic but there is no
Ingress rule. Please allow the destination IP / destination port in Ingress rule",
    "LambdaIpRules":{
      "{LambdaIp}":{
        "Egress":"notAllowed",
        "Ingress":"notAllowed",
        "Analysis":"This is a NAT subnet NACL. It does not have ingress or egress
rule allowed in it for Lambda's corresponding private ip {LambdaIp} Please allow this
IP in your egress and ingress NACL rules"
      }
    }
  },
  "subnet-0987654321":{
    "NACL":"acl-0987654321",
    "destinationIp_Egress":"Allowed",
    "destinationIp_Ingress":"notAllowed",
    "Analysis":"This NACL has an allow rule for Egress traffic but there is no
Ingress rule. Please allow the destination IP / destination port in Ingress rule"
  }
}
```

`checkSecurityGroups.secgrps`: analisi per il gruppo di sicurezza associato alla funzione Lambda. Il seguente contenuto è un esempio dell'output.

```
{
  "sg-123456789":{
    "Status":"Allowed",
    "Analysis":"This security group has allowed destintion IP and port in its
outbuond rule."
  }
}
```

`checkSubnet.subnets` - Analisi delle sottoreti nel tuo VPC associate alla tua funzione Lambda. Il seguente contenuto è un esempio dell'output.

```
{
  "subnet-0c4ee6cdexample15":{
    "Route":{
      "DestinationCidrBlock":"8.8.8.0/26",
      "NatGatewayId":"nat-00f0example69fdec",
      "Origin":"CreateRoute",
      "State":"active"
    },
    "Analysis":"This Route Table has an active NAT gateway path. Also, The NAT
gateway is launched in public subnet",
    "RouteTable":"rtb-0b1fexample16961b"
  }
}
```

AWSSupport-TroubleshootLambdaS3Event

Descrizione

Il AWSSupport-TroubleshootLambdaS3Event runbook fornisce una soluzione automatizzata per le procedure descritte negli articoli del AWS Knowledge Center [Perché la notifica degli eventi di Amazon S3 non attiva la mia funzione Lambda?](#) e [perché ricevo l'errore «Impossibile convalidare le seguenti configurazioni di destinazione» quando creo una notifica di evento Amazon S3 per attivare la mia](#) funzione Lambda? Questo runbook ti aiuta a identificare il motivo per cui una notifica di evento di Amazon Simple Storage Service (Amazon S3) non è riuscita ad attivare la funzione specificata. AWS Lambda [Se l'output del runbook suggerisce di convalidare e configurare la concorrenza della funzione Lambda, consulta Invocazione asincrona e scalabilità delle funzioni.](#)[AWS Lambda](#)

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- LambdaFunctionArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN della funzione Lambda attivata dalla notifica degli eventi di Amazon S3.

- S3 BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 le cui notifiche di eventi attivano la funzione Lambda.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- lambda:GetPolicy
- s3:GetBucketNotification

Fasi del documento

- aws:executeScript- Esegue lo script per convalidare le impostazioni di configurazione per la notifica degli eventi di Amazon S3. Convalida la policy IAM basata sulle risorse per la funzione Lambda e genera un comando AWS Command Line Interface (AWS CLI) per aggiungere le autorizzazioni necessarie se le autorizzazioni richieste non sono presenti nella policy. Convalida le politiche delle risorse di altre funzioni Lambda che fanno parte delle notifiche degli eventi per lo stesso bucket S3 e genera AWS CLI un comando come output se mancano le autorizzazioni richieste.

Output

Lambdas3Event.OUTPUT

Amazon Managed Workflows for Apache Airflow

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Managed Workflows for Apache Airflow. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSsupport-TroubleshootMWAAEnvironmentCreation](#)

AWSsupport-TroubleshootMWAAEnvironmentCreation

Descrizione

Il AWSsupport-TroubleshootMWAAEnvironmentCreation runbook fornisce informazioni per eseguire il debug dei problemi di creazione dell'ambiente Amazon Managed Workflows for Apache Airflow (Amazon MWAA) ed esegue controlli insieme ai motivi documentati con il massimo impegno per aiutare a identificare l'errore.

Come funziona?

Il runbook esegue i seguenti passaggi:

- Recupera i dettagli dell'ambiente Amazon MWAA.
- Verifica le autorizzazioni del ruolo di esecuzione.
- Verifica se l'ambiente dispone delle autorizzazioni per utilizzare la AWS KMS chiave fornita per la registrazione e se esiste il gruppo di log richiesto CloudWatch .
- Analizza i log nel gruppo di log fornito per individuare eventuali errori.
- Controlla la configurazione di rete per verificare se l'ambiente Amazon MWAA ha accesso agli endpoint richiesti.
- Genera un report con i risultati.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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:GetBucketAc1`
- `s3:GetBucketPolicyStatus`
- `s3:GetPublicAccessBlock`
- `s3control:GetPublicAccessBlock`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Istruzioni

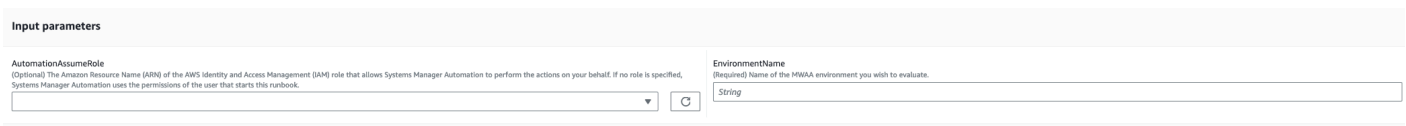
Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSsupport-TroubleshootMWAAEnvironmentCreation](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - `AutomationAssumeRole` (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `EnvironmentName` (Obbligatorio):

Nome dell'ambiente Amazon MWAA che desideri valutare.



Input parameters

Parameter Name	Parameter Type	Parameter Value
<code>AutomationAssumeRole</code> (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.	Text	
<code>EnvironmentName</code> (Required) Name of the MWAA environment you wish to evaluate.	Text	String

4. Seleziona Esegui.
5. L'automazione inizia.
6. Il documento esegue le seguenti operazioni:

- **`GetMWAAEnvironmentDetails`:**

Recupera i dettagli dell'ambiente Amazon MWAA. Se questo passaggio non riesce, il processo di automazione si interromperà e verrà visualizzato come. Failed

- **`CheckIAMPermissionsOnExecutionRole`:**

Verifica che il ruolo di esecuzione disponga delle autorizzazioni necessarie per le risorse Amazon MWAA, Amazon S3 CloudWatch , CloudWatch Logs e Amazon SQS. Se rileva una chiave gestita dal cliente AWS Key Management Service (AWS KMS), l'automazione convalida le autorizzazioni richieste dalla chiave. Questo passaggio utilizza `iam:SimulateCustomPolicyAPI` per verificare se il ruolo di esecuzione dell'automazione soddisfa tutte le autorizzazioni richieste.

- **CheckKMSPolicyOnKMSKey:**

Verifica se la policy delle AWS KMS chiavi consente all'ambiente Amazon MWAA di utilizzare la chiave per crittografare CloudWatch i log. Se la AWS KMS chiave è AWS gestita, l'automazione salta questo controllo.

- **CheckIfRequiredLogGroupsExists:**

Verifica se esistono i gruppi di CloudWatch log richiesti per l'ambiente Amazon MWAA. In caso contrario, l'automazione verifica CloudTrail eventuali eventi `CreateLogGroup`. `DeleteLogGroup` Questo passaggio verifica anche la presenza di `CreateLogGroup` eventi.

- **BranchOnLogGroupsFindings:**

Filiali basate sull'esistenza di gruppi di CloudWatch log relativi all'ambiente Amazon MWAA. Se esiste almeno un gruppo di log, l'automazione lo analizza per individuare gli errori. Se non sono presenti gruppi di log, l'automazione salta il passaggio successivo.

- **CheckForErrorsInLogGroups:**

Analizza i gruppi di CloudWatch log per individuare gli errori.

- **GetRequiredEndpointsDetails:**

Recupera gli endpoint di servizio utilizzati dall'ambiente Amazon MWAA.

- **CheckNetworkConfiguration:**

Verifica che la configurazione di rete dell'ambiente Amazon MWAA soddisfi i requisiti, inclusi i controlli sui gruppi di sicurezza, la rete ACLs, le sottoreti e le configurazioni delle tabelle di routing.

- **CheckEndpointsConnectivity:**

Richiama l'automazione `AWSSupport-ConnectivityTroubleshooter` secondaria per convalidare la connettività di Amazon MWAA agli endpoint richiesti.

- **CheckS3BlockPublicAccess:**

Verifica se il bucket Amazon S3 dell'ambiente Amazon MWAA Block Public Access è abilitato ed esamina anche le impostazioni generali di Amazon S3 Block Public Access dell'account.

- **GenerateReport:**

Raccoglie informazioni dall'automazione e stampa il risultato o l'output di ogni passaggio.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- Verifica delle autorizzazioni del ruolo di esecuzione dell'ambiente Amazon MWAA:

Verifica se il ruolo di esecuzione dispone delle autorizzazioni necessarie per le risorse Amazon MWAA, Amazon S3 CloudWatch, CloudWatch Logs e Amazon SQS. Se viene rilevata una AWS KMS chiave Customer Managed, l'automazione convalida le autorizzazioni richieste dalla chiave.

- Verifica della politica AWS KMS chiave dell'ambiente Amazon MWAA:

Verifica se il ruolo di esecuzione possiede le autorizzazioni necessarie per le risorse Amazon MWAA, Amazon S3, CloudWatch Logs e Amazon CloudWatch SQS. Inoltre, se viene rilevata una AWS KMS chiave Customer Managed, l'automazione verifica le autorizzazioni richieste dalla chiave.

- Verifica dei gruppi di CloudWatch log dell'ambiente Amazon MWAA:

Verifica se esistono i gruppi di CloudWatch log richiesti per l'ambiente Amazon MWAA. In caso contrario, l'automazione verifica la localizzazione `CreateLogGroup` e `CloudTrail DeleteLogGroup` gli eventi.

- Verifica delle tabelle di routing dell'ambiente Amazon MWAA:

Verifica se le tabelle di routing Amazon VPC nell'ambiente Amazon MWAA sono configurate correttamente.

- Verifica dei gruppi di sicurezza dell'ambiente Amazon MWAA:

Verifica se i gruppi di sicurezza Amazon VPC dell'ambiente Amazon MWAA sono configurati correttamente.

- Verifica della rete dell'ambiente Amazon MWAA: ACLs

Verifica se i gruppi di sicurezza Amazon VPC nell'ambiente Amazon MWAA sono configurati correttamente.

- Verifica delle sottoreti dell'ambiente Amazon MWAA:

Verifica se le sottoreti dell'ambiente Amazon MWAA sono private.

- Verifica della connettività degli endpoint richiesta dall'ambiente Amazon MWAA:

Verifica se l'ambiente Amazon MWAA può accedere agli endpoint richiesti. A tal fine, l'automazione richiama l'automazione `AWSSupport-ConnectivityTroubleshooter`.

- Verifica dell'ambiente Amazon MWAA, bucket Amazon S3:

Verifica se il bucket Amazon S3 dell'ambiente Amazon MWAA `Block Public Access` è abilitato ed esamina anche le impostazioni di Amazon S3 `Block Public Access` dell'account.

- Il controllo dei CloudWatch log dell'ambiente Amazon MWAA raggruppa gli errori:

Analizza i gruppi di CloudWatch log esistenti dell'ambiente Amazon MWAA per individuare gli errori.

▼ Outputs

GenerateReportAutomationReport

Troubleshooting report for MWAA environment

🔗 The automation found no issues with the MWAA environment configuration ✓

🔗 Checking the MWAA environment execution role permissions

All the required permissions for the MWAA environment execution role are in place ✓

🔗 Checking the MWAA environment KMS key policy

KMS key is an AWS managed key ✓

🔗 Checking the MWAA environment CloudWatch logs groups

The number of CloudWatch log groups found is 5 and the number of enabled log groups for the MWAA environment is 5. This suggests that all log groups were created successfully ✓

🔗 Checking the MWAA environment Route Tables

NAT GW has Internet route: subnet- → nat- → igw- ✓

NAT GW has Internet route: subnet- → nat- → igw- ✓

🔗 Checking the MWAA environment Security Groups

Security group has self-referencing rules for all traffic. ✓

🔗 Checking the MWAA environment Network ACLs

NACL- allows port 5432 on egress ✓ and allows port 5432 on ingress ✓

🔗 Checking the MWAA environment Subnets

Subnet: subnet- is private ✓

Subnet: subnet- is private ✓

🔗 Checking the MWAA environment required endpoints connectivity

✓ Testing connectivity with sqs.eu-west-1.amazonaws.com:

Connectivity test between ENI- and sqs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the sqs.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with api.ecr.eu-west-1.amazonaws.com:

Connectivity test between ENI- and api.ecr.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.ecr.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with monitoring.eu-west-1.amazonaws.com:

Connectivity test between ENI- and monitoring.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the monitoring.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with kms.eu-west-1.amazonaws.com:

Connectivity test between ENI- and kms.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the kms.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with s3.eu-west-1.amazonaws.com:

Connectivity test between ENI- and s3.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the s3.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI- and env.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI- and env.airflow.eu-west-1.amazonaws.com on port 5432 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with api.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI- and api.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with logs.eu-west-1.amazonaws.com:

Connectivity test between ENI- and logs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the logs.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with ops.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI- and ops.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the ops.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

🔗 Checking the MWAA environment S3 bucket

Environment's S3 bucket and/or account block public access ✓

🔗 Checking the MWAA environment CloudWatch logs groups errors

Parsed log group - DAGProcessing - no errors found ✓

Parsed log group - Scheduler - no errors found ✓

Parsed log group - Task - no errors found ✓

Parsed log group - WebServer - no errors found ✓

Parsed log group - Worker - no errors found ✓

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

Neptune

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Neptune. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-EnableNeptuneDbAuditLogsToCloudWatch](#)
- [AWS-EnableNeptuneDbBackupRetentionPeriod](#)
- [AWS-EnableNeptuneClusterDeletionProtection](#)

AWS-EnableNeptuneDbAuditLogsToCloudWatch

Descrizione

Il AWS-EnableNeptuneDbAuditLogsToCloudWatch runbook ti aiuta a inviare i log di controllo per un cluster Amazon Neptune DB ad Amazon Logs. CloudWatch

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `DbClusterResourceId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della risorsa del cluster Neptune DB per cui desideri abilitare i log di controllo.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- `GetNeptuneDbClusterIdentifier` (`aws:executeAwsApi`) - Restituisce l'ID del cluster Neptune DB.
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`) - Verifica che il tipo di motore Neptune DB sia. `neptune`
- `EnableNeptuneDbAuditLogs` (`aws:executeAwsApi`) - Consente l'invio dei log di controllo per il cluster Neptune DB. `CloudWatch`
- `VerifyNeptuneDbStatus` (`aws:waitAwsResourceProperty`) - Verifica che lo stato del cluster Neptune DB sia. `available`
- `VerifyNeptuneDbAuditLogs` (`aws:executeScript`) - Verifica che i log di controllo siano stati configurati correttamente per l'invio a `Logs`. `CloudWatch`

AWS-EnableNeptuneDbBackupRetentionPeriod

Descrizione

Il AWS-EnableNeptuneDbBackupRetentionPeriod runbook consente di abilitare backup automatici con un periodo di conservazione dei backup compreso tra 7 e 35 giorni per un cluster Amazon Neptune DB.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DbClusterResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della risorsa del cluster Neptune DB per cui desideri abilitare i backup.

- BackupRetentionPeriod

Tipo: integer

Valori validi: 7-35

Descrizione: (Obbligatorio) Il numero di giorni di conservazione dei backup.

- PreferredBackupWindow

Tipo: stringa

Descrizione: (Facoltativo) Un periodo di tempo giornaliero di almeno 30 minuti per l'esecuzione dei backup. Il valore deve essere espresso in UTC (Universal Time Coordinated) e utilizzare il formato: hh24:mm-hh24:mm Il periodo di conservazione del backup non può essere in conflitto con la finestra di manutenzione preferita.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

Fasi del documento

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Restituisce l'ID del cluster Neptune DB.
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty) - Verifica che il tipo di motore Neptune DB sia. neptune
- VerifyNeptuneDbStatus (aws:waitAwsResourceProperty) - Verifica che lo stato del cluster Neptune DB sia. available
- ModifyNeptuneDbRetentionPeriod (aws:executeAwsApi) - Imposta il periodo di conservazione per il cluster Neptune DB.
- VerifyNeptuneDbBackupsEnabled (aws:executeScript) - Verifica che il periodo di conservazione e la finestra di backup siano stati impostati correttamente.

AWS-EnableNeptuneClusterDeletionProtection

Descrizione

Il `AWS-EnableNeptuneClusterDeletionProtection` runbook abilita la protezione dall'eliminazione per il cluster Amazon Neptune specificato.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `DbClusterResourceId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del cluster Neptune su cui desideri abilitare la protezione dall'eliminazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- `GetNeptuneDbClusterIdentifier` (`aws:executeAwsApi`) - Restituisce l'ID del cluster Neptune DB.
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`) - Verifica che il tipo di motore del cluster DB specificato sia. `neptune`
- `VerifyNeptuneStatus` (`aws:waitForAwsResourceProperty`) - Verifica che lo stato del cluster sia. `available`
- `EnableNeptuneDbDeletionProtection` (`aws:executeAwsApi`) - Abilita la protezione dall'eliminazione sul cluster Neptune DB.
- `VerifyNeptuneDbDeletionProtection` (`aws:assertAwsResourceProperty`) - Verifica che la protezione da eliminazione sia abilitata sul cluster DB.

Output

- `EnableNeptuneDbDeletionProtection`. `EnableNeptuneDbDeletionProtectionResponse` - L'output dell'operazione API.

Amazon RDS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Relational Database Service. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-CreateEncryptedRdsSnapshot](#)
- [AWS-CreateRdsSnapshot](#)
- [AWSConfigRemediation-DeleteRDSCluster](#)

- [AWSConfigRemediation-DeleteRDSClusterSnapshot](#)
- [AWSConfigRemediation-DeleteRDSInstance](#)
- [AWSConfigRemediation-DeleteRDSInstanceSnapshot](#)
- [AWSConfigRemediation-DisablePublicAccessToRDSInstance](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance](#)
- [AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance](#)
- [AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS](#)
- [AWSConfigRemediation-EnableMultiAZOnRDSInstance](#)
- [AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance](#)
- [AWSConfigRemediation-EnableRDSClusterDeletionProtection](#)
- [AWSConfigRemediation-EnableRDSInstanceBackup](#)
- [AWSConfigRemediation-EnableRDSInstanceDeletionProtection](#)
- [AWSConfigRemediation-ModifyRDSInstancePortNumber](#)
- [AWSSupport-ModifyRDSSnapshotPermission](#)
- [AWSPremiumSupport-PostgreSQLWorkloadReview](#)
- [AWS-RebootRdsInstance](#)
- [AWSSupport-ShareRDSSnapshot](#)
- [AWS-StartRdsInstance](#)
- [AWS-StartStopAuroraCluster](#)
- [AWS-StopRdsInstance](#)
- [AWSSupport-TroubleshootConnectivityToRDS](#)
- [AWSSupport-TroubleshootRDSIAMAuthentication](#)
- [AWSSupport-ValidateRdsNetworkConfiguration](#)

AWS-CreateEncryptedRdsSnapshot

Descrizione

Il AWS-CreateEncryptedRdsSnapshot runbook crea uno snapshot crittografato da un'istanza Amazon Relational Database Service (Amazon RDS) non crittografata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DBInstanceIdentificatore

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza Amazon RDS di cui desideri creare uno snapshot.

- DBSnapshotIdentificatore

Tipo: stringa

Descrizione: (Facoltativo) Il modello di nome per lo snapshot Amazon RDS. Il modello di nome predefinito è *DBInstanceIdentifier-yyyymmddhhmmss*

- DBSnapshotIdentificatore crittografato

Tipo: stringa

Descrizione: (Facoltativo) Il nome dell'istantanea crittografata. Il nome predefinito è il valore specificato per il DBSnapshotIdentifier parametro aggiunto. -encrypted

- InstanceTags

Tipo: stringa

Descrizione: (Facoltativo) Tag da aggiungere all'istanza DB. (Esempio: key=tagkey1, value=tagValue1; key=tagkey2, value=tagValue2) '

- KmsKeyId

Tipo: stringa

Impostazione predefinita: alias/aws/rds

Descrizione: (Facoltativo) L'ARN, l'ID della chiave o l'alias della chiave gestita dal cliente che desideri utilizzare per crittografare l'istantanea.

- SnapshotTags

Tipo: stringa

Descrizione: (Facoltativo) Tag da aggiungere all'istantanea. (Esempio: key=tagkey1, value=tagValue1; key=tagkey2, value=tagValue2) '

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- rds:AddTagsToResource
- rds:CopyDBSnapshot
- rds>CreateDBSnapshot
- rds>DeleteDBSnapshot
- rds:DescribeDBSnapshots

Fasi del documento

- aws:executeScript- Crea un'istantanea dell'istanza DB specificata nel DBInstanceIdentifier parametro.
- aws:executeScript- Verifica che l'istantanea creata nel passaggio precedente esista e sia. available

- `aws:executeScript`- Copia l'istantanea creata in precedenza in un'istantanea crittografata.
- `aws:executeScript`- Verifica che l'istantanea crittografata creata nel passaggio precedente esista.

Output

`CopyRdsSnapshotToEncryptedRdsSnapshot`. `EncryptedSnapshotId` - L'ID dello snapshot crittografato di Amazon RDS.

AWS-CreateRdsSnapshot

Descrizione

Crea uno snapshot di Amazon Relational Database Service (Amazon RDS) per un'istanza Amazon RDS.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DBInstanceIdentificatore

Tipo: stringa

Descrizione: (Obbligatorio) L' DBInstanceID ID dell'istanza RDS da cui creare lo snapshot.

- DBSnapshotIdentificatore

Tipo: stringa

Descrizione: (Facoltativo) L'ID DBSnapshot identificativo dello snapshot RDS da creare.

- InstanceTags

Tipo: stringa

Descrizione: (Facoltativo) Tag da creare per esempio.

- SnapshotTags

Tipo: stringa

Descrizione: (Facoltativo) Tag da creare per l'istantanea.

Fasi del documento

createRDSSnapshot : crea l'istantanea RDS e restituisce l'ID dell'istantanea.

verifyRDSSnapshot : verifica che l'istantanea creata nel passaggio precedente esista.

Output

createRDSSnapshot. SnapshotId — L'ID dell'istantanea creata.

AWSConfigRemediation-DeleteRDSCluster

Descrizione

Il AWSConfigRemediation-DeleteRDSCluster runbook elimina il cluster Amazon Relational Database Service (Amazon RDS) specificato. AWS Config deve essere abilitato nel luogo in Regione AWS cui esegui questa automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DBClusterId

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per il cluster DB su cui si desidera abilitare la protezione da eliminazione.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds>DeleteDBCluster
- rds>DeleteDBInstance
- rds:DescribeDBClusters

Fasi del documento

- `aws:executeScript`- Elimina il cluster DB specificato nel `DBClusterId` parametro.

AWSConfigRemediation-DeleteRDSClusterSnapshot

Descrizione

Il `AWSConfigRemediation-DeleteRDSClusterSnapshot` runbook elimina lo snapshot del cluster Amazon Relational Database Service (Amazon RDS) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `DBClusterSnapshotId`

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore dello snapshot del cluster Amazon RDS da eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

Fasi del documento

- `aws:branch`- Verifica se l'istantanea del cluster è nello `available` stato. Se non è disponibile, il flusso termina.
- `aws:executeAwsApi`- Elimina lo snapshot del cluster Amazon RDS specificato utilizzando l'identificatore dello snapshot del cluster di database (DB).
- `aws:executeScript`- Verifica che lo snapshot del cluster Amazon RDS specificato sia stato eliminato.

AWSConfigRemediation-DeleteRDSInstance

Descrizione

Il `AWSConfigRemediation-DeleteRDSInstance` runbook elimina l'istanza di Amazon Relational Database Service (Amazon RDS) specificata. Quando elimini un'istanza di database (DB), tutti i backup automatici per quell'istanza vengono eliminati e non possono essere ripristinati. Le istantanee manuali del DB non vengono eliminate. Se l'istanza DB che si desidera eliminare si trova nello `incompatible-restore` stato `failedincompatible-network`, o,, è necessario impostare il `SkipFinalSnapshot` parametro su `true`

Note

Se l'istanza DB che desideri eliminare si trova in un cluster Amazon Aurora DB, il runbook non eliminerà l'istanza DB se è una replica di lettura e l'unica istanza nel cluster DB.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbiResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB che desideri eliminare.

- SkipFinalSnapshot

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se impostato su `true`, non viene creata un'istantanea finale prima dell'eliminazione dell'istanza DB.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBInstance`

- `rds:DescribeDBInstances`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie il nome dell'istanza DB dal valore specificato nel `DbiResourceId` parametro.
- `aws:branch`- Rami basati sul valore specificato nel `SkipFinalSnapshot` parametro.
- `aws:executeAwsApi`- Elimina l'istanza DB specificata nel `DbiResourceId` parametro.
- `aws:executeAwsApi`- Elimina l'istanza DB specificata nel `DbiResourceId` parametro dopo la creazione dello snapshot finale.
- `aws:assertAwsResourceProperty`- Verifica che l'istanza DB sia stata eliminata.

AWSConfigRemediation-DeleteRDSInstanceSnapshot

Descrizione

Il `AWSConfigRemediation-DeleteRDSInstanceSnapshot` runbook elimina lo snapshot dell'istanza Amazon Relational Database Service (Amazon RDS) specificato. Vengono eliminate solo le istantanee nello stato `available`. Questo runbook non supporta l'eliminazione di snapshot dalle istanze di database Amazon Aurora.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbSnapshotId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dello snapshot che desideri eliminare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds>DeleteDBSnapshot
- rds:DescribeDBSnapshots

Fasi del documento

- aws:executeAwsApi- Raccoglie lo stato dell'istantanea specificata nel parametro. DbSnapshotId
- aws:assertAwsResourceProperty- Conferma che lo stato dell'istantanea è. available
- aws:executeAwsApi- Elimina l'istantanea specificata nel parametro. DbSnapshotId
- aws:executeScript- Verifica che l'istantanea sia stata eliminata.

AWSConfigRemediation-DisablePublicAccessToRDSInstance

Descrizione

Il AWSConfigRemediation-DisablePublicAccessToRDSInstance runbook disabilita l'accessibilità pubblica per l'istanza di database (DB) di Amazon Relational Database Service (Amazon RDS) specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB per cui desideri disabilitare l'accessibilità pubblica.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- `aws:assertAwsResourceProperty`- Verifica che le istanze DB siano in uno stato. AVAILABLE
- `aws:executeAwsApi`- Disattiva l'accessibilità pubblica sull'istanza DB.
- `aws:waitForAwsResourceProperty`- Attende che l'istanza DB passi a uno stato. MODIFYING
- `aws:waitForAwsResourceProperty`- Attende che l'istanza DB passi a uno AVAILABLE stato.
- `aws:assertAwsResourceProperty`- Conferma che l'accessibilità pubblica è disabilitata sull'istanza DB.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

Descrizione

Il `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` runbook abilita l'CopyTagsToSnapshot impostazione sul cluster Amazon Relational Database Service (Amazon RDS) specificato. L'attivazione di questa impostazione copia tutti i tag dal cluster DB nelle istantanee del cluster DB. L'impostazione predefinita prevede di non copiarli. AWS Config deve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `ApplyImmediately`

Tipo: Booleano

Impostazione predefinita: `false`

Descrizione: (Facoltativo) Se si specifica `true` questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per il `PreferredMaintenanceWindow` cluster DB.

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `DbClusterResourceId`

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per il cluster DB su cui desideri abilitare l'`CopyTagsToSnapshot` impostazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore del cluster DB dall'identificatore di risorse del cluster DB.
- `aws:assertAwsResourceProperty`- Conferma che il cluster DB è in uno stato. `AVAILABLE`
- `aws:executeAwsApi`- Abilita l'`CopyTagsToSnapshot` impostazione sul cluster DB.

- `aws:assertAwsResourceProperty`- Conferma che l'`CopyTagsToSnapshot` impostazione è abilitata sul cluster DB.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

Descrizione

Il `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance` runbook abilita l'`CopyTagsToSnapshot` impostazione sull'istanza Amazon Relational Database Service (Amazon RDS) specificata. L'attivazione di questa impostazione copia tutti i tag dall'istanza DB negli snapshot dell'istanza DB. L'impostazione predefinita prevede di non copiarli. AWS Config deve essere abilitato nel Regione AWS luogo in cui si esegue questa automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `ApplyImmediately`

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se si specifica `true` questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per l'`PreferredMaintenanceWindow` istanza DB.

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `DbiResourceId`

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui desideri abilitare l'`CopyTagsToSnapshot` impostazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che l'istanza DB è in uno stato. `AVAILABLE`
- `aws:executeAwsApi`- Abilita l'`CopyTagsToSnapshot` impostazione sull'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che l'`CopyTagsToSnapshot` impostazione è abilitata sull'istanza DB.

AWSConfigRemediation- EnableEnhancedMonitoringOnRDSInstance

Descrizione

Il `AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance` runbook abilita il monitoraggio avanzato sull'istanza di database Amazon RDS specificata. Per informazioni su Enhanced Monitoring, consulta [Enhanced Monitoring](#) nella Amazon RDS User Guide.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `MonitoringInterval`

Tipo: integer

Valori validi: 1 | 5 | 10 | 15 | 30 | 60

Descrizione: (Obbligatorio) L'intervallo in secondi durante il quale le metriche di Enhanced Monitoring vengono raccolte dall'istanza DB.

- `MonitoringRoleArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo IAM che consente ad Amazon RDS di inviare parametri di Enhanced Monitoring ad Amazon Logs. CloudWatch

- ResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui desideri abilitare Enhanced Monitoring.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

Fasi del documento

- aws:executeAwsApi- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- aws:assertAwsResourceProperty- Conferma che l'istanza DB è in uno stato. AVAILABLE
- aws:executeAwsApi- Abilita il monitoraggio avanzato sull'istanza DB.
- aws:executeScript- Conferma che il monitoraggio avanzato è abilitato sull'istanza DB.

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

Descrizione

Il AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS runbook abilita l'AutoMinorVersionUpgradeimpostazione sull'istanza di database Amazon RDS specificata. L'abilitazione di questa impostazione significa che gli aggiornamenti delle versioni minori vengono applicati automaticamente all'istanza DB durante la finestra di manutenzione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbiResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui desideri AutoMinorVersionUpgrade impostare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

Fasi del documento

- aws:executeAwsApi- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.

- `aws:assertAwsResourceProperty`- Conferma che l'istanza DB è in uno stato. AVAILABLE
- `aws:executeAwsApi`- Abilita l'AutoMinorVersionUpgradeimpostazione sull'istanza DB.
- `aws:executeScript`- Conferma che l'AutoMinorVersionUpgradeimpostazione è abilitata sull'istanza DB.

AWSConfigRemediation-EnableMultiAZOnRDSInstance

Descrizione

Il AWSConfigRemediation-EnableMultiAZOnRDSInstance runbook trasforma l'istanza del database (DB) Amazon Relational Database Service (Amazon RDS) in una distribuzione Multi-AZ. La modifica di questa impostazione non comporta un'interruzione. La modifica viene applicata durante la finestra di manutenzione successiva, a meno che non si imposti il parametro su. `ApplyImmediately true`

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `ApplyImmediately`

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se si specifica `true` questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per l'`PreferredMaintenanceWindow`istanza DB.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbiResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore Regione AWS-unique e immutabile per l'istanza DB per abilitare l'impostazione. MultiAZ

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- rds:DescribeDBInstances
- rds:ModifyDBInstance
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

Fasi del documento

- aws:executeAwsApi- Recupera il nome dell'istanza DB utilizzando il valore fornito nel DBInstanceId parametro.
- aws:executeAwsApi- Verifica che sia. DBInstanceStatus available
- aws:branch- Verifica se MultiAZ è già impostato true su sull'istanza DB specificata nel DbiResourceId parametro.
- aws:executeAwsApi- Modifica l'MultiAZimpostazione true sull'istanza DB specificata nel DbiResourceId parametro.
- aws:assertAwsResourceProperty- Verifica che MultiAZ sia impostato true sull'istanza DB specificata nel DbiResourceId parametro.

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

Descrizione

Il AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance runbook abilita Performance Insights sull'istanza DB di Amazon RDS specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbiResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui si desidera abilitare Performance Insights.

- PerformanceInsightsKMSKeyId

Tipo: stringa

Impostazione predefinita: alias/aws/rds

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN), l'ID della chiave o l'alias chiave della chiave gestita dal cliente AWS Key Management Service (AWS KMS) che desideri che Performance Insights utilizzi per crittografare tutti i dati potenzialmente sensibili. Se inserisci l'alias della chiave per questo parametro, aggiungi al valore il prefisso. **alias/** Se non si specifica un valore per questo parametro, Chiave gestita da AWS viene utilizzato.

- `PerformanceInsightsRetentionPeriod`

Tipo: integer

Valori validi: 7.731

Impostazione predefinita: 7

Descrizione: (Facoltativo) Il numero di giorni in cui desideri conservare i dati di Performance Insights.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che lo stato dell'istanza DB è. `available`
- `aws:executeAwsApi`- Raccoglie l'ARN della chiave gestita AWS KMS dal cliente specificata nel `PerformanceInsightsKMSKeyId` parametro.

- `aws:branch`- Verifica se un valore è già assegnato alla `PerformanceInsightsKMSKeyId` proprietà dell'istanza DB.
- `aws:executeAwsApi`- Abilita Performance Insights sull'istanza DB specificata nel `DbResourceId` parametro.
- `aws:assertAwsResourceProperty`- Conferma che il valore specificato per il `PerformanceInsightsKMSKeyId` parametro è stato utilizzato per abilitare la crittografia per Performance Insights sull'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che Performance Insights è abilitato sull'istanza DB.

AWSConfigRemediation-EnableRDSClusterDeletionProtection

Descrizione

Il `AWSConfigRemediation-EnableRDSClusterDeletionProtection` runbook abilita la protezione dall'eliminazione sul cluster Amazon Relational Database Service (Amazon RDS) specificato. AWS Config deve essere abilitato nel luogo in Regione AWS cui esegui questa automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `ClusterId`

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per il cluster DB su cui desideri abilitare la protezione da eliminazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie il nome del cluster DB dall'identificatore di risorse del cluster DB.
- `aws:assertAwsResourceProperty`- Verifica che lo stato del cluster DB sia `available`
- `aws:executeAwsApi`- Abilita la protezione dall'eliminazione sul cluster DB specificato nel `ClusterId` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la protezione da eliminazione sia stata abilitata sul cluster DB.

AWSConfigRemediation-EnableRDSInstanceBackup

Descrizione

Il `AWSConfigRemediation-EnableRDSInstanceBackup` runbook consente i backup per l'istanza di database Amazon Relational Database Service (Amazon RDS) specificata. Questo runbook non supporta l'abilitazione dei backup per le istanze di database Amazon Aurora.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `ApplyImmediately`

Tipo: Booleano

Impostazione predefinita: `false`

Descrizione: (Facoltativo) Se si specifica `true` questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per l'`PreferredMaintenanceWindow` istanza DB.

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `BackupRetentionPeriod`

Tipo: integer

Valori validi: 1-35

Descrizione: (Obbligatorio) Il numero di giorni di conservazione dei backup.

- `DbiResourceId`

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB per cui desideri abilitare i backup.

- `PreferredBackupWindow`

Tipo: stringa

Descrizione: (Facoltativo) L'intervallo di tempo giornaliero (in UTC) durante il quale vengono creati i backup.

Vincoli:

- Deve essere nel formato `hh24:mi-hh24:mi`
- Deve essere in formato UTC (Coordinated Universal Time)
- Il valore non deve essere in conflitto con la finestra di manutenzione preferita
- Il valore deve essere almeno di 30 minuti

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeScript`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB. Abilita i backup per l'istanza DB. Conferma che i backup sono abilitati sull'istanza DB.

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

Descrizione

Il AWSConfigRemediation-EnableRDSInstanceDeletionProtection runbook abilita la protezione dall'eliminazione sull'istanza di database Amazon RDS specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- ApplyImmediately

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se si specifica true questo parametro, le modifiche in questa richiesta e tutte le modifiche in sospeso vengono applicate in modo asincrono il prima possibile, indipendentemente dall'impostazione per l'PreferredMaintenanceWindowistanza DB.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DbInstanceResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB su cui desideri abilitare la protezione da eliminazione.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.
- `aws:executeAwsApi`- Abilita la protezione dall'eliminazione sull'istanza DB.
- `aws:assertAwsResourceProperty`- Conferma che la protezione da eliminazione è abilitata sull'istanza DB.

AWSConfigRemediation-ModifyRDSInstancePortNumber

Descrizione

Il `AWSConfigRemediation-ModifyRDSInstancePortNumber` runbook modifica il numero di porta su cui l'istanza Amazon Relational Database Service (Amazon RDS) accetta le connessioni. L'esecuzione di questa automazione riavvierà il database.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- PortNumber

Tipo: stringa

Descrizione: (Facoltativo) Il numero di porta su cui desideri che l'istanza DB accetti le connessioni.

- RDSDBInstanceResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore di risorsa per l'istanza DB di cui desideri modificare il numero di porta in ingresso.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

Fasi del documento

- aws:executeAwsApi- Raccoglie l'identificatore dell'istanza DB dall'identificatore di risorsa dell'istanza DB.

- `aws:assertAwsResourceProperty`- Conferma che l'istanza DB è in uno stato. AVAILABLE
- `aws:executeAwsApi`- Modifica il numero di porta in entrata su cui l'istanza DB accetta le connessioni.
- `aws:waitForAwsResourceProperty`- Attende che l'istanza DB si trovi in uno stato. MODIFYING
- `aws:waitForAwsResourceProperty`- Attende che l'istanza DB si trovi in uno AVAILABLE stato.

AWSSupport-ModifyRDSnapshotPermission

Descrizione

Il `AWSSupport-ModifyRDSnapshotPermission` runbook ti aiuta a modificare le autorizzazioni per più snapshot di Amazon Relational Database Service (Amazon RDS). Usando questo runbook, puoi creare istantanee `Public` o condividerle con altri. `Private Account AWS` Le istantanee crittografate con una chiave KMS predefinita non possono essere condivise con altri account utilizzando questo runbook.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AccountIds

Tipo: StringList

Impostazione predefinita: none

Descrizione: (Facoltativo) Gli IDs account con cui si desidera condividere le istantanee. Questo parametro è obbligatorio se si immette No il valore del Private parametro.

- AccountPermissionOperation

Tipo: stringa

Valori validi: aggiungi | rimuovi

Impostazione predefinita: none

Descrizione: (Facoltativo) Il tipo di operazione da eseguire.

- Privata

Tipo: stringa

Valori validi: Sì | No

Descrizione: (Obbligatorio) Inserisci No il valore se desideri condividere istantanee con account specifici.

- SnapshotIdentifiers

Tipo: StringList

Descrizione: (Obbligatorio) I nomi degli snapshot di Amazon RDS di cui desideri modificare l'autorizzazione.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`
- `rds:ModifyDBSnapshotAttribute`

Fasi del documento

1. `aws:executeScript`- Verifica le IDs istantanee fornite nel parametro. `SnapshotIdentifiers`
Dopo aver verificato il IDs, lo script verifica la presenza di istantanee crittografate e genera un elenco, se ne vengono trovate.
2. `aws:branch`- Suddivide l'automazione in base al valore immesso per il parametro. `Private`
3. `aws:executeScript`- Modifica le autorizzazioni delle istantanee specificate per condividerle con gli account specificati.
4. `aws:executeScript`- Modifica le autorizzazioni delle istantanee per cambiarle da a. `Public`
`Private`

Output

`ValidateSnapshots.EncryptedSnapshots`

`SharewithOtherAccounts.Risultato`

`MakePrivate.Risultato`

`MakePrivate.Comandi`

AWSPremiumSupport-PostgreSQLWorkloadReview

Descrizione

Il `AWSPremiumSupport-PostgreSQLWorkloadReview` runbook acquisisce più istantanee delle statistiche sull'utilizzo del database PostgreSQL di Amazon Relational Database Service (Amazon RDS). Le statistiche acquisite sono necessarie a un esperto di Supporto [Proactive Services per eseguire una revisione operativa](#). Le statistiche vengono raccolte utilizzando un set di script SQL e shell personalizzati. Questi script vengono scaricati in un'istanza temporanea di Amazon Elastic Compute Cloud EC2 (Amazon) creata da questo runbook. Account AWS Il runbook richiede di fornire le credenziali utilizzando un AWS Secrets Manager segreto contenente una coppia chiave-valore

nome utente e password. Il nome utente deve disporre delle autorizzazioni per interrogare le viste e le funzioni statistiche standard di PostgreSQL.

Questo runbook crea automaticamente le seguenti AWS risorse utilizzando uno stack. Account AWS
AWS CloudFormation È possibile monitorare la creazione dello stack utilizzando la console. AWS
CloudFormation

- Un cloud privato virtuale (VPC) e un' EC2 istanza Amazon lanciati in una sottorete privata del VPC con connettività opzionale a Internet tramite un gateway NAT.
- Un ruolo AWS Identity and Access Management (IAM) collegato all' EC2 istanza Amazon temporanea con le autorizzazioni per recuperare il valore segreto di Secrets Manager. Il ruolo fornisce anche le autorizzazioni per caricare file su un bucket Amazon Simple Storage Service (Amazon S3) di tua scelta e, facoltativamente, su un case. Supporto
- Una connessione peering VPC per consentire la connettività tra l'istanza DB e l'istanza Amazon temporanea. EC2
- Systems Manager, Secrets Manager e endpoint VPC Amazon S3 collegati al VPC temporaneo.
- Una finestra di manutenzione con attività registrate che avviano e interrompono periodicamente l' EC2 istanza Amazon temporanea, eseguono script di raccolta dati e caricano file in un bucket Amazon S3. Viene inoltre creato un ruolo IAM per la finestra di manutenzione che fornisce le autorizzazioni per eseguire le attività registrate.

Al termine del runbook, lo AWS CloudFormation stack utilizzato per creare AWS le risorse necessarie viene eliminato e il report viene caricato nel bucket Amazon S3 di tua scelta e, facoltativamente, in un case. Supporto

Note

Per impostazione predefinita, viene preservato il volume root Amazon EBS dell' EC2 istanza Amazon temporanea. Puoi ignorare questa opzione impostando il `EbsVolumeDeleteOnTermination` parametro su `true`

Prerequisiti

- Abbonamento Enterprise Support Questo runbook e Proactive Services Workload Diagnostics and Reviews richiedono un abbonamento Enterprise Support. Prima di utilizzare questo runbook,

contattate il Technical Account Manager (TAM) o lo Specialist TAM (STAM) per istruzioni. [Per ulteriori informazioni, consulta Proactive Services.Supporto](#)

- Account e Regione AWS quote Assicurati di non aver raggiunto il numero massimo di EC2 istanze Amazon o di VPCs poterle creare nell'account e nella regione in cui utilizzi questo runbook. Se devi richiedere un aumento del limite, consulta il modulo Aumento del [limite di servizio](#).
- Configurazione del database
 1. L'`pg_stat_statements` estensione deve essere configurata nel database specificato nel `DatabaseName` parametro. Se non è stata effettuata la configurazione `pg_stat_statements` in `shared_preload_libraries`, è necessario modificare il valore nel DB Parameter Group e applicare le modifiche. Le modifiche al parametro `shared_preload_libraries` richiedono il riavvio dell'istanza DB. Per ulteriori informazioni, consulta la sezione [Uso di gruppi di parametri](#). L'aggiunta `pg_stat_statements` a `shared_preload_libraries` aggiungerà un sovraccarico prestazionale. Tuttavia, ciò è utile per tenere traccia delle prestazioni delle singole dichiarazioni. Per ulteriori informazioni sull'`pg_stat_statements` estensione, consulta la documentazione di [PostgreSQL](#). Se non configuri l'`pg_stat_statements` estensione o se l'estensione non è presente nel database utilizzato per la raccolta delle statistiche, l'analisi a livello di dichiarazione non verrà presentata nella revisione operativa.
 2. Assicurati che `track_counts` i `track_activities` parametri non siano disattivati. Se questi parametri sono disattivati nel DB Parameter Group, non saranno disponibili statistiche significative. La modifica di questi parametri richiederà il riavvio dell'istanza DB. Per ulteriori informazioni, consulta [Lavorare con i parametri sull'istanza database Amazon RDS for PostgreSQL](#).
 3. Se il `track_io_timing` parametro è disattivato, le statistiche a livello di I/O non verranno incluse nella revisione operativa. La modifica `track_io_timing` richiederà il riavvio dell'istanza DB e comporterà un sovraccarico di prestazioni aggiuntivo a seconda del carico di lavoro dell'istanza DB. Nonostante il sovraccarico di prestazioni per i carichi di lavoro critici, questo parametro fornisce informazioni utili relative al tempo di I/O per query.

Fatturazione e addebiti Ti Account AWS verranno addebitati i costi associati all' EC2 istanza Amazon temporanea, al volume Amazon EBS associato, al gateway NAT e ai dati trasferiti durante l'esecuzione di questa automazione. Per impostazione predefinita, questo runbook crea un'istanza `t3.micro` Amazon Linux 2 per raccogliere le statistiche. Il runbook avvia e arresta l'istanza tra i passaggi per ridurre i costi.

Sicurezza e governance dei dati [Questo runbook raccoglie statistiche interrogando le viste e le funzioni delle statistiche di PostgreSQL](#). Assicurati che le credenziali fornite nel `SecretId` parametro

consentano solo autorizzazioni di sola lettura per le visualizzazioni e le funzioni delle statistiche. Come parte dell'automazione, gli script di raccolta vengono caricati nel bucket Amazon S3 e possono essere collocati in. `s3://amzn-s3-demo-bucket/automation execution id/queries/`

Questi script raccolgono dati che vengono utilizzati da uno AWS specialista per esaminare gli indicatori chiave di prestazione a livello di oggetto. Lo script raccoglie informazioni come il nome della tabella, il nome dello schema e il nome dell'indice. Se una di queste informazioni contiene informazioni sensibili come indicatori di fatturato, nome utente, indirizzo e-mail o qualsiasi altra informazione di identificazione personale, ti consigliamo di interrompere questa revisione del carico di lavoro. Contatta il tuo AWS TAM per discutere di un approccio alternativo per la revisione del carico di lavoro.

Assicurati di avere l'approvazione e l'autorizzazione necessarie per condividere le statistiche e i metadati raccolti da questa automazione. AWS

Considerazioni sulla sicurezza Se imposti il `UpdateRdsSecurityGroup` parametro su `yes`, il runbook aggiorna il gruppo di sicurezza associato all'istanza DB per consentire il traffico in entrata dall'indirizzo IP privato dell' EC2 istanza Amazon temporanea.

Se imposti il `UpdateRdsRouteTable` parametro su `yes`, il runbook aggiorna la tabella di routing associata alla sottorete in cui è in esecuzione l'istanza DB per consentire il traffico verso l' EC2 istanza Amazon temporanea tramite la connessione peering VPC.

Creazione di utenti Per consentire allo script di raccolta di connettersi al tuo database Amazon RDS, devi configurare un utente con le autorizzazioni per leggere le visualizzazioni statistiche. Quindi è necessario memorizzare le credenziali in Secrets Manager. Ti consigliamo di creare un nuovo utente dedicato per questa automazione. La creazione di un utente separato consente di controllare e tenere traccia delle attività eseguite da questa automazione.

1. Crea un nuovo utente.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. Assicurati che questo utente possa effettuare solo connessioni di sola lettura.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. Imposta limiti a livello utente.

```
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. Concedi `pg_monitor` le autorizzazioni al nuovo utente in modo che possa accedere alle statistiche del DB. (Il `pg_monitor` ruolo è membro di `pg_read_all_settings`, `pg_read_all_stats`, `pg_stat_scan_table`.)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

Autorizzazioni aggiunte al profilo dell' EC2 istanza Amazon temporanea da questa Systems Manager Automation Le seguenti autorizzazioni vengono aggiunte al ruolo IAM associato all'istanza Amazon EC2 temporanea. La policy `AmazonSSMManagedInstanceCore` gestita è anche associata al ruolo IAM per consentire la gestione dell' EC2 istanza Amazon da parte di Systems Manager.

```
{
  "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:region:account id:secret:secret id",
        "Effect": "Allow"
    },
    {
        "Action": [
            "support:AddAttachmentsToSet",
            "support:AddCommunicationToCase",
            "support:DescribeCases"
        ],
        "Resource": "*",
        "Effect": "Allow"
    }
]
}

```

Autorizzazioni aggiunte alla finestra di manutenzione temporanea da questa Systems Manager Automation Le seguenti autorizzazioni vengono aggiunte automaticamente al ruolo IAM associato alle attività di manutenzione di Windows. Le attività di manutenzione di Windows vengono avviate, interrotte e inviano comandi all' EC2 istanza temporanea di Amazon.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:GetAutomationExecution",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation",
        "ssm:GetCalendarState",
        "ssm:CancelCommand",
        "ec2:DescribeInstanceStatus"
      ],

```

```

        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "ssm:SendCommand",
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ssm:StartAutomationExecution"
        ],
        "Resource": [
            "arn:aws:ec2:region:account id:instance/temporary instance id",
            "arn:aws:ssm:*:*:document/AWS-RunShellScript",
            "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:$DEFAULT",
            "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:$DEFAULT"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "ssm.amazonaws.com"
            }
        },
        "Action": "iam:PassRole",
        "Resource": "*",
        "Effect": "Allow"
    }
]
}

```

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DBInstanceIdentificatore

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza DB.

- DatabaseName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del database ospitato sull'istanza DB.

- SecretId

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del segreto di Secrets Manager contenente la coppia chiave-valore nome utente e password. Lo AWS CloudFormation stack crea una policy IAM con autorizzazioni per l'GetSecretValueoperazione su questo ARN. Le credenziali vengono utilizzate per consentire all'istanza temporanea di raccogliere le statistiche del database. Contatta il tuo TAM o STAM per discutere delle autorizzazioni minime richieste.

- Riconosci

Tipo: stringa

Descrizione: (Obbligatorio) Inserisci **yes** se riconosci che questo runbook creerà risorse temporanee nel tuo account per raccogliere statistiche dall'istanza DB. Ti consigliamo di contattare il tuo TAM o STAM prima di eseguire questa automazione.

- SupportCase

Tipo: stringa

Descrizione: (Facoltativo) Il numero del Supporto caso fornito dal TAM o dallo STAM. Se fornito, il runbook aggiorna il caso e allega i dati raccolti. Questa opzione richiede che l' EC2 istanza Amazon temporanea disponga di connettività Internet per accedere all'endpoint dell' Supporto API. È necessario impostare il AllowVpcInternetAccess parametro su. true L'oggetto del caso deve contenere la fraseAWSPremiumSupport-PostgreSQLWorkloadReview.

- S3 BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 nel tuo account in cui desideri caricare i dati raccolti dall'automazione. Verifica che la policy del bucket non conceda autorizzazioni di lettura o scrittura non necessarie ai principali che non hanno bisogno di accedere al contenuto del bucket. Ti consigliamo di creare un nuovo bucket Amazon S3 temporaneo ai fini di questa automazione. Il runbook fornisce le autorizzazioni per il funzionamento dell's3:PutObjectAPI per il ruolo IAM collegato all'istanza Amazon EC2 temporanea. I file caricati verranno archiviati in. s3://*bucket name/automation execution id/*

- InstanceType

Tipo: stringa

Descrizione: (Facoltativo) Il tipo di EC2 istanza Amazon temporanea che eseguirà gli script SQL e shell personalizzati.

Valori validi: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

Predefinito: t3.micro

- VpcCidr

Tipo: stringa

Descrizione: (Facoltativo) L'intervallo di indirizzi IP in notazione CIDR per il nuovo VPC (ad esempio,). 172.31.0.0/16 Assicurati di selezionare un CIDR che non si sovrapponga o corrisponda a nessun VPC esistente con connettività alla tua istanza DB. Il VPC più piccolo che puoi creare utilizza una subnet mask /28, mentre il VPC più grande utilizza una subnet mask /16.

Impostazione predefinita: 172.31.0.0/16

- StackResourcesNamePrefix

Tipo: stringa

Descrizione: (Facoltativo) Il prefisso e il tag del nome delle risorse AWS CloudFormation dello stack. Il runbook crea le risorse dello AWS CloudFormation stack utilizzando questo prefisso come parte del nome e del tag applicati alle risorse. La struttura per la coppia chiave-valore del tag è.

StackResourcesNamePrefix: {{automation:EXECUTION_ID}}

Impostazione predefinita: revisione AWSPostgre SQLWorkload

- Pianificazione

Tipo: stringa

Descrizione: (Facoltativo) La pianificazione della finestra di manutenzione. Specifica la frequenza con cui la finestra di manutenzione esegue le attività. Il valore predefinito è `every1 hour`.

Valori validi: 15 minuti | 30 minuti | 1 ora | 2 ore | 4 ore | 6 ore | 12 ore | 1 giorno | 2 giorni | 4 giorni

Impostazione predefinita: 1 ora

- Durata

Tipo: integer

Descrizione: (Facoltativo) La durata massima, in minuti, per cui si desidera consentire l'esecuzione dell'automazione. La durata massima supportata è di 8.640 minuti (6 giorni). Il valore predefinito è 4.320 minuti (3 giorni).

Valori validi: 30-8640

Valore predefinito: 4320

- UpdateRdsRouteTable

Tipo: stringa

Descrizione: (Facoltativo) Se impostato su `true`, il runbook aggiorna la tabella di routing associata alla sottorete in cui viene eseguita l'istanza DB. Viene aggiunto un IPv4 percorso per indirizzare il traffico verso l' IPv4 indirizzo privato temporaneo dell' EC2 istanza Amazon tramite la connessione peering VPC appena creata.

Valori validi: `true` | `false`

Impostazione predefinita: `false`

- `AllowVpcInternetAccess`

Tipo: stringa

Descrizione: (Facoltativo) Se impostato su `true`, il runbook crea un gateway NAT per fornire connettività Internet all' EC2 istanza Amazon temporanea per comunicare con l'endpoint Supporto API. Puoi lasciare questo parametro come `false` se desideri solo che il runbook carichi l'output nel tuo bucket Amazon S3.

Valori validi: `true` | `false`

Impostazione predefinita: `false`

- `UpdateRdsSecurityGroup`

Tipo: stringa

Descrizione: (Facoltativo) Se impostato su `true`, il runbook aggiorna il gruppo di sicurezza associato all'istanza DB per consentire il traffico proveniente dall'indirizzo IP privato dell'istanza temporanea.

Valori validi: `false` | `true`

Impostazione predefinita: `false`

- `EbsVolumeDeleteOnTermination`

Tipo: stringa

Descrizione: (Facoltativo) Se impostato su `true`, il volume root dell' EC2 istanza Amazon temporanea viene eliminato dopo il completamento del runbook e l'eliminazione dello stack. AWS CloudFormation

Valori validi: `false` | `true`

Impostazione predefinita: `false`

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

1. `aws:assertAwsResourceProperty`- Conferma che l'istanza DB è nello `available` stato.
2. `aws:executeAwsApi`- Raccoglie dettagli sull'istanza DB.
3. `aws:executeScript`- Verifica se il bucket Amazon S3 specificato in `S3BucketName` consente autorizzazioni di accesso anonime o pubbliche in lettura o scrittura.
4. `aws:executeScript`- Ottiene il contenuto del AWS CloudFormation modello dall'allegato Automation Runbook utilizzato per creare le risorse temporanee AWS nel tuo Account AWS

5. `aws:createStack`- Crea le risorse dello AWS CloudFormation stack.
6. `aws:waitForAwsResourceProperty`- Attende l'esecuzione dell' EC2istanza Amazon creata dal AWS CloudFormation modello.
7. `aws:executeAwsApi`- Ottiene IDs l' EC2istanza Amazon temporanea e la connessione peering VPC creata da. AWS CloudFormation
8. `aws:executeAwsApi`- Ottiene l'indirizzo IP per l' EC2 istanza Amazon temporanea per configurare la connettività con l'istanza DB.
9. `aws:executeAwsApi`- Etichetta il volume Amazon EBS collegato all' EC2 istanza Amazon temporanea.
10. `aws:waitForAwsResourceProperty`- Attende che l' EC2 istanza Amazon temporanea superi i controlli di stato.
11. `aws:waitForAwsResourceProperty`- Attende che l' EC2 istanza Amazon temporanea venga gestita da Systems Manager. Se questo passaggio scade o fallisce, il runbook riavvia l'istanza.
 - a. `aws:executeAwsApi`- Riavvia l' EC2istanza Amazon temporanea se il passaggio precedente non è riuscito o è scaduto.
 - b. `aws:waitForAwsResourceProperty`- Attende che l' EC2 istanza Amazon temporanea venga gestita da Systems Manager dopo il riavvio.
12. `aws:runCommand`- Installa i requisiti dell'applicazione Metadata Collector sull'istanza Amazon temporanea. EC2
13. `aws:runCommand`- Configura l'accesso alla tua istanza DB creando un file di configurazione sull' EC2 istanza Amazon temporanea.
14. `aws:executeAwsApi`- Crea una finestra di manutenzione per eseguire periodicamente l'applicazione di raccolta dei metadati utilizzando Run Command. La finestra di manutenzione avvia e interrompe l'istanza tra i comandi.
15. `aws:waitForAwsResourceProperty`- Attende che la finestra di manutenzione creata dal AWS CloudFormation modello sia pronta.
16. `aws:executeAwsApi`- Ottiene IDs la finestra di manutenzione e il calendario delle modifiche creato da AWS CloudFormation.
17. `aws:sleep`- Attende la data di fine della finestra di manutenzione.
18. `aws:executeAwsApi`- Disattiva la finestra di manutenzione.
19. `aws:executeScript`- Ottiene i risultati delle attività eseguite durante la finestra di manutenzione.
20. `aws:waitForAwsResourceProperty`- Attende che la finestra di manutenzione termini l'ultima operazione prima di continuare.

- 21 `aws:branch`- Suddivide il flusso di lavoro a seconda che sia stato fornito un valore per il `SupportCase` parametro.
- a. `aws:changeInstanceState`- Avvia l' EC2 istanza Amazon temporanea e attende il completamento dei controlli di stato prima di caricare il report.
 - b. `aws:waitForAwsResourceProperty`- Attende che l' EC2 istanza Amazon temporanea venga gestita da Systems Manager. Se questo passaggio si interrompe o fallisce, il runbook riavvia l'istanza.
 - i. `aws:executeAwsApi`- Riavvia l' EC2 istanza Amazon temporanea se il passaggio precedente non è riuscito o è scaduto.
 - ii. `aws:waitForAwsResourceProperty`- Attende che l' EC2 istanza Amazon temporanea venga gestita da Systems Manager dopo il riavvio.
 - c. `aws:runCommand`- Allega il rapporto sui metadati al Supporto caso se hai fornito un valore per il parametro. `SupportCase` Lo script comprime e divide il rapporto in file da 5 MB. Il numero massimo di file che lo script allega a un Supporto caso è 12.
- 22 `aws:changeInstanceState`- Interrompe l' EC2 istanza Amazon temporanea nel caso in cui lo AWS CloudFormation stack non riesca a eliminare.
- 23 `aws:executeAwsApi`- Descrive gli eventi AWS CloudFormation dello stack se i runbook non riescono a creare o aggiornare lo stack. AWS CloudFormation
- 24 `aws:waitForAwsResourceProperty`- Attende che lo AWS CloudFormation stack raggiunga lo stato di terminale prima di eliminarlo.
- 25 `aws:executeAwsApi`- Elimina lo AWS CloudFormation stack escludendo la finestra di manutenzione. Il volume root Amazon EBS associato all' EC2 istanza Amazon temporanea viene preservato se il valore del `EbsVolumeDeleteOnTermination` parametro è stato impostato `false` su.

AWS-RebootRdsInstance

Descrizione

Il `AWS-RebootRdsInstance` runbook riavvia un'istanza DB di Amazon Relational Database Service (Amazon RDS) se non è già in fase di riavvio.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza DB di Amazon RDS che desideri riavviare.

Fasi del documento

RebootInstance - Riavvia l'istanza DB se non è già in fase di riavvio.

WaitForAvailableState - Attende che l'istanza DB completi il processo di riavvio.

Output

Questa automazione non ha uscite.

AWSSupport-ShareRDSSnapshot

Descrizione

Il AWSSupport-ShareRDSSnapshot runbook fornisce una soluzione automatizzata per la procedura descritta nell'articolo del Knowledge Center [Come posso condividere uno snapshot](#)

[crittografato di Amazon RDS DB con un](#) altro account? Se lo snapshot di Amazon Relational Database Service (Amazon RDS) è stato crittografato utilizzando l' Chiave gestita da AWS impostazione predefinita, non è possibile condividere lo snapshot. In questo caso, devi copiare lo snapshot utilizzando una chiave gestita dal cliente e quindi condividerlo con l'account di destinazione. Questa automazione esegue questi passaggi utilizzando il valore specificato nel SnapshotName parametro o l'ultima istantanea trovata per l'istanza o il cluster di database Amazon RDS selezionato.

Note

Se non specifichi un valore per il KMSKey parametro, l'automazione crea una nuova chiave gestita AWS KMS dal cliente nell'account che viene utilizzata per crittografare lo snapshot.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AccountIds

Tipo: StringList

Descrizione: (Obbligatorio) Elenco di account separati da virgole con IDs cui condividere l'istantanea.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Database

Tipo: stringa

Descrizione: (Obbligatorio) Il nome dell'istanza o del cluster di Amazon RDS DB di cui desideri condividere lo snapshot. Questo parametro è facoltativo se si specifica un valore per il SnapshotName parametro.

- KMSKey

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) completo della chiave gestita dal AWS KMS cliente utilizzata per crittografare lo snapshot.

- SnapshotName

Tipo: stringa

Descrizione: (Facoltativo) L'ID del cluster DB o dello snapshot dell'istanza che desideri utilizzare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- rds:DescribeDBInstances
- rds:DescribeDBSnapshots
- rds:CopyDBSnapshot
- rds:ModifyDBSnapshotAttribute

Sono AutomationAssumeRole necessarie le seguenti azioni per avviare correttamente il runbook per un cluster DB.

- ssm:StartAutomationExecution
- rds:DescribeDBClusters

- `rds:DescribeDBClusterSnapshots`
- `rds:CopyDBClusterSnapshot`
- `rds:ModifyDBClusterSnapshotAttribute`

Il ruolo IAM utilizzato per eseguire l'automazione deve essere aggiunto come utente chiave per utilizzare la chiave KMS specificata nel `ARNKmsKey` parametro. Per informazioni sull'aggiunta di utenti chiave a una chiave KMS, consulta [Changing a key policy](#) nella AWS Key Management Service Developer Guide.

Sono `AutomationAssumeRole` necessarie le seguenti azioni aggiuntive per avviare correttamente il runbook se non si specifica un valore per il `KMSKey` parametro.

- `kms:CreateKey`
- `kms:ScheduleKeyDeletion`
- `kms:CreateGrant`
- `kms:DescribeKey`

Fasi del documento

1. `aws:executeScript`- Verifica se è stato fornito un valore per il `KMSKey` parametro e crea una chiave gestita AWS KMS dal cliente se non viene trovato alcun valore.
2. `aws:branch`- Verifica se è stato fornito un valore per il `SnapshotName` parametro e si ramifica di conseguenza.
3. `aws:executeAwsApi`- Verifica se l'istantanea fornita proviene da un'istanza DB.
4. `aws:executeScript`- Formatta il `SnapshotName` parametro sostituendo i due punti con un trattino.
5. `aws:executeAwsApi`- Copia l'istantanea utilizzando il codice specificato. `KMSKey`
6. `aws:waitForAwsResourceProperty`- Attende il completamento dell'operazione di copia dell'istantanea.
7. `aws:executeAwsApi`- Condivide la nuova istantanea con quella specificata. `AccountIds`
8. `aws:executeAwsApi`- Verifica se l'istantanea fornita proviene da un cluster DB.
9. `aws:executeScript`- Formatta il `SnapshotName` parametro sostituendo i due punti con un trattino.
10. `aws:executeAwsApi`- Copia l'istantanea utilizzando il codice specificato. `KMSKey`

- 11aws:waitForAwsResourceProperty- Attende il completamento dell'operazione di copia dell'istantanea.
- 12aws:executeAwsApi- Condivide la nuova istantanea con quella specificata. AccountIds
- 13aws:executeAwsApi- Verifica se il valore fornito per il Database parametro è un'istanza DB.
- 14aws:executeAwsApi- Verifica se il valore fornito per il Database parametro è un cluster DB.
- 15aws:executeAwsApi- Recupera un elenco di istantanee per quanto specificato. Database
- 16aws:executeScript- Determina l'ultima istantanea disponibile dall'elenco assemblato nel passaggio precedente.
- 17aws:executeAwsApi- Copia lo snapshot dell'istanza DB utilizzando il codice specificato. KMSKey
- 18aws:waitForAwsResourceProperty- Attende il completamento dell'operazione di copia dell'istantanea.
- 19aws:executeAwsApi- Condivide la nuova istantanea con quella specificata. AccountIds
- 20aws:executeAwsApi- Recupera un elenco di istantanee per quanto specificato. Database
- 21aws:executeScript- Determina l'ultima istantanea disponibile dall'elenco assemblato nel passaggio precedente.
- 22aws:executeAwsApi- Copia lo snapshot dell'istanza DB utilizzando il codice specificato. KMSKey
- 23aws:waitForAwsResourceProperty- Attende il completamento dell'operazione di copia dell'istantanea.
- 24aws:executeAwsApi- Condivide la nuova istantanea con quella specificata. AccountIds
- 25aws:executeScript- Elimina la chiave gestita dal AWS KMS cliente creata dall'automazione se non è stato specificato un valore per il KMSKey parametro e l'automazione fallisce.

AWS-StartRdsInstance

Descrizione

Avvia un'istanza Amazon Relational Database Service (Amazon RDS).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Instanceld

Tipo: stringa

Descrizione: (obbligatorio) ID dell'istanza Amazon RDS da avviare.

AWS-StartStopAuroraCluster

Descrizione

Questo runbook avvia o arresta un cluster Amazon Aurora.

Note

Per avviare un cluster, è necessario che sia in uno stopped stato. Per arrestare un cluster, è necessario che sia in uno available stato. Questo runbook non può essere utilizzato per avviare o arrestare un cluster Aurora Serverless, un cluster Aurora multimaster, parte di un database globale Aurora o un cluster che utilizza la query parallela Aurora.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- ClusterName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del cluster Aurora che desideri arrestare o avviare.

- Azione

Tipo: stringa

Valori validi: Start | Stop

Impostazione predefinita: Start

Descrizione: (Obbligatorio) Il nome del cluster Aurora che desideri arrestare o avviare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- rds:DescribeDBClusters

- `rds:StartDBCluster`
- `rds:StopDBCluster`

Fasi del documento

- `aws:executeScript`- Avvia o arresta il cluster in base ai valori specificati per.

Output

`StartStopAuroraCluster.ClusterName` - Il nome del cluster Aurora

`StartStopAuroraCluster.CurrentStatus` - Lo stato attuale del cluster Aurora

`StartStopAuroraCluster.Message` - Dettagli dell'automazione

AWS-StopRdsInstance

Descrizione

Arresta un'istanza di Amazon Relational Database Service (Amazon RDS).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (obbligatorio) ID dell'istanza Amazon RDS da interrompere.

AWSSupport-TroubleshootConnectivityToRDS

Descrizione

Il AWSSupport-TroubleshootConnectivityToRDS runbook diagnostica i problemi di connettività tra un' EC2 istanza e un'istanza di Amazon Relational Database Service. L'automazione garantisce la disponibilità dell'istanza DB, quindi verifica le regole dei gruppi di sicurezza associati, gli elenchi di controllo degli accessi alla rete (rete ACLs) e le tabelle di routing per potenziali problemi di connettività.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DBInstanceIdentificatore

Tipo: stringa

Descrizione: (obbligatorio) ID istanza DB su cui testare la connettività.

- SourceInstance

Tipo: stringa

Modello consentito: `^[a-z0-9]{8,17}$`

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza da cui testare la connettività.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che lo stato dell'istanza DB è `available`.
- `aws:executeAwsApi`- Ottiene informazioni sull'istanza DB.
- `aws:executeAwsApi`- Ottiene informazioni sulla rete di istanze DB ACLs.
- `aws:executeAwsApi`- Ottiene la sottorete CIDR dell'istanza DB.
- `aws:executeAwsApi`- Ottiene informazioni sull'istanza. EC2

- `aws:executeAwsApi`- Ottiene informazioni sulla rete dell' EC2 istanza ACLs.
- `aws:executeAwsApi`- Ottiene informazioni sui gruppi di sicurezza associati all' EC2 istanza.
- `aws:executeAwsApi`- Ottiene informazioni sui gruppi di sicurezza associati all'istanza DB.
- `aws:executeAwsApi`- Ottiene informazioni sulle tabelle di routing associate all' EC2 istanza.
- `aws:executeAwsApi`- Ottiene informazioni sulla tabella di routing principale associata ad Amazon VPC per l' EC2 istanza.
- `aws:executeAwsApi`- Ottiene informazioni sulle tabelle di routing associate all'istanza DB.
- `aws:executeAwsApi`- Ottiene informazioni sulla tabella di routing principale associata ad Amazon VPC per l'istanza DB.
- `aws:executeScript`- Valuta le regole dei gruppi di sicurezza.
- `aws:executeScript`- Valuta la rete. ACLs
- `aws:executeScript`- Valuta le tabelle dei percorsi.
- `aws:sleep`- Termina l'automazione.

Output

- ottieni RDSInstance Proprietà. DBInstanceIdentifier: l'istanza DB utilizzata nell'automazione.

get RDSInstance Properties. DBInstanceState: lo stato attuale di DBInstance.

evalSecurityGroupRegole. SecurityGroupEvaluation - Risultati del confronto delle regole del gruppo SourceInstance di sicurezza con le regole del gruppo di sicurezza dell'istanza DB.

evalNetworkAclRegole. NetworkAclEvaluation - Risultati del confronto tra la SourceInstance rete e ACLs la rete di istanze DB ACLs.

evalRouteTableVoci. RouteTableEvaluation - Risultati del confronto della tabella delle SourceInstance rotte con le rotte delle istanze DB.

AWSSupport-TroubleshootRDSIAMAuthentication

Descrizione

AWSSupport-TroubleshootRDSIAMAuthentication Aiuta a risolvere i problemi di autenticazione AWS Identity and Access Management (IAM) per Amazon RDS for PostgreSQL, Amazon RDS for MySQL, Amazon RDS for MariaDB, Amazon Aurora PostgreSQL e Amazon Aurora MySQL. Usa questo runbook per verificare la configurazione richiesta per l'autenticazione IAM con

un'istanza Amazon RDS o un cluster Aurora. Fornisce inoltre passaggi per correggere i problemi di connettività all'istanza Amazon RDS o al cluster Aurora.

 Important

Questo runbook non supporta Amazon RDS per Oracle o Amazon RDS per Microsoft SQL Server.

 Important

Se viene fornita un' EC2 istanza Amazon di origine e il database di destinazione è Amazon RDS, `AWSSupport-TroubleshootConnectivityToRDS` viene richiamata un'automazione secondaria per risolvere i problemi di connettività TCP. L'output fornisce anche comandi che puoi eseguire sull' EC2 istanza Amazon o sul computer di origine per connetterti alle istanze Amazon RDS utilizzando l'autenticazione IAM.

Come funziona?

Questo runbook è composto da sei passaggi:

- Fase 1: `ValidateInputs`: convalida gli input dell'automazione.
- Fase 2: `branchOnSource EC2 Fornito`: verifica se nei parametri di input viene fornito un ID Amazon EC2 Instance di origine.
- Fase 3: `convalidaRDSConnectivity`: convalida la connettività Amazon RDS dall' EC2 istanza Amazon di origine, se fornita.
- Fase 4: `convalidaRDSIAMAuthentication`: verifica se la funzionalità di autenticazione IAM è abilitata.
- Passaggio 5: `convalidaIAMPolicies`: verifica se le autorizzazioni IAM richieste sono presenti nell'utente/ruolo IAM fornito.
- Fase 6: `GenerateReport`: genera un report dei risultati dei passaggi eseguiti in precedenza.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- RDSType

Tipo: stringa

Descrizione: (obbligatorio): seleziona il tipo di database relazionale a cui stai tentando di connetterti e autenticarti.

Valori consentiti: o Amazon RDS Amazon Aurora Cluster.

- DBInstanceIdentifier

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore dell'istanza di database Amazon RDS o del cluster di database Aurora di destinazione.

Modello consentito: $^[A-Za-z0-9]+(-[A-Za-z0-9]+)*\$$

Numero massimo di caratteri: 63

- SourceEc2InstanceIdentifier

Tipo: AWS::EC2::Instance::Id

Descrizione: (Facoltativo) L'ID Amazon EC2 Instance se ti connetti all'istanza di database Amazon RDS da un' EC2 istanza Amazon in esecuzione nello stesso account e nella stessa regione. Non

specificare questo parametro se l'origine non è un' EC2 istanza Amazon o se il tipo di Amazon RDS di destinazione è un cluster di database Aurora.

Impostazione predefinita: ""

- **DBIAMRoleNome**

Tipo: stringa

Descrizione: (Facoltativo) Il nome del ruolo IAM utilizzato per l'autenticazione basata su IAM. Fornisci solo se il parametro non DBIAMUserName viene fornito, altrimenti lascialo vuoto. DBIAMRoleNameO DBIAMUserName deve essere fornito.

Modello consentito: `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

Numero massimo di caratteri: 64

Impostazione predefinita: ""

- **DBIAMUserName**

Tipo: stringa

Descrizione: (Facoltativo) Il nome utente IAM utilizzato per l'autenticazione basata su IAM. Fornisci solo se il DBIAMRoleName parametro non viene fornito, altrimenti lascialo vuoto. DBIAMRoleNameO DBIAMUserName deve essere fornito.

Modello consentito: `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

Numero massimo di caratteri: 64

Impostazione predefinita: ""

- **DBUserName**

Tipo: stringa

Descrizione: (Facoltativo) Il nome utente del database mappato a un ruolo/utente IAM per l'autenticazione basata su IAM all'interno del database. L'opzione predefinita * valuta se l' rds-db:connect autorizzazione è consentita a tutti gli utenti del database.

Modello consentito: `^[a-zA-Z0-9+=, .@*_]{1,64}$`

Numero massimo di caratteri: 64

Impostazione predefinita: *

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Istruzioni

1. Accedere a [AWSSupport-TroubleshootRDSIAMAuthentication](#) nella AWS Systems Manager console.
2. Seleziona `Execute Automation`
3. Per i parametri di input, inserisci quanto segue:

- AutomationAssumeRole(Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- RDSType(Obbligatorio):

Seleziona il tipo di Amazon RDS a cui stai tentando di connetterti e autenticarti. Scegli tra i due valori consentiti: oppure Amazon RDS Amazon Aurora Cluster.

- DBInstanceIdentificatore (obbligatorio):

Inserisci l'identificatore dell'istanza di database Amazon RDS di destinazione o del cluster Aurora a cui stai tentando di connetterti e utilizza le credenziali IAM per l'autenticazione.

- SourceEc2 (Facoltativo): InstanceIdentifier

Fornisci l'ID Amazon EC2 Instance se ti connetti all'istanza di database Amazon RDS da un' EC2 istanza Amazon presente nello stesso account e nella stessa regione. Lascia vuoto se l'origine non è Amazon EC2 o se il tipo di Amazon RDS di destinazione è un cluster Aurora.

- DBIAMRoleName (opzionale):

Inserisci il nome del ruolo IAM utilizzato per l'autenticazione basata su IAM. Fornisci solo se non DBIAMUserName viene fornito; in caso contrario, lascia vuoto il campo. Fornito DBIAMRoleName o DBIAMUserName deve essere fornito.

- DBIAMUserName (facoltativo):

Inserisci l'utente IAM utilizzato per l'autenticazione basata su IAM. Fornisci solo se non DBIAMRoleName viene fornito, altrimenti lascia vuoto. Fornito DBIAMRoleName o DBIAMUserName deve essere fornito.

- DBUserName (facoltativo):

Inserisci l'utente del database mappato a un ruolo/utente IAM per l'autenticazione basata su IAM all'interno del database. L'opzione predefinita * viene utilizzata per la valutazione; non viene fornito nulla in questo campo.

Input parameters

SourceEc2InstanceIdentifier
(Optional) The Amazon EC2 Instance ID if you are connecting to the RDS DB instance from an EC2 Instance running in the same account and region. Do not specify this parameter if the source is not an EC2 instance or if the target RDS type is an Aurora DB cluster.

☒ Show interactive instance picker

Name	Instance ID	State	Availability zone	Platform
There are no managed instances in this account.				

We recommend using [Quick Setup](#) to configure your instances for Systems Manager.

After configuring your instances for Systems Manager, the instances will be displayed here in a few minutes.

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the role that allows the Automation runbook to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your current IAM user permissions context to execute this runbook.

DBInstanceIdentifier
(Required) The identifier of the target Amazon RDS DB instance or Amazon Aurora DB cluster.

DBIAMUserName
(Optional) The IAM user name used for IAM-based authentication. Provide only if the 'DBIAMRoleName' parameter is not provided, otherwise leave it empty. Either 'DBIAMRoleName' or 'DBIAMUserName' must be provided.

RDSType
(Required) The type of Relational Database.

DBIAMRoleName
(Optional) The IAM role name being used for IAM-based authentication. Provide only if the parameter 'DBIAMUserName' is not provided, otherwise leave it empty. Either 'DBIAMRoleName' or 'DBIAMUserName' must be provided.

DBUserName
(Optional) The database user name mapped to an IAM role/user for IAM-based authentication within the database. The default option "" evaluates if the 'rds-db:connect' permission is allowed for all users in the DB.

4. Seleziona Esegui.

5. Notate che l'automazione si avvia.

6. Il documento esegue le seguenti operazioni:

- Fase 1: Convalida degli input:

Convalida gli input dell'automazione - `SourceEC2InstanceIdentifier` (opzionale), or, `DBInstanceIdentifier` and or. `ClusterID` `DBIAMRoleName` `DBIAMUserName` Verifica se i parametri di input inseriti sono presenti nel tuo account e nella tua regione. Verifica inoltre se l'utente ha inserito uno dei parametri IAM (ad esempio, `DBIAMRoleName` o `DBIAMUserName`). Inoltre, esegue altre verifiche, ad esempio se il database menzionato è nello stato Disponibile.

- Fase 2: branchOnSource EC2 Fornito:

Verifica se nei parametri di input EC2 viene fornito il codice sorgente Amazon e se il database è Amazon RDS. In caso affermativo, si procede alla fase 3. In caso contrario, salta il passaggio 3, che è la convalida della connettività Amazon EC2 -Amazon RDS, e procede al passaggio 4.

- Fase 3: convalida: `RDSConnectivity`

Se nei parametri di input EC2 viene fornito il codice Amazon di origine e il database è Amazon RDS, la fase 2 avvia la fase 3. In questa fase, `AWSSupport - TroubleshootConnectivityToRDS` viene richiamata l'automazione secondaria per convalidare la connettività Amazon RDS dall'origine Amazon. EC2 Il runbook di automazione

secondario `AWSSupport-TroubleshootConnectivityToRDS` verifica se le configurazioni di rete richieste (Amazon Virtual Private Cloud [Amazon VPC], Security Groups, Network Access Control List [NACL], disponibilità di Amazon RDS) sono presenti in modo da consentirti di connetterti dall'istanza Amazon all'istanza Amazon RDS. EC2

- `RDSIAMAuthenticationFase 4: convalida:`

Verifica se la funzionalità di autenticazione IAM è abilitata sull'istanza Amazon RDS o sul cluster Aurora.

- Fase 5: convalida: `IAMPolicies`

Verifica se le autorizzazioni IAM richieste sono presenti nell'utente/ruolo IAM passato per consentire alle credenziali IAM di autenticarsi nell'istanza Amazon RDS per l'utente del database specificato (se presente).

- Fase 6: `GenerateReport:`

Ottiene tutte le informazioni dei passaggi precedenti e stampa il risultato o l'output di ogni passaggio. Elenca inoltre i passaggi a cui fare riferimento ed eseguire per connettersi all'istanza Amazon RDS utilizzando le credenziali IAM.

7. Una volta completata l'automazione, consulta la sezione Output per i risultati dettagliati:

- Verifica dell'autorizzazione User/Role IAM per la connessione al database:

Verifica se le autorizzazioni IAM richieste sono presenti nell'utente/ruolo IAM passato per consentire alle credenziali IAM di autenticarsi nell'istanza Amazon RDS per l'utente del database specificato (se presente).

- Verifica dell'attributo di autenticazione basato su IAM per il database:

Verifica se la funzionalità dell'autenticazione IAM è abilitata per il cluster Amazon RDS Database/Aurora specificato.

- Verifica della connettività da Amazon EC2 Instance a Amazon RDS:

Verifica se le configurazioni di rete richieste (Amazon VPC, Security Groups, NACL, disponibilità di Amazon RDS) sono presenti in modo da poterti connettere dall'istanza Amazon all'istanza EC2 Amazon RDS.

- Fasi successive:

Elenca i comandi e i passaggi a cui fare riferimento ed eseguire per connettersi all'istanza Amazon RDS utilizzando le credenziali IAM.

Outputs

ScriptExecutionId

Ze1d[REDACTED]ba4

Output

[Troubleshooting Results]

1. Checking the IAM user/role permissions to connect to database:

✔ [PASSED]: Found permission 'rds-db:connect' for the resource 'a[REDACTED]-db1'.

2. Checking IAM-based authentication attribute for the database:

✔ [PASSED]: IAM-based authentication attribute is enabled for the database 'a[REDACTED]-db1'.

3. Checking connectivity from the EC2 instance to RDS instance:

✔ [SKIPPED]: No Source EC2 instance provided.

Run these commands to troubleshoot connectivity to your aurora-mysql DB instance:

\$ telnet a[REDACTED]-db1.cluster- [REDACTED].rds.amazonaws.com 3306

\$ nc -vz a[REDACTED]-db1.cluster- [REDACTED].rds.amazonaws.com 3306

[Next Steps]

1. Verify if the database user exists and have the required permissions to connect to the database using IAM authentication:

- Connect to DB a[REDACTED]-db1 using admin/master db user.

- Run the following query/command in your database:

SELECT user, plugin, host from mysql.user WHERE user LIKE '%<name of the DB user>%';

- From the output, verify if the user has the AWSAuthenticationPlugin.

2. Download the SSL bundle and connect to aurora-mysql database using IAM authentication by running the following commands:

\$ wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem

\$ export DBPASS=\$(aws rds generate-db-auth-token --hostname a[REDACTED]-db1.cluster- [REDACTED].rds.amazonaws.com --port 3306 --region us-[REDACTED]-2 --username <name of the DB user>)

mysql --host=a[REDACTED]-db1.cluster- [REDACTED].rds.amazonaws.com --port=3306 --ssl-ca=global-bundle.pem --enable-cleartext-plugin --user=<name of the DB user> --password=\$DBPASS

Reference: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html>

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWSSupport-ValidateRdsNetworkConfiguration

Descrizione

AWSSupport-ValidateRdsNetworkConfigurationl'automazione aiuta a evitare lo stato di incompatibilità della rete per l'istanza esistente di Amazon Relational Database Service (Amazon RDS) /Amazon Aurora/Amazon DocumentDB prima dell'esecuzione o dell'operazione. ModifyDBInstance StartDBInstance Se l'istanza è già in uno stato di rete incompatibile, il runbook ne fornirà il motivo.

Come funziona?

Questo runbook determina se l'istanza del database Amazon RDS entrerà in uno stato di rete incompatibile o, in caso affermativo, determina il motivo per cui si trova in uno stato di rete incompatibile.

Il runbook esegue i seguenti controlli sulla tua istanza di database Amazon RDS:

- Quota Amazon Elastic Network Interface (ENI) per regione.
- Esistono tutte le sottoreti del database Subnet Group.
- Sono disponibili un numero sufficiente di indirizzi IP gratuiti per le sottoreti.
- (Per le istanze Amazon RDS accessibili pubblicamente) Impostazioni degli attributi VPC (e).
`enableDnsSupport` `enableDnsHostnames`

 Important

Quando utilizzi questo documento su cluster Amazon Aurora/Amazon DocumentDB, assicurati di utilizzare invece di. `DBInstanceIdentifier` `ClusterIdentifier` In caso contrario, il documento fallirà nel primo passaggio.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `rds:DescribeDBInstances`
- `servicequotas:GetServiceQuota`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeVpcAttribute`

- `ec2:DescribeSubnets`

Politica di esempio:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ValidateRdsNetwork",
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "servicequotas:GetServiceQuota",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets"
      ],
      "Resource": [
        "arn:aws:rds:{Region}:{Account}:db:{DbInstanceName}"
      ]
    }
  ]
}
```

Istruzioni

1. Passa a [AWSSupport-ValidateRdsNetworkConfiguration](#) nella AWS Systems Manager console.
2. Seleziona Execute Automation
3. Per i parametri di input, inserisci quanto segue:

- AutomationAssumeRole(Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DBInstanceIdentificatore (obbligatorio):

Inserisci l'identificatore dell'istanza di Amazon Relational Database Service.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Select an existing IAM Role

AutomationAssumeRoleSSM
arn:aws:iam::<account>:role/AutomationAssumeRoleSSM

DBInstanceIdentifier
(Required) The Amazon Aurora or Amazon DocumentDB instance identifier.

my-rds-instance-01

4. Seleziona Esegui.

5. Nota che l'automazione si avvia.

6. Il documento esegue le seguenti operazioni:

- Fase 1 `assertRdsState`:

Verifica se l'identificatore di istanza fornito esiste e presenta uno dei seguenti stati: `available`, `stopped`, `incompatible-network`.

- Fase 2: `gatherRdsInformation`

Raccoglie le informazioni necessarie sull'istanza Amazon RDS da utilizzare successivamente nell'automazione.

- Fase 3: `checkEniQuota`

Verifica l'attuale quota disponibile di Amazon ENI per la regione.

- Fase 4 `validateVpcAttributes`:

Verifica che i parametri DNS (`enableDnsSupport` e `enableDnsHostnames`) di Amazon VPC siano impostati su `true` (o meno se l'istanza Amazon RDS lo è). `PubliclyAccessible`

- Fase 5: `validateSubnetAttributes`

Convalida l'esistenza di sottoreti in `DBSubnetGroup` e verifica se sono disponibili IP per ogni sottorete.

- Fase 6: `GenerateReport`:

Ottiene tutte le informazioni dei passaggi precedenti e stampa il risultato o l'output di ogni passaggio. Elenca inoltre i passaggi a cui fare riferimento ed eseguire per connettersi all'istanza Amazon RDS utilizzando le credenziali IAM.

7. Una volta completata l'automazione, consulta la sezione Output per i risultati dettagliati:

Istanza Amazon RDS con configurazione di rete valida:

▼ Outputs

```
generateReport.Report
```

```
# AWS RDS Network Configuration Checks: aws-rds-01rr (available)
## ✅ No Issue(s) Found
```

```
### [Troubleshooting Results]
```

```
1. Checking ENI Quota for region the RDS Instance is in:
```

```
✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4997) is sufficient at the moment.
```

```
2. Checking VPC Attribute ('enableDnsHostname' & 'enableDnsSupport') settings:
```

```
✅ [PASSED] : [PASSED] Value for both VPC attributes ('enableDnsHostnames' and 'enableDnsSupport') is set to 'true'.
```

```
3. Checking if subnets required for RDS exists or not:
```

```
✅ [PASSED] : All subnets in 'ap-south-1b' availability zone exists.
```

```
4. Checking if Available IPs are sufficient per subnets that are required:
```

```
✅ [PASSED] : There are sufficient available IPs in 'ap-south-1b' availability zone.
```

```
5. Checking if other Availability zone satisfy Check No# 3 & 4:
```

```
* Availability Zone: ap-south-1c
```

```
  i. Subnet Existence Check: ✅ [PASSED]
```

```
  ii. Available IP Check: ✅ [PASSED]
```

```
* Availability Zone: ap-south-1a
```

```
  i. Subnet Existence Check: ✅ [PASSED]
```

```
  ii. Available IP Check: ✅ [PASSED]
```

```
### [Next Steps]
```

```
✅ All the checks has passed so the RDS Network configuration is correct.
```

```
Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
```

```
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.
```

Istanza Amazon RDS con configurazione di rete errata (l' enableDnsHostnames attributo VPC è impostato su false):

▼ Outputs

```

generateReport.Report
# AWS RDS Network Configuration Checks: test-fail-sazrds-vpcattr (stopped)
### 🚫 Issue(s) Found!!!

### [Troubleshooting Results]
1. Checking ENI Quota for region the RDS Instance is in:
  ✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4996) is sufficient at the moment.

2. Checking VPC Attribute ('enableDnsHostname' & 'enableDnsSupport') settings:
  ❌ [FAILED] : Value for 'enableDnsHostnames' VPC Attribute is 'false'.

3. Checking if subnets required for RDS exists or not:
  ✅ [PASSED] : All subnets in 'ap-south-1b' availability zone exists.

4. Checking if Available IPs are sufficient per subnets that are required:
  ⚠️ [WARNING] : There are sufficient available IPs in 'ap-south-1b' availability zone, but it is recommended to have more than 9 IPs.

5. Checking if other Availability zone satisfy Check No# 3 & 4:
  * Availability Zone: ap-south-1a
    i. Subnet Existence Check: ✅ [PASSED]
    ii. Available IP Check: ⚠️ [WARNING]

### [Next Steps]
o Please set the value of 'enableDnsHostnames' VPC attribute to 'true'.
  [+] View and update DNS attributes for your VPC: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-updating
o Please free up some IPs before performing Modify/Stop operation on the instance.
  [+] Learn why a subnet in your VPC has insufficient IP addresses : https://repost.aws/knowledge-center/subnet-insufficient-ips

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.

```

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS documentazione di servizio

- [Come posso risolvere i problemi con un database Amazon RDS che si trova in uno stato di rete incompatibile?](#)
- [Come posso risolvere i problemi con un'istanza di Amazon DocumentDB che si trova in uno stato di rete incompatibile?](#)

Amazon Redshift

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Redshift. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSConfigRemediation-DeleteRedshiftCluster](#)
- [AWSConfigRemediation-DisablePublicAccessToRedshiftCluster](#)
- [AWSConfigRemediation-EnableRedshiftClusterAuditLogging](#)
- [AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot](#)
- [AWSConfigRemediation-EnableRedshiftClusterEncryption](#)
- [AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting](#)
- [AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster](#)
- [AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings](#)
- [AWSConfigRemediation-ModifyRedshiftClusterNodeType](#)

AWSConfigRemediation-DeleteRedshiftCluster

Descrizione

Il AWSConfigRemediation-DeleteRedshiftCluster runbook elimina il cluster Amazon Redshift specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- ClusterIdentifier

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del cluster Amazon Redshift che desideri eliminare.

- SkipFinalClusterSnapshot

Tipo: Booleano

Impostazione predefinita: false

Descrizione: (Facoltativo) Se impostata su false, l'automazione crea uno snapshot prima di eliminare il cluster Amazon Redshift. Se impostato su true, non viene creata una snapshot finale del cluster.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift>DeleteCluster
- redshift:DescribeClusters

Fasi del documento

- aws:branch- Rami basati sul valore specificato per il SkipFinalClusterSnapshot parametro.
- aws:executeAwsApi- Elimina il cluster Amazon Redshift specificato nel ClusterIdentifier parametro.
- aws:assertAwsResourceProperty- Verifica che il cluster Amazon Redshift sia stato eliminato.

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

Descrizione

Il `AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` runbook disabilita l'accessibilità pubblica per il cluster Amazon Redshift specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- ClusterIdentifier

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore univoco del cluster per cui desideri disabilitare l'accessibilità pubblica.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Fasi del documento

- `aws:executeAwsApi`- Disattiva l'accessibilità pubblica per il cluster specificato nel parametro. `ClusterIdentifier`
- `aws:waitForAwsResourceProperty`- Attende che lo stato del cluster cambi a. `available`
- `aws:assertAwsResourceProperty`- Conferma che l'impostazione di accessibilità pubblica è disabilitata nel cluster.

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

Descrizione

Il `AWSConfigRemediation-EnableRedshiftClusterAuditLogging` runbook consente la registrazione di audit per il cluster Amazon Redshift specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon Simple Storage Service (Amazon S3) in cui desideri caricare i log.

- ClusterIdentifier

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui desideri abilitare la registrazione di controllo.

- S3 KeyPrefix

Tipo: stringa

Descrizione: (Facoltativo) Il prefisso chiave di Amazon S3 (sottocartella) in cui desideri caricare i log.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

Fasi del documento

- `aws:branch`- Rami in base al fatto che sia stato specificato un valore per il `S3KeyPrefix` parametro.
- `aws:executeAwsApi`- Abilita la registrazione di controllo sul cluster specificato nel `ClusterIdentifier` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la registrazione di controllo sia stata abilitata sul cluster.

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

Descrizione

Il `AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` runbook abilita istantanee automatizzate per il cluster Amazon Redshift specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `AutomatedSnapshotRetentionPeriod`

Tipo: integer

Valori validi: 1-35

Descrizione: (Obbligatorio) Il numero di giorni in cui vengono conservate le istantanee automatiche.

- `ClusterIdentifier`

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui si desidera abilitare le istantanee automatiche.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Fasi del documento

- `aws:executeAwsApi`- Abilita le istantanee di automazione sul cluster specificato nel `ClusterIdentifier` parametro.
- `aws:waitForAwsResourceProperty`- Attende che lo stato del cluster cambi in `available`
- `aws:executeScript`- Conferma che le istantanee automatiche sono state abilitate nel cluster.

AWSConfigRemediation-EnableRedshiftClusterEncryption

Descrizione

Il `AWSConfigRemediation-EnableRedshiftClusterEncryption` runbook abilita la crittografia sul cluster Amazon Redshift specificato utilizzando AWS Key Management Service una chiave AWS KMS() gestita dal cliente. Questo runbook deve essere usato solo come base per garantire

che i cluster Amazon Redshift siano crittografati secondo le migliori pratiche di sicurezza minime consigliate. Consigliamo di crittografare più cluster con diverse chiavi gestite dal cliente. Questo runbook non può modificare la chiave gestita AWS KMS dal cliente utilizzata su un cluster già crittografato. Per modificare la chiave gestita AWS KMS dal cliente utilizzata per crittografare un cluster, è necessario innanzitutto disabilitare la crittografia sul cluster.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- ClusterIdentifier

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui desideri abilitare la crittografia.

- KMSKeyARN

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) della chiave gestita AWS KMS dal cliente che desideri utilizzare per crittografare i dati del cluster.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Fasi del documento

- `aws:executeAwsApi`- Abilita la crittografia sul cluster Amazon Redshift specificato nel `ClusterIdentifier` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la crittografia sia stata abilitata sul cluster.

AWSConfigRemediation- EnableRedshiftClusterEnhancedVPCRouting

Descrizione

Il `AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` runbook consente il routing avanzato del cloud privato virtuale (VPC) per il cluster Amazon Redshift specificato. Per informazioni sul routing VPC avanzato, consulta Amazon Redshift [Enhanced VPC routing nella Amazon Redshift](#) Management Guide.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- ClusterIdentifier

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui desideri abilitare il routing VPC avanzato.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

Fasi del documento

- aws:executeAwsApi- Abilita il routing VPC avanzato sul cluster specificato nel parametro. ClusterIdentifier
- assertAwsResourceProperty- Conferma che il routing VPC avanzato è stato abilitato sul cluster.

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

Descrizione

Il `AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` runbook richiede connessioni in entrata per utilizzare SSL per il cluster Amazon Redshift specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `ClusterIdentifier`

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui desideri abilitare il routing VPC avanzato.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie i dettagli dei parametri dal cluster specificato nel `ClusterIdentifier` parametro.
- `aws:executeAwsApi`- Abilita l'`require_ssl` impostazione sul cluster specificata nel `ClusterIdentifier` parametro.
- `aws:assertAwsResourceProperty`- Conferma che l'`require_ssl` impostazione è stata abilitata sul cluster.
- `aws:executeScript`- Verifica l'`require_ssl` impostazione per il cluster.

AWSConfigRemediation- ModifyRedshiftClusterMaintenanceSettings

Descrizione

Il `AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` runbook modifica le impostazioni di manutenzione per il cluster Amazon Redshift specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- **AllowVersionUpgrade**

Tipo: Booleano

Descrizione: (Obbligatorio) Se impostato su `true`, gli aggiornamenti delle versioni principali vengono applicati automaticamente al cluster durante la finestra di manutenzione.

- **AutomationAssumeRole**

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- **AutomatedSnapshotRetentionPeriod**

Tipo: integer

Valori validi: 1-35

Descrizione: (Obbligatorio) Il numero di giorni in cui vengono conservate le istantanee automatiche.

- **ClusterIdentifier**

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore univoco del cluster su cui desideri abilitare il routing VPC avanzato.

- **PreferredMaintenanceWindow**

Tipo: stringa

Descrizione: (Obbligatorio) L'intervallo di tempo settimanale (in UTC) durante il quale può essere effettuata la manutenzione del sistema.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

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

- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Fasi del documento

- `aws:executeAwsApi`- Modifica le impostazioni di manutenzione per il cluster specificato nel `ClusterIdentifier` parametro.
- `aws:assertAwsResourceProperty`- Conferma che le impostazioni di manutenzione modificate sono state configurate per il cluster.

AWSConfigRemediation-ModifyRedshiftClusterNodeType

Descrizione

Il `AWSConfigRemediation-ModifyRedshiftClusterNodeType` runbook modifica il tipo di nodo e il numero di nodi per il cluster Amazon Redshift specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Database

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- Classic

Tipo: Booleano

Descrizione: (Facoltativo) Se impostata su `true`, l'operazione di ridimensionamento utilizza il processo di ridimensionamento classico.

- ClusterIdentifier

Tipo: stringa

Descrizione: (Obbligatorio) L'identificatore univoco del cluster di cui si desidera modificare il tipo di nodo.

- ClusterType

Tipo: stringa

Valori validi: nodo singolo | nodo multiplo

Descrizione: (Obbligatorio) Il tipo di cluster che desideri assegnare al cluster.

- NodeType

Tipo: stringa

Valori validi: `ds2.xlarge` | `ds2.8xlarge` | `dc1.large` | `dc1.8xlarge` | `dc2.8xlarge` | `ra3.4xlarge` | `ra3.16xlarge`

Descrizione: (Obbligatorio) Il tipo di nodo che desideri assegnare al cluster.

- NumberOfNodes

Tipo: integer

Valori validi: 2-100

Descrizione: (Facoltativo) Il numero di nodi che desideri assegnare al cluster. Se il cluster è `single-node` di un tipo, non specificare un valore per questo parametro.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

Fasi del documento

- `aws:executeScript`- Modifica il tipo di nodo e il numero di nodi per il cluster specificato nel `ClusterIdentifier` parametro.

Amazon S3

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Simple Storage Service. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [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-EmptyS3Bucket](#)
- [AWSSupport-TroubleshootS3EventNotifications](#)

- [AWSSupport-ContainS3Resource](#)

AWS-ArchiveS3BucketToIntelligentTiering

Descrizione

Il AWS-ArchiveS3BucketToIntelligentTiering runbook crea o sostituisce una configurazione di tiering intelligente per il bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket S3 per cui desideri creare una configurazione di tiering intelligente.

- ConfigurationId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID per la configurazione di tiering intelligente. Può essere un nuovo ID di configurazione o l'ID di una configurazione esistente.

- NumberOfDaysToArchive

Tipo: stringa

Valori validi: 90-730

Descrizione: (Obbligatorio) Il numero di giorni consecutivi dopo che un oggetto nel bucket è idoneo alla transizione al livello Archive Access.

- NumberOfDaysToDeepArchive

Tipo: stringa

Valori validi: 180-730

Descrizione: (Obbligatorio) Il numero di giorni consecutivi dopo che un oggetto nel bucket è idoneo alla transizione al livello Deep Archive Access.

- S3Prefix

Tipo: stringa

Descrizione: (Facoltativo) Il prefisso del nome chiave degli oggetti a cui si desidera applicare la configurazione.

- Tag

Tipo: MapList

Descrizione: (Facoltativo) Metadati assegnati agli oggetti a cui si desidera applicare la configurazione. I tag sono costituiti da una chiave e da un valore definiti dall'utente.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

Fasi del documento

- `PutBucketIntelligentTieringConfiguration` (AWS:ExecuteScript): crea o aggiorna una configurazione Amazon S3 Intelligent-Tiering per il bucket specificato.
- `VerifyBucketIntelligentTieringConfiguration`(aws: assertAwsResource Property) - Verifica che la configurazione intelligente di S3 Bucket sia stata applicata al bucket specificato.

AWS-ConfigureS3BucketLogging

Descrizione

Abilita la registrazione su un bucket Amazon Simple Storage Service (Amazon S3).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 per il quale desideri configurare la registrazione.

- GrantedPermission

Tipo: stringa

Valori validi: FULL_CONTROL | READ | WRITE

Descrizione: (obbligatorio) autorizzazioni di registrazione assegnate all'assegnatario per il bucket.

- GranteeEmailAddress

Tipo: stringa

(Facoltativo) Indirizzo e-mail dell'assegnatario.

- GranteeId

Tipo: stringa

Descrizione: (facoltativo) ID utente canonico ID dell'assegnatario.

- GranteeType

Tipo: stringa

Valori validi: CanonicalUser | Group AmazonCustomerByEmail

Descrizione: (obbligatorio) Tipo di assegnatario.

- GranteeUri

Tipo: stringa

Descrizione: (facoltativo) URI del gruppo di assegnatari.

- TargetBucket

Tipo: stringa

Descrizione: (Obbligatorio) specifica il bucket in cui desideri che Amazon S3 memorizzi i log di accesso al server. È possibile impostare la distribuzione dei log a qualsiasi bucket di proprietà dell'utente. È anche possibile configurare più bucket in modo che distribuiscano i propri log allo stesso bucket di destinazione. In questo caso è necessario sceglierne uno diverso TargetPrefix per ogni bucket di origine in modo che i file di log forniti possano essere distinti per chiave.

- TargetPrefix

Tipo: stringa

Impostazione predefinita: /

Descrizione: (facoltativo) specifica un prefisso per le chiavi in base alle quali i file di log verranno archiviati.

AWS-ConfigureS3BucketVersioning

Descrizione

Configura il controllo delle versioni per un bucket Amazon Simple Storage Service (Amazon S3).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 per cui desideri configurare il controllo delle versioni.

- VersioningState

Tipo: stringa

Valori validi: Abilitato | Sospeso

Impostazione predefinita: Enabled

Descrizione: (Facoltativo) Applicato all' VersioningConfiguration.Status. Se impostato su "Enabled", questo processo abilita la funzione Versioni multiple per gli oggetti nel bucket; a tutti gli oggetti aggiunti al bucket viene assegnato un ID versione univoco. Se impostato suSuspended, questo processo disabilita il controllo delle versioni per gli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID della versione. null

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Descrizione

Il AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock runbook configura le impostazioni dei blocchi di accesso pubblico di Amazon Simple Storage Service (Amazon S3) per un bucket Amazon S3 in base ai valori specificati nei parametri del runbook.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- BlockPublicAcls

Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Facoltativo) Se impostato su true, Amazon S3 blocca gli elenchi di controllo degli accessi pubblici (ACLs) per il bucket S3 e gli oggetti archiviati nel bucket S3 specificato nel parametro. BucketName

- BlockPublicPolicy

Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Facoltativo) Se impostato su true, Amazon S3 blocca le policy dei bucket pubblici per il bucket S3 specificato nel parametro. BucketName

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket S3 che desideri configurare.

- IgnorePublicAcls

Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Facoltativo) Se impostato su true, Amazon S3 ignora tutto il pubblico ACLs per il bucket S3 specificato nel parametro. BucketName

- **RestrictPublicBuckets**

Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Facoltativo) Se impostato su true, Amazon S3 limita le politiche dei bucket pubblici per il bucket S3 specificato nel parametro. BucketName

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetAccountPublicAccessBlock
- s3:PutAccountPublicAccessBlock
- s3:GetBucketPublicAccessBlock
- s3:PutBucketPublicAccessBlock

Fasi del documento

- **aws:executeAwsApi**- Crea o modifica la PublicAccessBlock configurazione per il bucket S3 specificato nel parametro. BucketName
- **aws:executeScript**- Restituisce la PublicAccessBlock configurazione per il bucket S3 specificato nel BucketName parametro e verifica che le modifiche siano state apportate correttamente in base ai valori specificati nei parametri del runbook.

AWSConfigRemediation-ConfigureS3PublicAccessBlock

Descrizione

Il AWSConfigRemediation-ConfigureS3PublicAccessBlock runbook configura le impostazioni dei blocchi di accesso pubblico Account AWS Amazon Simple Storage Service (Amazon S3) di accesso pubblico in base ai valori specificati nei parametri del runbook.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AccountId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del proprietario del bucket S3 Account AWS che stai configurando.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- BlockPublicAcls

Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Facoltativo) Se impostato su true, Amazon S3 blocca gli elenchi di controllo degli accessi pubblici (ACLs) per i bucket S3 di proprietà dell' Account AWS utente specificato nel parametro. AccountId

- BlockPublicPolicy

Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Facoltativo) Se impostato su `true`, Amazon S3 blocca le policy dei bucket pubblici per i bucket S3 di proprietà del destinatario Account AWS specificato nel parametro. `AccountId`

- `IgnorePublicAcls`

Tipo: Booleano

Impostazione predefinita: `true`

Descrizione: (Facoltativo) Se impostato su `true`, Amazon S3 ignora tutti i bucket S3 pubblici ACLs di proprietà del tipo Account AWS specificato nel parametro. `AccountId`

- `RestrictPublicBuckets`

Tipo: Booleano

Impostazione predefinita: `true`

Descrizione: (Facoltativo) Se impostato su `true`, Amazon S3 limita le politiche dei bucket pubblici per i bucket S3 di proprietà del destinatario specificato nel Account AWS parametro. `AccountId`

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

Fasi del documento

- `aws:executeAwsApi`- Crea o modifica la `PublicAccessBlock` configurazione per Account AWS quanto specificato nel `AccountId` parametro.
- `aws:executeScript`- Restituisce la `PublicAccessBlock` configurazione per il valore Account AWS specificato nel `AccountId` parametro e verifica che le modifiche siano state apportate correttamente in base ai valori specificati nei parametri del runbook.

AWS-CreateS3PolicyToExpireMultipartUploads

Descrizione

Il `AWS-CreateS3PolicyToExpireMultipartUploads` runbook crea una politica del ciclo di vita per un bucket specifico che fa scadere i caricamenti incompleti in più parti in corso dopo un determinato numero di giorni. Questo runbook unisce la nuova politica del ciclo di vita a tutte le policy relative ai bucket del ciclo di vita esistenti già esistenti.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket S3 che desideri configurare.

- DaysUntilExpire

Tipo: integer

Descrizione: (Obbligatorio) Il numero di giorni di attesa di Amazon S3 prima di rimuovere definitivamente tutte le parti del caricamento.

- RuleId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID utilizzato per identificare la regola del bucket del ciclo di vita. Questo deve essere un valore univoco.

- S3Prefix

Tipo: stringa

Descrizione: (Facoltativo) Il prefisso del nome chiave degli oggetti a cui si desidera applicare la configurazione.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration

Fasi del documento

- ConfigureExpireMultipartUploads (aws:ExecuteScript): configura la politica del ciclo di vita per il bucket.
- VerifyExpireMultipartUploads (aws:ExecuteScript) - Verifica che la politica del ciclo di vita sia stata configurata per il bucket.

Output

- VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse
- VerifyExpireMultipartUploads.LifecycleConfigurationRule

AWS-DisableS3BucketPublicReadWrite

Descrizione

Usa Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon Block Public Access S3) per disabilitare l'accesso in lettura e scrittura per un bucket S3 pubblico. Per ulteriori informazioni, consulta [Using Amazon S3 Block Public Access](#) nella Guida per l'utente di Amazon Simple Storage Service.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- S3 BucketName

Tipo: stringa

Descrizione: (obbligatoria) bucket S3 in cui si desidera limitare l'accesso.

AWS-EnableS3BucketEncryption

Descrizione

Configura la crittografia predefinita per un bucket Amazon Simple Storage Service (Amazon S3).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- BucketName

Tipo: stringa

Descrizione: (obbligatoria) nome del bucket S3 in cui si desidera crittografare i contenuti.

- SSEAlgorithm

Tipo: stringa

Impostazione predefinita: AES256

Descrizione: (facoltativo) algoritmo di crittografia lato server da utilizzare per la crittografia predefinita.

AWS-EnableS3BucketKeys

Descrizione

Il `AWS-EnableS3BucketKeys` runbook abilita Bucket Keys sul bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente. Questa chiave a livello di bucket crea chiavi dati per nuovi oggetti durante il suo ciclo di vita. Se non specifichi un valore per il `KmsKeyId` parametro, la crittografia lato server con chiavi gestite di Amazon S3 (SSE-S3) viene utilizzata per la configurazione di crittografia predefinita.

Note

Le chiavi Bucket di Amazon S3 non sono supportate per la crittografia lato server a doppio livello con AWS Key Management Service chiavi () (DSSE-KMS).AWS KMS

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- **BucketName**

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket S3 per il quale desideri abilitare Bucket Keys.

- **KMSKeyId**

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN), l'ID della chiave o l'alias della chiave gestita dal cliente AWS Key Management Service (AWS KMS) che desideri utilizzare per la crittografia lato server.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

Fasi del documento

- `ChooseEncryptionType` (aws:branch) - Valuta il valore fornito per il `KmsKeyId` parametro per determinare se verranno utilizzati SSE-S3 (AES256) o SSE-KMS.
- `PutBucketKeysKMS` (aws:executeAwsApi) - Imposta la `BucketKeyEnabled` proprietà su `true` per il bucket S3 specificato utilizzando lo specificato. `true KmsKeyId`
- `PutBucketKeysAES256` (aws:executeAwsApi) - Imposta la `BucketKeyEnabled` proprietà su `true` per il bucket S3 specificato con crittografia. `AES256`
- `verifyS3 BucketKeysEnabled` (aws: assertAwsResource Property): verifica che le Bucket Keys siano abilitate sul bucket S3 di destinazione.

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

Descrizione

Il `AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy` runbook rimuove le principali dichiarazioni di policy che contengono caratteri speciali (`Principal: *oPrincipal: "AWS": *`) per Allow le azioni dalla tua policy sui bucket di Amazon Simple Storage Service (Amazon S3). Vengono inoltre rimosse le dichiarazioni politiche con condizioni.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 di cui desideri modificare la politica.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

Fasi del documento

- `aws:executeScript`- Modifica la policy del bucket e verifica che le principali dichiarazioni politiche con caratteri jolly siano state rimosse dal bucket Amazon S3 specificato nel parametro. `BucketName`

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

Descrizione

Il `AWSConfigRemediation-RestrictBucketSSLRequestsOnly` runbook crea una dichiarazione sulla policy del bucket Amazon Simple Storage Service (Amazon S3) che nega esplicitamente le richieste HTTP al bucket Amazon S3 specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket S3 a cui desideri negare le richieste HTTP.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:DeleteBucketPolicy
- s3:GetBucketPolicy
- s3:PutEncryptionConfiguration
- s3:PutBucketPolicy

Fasi del documento

- aws:executeScript- Crea una policy sui bucket per il bucket S3 specificato nel BucketName parametro che nega esplicitamente le richieste HTTP.

AWSSupport-TroubleshootS3PublicRead

Descrizione

Il AWSSupport-TroubleshootS3PublicRead runbook diagnostica i problemi di lettura degli oggetti dal bucket pubblico Amazon Simple Storage Service (Amazon S3) specificato nel parametro. S3BucketName Un sottoinsieme di impostazioni viene inoltre analizzato per gli oggetti nel bucket S3.

[Esegui questa automazione \(console\)](#)

Limitazioni

- Questa automazione non verifica i punti di accesso che consentono l'accesso pubblico agli oggetti.
- Questa automazione non valuta le chiavi delle condizioni nella policy del bucket S3.
- Se utilizzi AWS Organizations, questa automazione non valuta le politiche di controllo del servizio per confermare che l'accesso ad Amazon S3 è consentito.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- CloudWatchLogGroupName

Tipo: stringa

Descrizione: (Facoltativo) Il gruppo di log di Amazon CloudWatch Logs a cui desideri inviare l'output di automazione. Se non viene trovato un gruppo di log che corrisponde al valore specificato, l'automazione creerà un gruppo di log utilizzando questo valore di parametro. Il periodo di conservazione per il gruppo di log creato da questa automazione è di 14 giorni.

- CloudWatchLogStreamName

Tipo: stringa

Descrizione: (Facoltativo) Il flusso di log di CloudWatch Logs a cui si desidera inviare l'output dell'automazione. Se non viene trovato un flusso di log che corrisponde al valore specificato, l'automazione creerà un flusso di log utilizzando questo valore di parametro. Se non si specifica un valore per questo parametro, l'automazione utilizzerà il `ExecutionId` come nome del flusso di log.

- `HttpGet`

Tipo: Booleano

Valori validi: `true` | `false`

Impostazione predefinita: `true`

Descrizione: (Facoltativo) Se questo parametro è impostato su `true`, l'automazione effettua una richiesta HTTP parziale agli oggetti nel `S3BucketName` campo specificato. Solo il primo byte dell'oggetto viene restituito utilizzando l'intestazione HTTP Range.

- `IgnoreBlockPublicAccess`

Tipo: Booleano

Valori validi: `true` | `false`

Impostazione predefinita: `false`

Descrizione: (Facoltativo) Se questo parametro è impostato su `true`, l'automazione ignora le impostazioni del blocco di accesso pubblico del bucket S3 specificato nel parametro. `S3BucketName` La modifica di questo parametro rispetto al valore predefinito non è consigliata.

- `MaxObjects`

Tipo: integer

Valori validi: 1-25

Impostazione predefinita: 5

Descrizione: (Facoltativo) Il numero di oggetti da analizzare nel bucket S3 specificato nel parametro. `S3BucketName`

- `S3 BucketName`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del bucket S3 da risolvere.

- S3 PrefixName

Tipo: stringa

Descrizione: (Facoltativo) Il prefisso del nome chiave degli oggetti che desideri analizzare nel tuo bucket S3. Per ulteriori informazioni, consulta [Object keys](#) nella Amazon Simple Storage Service User Guide.

- StartAfter

Tipo: stringa

Descrizione: (Facoltativo) Il nome della chiave dell'oggetto su cui desideri che l'automazione inizi ad analizzare gli oggetti nel tuo bucket S3.

- ResourcePartition

Tipo: stringa

Valori validi: aws | aws-us-gov | aws-cn

Impostazione predefinita: aws

Descrizione: (Obbligatoria) La partizione in cui si trova il bucket S3.

- Modalità dettagliata

Tipo: Booleano

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (Facoltativo) Per restituire informazioni più dettagliate durante l'automazione, imposta questo parametro su `true`. Se il parametro è impostato su `true`, verranno restituiti solo i messaggi di avviso e di errore `false`.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Le `logs:PutLogEvents` autorizzazioni `logs:CreateLogGroup` `logs:CreateLogStream`, e sono necessarie solo se si desidera che l'automazione invii i dati di registro a Logs. CloudWatch

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

Fasi del documento

- `aws:assertAwsResourceProperty`- Conferma che il bucket S3 esiste ed è accessibile.
- `aws:executeScript`- Restituisce la posizione del bucket S3 e il tuo ID utente canonico.
- `aws:executeScript`- Restituisce le impostazioni del blocco di accesso pubblico per il tuo account e il bucket S3.
- `aws:assertAwsResourceProperty`- Conferma che il bucket payer S3 è impostato su. `BucketOwner Se Requester Pays` è abilitato sul bucket S3, l'automazione termina.
- `aws:executeScript`- Restituisce lo stato della policy del bucket S3 e determina se è considerata pubblica. Per ulteriori informazioni sui bucket S3 pubblici, consulta [Il significato di «pubblico»](#) nella Guida per l'utente di Amazon Simple Storage Service.
- `aws:executeAwsApi`- Restituisce la policy sui bucket S3.
- `aws:executeAwsApi`- Restituisce tutte le chiavi di contesto presenti nella policy del bucket S3.
- `aws:assertAwsResourceProperty`- Conferma se esiste una negazione esplicita nella policy del bucket S3 per l'azione dell'API. `GetObject`
- `aws:executeAwsApi`- Restituisce l'elenco di controllo degli accessi (ACL) per il bucket S3.
- `aws:executeScript`- Crea un gruppo di log CloudWatch Logs e un flusso di log se si specifica un valore per il parametro. `CloudWatchLogGroupName`
- `aws:executeScript`- In base ai valori specificati nei parametri di input del runbook, valuta se alcune delle impostazioni del bucket S3 raccolte durante l'automazione impediscono l'accesso agli oggetti da parte del pubblico. Questo script esegue le seguenti funzioni:
 - Valuta le impostazioni dei blocchi di accesso pubblico
 - Restituisce gli oggetti dal bucket S3 in base ai valori specificati nei parametri `MaxObjectsS3PrefixName`, e. `StartAfter`
 - Restituisce la policy del bucket S3 per simulare una policy IAM personalizzata per gli oggetti restituiti dal bucket S3.
 - Esegue una richiesta HTTP parziale agli oggetti restituiti se il `HttpGet` parametro è impostato su. `true` Solo il primo byte dell'oggetto viene restituito utilizzando l'intestazione HTTP `Range`.

- Controlla il nome della chiave dell'oggetto restituito per confermare se termina con uno o due punti. I nomi delle chiavi degli oggetti che terminano in periodi non possono essere scaricati dalla console Amazon S3.
- Verifica se il proprietario dell'oggetto restituito corrisponde al proprietario del bucket S3.
- Verifica se l'ACL dell'oggetto concede READ o FULL_CONTROL autorizzazioni a utenti anonimi.
- Restituisce i tag associati all'oggetto.
- Utilizza la policy IAM simulata per confermare se esiste una negazione esplicita per questo oggetto nella policy del bucket S3 per l'azione API. `GetObject`
- Restituisce i metadati dell'oggetto per confermare che la classe di archiviazione è supportata.
- Verifica le impostazioni di crittografia lato server dell'oggetto per confermare se l'oggetto è crittografato utilizzando una chiave AWS Key Management Service (AWS KMS) gestita dal cliente.

Output

AnalyzeObjects.bucket

AnalyzeObjects.oggetto

AWSSupport-EmptyS3Bucket

Descrizione

Il runbook di `AWSSupport-EmptyS3Bucket` automazione svuota un bucket Amazon Simple Storage Service (Amazon S3) esistente utilizzando una regola di configurazione della scadenza del ciclo di vita.

Important

- I bucket Amazon S3 con autenticazione a più fattori (MFA) abilitata non sono supportati.
- Le regole del ciclo di vita modificate da questo runbook eliminano definitivamente tutti gli oggetti e le relative versioni nel bucket Amazon S3 specificato. Non è possibile recuperare oggetti eliminati definitivamente. Per ulteriori informazioni, [consulta la sezione Oggetti in scadenza](#).

Come funziona?

Il runbook `AWSsupport-EmptyS3Bucket` esegue i seguenti passaggi di alto livello:

- Sospende il controllo delle versioni del bucket, se abilitato.
- Aggiorna la policy del bucket per rifiutare qualsiasi chiamata `s3:PutObject` API (per impedire nuovi caricamenti mentre viene svuotato).
- Aggiorna le regole del ciclo di vita per eliminare tutti gli oggetti in base ai giorni di scadenza specificati nei parametri di input.

Note

- Le versioni degli oggetti protette con Amazon S3 Object Lock non vengono eliminate o sovrascritte dalle configurazioni del ciclo di vita.
- Il processo di eliminazione è asincrono e può richiedere del tempo per essere completato al termine dell'esecuzione del runbook.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

/

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook:

- `ssm: DescribeAutomationExecutions`

- ssm: GetAutomationExecution
- s3: GetBucketVersioning
- s3: PutBucketVersioning
- s3: GetBucketPolicy
- s3: GetBucketLifecycleConfiguration
- s3: GetLifecycleConfiguration
- s3: PutBucketPolicy
- s3: PutBucketLifecycleConfiguration
- s3: PutLifecycleConfiguration
- s3: DeleteBucketPolicy
- s3: DeleteBucketLifecycle

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWS Support - Empty S3 Bucket](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- S3: BucketName

Il nome del bucket Amazon S3 che desideri svuotare.

- SNSTopicArn:

Fornisci l'ARN dell'argomento Amazon SNS per la notifica di approvazione. Questo argomento di Amazon SNS viene utilizzato per inviare notifiche di approvazione quando richiesto durante l'esecuzione dell'automazione.

- Approvatore IAM:

Fornisci un elenco di responsabili autenticati da AWS che sono in grado di approvare o rifiutare l'azione. Il numero massimo di approvatori è 10. Puoi specificare i principali utilizzando uno di questi formati, un nome utente AWS Identity and Access Management (IAM), un ARN utente IAM, un ARN del ruolo IAM o un ARN dell'utente di assunzione del ruolo IAM.

- `MinimumRequiredApprovals` (Facoltativo):

Numero minimo di approvazioni richieste per riprendere l'automazione. Se non si specifica un valore, il sistema utilizza come impostazione predefinita 1. Il valore di questo parametro deve essere un numero intero positivo. Il valore di questo parametro non può superare il numero di approvatori definito dal parametro `approverIAM`.

- `NoncurrentVersionExpirationDays` (Facoltativo):

Specificate il numero di giorni in cui scadono le versioni non correnti degli oggetti. Alla scadenza, Amazon S3 elimina in modo definitivo le versioni degli oggetti non correnti.

- Impostazione predefinita: 1
- Valore massimo: 365
- `ExpirationDays` (Facoltativo):

Specificare la scadenza del ciclo di vita dell'oggetto nei giorni del modulo.

- Impostazione predefinita: 1
- Valore massimo: 365
- `AbortIncompleteMultipartUpload` (Facoltativo):

Specificate i giorni trascorsi dall'avvio di un caricamento multiparte incompleto che Amazon S3 dovrà attendere prima di rimuovere definitivamente tutte le parti del caricamento.

- Impostazione predefinita: 1
- Valore massimo: 365
- Riconoscimento:

Leggi i dettagli completi delle azioni eseguite da questo runbook di automazione e fornisci il consenso `Yes, I understand and acknowledge` se riconosci i passaggi.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

SNSTopicArn
(Required) The ARN of the Amazon Simple Notification Service (Amazon SNS) Topic for approval notification. This SNS topic is used to send the approval notifications required during the automation execution.

MinimumRequiredApprovals
(Optional) The minimum number of approvals required to resume the automation. If you don't specify a value, the system defaults to one. The value for this parameter must be a positive number. The value for this parameter can't exceed the number of approvers defined in the 'ApproverIAM' parameter.

ExpirationDays
(Optional) Specify the expiration for the lifecycle of the object in days. Default value is 1 and max value is 365.

Acknowledgement
(Required) Please read the complete details of the actions performed by this automation runbook and write 'Yes, I understand and acknowledge' if you acknowledge the steps. ****Important:**** You cannot recover permanently removed objects. For more information please review [Expiring objects] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-expire-general-considerations.html>).

S3BucketName
(Required) The name of the Amazon S3 bucket you want to empty.

ApproverIAM
(Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats, 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN.

NoncurrentVersionExpirationDays
(Optional) Specify the number of days when noncurrent object versions expire. Upon expiration, Amazon S3 permanently deletes the noncurrent object versions. Default value is 1 and max value is 365.

AbortIncompleteMultipartUpload
(Optional) Specify the days since the initiation of an incomplete multipart upload that Amazon S3 will wait before permanently removing all parts of the upload. Default value is 1 and max value is 365.

4. Seleziona Esegui.

5. L'automazione inizia.

6. Il documento esegue le seguenti operazioni:

- **checkConcurrency:**

Assicura che vi sia una sola esecuzione di questo runbook destinata al bucket Amazon S3 specificato. Se il runbook trova un'altra esecuzione in corso con lo stesso nome di bucket, restituisce un errore e termina.

- **getBucketVersioningConfiguration:**

Recupera lo stato di controllo delle versioni del bucket Amazon S3 specificato.

- **branchOnStoppingIfMFADeleteEnabled**(condizionale):

Interrompe l'automazione se l'autenticazione a più fattori (MFA) è abilitata sul bucket Amazon S3 specificato.

- **approvalToMakeChangesToTheProvidedS3Bucket:**

Attende l'approvazione dei responsabili designati per disabilitare il controllo delle versioni del bucket e aggiornare la policy del bucket e la configurazione delle regole del ciclo di vita per il bucket Amazon S3 specificato.

- **branchOnBucketVersioningStatus**(condizionale):

Se il controllo delle versioni è abilitato sul bucket Amazon S3 specificato, disabilitalo, altrimenti continua ad aggiornare la policy del bucket e la configurazione del ciclo di vita.

- **suspendBucketVersioning**:

Sospende lo stato di controllo delle versioni del bucket Amazon S3 specificato.

- **updateBucketPolicyAndLifeCycleConfiguration**:

Aggiunge o aggiorna la policy del bucket per rifiutare tutte le `s3:PutObject` richieste e aggiorna la configurazione del ciclo di vita per far scadere gli oggetti in base ai parametri di input forniti dall'utente.

- **branchOnFailingIfBucketPropertiesNotUpdated**(condizionale):

Controlla lo stato del `updateBucketPolicyAndLifeCycleConfiguration` passaggio e tenta di ripristinare lo stato di versione originale del bucket se modificato dall'automazione.

- **branchOnFailureOriginalVersioningStatus**(condizionale):

In caso di errore, si ramifica per determinare lo stato originale del controllo delle versioni. Se è stato abilitato e sospeso da questa automazione, prova a riattivarlo.

- **onFailureRestoreBucketVersioning**

Ripristina lo stato di versione abilitato del bucket Amazon S3 specificato.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

✓ Execution has been initiated.

Execution detail: AWSSupport-EmptyS3Bucket

Cancel execution

Actions

► Execution description

▼ Outputs

updateBucketPolicyAndLifecycleConfiguration.Message

===== Execution Result =====

INFO: Getting the configured lifecycle rules for the S3 Bucket: sample-not-empty-bucket
INFO: Getting bucket policy for S3 Bucket: sample-not-empty-bucket
INFO: Creating new bucket policy to deny any s3:PutObject API calls (to prevent new uploads while it is being emptied).
INFO: Creating a new lifecycle rule to delete all the objects according to the expiration days specified in the input parameters
INFO: The bucket updates have been successfully completed.
Upon the expiration of items, as specified in the parameters, the bucket will be emptied.
Meanwhile, S3 'put object' requests are denied by the bucket policy to prevent the upload of new items.

Execution status

Overall status

✓ Success

Failed

0

All executed steps

7

Cancelled

0

Succeeded

7

TimedOut

0

Executed steps (10)

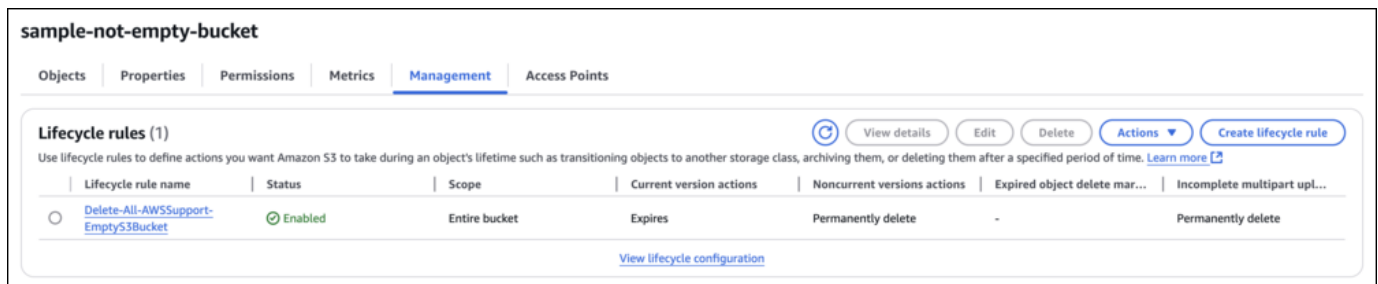
Find Steps

< 1 >

Step ID	Step #	Step name	Action	Status	Start time
17e09354-6a90-4216-9797-a9d6fa18d57c	1	checkConcurrency	aws:executeScript	✓ Success	Wed, 18 Dec 2024 08:01:54 GM
44bc75db-0bd9-44c1-9537-0b9ff9eea87a	2	getBucketVersioningConfiguration	aws:executeAwsApi	✓ Success	Wed, 18 Dec 2024 08:02:08 GM
1e942013-e886-4fce-b685-bc8e578bcb2a	3	branchOnStoppingIfMFADeleteEnabled	aws:branch	✓ Success	Wed, 18 Dec 2024 08:02:09 GM
742066ac-39a8-4699-8aa4-13a7a8b0239f	4	approvalToMakeChangesToTheProvidedS3Bucket	aws:approve	✓ Success	Wed, 18 Dec 2024 08:02:09 GM
34c276bb-f7e3-43f8-a89f-8d457040cc31	5	branchOnBucketVersioningStatus	aws:branch	✓ Success	Wed, 18 Dec 2024 08:03:24 GM
5f3efb16-d6f8-441e-b090-ab6c88ab2a9d	6	updateBucketPolicyAndLifecycleConfiguration	aws:executeScript	✓ Success	Wed, 18 Dec 2024 08:03:25 GM
739dd72a-e7de-42d9-900a-7a0aa5e826d0	7	branchOnFailingIfBucketPropertiesNotUpdated	aws:branch	✓ Success	Wed, 18 Dec 2024 08:03:29 GM
f97fc493-3d62-4884-901f-dcc2a2a3bcd0	8	suspendBucketVersioning	aws:executeAwsApi	⌚ Pending	-
4b02a204-8de7-49c8-b079-e94741c40a37	9	branchOnFailureOriginalVersioningStatus	aws:branch	⌚ Pending	-
92645daf-8587-4947-bc53-b4c440d07f84	10	onFailureRestoreBucketVersioning	aws:executeAwsApi	⌚ Pending	-

- Esecuzione riuscita

Questo flusso di lavoro aggiorna la regola del ciclo di vita del bucket. Gli oggetti verranno eliminati in base alla politica del ciclo di vitaDelete-All-AWSSupport-EmptyS3-Bucket.



- Esecuzione fallita

L'eliminazione parziale non verrà eseguita. Se l'esecuzione fallisce, il ciclo di vita e le altre impostazioni del bucket vengono ripristinate.

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Flussi di lavoro di Support Automation](#)

Per ulteriori informazioni sulla gestione di bucket e oggetti Amazon S3, consulta [Svuotare](#) un bucket.

AWSSupport-TroubleshootS3EventNotifications

Descrizione

Il runbook di AWSSupport-TroubleshootS3EventNotifications AWS Systems Manager automazione aiuta a risolvere i problemi di Amazon Simple Storage Service (Amazon S3) Bucket Event Notifications configurate AWS Lambda con Functions, Amazon Simple Notification Service (Amazon SNS) Topics o Amazon Simple Queue Service (Amazon SQS) Queues. Fornisce un rapporto sulle impostazioni di configurazione delle diverse risorse configurate con Amazon S3 Bucket come notifica degli eventi di destinazione.

Come funziona?

Il runbook esegue i seguenti passaggi:

- Verifica se il bucket Amazon S3 esiste nello stesso account in cui viene AWSSupport-TroubleshootS3EventNotifications eseguito.

- Recupera le risorse di destinazione (AWS Lambda Function, Amazon SNS Topic o Amazon SQS queue) configurate come notifiche di eventi per il bucket Amazon S3 utilizzando l'API. [GetBucketNotificationConfiguration](#)
- Verifica l'esistenza della risorsa di destinazione, quindi esamina la politica basata sulle risorse delle risorse di destinazione per determinare se Amazon S3 è autorizzato a pubblicare sulla destinazione.
- Se hai crittografato la destinazione con una chiave AWS Key Management Service (AWS KMS), la policy della chiave viene verificata per determinare se l'accesso ad Amazon S3 è consentito.
- Genera un report di tutti i controlli delle risorse di destinazione.

 Important

- Questo runbook può valutare le configurazioni di notifica degli eventi solo se il proprietario del bucket Amazon S3 è lo stesso proprietario del quale viene eseguito Account AWS il runbook di automazione.
- Inoltre, questo runbook non può valutare le politiche sulle risorse di destinazione ospitate in un altro. Account AWS

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- S3 BucketName

Tipo: AWS::S3::Bucket::Name

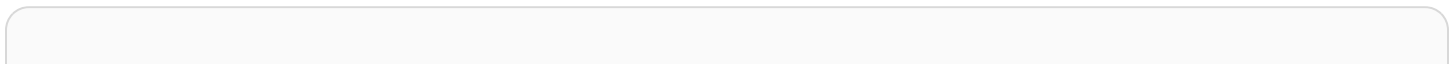
Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 configurato con le notifiche degli eventi.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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

Esempio di politica IAM per l'automazione Assume Role



```
{
  "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:::<bucket-name>"
    },
    {
      "Sid": "SQSPermission",
      "Effect": "Allow",
      "Action": [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource": "arn:aws:sqs:<region>:123456789012:*"
    },
    {
      "Sid": "SNSPermission",
      "Effect": "Allow",
      "Action": [
        "sns:GetTopicAttributes"
      ],
      "Resource": "arn:aws:sns:<region>:123456789012:*"
    },
    {
      "Sid": "KMSPermission",
      "Effect": "Allow",
      "Action": [
        "kms:GetKeyPolicy",
        "kms:DescribeKey",
        "kms:ListAliases"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:kms:<region>:123456789012:key/
<key-id>"
  },
  {
    "Sid": "LambdaPermission",
    "Effect": "Allow",
    "Action": [
      "lambda:GetPolicy",
      "lambda:GetFunction"
    ],
    "Resource":
"arn:aws:lambda:<region>:123456789012:function:*"
  },
  {
    "Sid": "IAMPermission",
    "Effect": "Allow",
    "Action": [
      "iam:GetContextKeysForCustomPolicy",
      "iam:SimulateCustomPolicy",
      "iam:ListRoles"
    ],
    "Resource": "*"
  },
  {
    "Sid": "SSMPermission",
    "Effect": "Allow",
    "Action": [
      "ssm:DescribeAutomationStepExecutions"
    ],
    "Resource": "*"
  }
]
}

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWS Support-TroubleshootS3EventNotifications](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).

3. Per i parametri di input, immettete quanto segue:

- AutomationAssumeRole (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- S3 BucketName (richiesto):

Il nome del bucket Amazon S3 configurato con le notifiche degli eventi.

The screenshot shows the 'Input parameters' section of an AWS Systems Manager console. It contains two parameters: 'AutomationAssumeRole' and 'S3BucketName'. 'AutomationAssumeRole' is optional and has a dropdown menu with 'AWS-SystemsManager-AutomationAdministrationRole' selected. 'S3BucketName' is required and has an empty text input field. Both fields have a copy icon to the right.

4. Seleziona Esegui.

5. L'automazione inizia.

6. Il documento esegue le seguenti operazioni:

- ValidateInputs

Verifica che il bucket Amazon S3 fornito appartenga allo stesso account in cui viene eseguita l'automazione e recupera la regione in cui è ospitato il bucket.

- GetBucketNotificationConfiguration

Richiama GetBucketNotificationConfiguration l'API per esaminare le notifiche degli eventi configurate con il bucket Amazon S3 e i formati di output.

- BranchOnSQSResourcePolicy

Indica se ci sono risorse Amazon SQS nelle notifiche degli eventi.

- Convalida la politica SQSResource

Convalida la politica delle risorse sugli attributi di Amazon SQS Queue e sqs:SendMessage dispone dell'autorizzazione per Amazon S3. Se la risorsa Amazon SQS è crittografata, verifica che la crittografia non utilizzi la AWS KMS chiave predefinita, ad esempio, aws/sqs e verifica che la policy della AWS KMS chiave disponga delle autorizzazioni per Amazon S3.

- BranchOnSNSResourcePolicy

Verifica se sono presenti risorse Amazon SNS nelle notifiche degli eventi.

- Convalida la politica SNSResource

Convalida la politica delle risorse su Amazon SNS Topic Attributes `sns:Publish` dispone dell'autorizzazione per Amazon S3. Se la risorsa Amazon SNS è crittografata, verifica che la crittografia non utilizzi la AWS KMS chiave predefinita, ad esempio, `aws/sns` e verifica che la policy della AWS KMS chiave disponga delle autorizzazioni per Amazon S3.

- BranchOnLambdaFunctionResourcePolicy

Indica se ci sono AWS Lambda funzioni nelle notifiche degli eventi.

- ValidateLambdaFunctionResourcePolicy

Convalida la politica delle risorse sulla AWS Lambda funzione `lambda:InvokeFunction` autorizzata per Amazon S3.

- GenerateReport

Restituisce i dettagli dei passaggi, degli output del runbook e consigli per risolvere qualsiasi problema con le notifiche degli eventi configurate con il bucket Amazon S3.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- Notifiche di eventi Amazon SQS

Se sono presenti notifiche di destinazione Amazon SQS configurate con il bucket Amazon S3, viene visualizzato un elenco delle code Amazon SQS insieme ai risultati dei controlli. Il report include il controllo delle risorse di Amazon SQS, il controllo delle politiche di accesso di Amazon SQS, il controllo delle chiavi AWS KMS, il controllo AWS KMS dello stato delle chiavi AWS KMS e il controllo delle politiche chiave.

- Notifiche di eventi Amazon SNS

Se sono presenti notifiche di destinazione Amazon SNS configurate con il bucket Amazon S3, accanto ai risultati dei controlli viene visualizzato un elenco degli argomenti di Amazon SNS. Il rapporto include il controllo delle risorse di Amazon SNS, il controllo della politica di accesso di Amazon SNS, il controllo delle chiavi AWS KMS, il controllo AWS KMS dello stato delle chiavi AWS KMS e il controllo delle politiche delle chiavi.

- AWS Lambda Notifiche di eventi

Se sono presenti notifiche di AWS Lambda destinazione configurate con il bucket Amazon S3, accanto ai risultati dei controlli viene visualizzato un elenco delle funzioni Lambda. Il rapporto include il controllo delle risorse Lambda e il controllo della politica di accesso Lambda.

```
▼ Outputs
generateReportOutput

-----
| Amazon S3 Event Notification Troubleshooting Results for S3 Bucket |
|-----|
| Amazon S3 Event Notifications |
|-----|
| S3 Queue: 1. arn:aws:sqs:us-east-1:123456789012:SAW-Core-TroubleshootS3EventNotification-EncryptedQueue | KMS Key: |
| S3 resource check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| S3 access policy check | ✓ [PASSED]: The resource policy is properly configured for use with S3 Bucket. |
| KMS key check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| KMS key status check | ✗ [FAILED]: The KMS key is disabled. |
| KMS key policy check | ✓ [PASSED]: The resource policy is properly configured for use with S3 Bucket. |
|-----|
| Amazon SNS Event Notifications |
|-----|
| SNS Topic: 1. arn:aws:sns:us-east-1:123456789012:SAW-CoreInfra-TestSNSTopic-1AW0EaySLdmr | KMS Key: alias/aws/sns |
| SNS resource check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| SNS access policy check | ✓ [PASSED]: The resource policy is properly configured for use with S3 Bucket. |
| KMS key check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| KMS key status check | ➤ [INFO]: Not Applicable. |
| KMS key policy check | ✗ [FAILED]: Amazon S3 Event Notifications does not support using SQS or SNS targets encrypted using AWS managed keys, i.e., aws/sns or aws/sqs respectively. |
|-----|
| AWS Lambda Event Notifications |
|-----|
| Lambda Function: 1. arn:aws:lambda:us-east-1:123456789012:function:SAW-Core-TroubleshootS3EventNotification-LambdaFunction |
| Lambda resource check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| Lambda access policy check | ✗ [FAILED]: No resource policies found on the resource. Please update the resource with a valid policy using this guide: https://docs.aws.amazon.com/AmazonS3/latest/userguide/grant-destin
```

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWSupport-ContainS3Resource

Descrizione

Il `AWSSupport-ContainS3Resource` runbook fornisce una soluzione automatizzata per la procedura descritta nell'articolo [Support Automation Workflow \(SAW\) Runbook: Contain a Amazon AWS S3 Bucket compromesso](#)

 Important

- Questo runbook esegue diverse operazioni che richiedono privilegi elevati, come la modifica delle policy, dei tag e delle configurazioni dei bucket di Amazon S3. Queste azioni potrebbero potenzialmente portare a un aumento dei privilegi o influire su altri carichi di lavoro che dipendono dal bucket Amazon S3 di destinazione. È necessario esaminare le autorizzazioni concesse al ruolo specificato dal `AutomationAssumeRole` parametro e assicurarsi che siano appropriate per il caso d'uso previsto. Puoi fare riferimento alla

seguente AWS documentazione per ulteriori informazioni sulle autorizzazioni IAM:.

[Identity and Access Management \(IAM\) PermissionsAWS AWS Systems Manager Automation Permissions](#)

- Questo runbook esegue azioni mutative che potrebbero potenzialmente causare indisponibilità o interruzione dei carichi di lavoro. In particolare, l'Containment blocca tutti gli accessi al bucket Amazon S3 specificato, ad eccezione dei ruoli specificati nel parametro. SecureRoles Ciò potrebbe influire su tutte le applicazioni o i servizi che si basano sul bucket Amazon S3 di destinazione.
- Durante l'Containment, questo runbook può creare un bucket Amazon S3 aggiuntivo (specificato dal BackupS3BucketName parametro) per archiviare il backup della configurazione del bucket originale, se non esiste già.
- Se il Action parametro è impostato suRestore, questo runbook tenta di ripristinare la configurazione del bucket Amazon S3 allo stato originale in base al backup archiviato nel bucket. BackupS3BucketName Tuttavia, esiste il rischio che il processo di ripristino non riesca, lasciando il bucket Amazon S3 in uno stato incoerente. Il runbook fornisce istruzioni per il ripristino manuale in caso di tali errori, ma è necessario essere preparati a gestire potenziali problemi durante il processo di ripristino.

Si consiglia di esaminare attentamente il runbook, comprenderne i potenziali impatti e testarlo in un ambiente non di produzione prima di eseguirlo nell'ambiente di produzione.

Come funziona?

Questo runbook funziona in modo diverso in base al tipo di risorsa e all'azione:

- Per Amazon S3 General Purpose BucketContainment: l'automazione blocca l'accesso pubblico al bucket, disabilita la configurazione ACL, impone la proprietà del Bucket Owner Object e impone una policy restrittiva che nega tutte le azioni di Amazon S3 al bucket ad eccezione dei ruoli IAM consentiti elencati.
- Per Amazon S3 General Purpose ObjectContainment: l'automazione blocca l'accesso pubblico al bucket, disabilita la configurazione ACL, impone la proprietà del Bucket Owner Object e applica una policy restrittiva sui bucket che nega tutte le azioni di Amazon S3 sull'oggetto ad eccezione dei ruoli IAM consentiti elencati.

- Per Amazon S3 Directory BucketContainment: l'automazione applica una politica restrittiva sui bucket che nega tutte le azioni di Amazon S3 al bucket ad eccezione dei ruoli IAM consentiti elencati.
- Per Amazon S3 General Purpose BucketRestore: l'automazione ripristina la configurazione Block Public Access, la configurazione Bucket ACL, la proprietà dell'oggetto Bucket Owner e la Bucket Policy alla configurazione iniziale prima del contenimento.
- Per Amazon S3 General Purpose ObjectRestore: l'automazione ripristina la configurazione Block Public Access, la configurazione Bucket ACL, la configurazione Object ACL, la proprietà dell'oggetto Bucket Owner e la Bucket Policy alla configurazione iniziale prima del contenimento.
- Per Amazon S3 Directory BucketRestore: l'automazione ripristina la policy del bucket alla configurazione iniziale prima del contenimento.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Platform (Piattaforma)

/

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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: ACL PutBucket
- s3: PutBucketOwnershipControls
- s3: PutBucketPolicy
- s3: PutBucketPublicAccessBlock
- s3: PutBucketTagging
- s3: PutBucketVersioning
- s3: PutObject
- s3: PutObjectAcl
- s3 express: CreateSession
- s3 express: DeleteBucketPolicy
- s3 express: GetBucketPolicy
- s3 express: PutBucketPolicy
- ssm: DescribeAutomationExecutions

Ecco un esempio di policy IAM che concede le autorizzazioni necessarie per:
AutomationAssumeRole

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

```

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWSSupport-ContainS3Resource](#) a Systems Manager nella sezione Documenti.
2. Seleziona Execute automation (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - BucketName (Obbligatorio):
 - Descrizione: (Obbligatorio) Il nome del bucket Amazon S3.
 - Tipo: `AWS::S3::Bucket::Name`
 - Azione (richiesta):
 - Descrizione: (Obbligatorio) Seleziona `Contain` per isolare la risorsa Amazon S3 `Restore` o provare a ripristinare la configurazione della risorsa allo stato originale da un backup precedente.
 - Tipo: stringa
 - Valori consentiti: `Contain|Restore`
 - DryRun (Facoltativo):
 - Descrizione: (Facoltativo) Se impostata su `true`, l'automazione non apporterà alcuna modifica alla risorsa Amazon S3 di destinazione, ma restituirà ciò che avrebbe tentato di modificare. Valore predefinito: `true`.
 - Tipo: Booleano
 - Valori consentiti: `true|false`
 - BucketKeyName (Facoltativo):
 - Descrizione: (Facoltativo) La chiave dell'oggetto Amazon S3 che desideri contenere o ripristinare. Utilizzato durante il contenimento a livello di oggetto.
 - Tipo: stringa
 - Pattern consentito: `^[a-zA-Z0-9\\.\_-\\\\!*'()/{0,1024}]$`
 - BucketRestrictAccess (Condizionale):

- **Descrizione:** (Condizionale) L'ARN degli utenti o dei ruoli IAM a cui sarà consentito l'accesso alla risorsa Amazon S3 di destinazione dopo l'esecuzione delle azioni di contenimento. Questo parametro è obbligatorio quando Action è impostato su. `Contain`
- **Tipo:** `StringList`
- **Modello consentito:** `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=, .@-]+$`
- **TagIdentifier (Facoltativo):**
 - **Descrizione:** (Facoltativo) Un tag nel formato `Key=BatchId`, `Value=78925` che verrà aggiunto alle risorse create o modificate da questo runbook durante il flusso di lavoro di contenimento.
 - **Tipo:** stringa
 - **Modello consentito:** `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{0,128}$`
- **BackupS3 BucketName (condizionale):**
 - **Descrizione:** (Condizionale) Il bucket Amazon S3 per il backup della configurazione della risorsa di destinazione quando Action è impostato su o `Contain` per ripristinare la configurazione da quando Action è impostato su. `Restore`
 - **Tipo:** `AWS::S3::Bucket::Name`
- **Backup S3 KeyName (condizionale):**
 - **Descrizione:** (Condizionale) Se Action impostato su `Restore`, specifica la chiave Amazon S3 che l'automazione utilizzerà per tentare di ripristinare la configurazione delle risorse di destinazione.
 - **Tipo:** stringa
 - **Modello consentito:** `^[a-zA-Z0-9\\.\\-_\\\\\\!*'()/{0,1024}$`
- **BackupS3 BucketAccess (condizionale):**
 - **Descrizione:** (Condizionale) L'ARN degli utenti o dei ruoli IAM a cui sarà consentito l'accesso al bucket Amazon S3 di backup dopo l'esecuzione delle azioni di contenimento. Questo parametro è obbligatorio quando è. Action `Contain`
 - **Tipo:** `StringList`
 - **Modello consentito:** `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=, .@-]+$`

- **Descrizione:** (Facoltativo) L'Amazon Resource Name (ARN) del ruolo IAM che consente a Systems Manager Automation di eseguire le azioni per tuo conto.
- **Tipo:** `AWS::IAM::Role::Arn`

4. Seleziona Esegui.

5. L'automazione inizia.

6. Il documento esegue le seguenti operazioni:

- `validateRequiredInputs`

Convalida i parametri di input di automazione richiesti in base all'azione specificata.

- `assertBucketExists`

Verifica se il bucket Amazon S3 di destinazione esiste ed è accessibile.

- `backupBucketPreControlli`

Verifica se il bucket Amazon S3 di backup concede potenzialmente l'accesso pubblico in lettura o scrittura ai suoi oggetti.

- `backupTargetBucketMetadati`

Descrive la configurazione corrente del bucket Amazon S3 di destinazione e carica il backup nel bucket Amazon S3 di backup specificato.

- `ContainBucket`

Esegue operazioni a livello di bucket per contenere il bucket Amazon S3 di destinazione.

- `BranchOnActionAndMode`

Suddivide l'automazione in base ai parametri di input Action e DryRun

- `RestoreInstanceConfiguration`

Ripristina la configurazione del bucket Amazon S3 dal backup.

- `containFinalOutput`

Consolida l'attività di contenimento in un formato leggibile.

- `ReportContain`

Fornisce i dettagli del funzionamento a secco per le azioni di contenimento.

Fornisce i dettagli del funzionamento a secco per le azioni di ripristino.

- `ReportRestoreFailure`

Fornisce istruzioni per ripristinare la configurazione originale del bucket Amazon S3 durante uno scenario di errore del flusso di lavoro di ripristino.

- `ReportContainmentFailure`

Fornisce istruzioni per ripristinare la configurazione originale del bucket Amazon S3 durante uno scenario di errore del flusso di lavoro di contenimento.

- `FinalOutput`

Fornisce i dettagli delle azioni di contenimento.

7. Una volta completata l'esecuzione, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- `ContainFinalOutput.Output`

Restituisce i dettagli delle azioni di contenimento eseguite da questo runbook quando `DryRun` è impostato su `False`.

- `RestoreFinalOutput.Output`

Restituisce i dettagli delle azioni di ripristino eseguite da questo runbook quando `DryRun` è impostato su `False`.

- Contiene 3. Output `ResourceDryRun`

Restituisce i dettagli delle azioni di contenimento eseguite da questo runbook quando è impostato su `True`. `DryRun`

- `ResourceDryRunRipristina S3. Output`

Restituisce i dettagli delle azioni di ripristino eseguite da questo runbook quando `DryRun` è impostato su `True`.

- `ReportContainmentFailure.Output`

Fornisce istruzioni per ripristinare la configurazione originale della risorsa Amazon S3 di destinazione durante uno scenario di errore del flusso di lavoro di contenimento.

- `ReportRestoreFailure.Output`

Fornisce istruzioni per ripristinare la configurazione originale della risorsa Amazon S3 di destinazione durante uno scenario di errore del flusso di lavoro di ripristino.

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Flussi di lavoro di Support Automation](#)

Amazon SES

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Simple Email Service. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSSupport-AnalyzeSESMessagesSendingStatus](#)

AWSSupport-AnalyzeSESMessagesSendingStatus

Descrizione

Il runbook di AWSSupport-AnalyzeSESMessagesSendingStatus automazione riassume lo stato di consegna dei messaggi e-mail non recapitati e fornisce consigli per risolvere il motivo del mancato recapito. Il runbook recupera gli eventi di invio e-mail di Amazon Simple Email Service (Amazon SES) archiviati in un gruppo Amazon CloudWatch Logs pubblicato da Amazon SES. Per i dettagli sulla pubblicazione degli eventi di Amazon SES, consulta [Monitoraggio tramite la pubblicazione degli eventi di Amazon Simple Email Service](#). Il runbook fornisce anche un riepilogo e la tempistica delle consegne delle e-mail, nonché consigli che possono potenzialmente influire sui messaggi e-mail non recapitati. Puoi trovare questi messaggi nella sezione di output di ogni esecuzione. Tieni presente che questo runbook può risolvere i problemi degli eventi solo dopo l'implementazione dell'Event Store.

Come funziona?

Il runbook esegue i seguenti passaggi:

- Controlla le esecuzioni di automazione simultanee per lo stesso CloudWatch gruppo Logs.
- Analizza gli eventi di Amazon SES corrispondenti al messaggio IDs fornito dal parametro di automazione.
- Riepiloghi della distribuzione dell'output nella sezione di output dell'esecuzione dell'automazione.

 Important

- Prima di eseguire questo runbook, devi archiviare gli eventi Amazon SES pubblicati in un gruppo di log CloudWatch Logs specificato dal parametro automation. Questo runbook analizza solo gli eventi Amazon SES memorizzati nel gruppo di log.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- logs:StartQuery
- logs:GetQueryResults
- ses:GetIdentityMailFromDomainAttributes

- `ses:GetSendQuota`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Accedere [AWS Support - Analyze SES Message Sending Status](#) a Systems Manager nella sezione Documenti.
2. Seleziona `Execute automation` (Esegui automazione).
3. Per i parametri di input, immettete quanto segue:
 - `AutomationAssumeRole` (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `MessageIds` (Obbligatorio)

Messaggio IDs di Amazon Simple Email Service separato da virgole contenente gli eventi di Amazon Simple Email Service che desideri analizzare.

- `CloudWatchLogsGroup` (Facoltativo)

Il gruppo Amazon CloudWatch Logs che archivia gli eventi di Amazon Simple Email Service. Il nome del gruppo di log predefinito è `/ses/sending_event_logs`. Se desideri utilizzare un gruppo di log diverso da quello predefinito, inserisci il nome del gruppo di log in questo campo. «,

- `QueryStartTime` (Opzionale)

L'ora di inizio dell'intervallo di tempo per l'analisi dell'evento. Il formato orario valido è ISO86 01 (ad esempio `YYYY-MM-DDTHH:mm:ss``, `1970-01-01T 00:00:00 ``). La data/ora predefinita è 30 giorni fa.

- `QueryEndTime` (Facoltativo)

L'ora di fine dell'intervallo di tempo per l'analisi degli eventi. Il formato orario valido è ISO86 01 (ad esempio `YYYY-MM-DDTHH:mm:ss``, `1970-01-01T 00:00:00 ``). La data e l'ora predefinita è l'ora corrente.

Input parameters**AutomationAssumeRole**

(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

 
CloudWatchLogsGroup

(Optional) The Amazon CloudWatch Logs group which stores Amazon SES events. The default log group name is `/ses/sending_event_logs`. If you would like to utilize another log group than the default log group, please enter your log group name in this field.

QueryEndTime

(Optional) The end time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is the current time.

MessageIds

(Required) Comma separated Amazon SES message IDs of the Amazon SES events that you would like to analyze.

QueryStartTime

(Optional) The start time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is 30 days ago.

4. Seleziona Esegui.

5. L'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- **CheckConcurrency:**

Assicura che esista una sola esecuzione di questo runbook destinata al gruppo Amazon CloudWatch Logs. Se il runbook trova un'altra esecuzione destinata allo stesso gruppo di log, restituisce un errore e termina.

- **AnalyzeSesEvents:**

Analizza gli eventi di Amazon Simple Email Service memorizzati nel gruppo Amazon CloudWatch Logs specificato dal parametro di automazione.

- **OutputFailureReason:**

Invia messaggi di errore della fase di esecuzione quando la `AnalyzeSESMessagesSendingStatus` fase non è riuscita.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

- Risultato dell'analisi su un messaggio e-mail non recapitato a causa di un rimbalzo

Emissione di un'esecuzione automatizzata per un messaggio di posta elettronica che non ha raggiunto la casella di posta di destinazione a causa di un rimbalzo.

▼ Outputs

OutputFailureReason.FailureReason

No output available yet because the step is not successfully executed

AnalyzeSesEvents.ResultMessage

```
==== Delivery summary of the message ID [REDACTED] ====
SES received bounces or complaints.
```

```
==== Timeline of [REDACTED] =====
```

```
[2024-08-21 06:22:58.193000+00:00] Your email message was sent from SES.
```

```
[2024-08-21 06:22:58.193000+00:00] SES received a bounce from [REDACTED].
```

```
Bounce type: Permanent(General)
```

```
Bounce sources:
```

```
- email address: [REDACTED] diagnostic code: "smtp; 550 5.1.1 user unknown"
```

```
==== Next Action ====
```

```
Please fix the issues described in the delivery error messages returned from the destination email servers in the Timeline section. In the case you received s
```

```
===== Recommendations for arn:aws:ses:[REDACTED] =====
```

```
- The SES account in this region seems to be in the sandbox environment. If you haven't requested the production access, please consider to move out of the san
```

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

SageMaker AI

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon SageMaker AI.

Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come

visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-DisableSageMakerNotebookRootAccess](#)

AWS-DisableSageMakerNotebookRootAccess

Descrizione

Il `AWS-DisableSageMakerNotebookRootAccess` runbook disabilita l'accesso root su un'istanza di notebook Amazon SageMaker AI. Durante l'automazione, l'istanza del notebook viene interrotta per apportare le modifiche richieste. SageMaker Le istanze per notebook AI Studio non sono supportate.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `NotebookInstanceName`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome dell'istanza del notebook SageMaker AI su cui disabilitare l'accesso root.

- `StartInstanceAfterUpdate`

Tipo: Booleano

Impostazione predefinita: `true`

Descrizione: (Facoltativo) Determina se l'istanza del notebook viene avviata dopo aver disabilitato l'accesso root. L'impostazione predefinita per questo parametro è `true`. Se impostato su `true`,

l'istanza viene avviata dopo la disabilitazione dell'accesso root. Se impostato su `false`, l'istanza viene lasciata nello `stopped` stato dopo la disabilitazione dell'accesso root.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

Fasi del documento

- `CheckNotebookInstanceStatus` (`aws:executeAwsApi`): Verifica lo stato corrente dell'istanza del notebook.
- `StopOrUpdateNotebookInstance` (`aws:branch`): rami basati sullo stato dell'istanza del notebook.
- `StopNotebookInstance` (`aws:executeAwsApi`): avvia l'istanza se lo stato è `stopped`
- `WaitForInstanceToStop` (`aws: waitAwsResourceProperty`): Verifica che l'istanza sia `stopped`.
- `UpdateNotebookInstance` (`aws:executeAwsApi`): disabilita l'accesso root sull'istanza del notebook.
- `WaitForNotebookUpdate` (`aws: waitAwsResourceProperty`): verifica che l'accesso root sia stato disabilitato e che l'istanza abbia uno `stopped` stato.
- `ChooseInstanceStart` (`aws:branch`): Branch in base al fatto che l'istanza debba essere avviata.
- `StartNotebookInstance` (`aws:executeAwsApi`): avvia l'istanza del notebook.
- `VerifyNotebookInstanceStatus` (`aws: waitAwsResourceProperty`): Verifica se l'istanza è `available` prima di disabilitare l'accesso root.
- `VerifyNotebookInstanceRootAccess` (`aws: assertAwsResource Property`): verifica che l'impostazione di accesso root dell'istanza del notebook sia disabilitata correttamente.

Secrets Manager

AWS Systems Manager Automation fornisce runbook predefiniti per. AWS Secrets Manager Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSConfigRemediation-DeleteSecret](#)
- [AWSConfigRemediation-RotateSecret](#)

AWSConfigRemediation-DeleteSecret

Descrizione

Il AWSConfigRemediation-DeleteSecret runbook elimina un segreto e tutte le versioni memorizzate in. AWS Secrets Manager Facoltativamente, è possibile specificare la finestra di ripristino durante la quale è possibile ripristinare il segreto. Se non si specifica un valore per il RecoveryWindowInDays parametro, l'operazione ha come valore predefinito 30 giorni.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `RecoveryWindowInDays`

Tipo: integer

Valori validi: 7-30

Impostazione predefinita: 30

Descrizione: (Facoltativo) Il numero di giorni in cui è possibile ripristinare il segreto.

- `SecretId`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del segreto che desideri eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager>DeleteSecret`
- `secretsmanager:DescribeSecret`

Fasi del documento

- `aws:executeAwsApi`- Elimina il segreto specificato nel parametro. `SecretId`
- `aws:executeScript`- Verifica che il segreto sia stato pianificato per l'eliminazione.

AWSConfigRemediation-RotateSecret

Descrizione

Il `AWSConfigRemediation-RotateSecret` runbook ruota un segreto memorizzato in. AWS Secrets Manager

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `RotationInterval`

Tipo: Intervallo

Valori validi: 1-365

Descrizione: (Obbligatorio) Il numero di giorni tra le rotazioni del segreto.

- `RotationLambdaArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) della AWS Lambda funzione che può ruotare il segreto.

- `SecretId`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del segreto che desideri ruotare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

Fasi del documento

- `aws:executeAwsApi`- Ruota il segreto specificato nel `SecretId` parametro.
- `aws:executeScript`- Verifica che la rotazione sia stata abilitata sul segreto.

Security Hub

AWS Systems Manager Automation fornisce runbook predefiniti per. AWS Security Hub Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSConfigRemediation-EnableSecurityHub](#)

AWSConfigRemediation-EnableSecurityHub

Descrizione

Il `AWSConfigRemediation-EnableSecurityHub` runbook abilita AWS Security Hub (Security Hub) per Account AWS e Regione AWS dove si esegue l'automazione. Per informazioni su Security Hub, vedi [Cos'è AWS Security Hub?](#) nella Guida AWS Security Hub per l'utente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- EnableDefaultStandards

Tipo: Booleano

Impostazione predefinita: true

Descrizione: (Obbligatorio) Se impostato su true, sono abilitati gli standard di sicurezza predefiniti designati da Security Hub.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- securityhub:DescribeHub
- securityhub:EnableSecurityHub
- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`

Fasi del documento

- `aws:executeAwsApi`- Abilita Security Hub nell'account e nella regione correnti.
- `aws:executeAwsApi`- Verifica che Security Hub sia stato abilitato.

AWS Shield

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS Shield Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSPremiumSupport-DDoSResiliencyAssessment](#)

AWSPremiumSupport-DDoSResiliencyAssessment

Descrizione

Il `AWSPremiumSupport-DDoSResiliencyAssessment` runbook di AWS Systems Manager automazione consente di verificare le vulnerabilità di DDoS e la configurazione delle risorse in base alla AWS Shield Advanced protezione richiesta. Account AWS Fornisce un rapporto sulle impostazioni di configurazione per le risorse vulnerabili agli attacchi Distributed Denial of Service (DDoS). Viene utilizzato per raccogliere, analizzare e valutare le seguenti risorse: Amazon Route 53, Amazon Load Balancers, CloudFront distribuzioni Amazon AWS Global Accelerator ed AWS Elastic IPs per le relative impostazioni di configurazione in conformità con le migliori pratiche consigliate per la protezione. AWS Shield Advanced Il report di configurazione finale è disponibile in un bucket Amazon S3 di tua scelta come file HTML.

Come funziona?

Questo runbook contiene una serie di controlli relativi ai vari tipi di risorse abilitate all'accesso pubblico e alla presenza di protezioni configurate secondo le raccomandazioni contenute nel white paper [AWS DDoS Best Practices](#). Il runbook esegue le seguenti operazioni:

- Verifica se AWS Shield Advanced è abilitato un abbonamento a.

- Se abilitato, rileva se ci sono risorse protette Shield Advanced.
- Trova tutte le risorse globali e regionali Account AWS e verifica se queste sono protette dallo Shield.
- Richiede i parametri del tipo di risorsa per la valutazione, il nome del bucket Amazon S3 e l'ID del Account AWS bucket Amazon S3 (S3). BucketOwner
- Restituisce i risultati sotto forma di report HTML archiviato nel bucket Amazon S3 fornito.

I parametri di input AssessmentType decidono se verranno eseguiti i controlli su tutte le risorse. Per impostazione predefinita, il runbook verifica la presenza di tutti i tipi di risorse. Se è selezionato solo il RegionalResources parametro GlobalResources or, il runbook esegue i controlli solo sui tipi di risorse selezionati.

Important

- L'accesso ai AWSPremiumSupport-* runbook richiede un abbonamento Enterprise o Business Support. Per ulteriori informazioni, [consulta Confronta Supporto i piani](#).
- Questo runbook richiede un ACTIVE [AWS Shield Advanced abbonamento](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- **AssessmentType**

Tipo: stringa

Descrizione: (Facoltativo) Determina il tipo di risorse da valutare per la valutazione della resilienza DDoS. Per impostazione predefinita, il runbook valuterà sia le risorse globali che quelle regionali. Per le risorse regionali, il runbook descrive tutti i load balancer Application (ALB) e Network (NLB), nonché tutto il gruppo Auto Scaling nella tua /region. Account AWS

Valori validi: ['Global Resources', 'Regional Resources', 'Global and Regional Resources']

Impostazione predefinita: risorse globali e regionali

- **S3 BucketName**

Tipo: AWS::S3::Bucket::Name

Descrizione: (Obbligatorio) Il nome del bucket Amazon S3 in cui verrà caricato il report.

Modello consentito: `^[0-9a-z][a-z0-9\-\.\.]{3,63}$`

- **S3 BucketOwnerAccount**

Tipo: stringa

Descrizione: (Facoltativo) Il Account AWS proprietario del bucket Amazon S3. Specificate questo parametro se il bucket Amazon S3 appartiene a un altro bucket Account AWS, altrimenti potete lasciare questo parametro vuoto.

Pattern consentito: `^$|^[0-9]{12,13}$`

- **S3 BucketOwnerRoleArn**

Tipo: AWS::IAM::Role::Arn

Descrizione: (Facoltativo) L'ARN di un ruolo IAM con le autorizzazioni per descrivere il bucket Amazon S3 e Account AWS bloccare la configurazione dell'accesso pubblico se il bucket si

trova in un altro. Account AWS Se questo parametro non è specificato, il runbook utilizza l'utente `AutomationAssumeRole` o l'utente IAM che avvia questo runbook (se non è specificato). `AutomationAssumeRole` Consulta la sezione sulle autorizzazioni richieste nella descrizione del runbook.

Modello consentito: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- `S3 BucketPrefix`

Tipo: stringa

Descrizione: (Facoltativo) Il prefisso per il percorso all'interno di Amazon S3 per l'archiviazione dei risultati.

Modello consentito: `^[a-zA-Z0-9][-. /a-zA-Z0-9]{0,255}$|^$`

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Esempio di politica IAM per l'automazione Assume Role

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

```

        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::<bucket-name>",
    "Effect": "Allow"
},
{
    "Action": [
        "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::<bucket-name>/*",
    "Effect": "Allow"
},
{
    "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:ListDistributions",
        "ec2:DescribeInstances",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkAcls",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "globalaccelerator:ListAccelerators",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "route53:ListHostedZones",
        "route53:GetHealthCheck",
        "shield:ListProtections",
        "shield:GetSubscriptionState",
        "shield:DescribeSubscription",
        "shield:DescribeEmergencyContactSettings",
        "shield:DescribeDRTAccess",
        "waf:GetWebACL",
        "waf:GetRateBasedRule",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "waf-regional:GetWebACLForResource",
        "waf-regional:GetWebACL"
    ],
    "Resource": "*",
    "Effect": "Allow"
}

```

```
        },
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/
<AutomationAssumeRole-Name>",
            "Effect": "Allow"
        }
    ]
}
```

Istruzioni

1. Passa a [AWSPremiumSupport-DDoSResiliencyAssessment](#) nella AWS Systems Manager console.
2. Seleziona Execute Automation
3. Per i parametri di input, inserisci quanto segue:

- AutomationAssumeRole(Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AssessmentType(Facoltativo):

Determina il tipo di risorse da valutare per la valutazione della resilienza DDoS. Per impostazione predefinita, il runbook valuta sia le risorse globali che quelle regionali.

- S3 BucketName (richiesto):

Il nome del bucket Amazon S3 per salvare il report di valutazione in formato HTML.

- S3 BucketOwner (opzionale):

L' Account AWS ID del bucket Amazon S3 per la verifica della proprietà. L' Account AWS ID è obbligatorio se il report deve essere pubblicato su un bucket Amazon S3 con più account e facoltativo se il bucket Amazon S3 è nella stessa fase di avvio dell'automazione. Account AWS

- S3 (opzionale): BucketPrefix

Qualsiasi prefisso per il percorso all'interno di Amazon S3 per l'archiviazione dei risultati.

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. Select an existing IAM Role X Refresh ssm-admin arn:aws:iam::[redacted]:role/ssm-admin	ResourceType (Required) Determines the type of resources to be evaluated for DDoS resiliency assessment. By default, the runbook will evaluate both global and regional resources. Global and Regional Resources X Refresh
S3BucketName (Required) The name of the Amazon S3 bucket to save the assessment report in HTML format. Select an existing S3 Bucket X Refresh [redacted]	S3BucketOwner (Required) The Account ID of the Amazon S3 bucket for ownership verification. [redacted] X Refresh
S3BucketPrefix (Optional) Any prefix for the path inside Amazon S3 for storing the results. Example path with prefix: S3://<BucketName>/<Prefix> String	

4. Seleziona Esegui.

5. L'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- CheckShieldAdvancedState:

Verifica se Account AWS è abbonato AWS Shield Advanced e se il runbook ha accesso al bucket Amazon S3.

- S3: BucketSecurityChecks

Verifica se il bucket Amazon S3 specificato in «S3BucketName» consente autorizzazioni di accesso anonime o pubbliche in lettura o scrittura, se il bucket ha la crittografia a riposo abilitata e se l' Account AWS ID fornito in «S3BucketOwner» è il proprietario del bucket Amazon S3.

- BranchOnShieldAdvancedStatus:

Le filiali documentano i passaggi in base allo stato dell' AWS Shield Advanced abbonamento e/o allo stato di proprietà del bucket Amazon S3.

- ShieldAdvancedConfigurationReview:

Esamina le configurazioni Shield Advanced per garantire che siano presenti i dettagli minimi richiesti. Ad esempio: team IAM Access for AWS Shield Response Team (SRT), Contact List Details e SRT Proactive Engagement Status.

- ListShieldAdvancedProtections:

Elenca le Shield Protected Resources e crea un gruppo di risorse protette per ogni servizio.

- BranchOnResourceTypeAndCount:

I rami documentano i passaggi in base al valore del parametro Resource Type e al numero di risorse globali protette da Shield.

- ReviewGlobalResources:

Esamina le risorse globali protette di Shield Advanced come Route 53 Hosted Zones, CloudFront Distributions e Global Accelerators.

- BranchOnResourceType:

Le filiali documentano i passaggi in base alle selezioni del tipo di risorsa, se globale, regionale o entrambi.

- ReviewRegionalResources:

Esamina le risorse regionali protette di Shield Advanced come Application Load Balancer, Network Load Balancers, Classic Load Balancer, Amazon Elastic Compute Cloud (Amazon) Instances (Elastic). EC2 IPs

- SendReportToS3:

Carica i dettagli del report di valutazione DDoS nel bucket Amazon S3.

- Una volta completato, l'URI per il file HTML del report di valutazione viene fornito nel bucket Amazon S3:

Collegamento alla console S3 e URI Amazon S3 per il report sull'esecuzione riuscita del runbook

▼ Outputs

SendReportToS3.AssessmentReportS3ConsoleUrl
https://s3.console.aws.amazon.com/s3/object/ddos-readiness-review?region=us-east-1&prefix=ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html

SendReportToS3.AssessmentReportS3Uri
s3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html

Execution status

Overall status ✔ Success	All executed steps 9	# Succeeded 9
# Failed 0	# Cancelled 0	# TimedOut 0

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)

- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS documentazione di servizio

- [AWS Shield Advanced](#)

Amazon SNS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Simple Notification Service. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-EnableSNSTopicDeliveryStatusLogging](#)
- [AWSConfigRemediation-EncryptSNSTopic](#)
- [AWS-PublishSNSNotification](#)

AWS-EnableSNSTopicDeliveryStatusLogging

Descrizione

Il AWS-EnableSNSTopicDeliveryStatusLogging runbook configura la registrazione dello stato di consegna per un endpoint HTTP Amazon Data Firehose, Lambda o Amazon Simple Queue Platform application Service (Amazon SQS). Ciò consente ad Amazon SNS di registrare gli avvisi non riusciti e una percentuale campione di notifiche di avviso riuscite su Amazon. CloudWatch Se la registrazione dello stato della consegna è già configurata per l'argomento, il runbook sostituisce la configurazione esistente con i nuovi valori specificati per i parametri di input.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- EndpointType

Tipo: stringa

Valori validi:

- HTTP
- Firehose
- Lambda
- Applicazione
- SQS

Descrizione: (Obbligatorio) Il tipo di endpoint tematico Amazon SNS per cui desideri registrare i messaggi di notifica dello stato di consegna.

- TopicArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN dell'argomento Amazon SNS per cui desideri configurare la registrazione dello stato della consegna.

- SuccessFeedbackRoleArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo IAM utilizzato da Amazon SNS per inviare i log per i messaggi di notifica riusciti. CloudWatch

- `SuccessFeedbackSampleRate`

Tipo: stringa

Valori validi: 0-100

Descrizione: (Obbligatorio) La percentuale di messaggi riusciti da campionare per l'argomento Amazon SNS specificato.

- `FailureFeedbackRoleArn`

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo IAM utilizzato da Amazon SNS per inviare i log per i messaggi di notifica degli errori. CloudWatch

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Fasi del documento

- `aws:executeAwsApi`- Applica il valore del `SuccessFeedbackRoleArn` parametro all'argomento Amazon SNS.
- `aws:executeAwsApi`- Applica il valore del `SuccessFeedbackSampleRate` parametro all'argomento Amazon SNS.
- `aws:executeAwsApi`- Applica il valore del `FailureFeedbackRoleArn` parametro all'argomento Amazon SNS.
- `aws:executeScript`- Conferma che la registrazione dello stato della consegna è abilitata sull'argomento Amazon SNS.

Output

VerifyDeliveryStatusLoggingEnabled. GetTopicAttributesResponse - Risposta dalle operazioni GetTopicAttributes API.

VerifyDeliveryStatusLoggingEnabled. VerifyDeliveryStatusLoggingEnabled - Messaggio che indica l'avvenuta verifica della registrazione dello stato di consegna.

AWSConfigRemediation-EncryptSNSTopic

Descrizione

Il AWSConfigRemediation-EncryptSNSTopic runbook abilita la crittografia sull'argomento Amazon Simple Notification Service (Amazon SNS) specificato utilizzando una chiave AWS Key Management Service (AWS KMS) gestita dal cliente. Questo runbook deve essere usato solo come base per garantire che gli argomenti di Amazon SNS siano crittografati secondo le migliori pratiche di sicurezza minime consigliate. Consigliamo di crittografare più argomenti con diverse chiavi gestite dal cliente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- **KmsKeyArn**

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) della chiave gestita AWS KMS dal cliente che desideri utilizzare per crittografare l'argomento Amazon SNS.

- **TopicArn**

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN dell'argomento Amazon SNS che desideri crittografare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Fasi del documento

- `aws:executeAwsApi`- Crittografa l'argomento Amazon SNS specificato nel `TopicArn` parametro.
- `aws:assertAwsResourceProperty`- Conferma che la crittografia è abilitata sull'argomento Amazon SNS.

AWS-PublishSNSNotification

Descrizione

Pubblica una notifica su Amazon SNS.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Messaggio

Tipo: stringa

Descrizione: (obbligatorio) il messaggio da includere nella notifica SNS.

- TopicArn

Tipo: stringa

Descrizione: (obbligatorio) l'ARN dell'argomento SNS in cui pubblicare la notifica.

Amazon SQS

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Simple Queue Service (Amazon SQS). Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-EnableSQSEncryption](#)

AWS-EnableSQSEncryption

Descrizione

Il `AWS-EnableSQSEncryption` runbook abilita la crittografia a riposo per una coda Amazon Simple Queue Service (Amazon SQS). Una coda Amazon SQS può essere crittografata con chiavi gestite Amazon SQS (SSE-SQS) o con AWS Key Management Service (AWS KMS) chiavi gestite (SSE-KMS). AWS KMS La chiave assegnata alla coda deve avere una politica di chiave che includa le autorizzazioni per tutti i principali autorizzati a utilizzare la coda. Con la crittografia abilitata, le richieste anonime `SendMessage` e `ReceiveMessage` le richieste alla coda crittografata vengono rifiutate.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- QueueUrl

Tipo: stringa

Descrizione: (Obbligatorio) L'URL della coda Amazon SQS su cui desideri abilitare la crittografia.

- KmsKeyId

Tipo: stringa

Descrizione: (Facoltativo) La AWS KMS chiave da utilizzare per la crittografia. Questo valore può essere un identificatore univoco globale, un ARN per un alias o una chiave o un nome alias preceduto da «alias/». È inoltre possibile utilizzare la chiave AWS gestita specificando l'alias aws/sqs.

- `KmsDataKeyReusePeriodSeconds`

Tipo: stringa

Valori validi: 60-86400

Impostazione predefinita: 300

Descrizione: (Facoltativo) Il periodo di tempo, in secondi, in cui una coda Amazon SQS può riutilizzare una chiave dati per crittografare o decrittografare i messaggi prima di effettuare una nuova chiamata. AWS KMS

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

Fasi del documento

- `SelectKeyType (aws:branch)`: rami basati sulla chiave specificata.
- `PutAttributeSseKms (aws:executeAwsApi)` - Aggiorna la coda Amazon SQS per utilizzare la AWS KMS chiave specificata per la crittografia.
- `PutAttributeSseSqs (aws:executeAwsApi)` - Aggiorna la coda Amazon SQS per utilizzare la chiave predefinita per la crittografia.

- `VerifySqsEncryptionKms` (`aws:assertAwsResourceProperty`) - Verifica che la crittografia sia abilitata nella coda Amazon SQS.
- `VerifySqsEncryptionDefault` (`aws:assertAwsResourceProperty`) - Verifica che la crittografia sia abilitata nella coda Amazon SQS.

Step Functions

AWS Systems Manager Automation fornisce runbook predefiniti per AWS Step Functions (Step Functions). Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, consulta [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-EnableStepFunctionsStateMachineLogging](#)

AWS-EnableStepFunctionsStateMachineLogging

Descrizione

Il `AWS-EnableStepFunctionsStateMachineLogging` runbook abilita o aggiorna la registrazione sulla macchina a AWS Step Functions stati specificata. Il livello di registrazione minimo deve essere impostato su `ALL`, `ERROR` o `FATAL`

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Livello

Tipo: stringa

Valori validi: ALL | ERROR | FATAL

Descrizione: (Obbligatorio) L'URL della coda Amazon SQS su cui desideri abilitare la crittografia.

- LogGroupArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del gruppo di log Amazon CloudWatch Logs a cui desideri inviare i log della macchina a stati.

- StateMachineArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN della macchina a stati su cui si desidera abilitare l'accesso.

- IncludeExecutionData

Tipo: Booleano

Impostazione predefinita: False

Descrizione: (Facoltativo) Determina se i dati di esecuzione sono inclusi nei log.

- TracingConfiguration

Tipo: Booleano

Impostazione predefinita: False

Descrizione: (Facoltativo) Determina se la AWS X-Ray traccia è abilitata.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `states:DescribeStateMachine`
- `states:UpdateStateMachine`

Fasi del documento

- `EnableStepFunctionsStateMachineLogging` (`aws:executeAwsApi`)- Aggiorna la macchina a stati specificata con la configurazione di registrazione specificata.
- `VerifyStepFunctionsStateMachineLoggingEnabled` (`aws:assertAwsResourceProperty`)- Verifica che la registrazione sia stata abilitata per la macchina a stati specificata.

Output

- `EnableStepFunctionsStateMachineLogging.Response`: risposta dalla chiamata API.
`UpdateStateMachine`

Systems Manager

AWS Systems Manager Automation fornisce runbook predefiniti per Systems Manager. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, vedere. [Visualizza il contenuto del runbook](#)

Argomenti

- [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

Descrizione

Il `AWS-BulkDeleteAssociation` runbook consente di eliminare fino a 50 associazioni di Systems Manager State Manager alla volta.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `AssociationIds`

Tipo: `StringList`

Descrizione: (Obbligatorio) Un elenco separato da virgole IDs delle associazioni che si desidera eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:DeleteAssociation`

Fasi del documento

- `aws:executeScript`- Elimina le associazioni specificate nel `AssociationIds` parametro.

AWS-BulkEditOpsItems

Descrizione

Il `AWS-BulkEditOpsItems` runbook consente di modificare lo stato, la gravità, la categoria o la priorità di AWS Systems Manager OpsItems. Questa automazione può modificarne un massimo di 50 OpsItems alla volta.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Categoria

Tipo: stringa

Valori validi:

- Disponibilità
- Costo
- Nessuna modifica
- Prestazioni
- Ripristino
- Sicurezza

Impostazione predefinita: nessuna modifica

Descrizione: (Facoltativo) La nuova categoria che desideri specificare per la modifica OpsItems.

- OpsItemIds

Tipo: StringList

Descrizione: (Obbligatorio) Un elenco separato da virgole da modificare (ad esempio, OI-xxxxxxxxxxxxx, OI-xxxxxxxxxxxxx). OpsItems IDs

- Priorità

Tipo: stringa

Valori validi:

- Nessuna modifica

- 2
- 3
- 4
- 5

Impostazione predefinita: nessuna modifica

Descrizione: (Facoltativo) L'importanza delle modifiche OpsItems rispetto agli altri OpsItems elementi del sistema.

- Gravità

Tipo: stringa

Valori validi:

- Nessuna modifica
- 1
- 2
- 3
- 4

Impostazione predefinita: nessuna modifica

Descrizione: (Facoltativa) La gravità della modifica OpsItems.

- WaitTimeBetweenEditsInSecs

Tipo: stringa

Valori validi: 0.0-2.0

Predefinito: 0.8

Descrizione: (Facoltativo) Il tempo di attesa dell'automazione tra una chiamata all'operazione. UpdateOpsItems

- Stato

Tipo: stringa

- InProgress
- Nessuna modifica
- Aperta
- Risolto

Impostazione predefinita: nessuna modifica

Descrizione: (Facoltativo) Il nuovo stato della modifica OpsItems.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

Fasi del documento

- aws:executeScript- Modifica il valore OpsItems specificato nel OpsItemIds parametro in base ai valori specificati per i parametriCategory, PrioritySeverity, eStatus.

AWS-BulkResolveOpsItems

Descrizione

Il AWS-BulkResolveOpsItems runbook risolve le risoluzioni AWS Systems Manager OpsItems che corrispondono al filtro specificato. È inoltre possibile specificare un elemento OpsItemId da aggiungere alla risoluzione OpsItems utilizzando il parametro. OpsInsightsId Se specifichi un valore per il S3BucketName parametro, viene inviato un riepilogo dei risultati al bucket Amazon Simple Storage Service (Amazon S3). Per ricevere una notifica dopo l'invio del riepilogo dei risultati al bucket Amazon S3, specifica un valore per il parametro. SnsTopicArn Questa automazione risolverà un massimo di 1.000 OpsItems alla volta.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Filtri

Tipo: stringa

Descrizione: (Obbligatorio) Le coppie di filtri chiave-valore da restituire. OpsItems Ad esempio, [{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]. Per ulteriori informazioni sulle opzioni disponibili per filtrare le OpsItems risposte, consulta l'AWS Systems Manager API [OpsItemFilters](#)Reference.

- OpsInsightId

Tipo: stringa

Descrizione: (Facoltativo) L'identificatore di risorsa correlato che desideri aggiungere a risolto. OpsItems

- S3 BucketName

Tipo: stringa

Descrizione: (Facoltativo) Il nome del bucket Amazon S3 a cui desideri inviare il riepilogo dei risultati.

- SnsMessage

Tipo: stringa

Descrizione: (Facoltativo) La notifica che desideri che Amazon Simple Notification Service (Amazon SNS) invii al termine dell'automazione.

- SnsTopicArn

Tipo: stringa

Descrizione: (Facoltativo) L'ARN dell'argomento Amazon SNS che desideri notificare quando il riepilogo dei risultati viene inviato ad Amazon S3.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- s3:GetBucketAcl
- s3:PutObject
- sns:Publish
- ssm:DescribeOpsItems
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

Fasi del documento

- aws:executeScript- Raccoglie e risolve i dati in OpsItems base ai filtri specificati. Se è stato specificato un valore per il OpsInsightId parametro, il valore viene aggiunto come risorsa correlata.
- aws:executeScript- Se hai specificato un valore per il S3BucketName parametro, viene quindi inviato un riepilogo dei risultati al bucket Amazon S3.
- aws:executeScript- Se hai specificato un valore per il SnsTopicArn parametro, viene inviata una notifica all'argomento Amazon SNS dopo l'invio del riepilogo dei risultati ad Amazon S3, incluso SnsMessage il valore del parametro, se specificato.

AWS-ConfigureMaintenanceWindows

Descrizione

Il AWS-ConfigureMaintenanceWindows runbook consente di abilitare o disabilitare più finestre di manutenzione di Systems Manager.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- MaintenanceWindows

Tipo: StringList

Descrizione: (Obbligatorio) Un elenco separato da virgole delle finestre IDs di manutenzione che si desidera abilitare o disabilitare.

- MaintenanceWindowsStatus

Tipo: stringa

Valori validi: «True» | «False»

Predefinito: «False»

Descrizione: (Obbligatorio) Determina se le finestre di manutenzione sono abilitate o disabilitate. Specificare «True» per abilitare le finestre di manutenzione e «False» per disabilitarle.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

Fasi del documento

- `aws:executeScript`- Raccoglie lo stato delle finestre di manutenzione specificate nel `MaintenanceWindows` parametro e abilita o disabilita le finestre di manutenzione.

AWS-CreateManagedLinuxInstance

Descrizione

Crea un' EC2 istanza per Linux configurata per Systems Manager.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux

Parametri

- `Amild`

Tipo: stringa

Descrizione: (Obbligatorio) AMI ID da utilizzare per avviare l'istanza.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- GroupName

Tipo: stringa

Impostazione predefinita: SSMSecurity GroupForLinuxInstances

Descrizione: (obbligatorio) nome del gruppo di sicurezza da creare.

- HttpTokens

Tipo: stringa

Valori validi: opzionale | obbligatorio

Predefinito: opzionale

Descrizione: (Facoltativo) IMDSv2 utilizza sessioni supportate da token. Imposta l'uso dei token HTTP su `optional` o per `required` determinare se IMDSv2 è facoltativo o obbligatorio.

- InstanceType

Tipo: stringa

Impostazione predefinita: t2.medium

Descrizione: (obbligatorio) tipo di istanza da avviare. Impostazione predefinita: t2.medium

- KeyPairName

Tipo: stringa

Descrizione: (obbligatorio) coppia di chiavi da utilizzare durante la creazione dell'istanza.

- RemoteAccessCidr

Tipo: stringa

Impostazione predefinita: 0.0.0.0/0

Descrizione: (Obbligatorio) Crea un gruppo di sicurezza con porta per SSH (intervallo di porte 22) aperta a IPs quanto specificato da CIDR (l'impostazione predefinita è 0.0.0.0/0). Se il gruppo di sicurezza esiste già, non verrà modificato e le regole non saranno modificate.

- RoleName

Tipo: stringa

Predefinito: SSMMManaged InstanceProfileRole

Descrizione: (obbligatorio) nome del ruolo da creare.

- StackName

Tipo: stringa

Predefinito: CreateManagedInstanceStack {{automation:execution_id}}

Descrizione: (Facoltativo) Specificare il nome dello stack utilizzato da questo runbook

- SubnetId

Tipo: stringa

Impostazione predefinita: Default

Descrizione: (obbligatorio) la nuova istanza verrà distribuita nella sottorete oppure, se non ne è specificata una, nella sottorete predefinita.

- VpcId

Tipo: stringa

Impostazione predefinita: Default

Descrizione: (Obbligatorio) La nuova istanza verrà distribuita in questo Amazon Virtual Private Cloud (Amazon VPC) o nell'Amazon VPC predefinito, se non specificato.

AWS-CreateManagedWindowsInstance

Descrizione

Crea un' EC2 istanza per un Windows Server configurato per Systems Manager.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Windows

Parametri

Parametri

- Amild

Tipo: stringa

Impostazione predefinita: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

Descrizione: (Obbligatorio) AMI ID da utilizzare per avviare l'istanza.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- GroupName

Tipo: stringa

Impostazione predefinita: SSMSecurity GroupForLinuxInstances

Descrizione: (obbligatorio) nome del gruppo di sicurezza da creare.

- HttpTokens

Tipo: stringa

Valori validi: opzionale | obbligatorio

Predefinito: opzionale

Descrizione: (Facoltativo) IMDSv2 utilizza sessioni supportate da token. Imposta l'uso dei token HTTP su optional o per required determinare se IMDSv2 è facoltativo o obbligatorio.

- InstanceType

Tipo: stringa

Impostazione predefinita: t2.medium

Descrizione: (obbligatorio) tipo di istanza da avviare. Impostazione predefinita: t2.medium

- KeyPairName

Tipo: stringa

Descrizione: (obbligatorio) coppia di chiavi da utilizzare durante la creazione dell'istanza.

- RemoteAccessCidr

Tipo: stringa

Impostazione predefinita: 0.0.0.0/0

Descrizione: (Obbligatorio) Crea un gruppo di sicurezza con la porta per RDP (Port range 3389) aperta a IPs quanto specificato da CIDR (l'impostazione predefinita è 0.0.0.0/0). Se il gruppo di sicurezza esiste già, non verrà modificato e le regole non saranno modificate.

- RoleName

Tipo: stringa

Predefinito: `SSMManaged InstanceProfileRole`

Descrizione: (obbligatorio) nome del ruolo da creare.

- `StackName`

Tipo: stringa

Predefinito: `CreateManagedInstanceStack {{automation:execution_id}}`

Descrizione: (Facoltativo) Specificare il nome dello stack utilizzato da questo runbook

- `SubnetId`

Tipo: stringa

Impostazione predefinita: Default

Descrizione: (obbligatorio) la nuova istanza verrà distribuita nella sottorete oppure, se non ne è specificata una, nella sottorete predefinita.

- `VpcId`

Tipo: stringa

Impostazione predefinita: Default

Descrizione: (Obbligatorio) La nuova istanza verrà distribuita in questo Amazon Virtual Private Cloud (Amazon VPC) o nell'Amazon VPC predefinito, se non specificato.

AWSConfigRemediation-EnableCWLoggingForSessionManager

Descrizione

Il `AWSConfigRemediation-EnableCWLoggingForSessionManager` runbook consente alle sessioni di AWS Systems Manager Session Manager (Session Manager) di archiviare i log di output in un gruppo di log Amazon CloudWatch (CloudWatch).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- DestinationLogGroup

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del gruppo di CloudWatch log.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:UpdateDocument
- ssm:CreateDocument
- ssm:UpdateDefaultDocumentVersion
- ssm:DescribeDocument

Fasi del documento

- `aws:executeScript`- Accetta il gruppo di CloudWatch log per aggiornare il documento che memorizza le preferenze dei log di output della sessione di Session Manager o ne crea uno se non esiste.

AWS-ExportOpsDataToS3

Descrizione

Questo runbook recupera un elenco di OpsData riepiloghi in AWS Systems Manager Explorer e li esporta in un oggetto in un bucket Amazon Simple Storage Service (Amazon S3) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- columnFields

Tipo: StringList

Descrizione: campi Colonna (Obbligatorio) da scrivere nel file di output.

- filtri

Tipo: stringa

Descrizione: (Facoltativo) Filtri per la getOpsSummary richiesta.

- resultAttribute

Tipo: stringa

Descrizione: (Facoltativo) L'attributo del risultato per la getOpsSummary richiesta.

- s3 BucketName

Tipo: stringa

Descrizione: (obbligatoria) bucket S3 in cui si desidera scaricare il file di output.

- snsSuccessMessage

Tipo: stringa

Descrizione: (Facoltativo) Messaggio da inviare al termine del runbook.

- snsTopicArn

Tipo: stringa

Descrizione: (Obbligatorio) Argomento Amazon Simple Notification Service (Amazon SNS) ARN per notificare il completamento del download.

- syncName

Tipo: stringa

Descrizione: (Facoltativo) Il nome della sincronizzazione dei dati delle risorse.

Fasi del documento

getOpsSummaryPassaggio: recupera ora fino a 5.000 riepiloghi delle operazioni da esportare in un file CSV.

Output

OpsData oggetto: se il runbook viene eseguito correttamente, troverai l' OpsData oggetto esportato nel bucket S3 di destinazione.

AWS-ExportPatchReportToS3

Descrizione

Questo runbook recupera gli elenchi di dati di riepilogo delle patch e i dettagli delle AWS Systems Manager patch in Patch Manager e li esporta in file.csv in un bucket Amazon Simple Storage Service (Amazon S3) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- assumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che esegue questo documento.

- s3 BucketName

Tipo: stringa

Descrizione: (Obbligatorio) Il bucket S3 in cui vuoi scaricare il file di output.

- snsTopicArn

Tipo: stringa

Descrizione: (Facoltativo) L'argomento Amazon Simple Notification Service (Amazon SNS) Amazon Resource Name (ARN) per notificare il completamento del download.

- snsSuccessMessage

Tipo: stringa

Descrizione: (Facoltativo) Testo del messaggio da inviare al termine del runbook.

- targets

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'istanza o un carattere jolly (*) per indicare se riportare i dati della patch per un'istanza specifica o per tutte le istanze.

Fasi del documento

ExportReportStep — L'azione per questo passaggio dipende dal valore del targets parametro. Se targets è nel formato diinstanceids=*, il passaggio recupera fino a 10.000 riepiloghi delle patch per le istanze presenti nell'account ed esporta i dati in un file.csv.

Se targets è nel formatoinstanceids=<instance-id>, il passaggio recupera sia il riepilogo delle patch che tutte le patch per l'istanza specificata nell'account e le esporta in un file.csv.

Output

PatchSummaryOggetto /Patches: se il runbook viene eseguito correttamente, l'oggetto del report sulle patch esportato viene scaricato nel bucket S3 di destinazione.

AWS-SetupInventory

Descrizione

Crea un'associazione Systems Manager Inventory per una o più istanze gestite. Il sistema raccoglie i metadati dalle istanze in base alla pianificazione definita nell'associazione. Per ulteriori informazioni, consulta [AWS Systems Manager Inventario](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- Applicazioni

Tipo: stringa

Impostazione predefinita: Enabled

Descrizione: (facoltativo) raccoglie i metadati relativi alle applicazioni installate.

- AssociatedDocName

Tipo: stringa

Impostazione predefinita: AWS-GatherSoftwareInventory

Descrizione: (Facoltativo) Il nome del runbook utilizzato per raccogliere l'inventario dall'istanza gestita.

- AssociationName

Tipo: stringa

Descrizione: (facoltativo) nome dell'associazione di Inventory che verrà assegnata all'istanza.

- AssocWaitTime

Tipo: stringa

Impostazione predefinita: M PT5

Descrizione: (facoltativo) intervallo di tempo durante il quale la raccolta di Inventory deve essere messa in pausa quando viene raggiunta l'ora di inizio dell'associazione di Inventory. L'ora utilizza il formato ISO 8601.

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `AwsComponents`

Tipo: stringa

Impostazione predefinita: Enabled

Descrizione: (Facoltativo) Raccogli metadati per AWS componenti come. amazon-ssm-agent

- `CustomInventory`

Tipo: stringa

Impostazione predefinita: Enabled

Descrizione: (facoltativo) raccoglie i metadati di inventario personalizzati.

- `File`

Tipo: stringa

Descrizione: (facoltativo) raccoglie i metadati relativi ai file nelle istanze. Per ulteriori informazioni su come raccogliere questo tipo di dati di inventario, vedi [Utilizzo dei file e dell'inventario del registro di Windows](#). Richiede SSMAgent versione 2.2.64.0 o successiva. Esempio di Linux:

```
[{"Path":"/usr/bin", "Pattern":["aws*", "*ssm*"],"Recursive":false}, {"Path":"/var/log", "Pattern":["amazon*.*"], "Recursive":true, "DirScanLimit":1000}] Windows example: [{"Path":"%PROGRAMFILES%", "Pattern":["*.exe"],"Recursive":true}]
```

- `InstanceDetailedInformation`

Tipo: stringa

Impostazione predefinita: Enabled

Descrizione: (facoltativo) raccoglie le informazioni aggiuntive sull'istanza, ad esempio il modello di CPU, la velocità e il numero di core.

- **InstanceIds**

Tipo: stringa

Impostazione predefinita: *

Descrizione: EC2 istanze (obbligatorie) che desideri inventariare.

- **LambdaAssumeRole**

Tipo: stringa

Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

- **NetworkConfig**

Tipo: stringa

Impostazione predefinita: Enabled

Descrizione: (facoltativo) raccoglie i metadati relativi alle configurazioni di rete.

- **Uscite (3) BucketName**

Tipo: stringa

Descrizione: (Facoltativo) Nome di un bucket Amazon S3 in cui desideri scrivere i dati del registro di inventario.

- **Uscite S3 KeyPrefix**

Tipo: stringa

Descrizione: (Facoltativo) Un prefisso chiave Amazon S3 (sottocartella) in cui desideri scrivere i dati del registro di inventario.

- **OutputS3Region**

Tipo: stringa

Descrizione: (Facoltativo) Il nome del Regione AWS luogo in cui si trova Amazon S3.

- **Pianificazione**

Tipo: stringa

Impostazione predefinita: cron(0 */30 * * * ? *)

Descrizione: (facoltativo) espressione cron per la pianificazione dell'associazione di Inventory. Il valore predefinito è ogni 30 minuti.

- Servizi

Tipo: stringa

Impostazione predefinita: Enabled

Descrizione: (Facoltativo, solo sistema operativo Windows, richiede la SSMAgent versione 2.2.64.0 e successive) Raccogli dati per le configurazioni dei servizi.

- WindowsRegistry

Tipo: stringa

Descrizione: (facoltativo) raccoglie i metadati relativi alle chiavi del Registro di sistema di Microsoft Windows. Per ulteriori informazioni su come raccogliere questo tipo di dati di inventario, vedere [Utilizzo dei file e dell'inventario del registro](#) di Windows. Richiede SSM Agent versione 2.2.64.0 o versioni successive. Esempio: [{"Path» : "HKEY_CURRENT_CONFIG\ System», "Recursive» : true}, {"Path» : "HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\ «," «: [» «]]} MachinelImage ValueNames AMIName

- WindowsRoles

Tipo: stringa

Impostazione predefinita: Enabled

Descrizione: (facoltativo) raccoglie le informazioni sui ruoli di Windows nell'istanza. Si applica solo ai sistemi operativi Windows. Richiede SSMAgent versione 2.2.64.0 o successiva.

- WindowsUpdates

Tipo: stringa

Impostazione predefinita: Enabled

Descrizione: (facoltativo) raccoglie i dati su tutti gli aggiornamenti di Windows nell'istanza.

AWS-SetupManagedInstance

Descrizione

Configura un'istanza con un ruolo AWS Identity and Access Management (IAM) per l'accesso a Systems Manager.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) ID dell' EC2 istanza da configurare

- LambdaAssumeRole

Tipo: stringa

Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

- RoleName

Tipo: stringa

Predefinito: SSMRole ForManagedInstance

Descrizione: (Facoltativo) Il nome del ruolo IAM per l' EC2 istanza. Se il ruolo non esiste, ne verrà creato uno. Quando specifichi questo valore, verifica che il ruolo contenga Amazon SSMManaged InstanceCore Managed Policy.

AWS - SetupManagedRoleOnEC2Instance

Descrizione

Configura un'istanza con il ruolo IAM SSMRole ForManagedInstance gestito per l'accesso a Systems Manager.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) ID dell' EC2 istanza da configurare

- LambdaAssumeRole

Tipo: stringa

Descrizione: (facoltativo) ARN del ruolo che consente alla funzione Lambda creata dall'automazione di eseguire le operazioni a nome dell'utente. Se non specificato, per eseguire la funzione Lambda verrà creato un ruolo temporaneo.

- RoleName

Tipo: stringa

Predefinito: SSMRole ForManagedInstance

Descrizione: (Facoltativo) Il nome del ruolo IAM per l' EC2 istanza. Se il ruolo non esiste, ne verrà creato uno. Quando specifichi questo valore, verifica che il ruolo contenga Amazon SSMManaged InstanceCore Managed Policy.

AWSsupport-TroubleshootManagedInstance

Descrizione

Il AWSsupport-TroubleshootManagedInstance runbook ti aiuta a determinare perché un'istanza Amazon Elastic Compute Cloud EC2 (Amazon) non riporta come gestita da AWS Systems Manager. Questo runbook esamina la configurazione VPC per l'istanza, incluse le regole dei gruppi di sicurezza, gli endpoint VPC, le regole della lista di controllo degli accessi alla rete (ACL) e le tabelle di routing. Inoltre, conferma che all'istanza è associato un profilo di istanza AWS Identity and Access Management (IAM) contenente le autorizzazioni richieste.

Important

Questo runbook di automazione non valuta le IPv6 regole.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon che non riporta come gestita da Systems Manager.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

- `aws:executeScript`- Raccoglie l'`PingStatus`istanza.
- `aws:branch`- Filiali a seconda che l'istanza stia già segnalando come gestita da Systems Manager.
- `aws:executeAwsApi`- Raccoglie dettagli sull'istanza, inclusa la configurazione VPC.
- `aws:executeScript`- Se applicabile, raccoglie ulteriori dettagli relativi agli endpoint VPC che sono stati implementati per l'uso con Systems Manager e conferma che i gruppi di sicurezza collegati all'endpoint VPC consentano il traffico in entrata sulla porta TCP 443 dall'istanza.
- `aws:executeScript`- Verifica se la tabella delle rotte consente il traffico verso l'endpoint VPC o gli endpoint pubblici di Systems Manager.
- `aws:executeScript`- Verifica se le regole ACL di rete consentono il traffico verso l'endpoint VPC o gli endpoint pubblici di Systems Manager.
- `aws:executeScript`- Verifica se il traffico in uscita verso l'endpoint VPC o gli endpoint pubblici di Systems Manager è consentito dal gruppo di sicurezza associato all'istanza.
- `aws:executeScript`- Verifica se il profilo dell'istanza collegato all'istanza include una policy gestita che fornisce le autorizzazioni richieste.
- `aws:branch`- Filiali basate sul sistema operativo dell'istanza.
- `aws:executeScript`- Fornisce un riferimento allo script di `ssmagent-toolkit-linux` shell.

- `aws:executeScript`- Fornisce un riferimento allo `ssmagent-toolkit-windows` PowerShell script.
- `aws:executeScript`- Genera l'output finale per l'automazione.
- `aws:executeScript`- Se l'`PingStatus`istanza è `Online`, restituisce che l'istanza è già gestita da Systems Manager.

AWSSupport-TroubleshootPatchManagerLinux

Descrizione

Il `AWSSupport-TroubleshootPatchManagerLinux` runbook risolve i problemi più comuni che possono causare un errore di patch sui nodi gestiti basati su Linux utilizzando Patch Manager, uno strumento di. AWS Systems Manager L'obiettivo principale di questo runbook è identificare la causa principale dell'errore del comando patch e suggerire un piano di correzione.

Come funziona?

Il `AWSSupport-TroubleshootPatchManagerLinux` runbook considera la coppia ID di istanza/ID di comando forniti dall'utente per la risoluzione dei problemi. Se non viene fornito alcun Command ID, seleziona l'ultimo comando di patch non riuscito negli ultimi 30 giorni sull'istanza fornita. Dopo aver verificato lo stato del comando, il rispetto dei prerequisiti e la distribuzione del sistema operativo, il runbook scarica ed esegue un pacchetto log analyzer. L'output include la causa principale del problema e l'azione necessaria per risolverlo.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

- Amazon Linux 2 e AL2 023
- Red Hat Enterprise Linux 8.X e 9.X
- Centos 8.X e 9.X
- USA 15.X

Parametri

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Istruzioni

Segui questi passaggi per configurare l'automazione:

1. Passa a [AWSSupport-TroubleshootPatchManagerLinux](#) nella AWS Systems Manager console.
2. Seleziona `Execute automation` (Esegui automazione).
3. Per i parametri di input, inserisci quanto segue:
 - `InstanceId` (Obbligatorio):

Utilizza il selettore interattivo di istanze per scegliere l'ID del nodo gestito SSM basato su Linux (Amazon Elastic Compute Cloud (Amazon EC2) o server Hybrid Activated) rispetto al quale il comando di patch non è riuscito, oppure inserisci manualmente l'ID dell'istanza gestita SSM.

- `AutomationAssumeRole` (Facoltativo):

Inserisci l'ARN del ruolo IAM che consente all'automazione di eseguire azioni per tuo conto. Se non viene specificato un ruolo, Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `RunCommandId` (Facoltativo):

Immettere l'ID del comando Failed AWS-RunPatchBaseline Run del documento. Se non fornite un Command ID, il runbook cercherà l'ultimo comando di patch non riuscito negli ultimi 30 giorni sull'istanza selezionata.

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.
☒ Show interactive instance picker

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Choose an option ▼ 

RunCommandId
(Optional) Failed Run Command ID of AWS-RunPatchBaseline. If not provided, we look for the latest unsuccessful execution of AWS-RunPatchBaseline for the instance and evaluate it. To confirm the command ID, look under Command History tab in the Run Command Console under AWS Systems Manager.

4. Seleziona Esegui.

5. L'automazione viene avviata.

6. Il documento esegue le seguenti operazioni:

- CheckConcurrency:

Assicura che esista una sola esecuzione di questo runbook destinata alla stessa istanza. Se il runbook rileva un'altra esecuzione in corso relativa alla stessa istanza, restituisce un errore e termina.

- ValidateCommandID:

Verifica se l'ID di comando fornito, come parametro di input, è stato eseguito per il documento AWS-RunPatchBaseline SSM. Se non viene fornito alcun Command ID, il runbook prenderà in considerazione l'ultima esecuzione non riuscita degli AWS-RunPatchBaseline ultimi 30 giorni sull'istanza selezionata.

- BranchOnCommandStatus:

Conferma che lo stato del comando fornito non è riuscito. In caso contrario, il runbook termina l'esecuzione e genera un rapporto che indica che il comando fornito è stato eseguito correttamente.

- VerifyPrerequisites:

Conferma che i prerequisiti sopra menzionati sono soddisfatti.

- GetPlatformDetails:

Recupera la distribuzione e la versione del sistema operativo (OS).

- **GetDownloadURL:**

Recupera l'URL di download per il pacchetto PatchManager Log Analyzer.

- **EvaluatePatchManagerLogs:**

Scarica ed esegue il pacchetto python PatchManager Log Analyzer sull'istanza per valutare il file di registro.

- **GenerateReport:**

Genera un rapporto finale sull'esecuzione del runbook che include il problema identificato e la soluzione suggerita.

7. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione:

```
▼ Outputs

GenerateReportOutput
Starting 'python3 main.py i-0[redacted] 3e016680-82f4-45f4-845c-aa4685b4fab Ubuntu 22.04'

TROUBLESHOOTING RESULTS
=====
[PROBLEM] :
The error found in the log file at /var/lib/amazon/ssm/i-0[redacted]/document/orchestration/3e016680-82f4-45f4-845c-aa4685b4fab/awsrunShellScript/PatchLinux/stdout is :
Unable to download payload: https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz.failed to run commands: exit status 156
=====
[SOLUTION] :
Here are some suggestions to troubleshoot the issue:

Possible reasons for the above error are :

1. Network connectivity issue while accessing the s3 service endpoint from the instance to download the payload.
2. Instance doesn't have the required permissions to access the specified Amazon Simple Storage Service (Amazon S3) bucket.
3. No space left on the Instance.

To resolve this, ensure network connectivity to S3 endpoint from the instance. For more details, see information about required access to S3 buckets for Patch Manager in https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent-minimum-s3-permissions.

For testing purpose, try to manually access the above payload URL using curl or wget from within Instance. Command to run:

curl https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz --output payload.tar.gz
```

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWSSupport-TroubleshootSessionManager

Descrizione

Il `AWSSupport-TroubleshootSessionManager` runbook ti aiuta a risolvere i problemi più comuni che impediscono la connessione a istanze gestite di Amazon Elastic Compute Cloud (Amazon EC2) utilizzando Session Manager. Session Manager è uno strumento in. AWS Systems Manager Questo runbook verifica quanto segue:

- Verifica se l'istanza è in esecuzione e riporta i report come gestito da Systems Manager.
- Esegue il `AWSSupport-TroubleshootManagedInstance` runbook se l'istanza non riporta i dati come gestiti da Systems Manager.
- Verifica la versione dell'agente SSM installata sull'istanza.
- Verifica se un profilo di istanza contenente una policy consigliata AWS Identity and Access Management (IAM) per Session Manager è collegato all' EC2 istanza Amazon.
- Raccoglie i log dell'agente SSM dall'istanza.
- Analizza le preferenze del Session Manager.
- Esegue il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook per analizzare la connettività dell'istanza agli endpoint per Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3) e Amazon CloudWatch Logs (Logs). CloudWatch

Considerazioni

- I nodi gestiti ibridi non sono supportati.
- Questo runbook verifica solo se una policy IAM gestita consigliata è allegata al profilo dell'istanza. Non analizza IAM o le AWS KMS autorizzazioni contenute nel profilo dell'istanza.

Important

Il `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook utilizza [VPC Reachability Analyzer per analizzare la](#) connettività di rete tra un endpoint di origine e un endpoint di servizio. Ti viene addebitato un costo per ogni esecuzione di analisi tra un'origine e una destinazione. Per ulteriori dettagli, consulta la pagina dei prezzi di [Amazon VPC](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- InstanceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell' EC2 istanza Amazon a cui non riesci a connetterti tramite Session Manager.

- SessionPreferenceDocument

Tipo: stringa

Impostazione predefinita: SSM- SessionManagerRunShell

Descrizione: (Facoltativo) Il nome del documento delle preferenze di sessione. Se non specificate un documento personalizzato con le preferenze di sessione all'avvio delle sessioni, utilizzate il valore predefinito.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `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`

Fasi del documento

1. `aws:waitForAwsResourceProperty`: Attende fino a 6 minuti che l'istanza di destinazione superi i controlli di stato.
2. `aws:executeScript`: analizza il documento delle preferenze di sessione.
3. `aws:executeAwsApi`: ottiene l'ARN del profilo dell'istanza collegato all'istanza.
4. `aws:executeAwsApi`: verifica se l'istanza riporta i report come gestita da Systems Manager.
5. `aws:branch`: filiali in base al fatto che l'istanza riporti o meno come gestita da Systems Manager.
6. `aws:executeScript`: verifica se l'agente SSM installato sull'istanza supporta Session Manager.
7. `aws:branch`: filiali basate sulla piattaforma dell'istanza per la raccolta dei `ssm-cli` log.
8. `aws:runCommand`: raccoglie l'output dei log `ssm-cli` da un'istanza Linux o macOS.
9. `aws:runCommand`: raccoglie l'output dei log da `ssm-cli` un'istanza Windows.
10. `aws:executeScript`: analizza i log `ssm-cli`.
11. `aws:executeScript`: verifica se una policy IAM consigliata è associata al profilo dell'istanza.
12. `aws:branch`: Determina se valutare la connettività `ssmmessages` degli endpoint in base ai `ssm-cli` log.
13. `aws:executeAutomation`: valuta se l'istanza può connettersi a un endpoint `ssmmessages`.
14. `aws:branch`: determina se valutare la connettività degli endpoint Amazon S3 in base ai `ssm-cli` log e alle preferenze di sessione.
15. `aws:executeAutomation`: valuta se l'istanza può connettersi a un endpoint Amazon S3.
16. `aws:branch`: determina se valutare la connettività AWS KMS degli endpoint in base ai `ssm-cli` log e alle preferenze di sessione.
17. `aws:executeAutomation`: valuta se l'istanza può connettersi a un endpoint AWS KMS.
18. `aws:branch`: Determina se valutare la connettività CloudWatch degli endpoint di Logs in base ai `ssm-cli` log e alle preferenze di sessione.
19. `aws:executeAutomation`: valuta se l'istanza può connettersi a un endpoint Logs CloudWatch.
20. `aws:executeAutomation`: esegue il runbook `AWSsupport-TroubleshootManagedInstance`.
21. `aws:executeScript`: compila l'output dei passaggi precedenti e genera un rapporto.

Uscite

- `generateReport.EvalReport`- I risultati dei controlli eseguiti dal runbook in testo semplice.

Terze parti

AWS Systems Manager Automation fornisce runbook predefiniti per prodotti e servizi di terze parti. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto del runbook, consulta [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-CreateJiraIssue](#)
- [AWS-CreateServiceNowIncident](#)
- [AWS-RunPacker](#)

AWS-CreateJiraIssue

Descrizione

Crea un problema in Jira.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AssigneeName`

Tipo: stringa

Descrizione: (facoltativo) il nome utente della persona a cui assegnare il problema.

- DueDate

Tipo: stringa

Descrizione: (Facoltativa) La data di scadenza del problema in yyyy-mm-dd formato.

- IssueDescription

Tipo: stringa

Descrizione: (obbligatorio) una descrizione dettagliata del problema.

- IssueSummary

Tipo: stringa

Descrizione: (obbligatorio) breve riepilogo del problema.

- IssueTypeName

Tipo: stringa

Descrizione: (obbligatorio) il nome del tipo di problema da creare (ad esempio, attività, attività secondaria, bug e così via).

- JiraURL

Tipo: stringa

Descrizione: (obbligatorio) l'URL dell'istanza Jira.

- JiraUsername

Tipo: stringa

Descrizione: (obbligatorio) il nome dell'utente con cui sarà creato il problema.

- PriorityName

Tipo: stringa

Descrizione: (facoltativo) il nome della priorità del problema.

- **ProjectKey**

Tipo: stringa

Descrizione: (obbligatorio) la chiave del progetto in cui dovrebbe essere creato il problema.

- **SSMParameterNome**

Tipo: stringa

Descrizione: (obbligatorio) il nome di un parametro SSM criptato contenente la chiave API o la password per l'utente Jira.

Fasi del documento

`aws:createStack`- Crea uno CloudFormation stack per creare ruoli e funzioni Lambda IAM.

`aws:invokeLambdaFunction`- Invoca la funzione Lambda per creare il problema Jira

`aws:deleteStack`- Elimina lo stack creato CloudFormation .

Output

IssuedId: ID del problema Jira appena creato

AWS-CreateServiceNowIncident

Descrizione

Crea un incidente nella tabella degli ServiceNow incidenti.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Categoria

Tipo: stringa

Descrizione: (Facoltativo) La categoria dell'incidente.

Valori validi: Nessuno | Richiesta/Aiuto | Software | Hardware | Rete | Database

Valore predefinito: nessuno

- Descrizione

Tipo: stringa

Descrizione: (Obbligatorio) Una spiegazione dettagliata dell'incidente.

- Impatto

Tipo: stringa

Descrizione: (Facoltativo) L'effetto che un incidente ha sul business.

Valori validi: Alto | Medio | Basso

Valore predefinito: Basso

- ServiceNowInstanceUsername

Tipo: stringa

Descrizione: (Obbligatorio) il nome dell'utente con cui sarà creato l'incidente.

- ServiceNowInstancePassword

Tipo: stringa

Descrizione: (Obbligatorio) Il nome di un parametro SSM crittografato contenente la password dell' ServiceNow utente.

- ServiceNowInstanceURL

Tipo: stringa

Descrizione: (Obbligatorio) L'URL dell' ServiceNow istanza

- ShortDescription

Tipo: stringa

Descrizione: (Obbligatorio) Una breve descrizione dell'incidente.

- Sottocategoria

Tipo: stringa

Descrizione: (Facoltativo) La sottocategoria dell'incidente.

Valori validi: Nessuno | Antivirus | Email | Applicazione interna | Sistema operativo | CPU | Disco | Tastiera | Hardware | Memoria | Monitor | Mouse | DHCP | DNS | Indirizzo IP | VPN | Wireless | | MS SQL Server DB2 | Oracle

Valore predefinito: nessuno

Fasi del documento

Push_incident: invia le informazioni sull'incidente a. ServiceNow

Output

push_incident.incidentID — L'ID dell'incidente creato.

AWS-RunPacker

Descrizione

Questo runbook utilizza lo strumento HashiCorp [Packer](#) per convalidare, correggere o creare modelli di packer utilizzati per creare immagini di macchine. Questo runbook utilizza Packer v1.7.2.

 Note

Se specifichi un valore `vpc_id`, devi anche specificare il valore `subnet_id` di una sottorete pubblica. A meno che non si modifichi l'attributo di indirizzamento IPv4 pubblico della sottorete, è necessario impostare anche su `true`. `associate_public_ip_address`

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Force

Tipo: Booleano

Descrizione: un'opzione Packer per forzare l'esecuzione di un costruttore quando gli artefatti di una build precedente impediscono l'esecuzione di una build.

- Modalità

Tipo: stringa

Descrizione: la modalità o il comando in cui utilizzare Packer durante la convalida rispetto al modello. Le opzioni includono BuildValidate, e. Fix

- TemplateFileName

Tipo: stringa

Descrizione: il nome o la chiave del file modello nel bucket S3.

- Modelli 3 BucketName

Tipo: stringa

Descrizione: il nome del bucket S3 contenente il modello di packer.

Fasi del documento

RunPackerProcessTemplate — Esegue la modalità selezionata sul modello utilizzando lo strumento Packer.

Output

RunPackerProcessTemplate.output — Lo stdout dello strumento Packer.

RunPackerProcessTemplate.fixed_template_key — Il nome del modello memorizzato in un bucket S3 da utilizzare solo durante l'esecuzione in modalità «Fix».

RunPackerProcessTemplate.s3_bucket: il nome del bucket S3 che contiene il modello fisso da utilizzare solo durante l'esecuzione in modalità «Fix».

Amazon VPC

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon Virtual Private Cloud. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare i contenuti dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [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

Descrizione

Questo runbook rimuove tutte le regole di ingresso e uscita dal gruppo di sicurezza specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- SecurityGroupId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza che si desidera chiudere.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

Fasi del documento

- aws:executeScript- Rimuove tutte le regole di ingresso e uscita dal gruppo di sicurezza specificato nel parametro. SecurityGroupId

AWSSupport-ConfigureDNSQueryLogging

Descrizione

Il `AWSSupport-ConfigureDNSQueryLogging` runbook configura la registrazione per le query DNS che provengono dal tuo cloud privato virtuale (VPC) o per le zone ospitate di Amazon Route 53. Puoi scegliere di pubblicare i log delle query su Amazon Logs, Amazon CloudWatch Simple Storage Service (Amazon S3) o Amazon Data Firehose. [Per ulteriori informazioni sulla registrazione delle query e sui log delle query con resolver, consulta Public DNS query logging e Resolver query logging.](#)

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- LogDestinationArn

Tipo: stringa

Descrizione: (Facoltativo) L'ARN del gruppo CloudWatch Logs, del bucket Amazon S3 o dello stream Firehose a cui desideri inviare i log delle query. Tieni presente che la registrazione delle query DNS pubbliche di Route 53 supporta solo i gruppi Logs. CloudWatch Se non si specifica un valore per questo parametro, l'automazione crea un gruppo CloudWatch Logs con il formato `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID }` e una policy delle risorse IAM per pubblicare i log delle query. Il gruppo CloudWatch Logs creato dall'automazione ha un periodo di conservazione di 14 giorni.

- QueryLogType

Tipo: stringa

Descrizione: (Facoltativo) I tipi di interrogazioni che si desidera registrare.

Valori validi: Public | Resolver/Private

Predefinito: pubblico

- ResourceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della risorsa di cui desideri registrare le interrogazioni. Se si specifica Public il QueryLogType parametro, la risorsa deve essere l'ID di una zona ospitata privata sulla Route 53. Se si specifica Resolver/Private il QueryLogType parametro, la risorsa deve essere l'ID di un VPC.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Fasi del documento

- `aws:executeScript`- Verifica l'esistenza della risorsa specificata per il `ResourceId` parametro e verifica se il tipo di risorsa corrisponde all'opzione `richiestaQueryLogType`.
- `aws:executeScript`- Verifica che il valore specificato per il `LogDestinationArn` parametro corrisponda a quello richiesto. `QueryLogType`

- `aws:executeScript`- Verifica le autorizzazioni richieste a Route 53 per pubblicare i log nel gruppo di log CloudWatch Logs e crea la politica delle risorse IAM richiesta se non esiste.
- `aws:executeScript`- Abilita la registrazione delle query DNS sulla destinazione selezionata.

AWSSupport-ConfigureTrafficMirroring

Descrizione

Il `AWSSupport-ConfigureTrafficMirroring` runbook configura il mirroring del traffico per aiutarti a risolvere i problemi di connettività tra un sistema di bilanciamento del carico e le istanze Amazon Elastic Compute Cloud (Amazon). EC2 Il mirroring del traffico copia il traffico in entrata e in uscita dalle interfacce di rete collegate alle istanze. Per configurare il mirroring del traffico, questo runbook crea gli obiettivi, i filtri e le sessioni richiesti. Per impostazione predefinita, il runbook configura il mirroring per tutto il traffico in entrata e in uscita per tutti i protocolli tranne Amazon DNS. Se desideri rispecchiare il traffico proveniente da fonti e destinazioni specifiche, puoi modificare le regole in entrata e in uscita dopo il completamento dell'automazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- Fonte ENI

Tipo: stringa

Descrizione: (Obbligatorio) L'interfaccia elastica di rete per cui desideri configurare il mirroring del traffico.

- Target

Tipo: stringa

Descrizione: (Obbligatorio) La destinazione per il traffico rispecchiato. È necessario specificare l'ID di un'interfaccia di rete, un Network Load Balancer o un endpoint Gateway Load Balancer. Se si specifica un Network Load Balancer, devono essere presenti listener UDP sulla porta 4789.

- SessionNumber

Tipo: stringa

Valori validi: 1-32766

Descrizione: (Obbligatorio) Il numero della sessione mirror che desideri utilizzare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ec2:CreateTrafficMirrorTarget`
- `ec2:CreateTrafficMirrorFilter`
- `ec2:CreateTrafficMirrorFilterRule`
- `ec2:CreateTrafficMirrorSession`
- `ec2>DeleteTrafficMirrorSession`
- `ec2>DeleteTrafficMirrorFilter`
- `ec2>DeleteTrafficMirrorSession`
- `ec2>DeleteTrafficMirrorFilterRule`
- `iam:ListRoles`
- `ssm:GetAutomationExecution`

- `ssm:StartAutomationExecution`

Fasi del documento

- `aws:executeScript`- Esegue uno script per creare un obiettivo.
- `aws:executeAwsApi`- Crea una regola di filtro.
- `aws:executeAwsApi`- Crea una regola di filtro speculare per tutto il traffico in entrata.
- `aws:executeAwsApi`- Crea una regola di filtro speculare per tutto il traffico in uscita.
- `aws:executeAwsApi`- Crea una sessione mirror sul traffico.
- `aws:executeAwsApi`- Elimina il filtro se la creazione del filtro o della sessione fallisce.
- `aws:executeAwsApi`- Elimina la destinazione se la creazione del filtro o della sessione fallisce.

Output

`CreateFilter.FilterId`

`CreateSession.SessionId`

`CreateTarget.Obiettivo IDOutput`

AWSSupport-ConnectivityTroubleshooter

Descrizione

Il `AWSSupport-ConnectivityTroubleshooter` runbook diagnostica i problemi di connettività tra i seguenti:

- AWS risorse all'interno di un Amazon Virtual Private Cloud (Amazon VPC)
- AWS risorse in diversi Amazon VPCs all'interno dello stesso Regione AWS che sono collegate tramite peering VPC
- AWS risorse in un Amazon VPC e una risorsa Internet che utilizza un gateway Internet
- AWS risorse in un Amazon VPC e una risorsa Internet che utilizza un gateway NAT (Network Address Translation)

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- IP di destinazione

Tipo: stringa

Descrizione: (Obbligatorio) L' IPv4 indirizzo della risorsa a cui desideri connetterti.

- DestinationPort

Tipo: stringa

Impostazione predefinita: true

Descrizione: (Obbligatorio) Il numero di porta a cui vuoi connetterti sulla risorsa di destinazione.

- DestinationVpc

Tipo: stringa

Predefinito: Tutto

Descrizione: (Facoltativo) L'ID dell'Amazon VPC a cui desideri testare la connettività.

- SourceIP

Tipo: stringa

Descrizione: (Obbligatorio) L' IPv4 indirizzo privato della AWS risorsa nel tuo Amazon VPC da cui desideri testare la connettività.

- SourcePortRange

Tipo: stringa

Descrizione: (Facoltativo) L'intervallo di porte utilizzato dalla AWS risorsa nel tuo Amazon VPC da cui desideri testare la connettività.

- SourceVpc

Tipo: stringa

Impostazione predefinita: Tutte

Descrizione: (Facoltativo) L'ID dell'Amazon VPC da cui desideri testare la connettività.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcPeeringConnections

Fasi del documento

- aws:executeScript- Raccoglie dettagli sulla AWS risorsa specificata nel SourceIP parametro.
- aws:executeScript- Determina la destinazione del traffico di rete proveniente dalla AWS risorsa utilizzando le rotte raccolte nel passaggio precedente.
- aws:branch- Filiali in base alla destinazione del traffico di rete.

- `aws:executeAwsApi`- Raccoglie dettagli sulla risorsa di destinazione.
- `aws:executeScript`- Conferma che l'ID restituito per l'Amazon VPC di destinazione corrisponde all'eventuale valore specificato nel `DestinationVpc` parametro.
- `aws:executeAwsApi`- Raccoglie le regole del gruppo di sicurezza per le risorse di origine e di destinazione.
- `aws:executeScript`- Conferma se le regole del gruppo di sicurezza consentono il traffico necessario tra le risorse di origine e di destinazione.
- `aws:executeAwsApi`- Raccoglie gli elenchi di controllo degli accessi alla rete (NACLs) associati alle sottoreti per le risorse di origine e di destinazione.
- `aws:executeScript`- Conferma se NACLs consente il traffico necessario tra le risorse di origine e di destinazione.
- `aws:executeScript`- Conferma se la sorgente ha un indirizzo IP pubblico associato alla risorsa, se la destinazione del percorso è un gateway Internet.
- `aws:executeAwsApi`- Raccoglie le regole del gruppo di sicurezza per la risorsa di origine.
- `aws:executeScript`- Conferma se le regole del gruppo di sicurezza consentono il traffico necessario dalla risorsa di origine alla risorsa di destinazione.
- `aws:executeAwsApi`- Raccoglie i dati NACLs associati alla sottorete per la risorsa di origine.
- `aws:executeScript`- Conferma se NACLs consente il traffico necessario dalla risorsa di origine.
- `aws:executeAwsApi`- Raccoglie dettagli sul gateway NAT.
- `aws:executeAwsApi`- Raccoglie i dati NACLs associati alla sottorete per il gateway NAT.
- `aws:executeScript`- Conferma se NACLs consente il traffico necessario dalla sottorete per il gateway NAT.
- `aws:executeScript`- Raccoglie le rotte associate alla sottorete per il gateway NAT.
- `aws:executeScript`- Conferma se il gateway NAT dispone di un percorso verso un gateway Internet.
- `aws:executeAwsApi`- Raccoglie dettagli sulla connessione peering VPC.
- `aws:executeScript`- Conferma che entrambi VPCs si trovano nella stessa regione e che l'ID restituito per il VPC di destinazione corrisponde al valore specificato, se presente, nel `DestinationVpc` parametro.
- `aws:executeAwsApi`- Restituisce la sottorete della risorsa di destinazione.
- `aws:executeScript`- Raccoglie i percorsi associati alla sottorete per il VPC peerizzato.

- `aws:executeScript`- Conferma se il VPC peered ha un percorso verso la connessione peering.
- `aws:executeScript`- Conferma se il traffico è consentito dalla risorsa di origine se la destinazione non è supportata dall'automazione.

AWSSupport-TroubleshootVPN

Descrizione

Il `AWSSupport-TroubleshootVPN` runbook consente di tracciare e risolvere gli errori in una AWS Site-to-Site VPN connessione. L'automazione include diversi controlli automatici progettati per tracciare IKEv2 gli errori IKEv1 relativi ai tunnel di AWS Site-to-Site VPN connessione. L'automazione cerca di individuare errori specifici e la relativa risoluzione forma un elenco di problemi comuni.

Nota: questa automazione non corregge gli errori. Viene eseguito per l'intervallo di tempo indicato e analizza il gruppo di log alla ricerca di errori nel gruppo di [CloudWatch log VPN](#).

Come funziona?

Il runbook esegue una convalida dei parametri per confermare se il gruppo di CloudWatch log Amazon incluso nel parametro di input esiste, se nel gruppo di log sono presenti flussi di log che corrispondono al logging del tunnel VPN, se esiste un ID di connessione VPN e se esiste l'indirizzo IP del tunnel. Effettua chiamate API Logs Insights sul tuo gruppo di CloudWatch log configurate per la registrazione VPN.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- LogGroupName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del gruppo di CloudWatch log Amazon configurato per la registrazione delle AWS Site-to-Site VPN connessioni

Modello consentito: `^[\\.\-_/#A-Za-z0-9]{1,512}`

- VpnConnectionId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID di AWS Site-to-Site VPN connessione da risolvere.

Modello consentito: `^vpn-[0-9a-f]{8,17}$`

- Tunnel AIPAddress

Tipo: stringa

Descrizione: (Obbligatorio) L'IPv4 indirizzo numero 1 del tunnel associato al tuo AWS Site-to-Site VPN.

Modello consentito: `^((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

Tipo: stringa

Descrizione: (Facoltativo) L'IPv4 indirizzo del tunnel numero 2 associato al tuo AWS Site-to-Site VPN.

Modello consentito: `^((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

Tipo: stringa

Descrizione: (Obbligatorio) Seleziona la versione IKE che stai utilizzando. Valori consentiti: IKEv1, IKEv2

Valori validi: ['IKEv1' , 'IKEv2']

- StartTimeinEpoch

Tipo: stringa

Descrizione: (Facoltativo) Ora di inizio dell'analisi del registro. È possibile utilizzare StartTimeinEpoch/EndTimeinEpoch o LookBackPeriod per l'analisi dei log

Modello consentito: ^\d{10} | ^\$

- EndTimeinEpoch

Tipo: stringa

Descrizione: (Facoltativo) Ora di fine dell'analisi dei log. È possibile utilizzare StartTimeinEpoch/EndTimeinEpoch o LookBackPeriod per l'analisi dei log. Se vengono dati entrambi StartTimeinEpoch/EndTimeinEpoch e LookBackPeriod allora hanno la LookBackPeriod precedenza

Modello consentito: ^\d{10} | ^\$

- LookBackPeriod

Tipo: stringa

Descrizione: (Facoltativo) Tempo a due cifre in ore per esaminare l'analisi dei log. Intervallo valido: 01 - 99. Questo valore ha la precedenza se dai StartTimeinEpoch anche e EndTime

Modello consentito: ^(\d?[1-9] | [1-9]0) | ^\$

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`
- `ec2:DescribeVpnConnections`

Istruzioni

Nota: questa automazione funziona sui gruppi di CloudWatch log configurati per la registrazione del tunnel VPN, quando il formato di output della registrazione è JSON.

Segui questi passaggi per configurare l'automazione:

1. Passa a [AWSSupport-TroubleshootVPN](#) nella AWS Systems Manager console.
2. Per i parametri di input, inserisci quanto segue:

- `AutomationAssumeRole` (Facoltativo):

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `LogGroupName` (Obbligatorio):

Il nome del gruppo di CloudWatch log Amazon da convalidare. Questo deve essere il gruppo di CloudWatch log configurato per l'invio dei log da parte della VPN.

- `VpnConnectionId` (Obbligatorio):

L'ID di AWS Site-to-Site VPN connessione il cui gruppo di log viene tracciato per rilevare eventuali errori VPN.

- `Tunnel AIPAddress` (richiesto):

Il tunnel Un indirizzo IP associato alla AWS Site-to-Site VPN connessione.

- `Tunnel BIPAddress` (opzionale):

L'indirizzo IP B del tunnel associato alla AWS Site-to-Site VPN connessione.

- `IKEVersion` (Obbligatorio):

Seleziona quello IKEVersion che stai usando. Valori consentiti: IKEv1, IKEv2.

- StartTimeinEpoch (Facoltativo):

L'inizio dell'intervallo di tempo in cui eseguire la ricerca di errori. L'intervallo è inclusivo, quindi l'ora di inizio specificata viene inclusa nella query. Specificato come ora dell'epoca, il numero di secondi trascorsi dal 1° gennaio 1970, 00:00:00 UTC.

- EndTimeinEpoch (Facoltativo):

La fine dell'intervallo di tempo in cui eseguire la ricerca di errori. L'intervallo è inclusivo, quindi l'ora di fine specificata viene inclusa nella query. Specificato come ora dell'epoca, il numero di secondi trascorsi dal 1° gennaio 1970, 00:00:00 UTC.

- LookBackPeriod (Obbligatorio):

Tempo, espresso in ore, per verificare la presenza di errori nella ricerca di errori.

Nota: configura un StartTimeinEpoch EndTimeinEpoch, o fissa LookBackPeriod l'intervallo di tempo per l'analisi dei log. Fornisci un numero a due cifre in ore per verificare la presenza di errori passati dall'ora di inizio dell'automazione. Oppure, se l'errore riguarda il passato e rientra in un intervallo di tempo specifico, includi StartTimeinEpoch e EndTimeinEpoch, invece di.

LookBackPeriod

Input parameters	
AutomationAssumeRole (Optional) The ARN of the role that allows Automation to perform the actions on your behalf. Choose an option	LogGroupName (Required) The Amazon CloudWatch log group name to be validated. This must be the CloudWatch log group which is destined for VPN logs vpnlog
VpnConnectionId (Required) The AWS Site-to-Site VPN connection id to be validated. vpn-123abc456zxc	Tunnel1IPAddress (Required) The tunnel number 1 IP address associated with your AWS Site-to-Site VPN to be validated. 1.1.1.1
Tunnel2IPAddress (Optional) The tunnel number 2 IP address associated with your AWS Site-to-Site VPN to be validated. String	IKEVersion (Required) Select what IKE Version you are using. Allowed values : IKEv1, IKEv2 or both IKEv1
StartTimeEpoch (Optional) Start time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis String	EndTimeEpoch (Optional) End time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis String
LookBackPeriod (Required) Time in hours to look back for log analysis 05	

3. Seleziona Esegui.

4. L'automazione si avvia.

5. Il runbook di automazione esegue i seguenti passaggi:

- Convalida dei parametri:

Esegue una serie di convalide sui parametri di input inclusi nell'automazione.

- branchOnValidationOfLogGroup:

Verifica se il gruppo di log menzionato nel parametro è valido. Se non è valido, interrompe l'ulteriore avvio delle fasi di automazione.

- `branchOnValidationOfLogStream`:

Verifica se il flusso di log esiste nel gruppo di log incluso. CloudWatch Se non è valido, interrompe l'ulteriore avvio delle fasi di automazione.

- `branchOnValidationOfVpnConnectionId`:

Verifica se la connessione VPN inclusa nel parametro è valida. Se non è valido, interrompe l'ulteriore avvio delle fasi di automazione.

- `branchOnValidationOfVpnIp`:

Verifica se l'indirizzo IP del tunnel menzionato nel parametro è valido o meno. Se non è valido, interrompe l'ulteriore esecuzione delle fasi di automazione.

- `TraceError`:

Effettua una chiamata all'API Logs Insight nel gruppo di CloudWatch log incluso e cerca l'errore relativo a IKEv1/IKEv2 insieme a una relativa risoluzione suggerita.

6. Al termine, consulta la sezione Output per i risultati dettagliati dell'esecuzione.

▼ Outputs

parameterValidation.LogGroupName LogGroupValid	parameterValidation.LogStream validLogStream
parameterValidation.VpnConnection validVpnConnection	parameterValidation.VpnIpAddress validVpnIP
traceError.TunnelIkeV2 {"IkeV2ErrorCount":0}	traceError.TunnelIkeV1 {"IkeV1ErrorCount":0}
traceError.TunnelIkeV2 {"IkeV2ErrorCount":0}	
traceError.TunnelIkeV1 {"Error related to : AWS tunnel received DELETE for Phase 2 SA":" Please treat below as Potential resolution of this error : AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent Delete_SA message for Phase 2. When AWS receives Delete_SA for Phase 2 from CGW it deletes the Phase 2 of SPI mentioned in Delete_SA request. Possible reason of CGW sending Delete_SA message can be due to any configurational changes made in CGW side Next Steps: * Check IPsec Logs on the CGW Device to verify if you are able to see information pertaining to this issue. References: [1] Tunnel stability issues during a rekey: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-flx-ikev2-tunnel-instability-rekey/ [2] Phase 2 Troubleshooting: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-phase-2-issues/ ","Error related to : AWS tunnel received DELETE for IKE SA from CGW":" Please treat below as Potential resolution of this error : AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent the Delete_SA message for Parent/IKE_SA. When AWS receives Delete_SA from CGW, it honours the message and brings down the VPN tunnel. There can be various reasons for CGW sending Delete_SA message like : * A reset to clear active SAs has been performed on the CGW side * IKE SA has been timed out * Configurational changes have been made on CGW Next Steps: * Review your VPN device idle timeout settings using information from your device vendor. When there is no traffic through a VPN tunnel for the duration of your vendor-specific VPN idle time, the IPsec session terminates. For more information on tunnel inactivity and instability refer to this documentation [1] * Check logs on your CGW device to verify if you are able to see information pertaining to this issue. References: [1] Tunnel inactivity or instability: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-instability-inactivity/ ","Error related to : No proposal chosen":" Please treat below as Potential resolution of this error : AWS CloudWatch monitoring has detected that IKE Phase 2 parameters (such as encryption algorithm, hashing algorithm and DH group) configured on Customer Gateway (CGW) device and AWS VPN endpoint do not match or the CGW is using parameters that are not supported by the AWS VPN. Next Steps: * Verify that the Phase 2 parameters (Integrity algorithm, Encryption algorithm and DH group) being proposed by CGW are matching with those configured on AWS side. If you are using default settings on AWS side then verify that parameters being proposed are supported by AWS VPN. To Find list of parameters supported by * If you want to modify the parameters on the AWS VPN side you can follow below steps: Step 1: Open the Amazon VPC console at https://console.aws.amazon.com/vpc/ Step 2: In the navigation pane, choose Site-to-Site VPN Connections. Step 3: Select the Site-to-Site VPN connection, and choose Actions, Modify VPN Tunnel Options. Step 4: For VPN Tunnel Outside IP Address, choose the tunnel endpoint IP of the VPN tunnel that you are modifying options for. Step 5: Choose or enter new values for the tunnel options . Step 6: Choose Save.	

Riferimenti

Systems Manager Automation

- [Esegui questa automazione \(console\)](#)
- [Esegui un'automazione](#)
- [Configurazione di un'automazione](#)
- [Pagina iniziale Support Automation Workflows](#)

AWS documentazione di servizio

- [Contenuto dei log Site-to-Site VPN](#)

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Descrizione

Il AWSConfigRemediation-DeleteEgressOnlyInternetGateway runbook elimina il gateway Internet di sola uscita specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- EgressOnlyInternetGatewayId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gateway Internet di sola uscita che desideri eliminare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteEgressOnlyInternetGateway
- ec2:DescribeEgressOnlyInternetGateways

Fasi del documento

- aws:executeScript- Elimina il gateway Internet di sola uscita specificato nel parametro. EgressOnlyInternetGatewayId
- aws:executeScript- Verifica che il gateway Internet di sola uscita sia stato eliminato.

AWSConfigRemediation-DeleteUnusedENI

Descrizione

Il AWSConfigRemediation-DeleteUnusedENI runbook elimina un'elastic network interface (ENI) con uno stato di allegato pari a. detached

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- NetworkInterfaceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ENI che desideri eliminare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces

Fasi del documento

- aws:executeAwsApi- Elimina l'ENI specificato nel parametro. NetworkInterfaceId
- aws:executeScript- Verifica che l'ENI sia stato eliminato.

AWSConfigRemediation-DeleteUnusedSecurityGroup

Descrizione

Il `AWSConfigRemediation-DeleteUnusedSecurityGroup` runbook elimina il gruppo di sicurezza specificato nel `GroupId` parametro. Se tenti di eliminare un gruppo di sicurezza associato a un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o a cui fa riferimento un altro gruppo di sicurezza, l'automazione fallisce. Questa automazione non elimina un gruppo di sicurezza predefinito.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- GroupId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza che desideri eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

Fasi del documento

- `aws:executeAwsApi`- Restituisce il nome del gruppo di sicurezza utilizzando il valore fornito nel `GroupId` parametro.
- `aws:branch`- Conferma che il nome del gruppo non è «predefinito».
- `aws:executeAwsApi`- Elimina il gruppo di sicurezza specificato nel `GroupId` parametro.
- `aws:executeScript`- Conferma che il gruppo di sicurezza è stato eliminato.

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

Descrizione

Il `AWSConfigRemediation-DeleteUnusedVPCNetworkACL` runbook elimina una lista di controllo dell'accesso alla rete (ACL) che non è associata a una sottorete.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- NetworkAcId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ACL di rete che desideri eliminare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkAcl
- ec2:DescribeNetworkAcls

Fasi del documento

- aws:executeAwsApi- Elimina l'ACL di rete specificato nel parametro. NetworkAclId
- aws:executeScript- Conferma che l'ACL di rete specificato nel NetworkAclId parametro è stato eliminato.

AWSConfigRemediation-DeleteVPCFlowLog

Descrizione

Il AWSConfigRemediation-DeleteVPCFlowLog runbook elimina il log di flusso del cloud privato virtuale (VPC) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- FlowLogId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del log di flusso che desideri eliminare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2>DeleteFlowLogs
- ec2:DescribeFlowLogs

Fasi del documento

- aws:executeAwsApi- Elimina il log di flusso specificato nel FlowLogId parametro.
- aws:executeScript- Verifica che il log di flusso sia stato eliminato.

AWSConfigRemediation-DetachAndDeleteInternetGateway

Descrizione

Il AWSConfigRemediation-DetachAndDeleteInternetGateway runbook scollega ed elimina il gateway Internet specificato. Se EC2 alcune istanze Amazon nel tuo cloud privato virtuale (VPC) hanno indirizzi IP elastici o indirizzi IPv4 pubblici associati, il runbook fallisce.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- InternetGatewayId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gateway Internet che desideri eliminare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

Fasi del documento

- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà di stato del gateway privato virtuale cambi `available` o `scada`.
- `aws:executeAwsApi`- Recupera una configurazione di gateway privato virtuale specificata.
- `aws:branch`- Rami basati sul `VpcAttachments` valore del parametro `.state`.
- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà `VpcAttachments .state` del gateway privato virtuale cambi `attached` o `scada`.
- `aws:executeAwsApi`- Accetta l'ID del gateway privato virtuale e l'ID di Amazon VPC come input e scollega il gateway privato virtuale da Amazon VPC.
- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la `VpcAttachments` proprietà `.state` del gateway privato virtuale cambi o `scada`. `detached`
- `aws:executeAwsApi`- Accetta l'ID del gateway privato virtuale come input e lo elimina.
- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale come input e ne verifica l'eliminazione.
- `aws:executeAwsApi`- Raccoglie l'ID VPC dall'ID del gateway Internet.
- `aws:executeAwsApi`- Rimuove l'ID del gateway Internet dal VPC.
- `aws:executeAwsApi`- Elimina il gateway Internet.

AWSConfigRemediation- DetachAndDeleteVirtualPrivateGateway

Descrizione

Il `AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` runbook scollega ed elimina un determinato gateway privato virtuale Amazon Elastic Compute Cloud (Amazon EC2) collegato a un cloud privato virtuale (VPC) creato con Amazon Virtual Private Cloud (Amazon VPC).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `VpnGatewayId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gateway privato virtuale da eliminare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2>DeleteVpnGateway`

- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

Fasi del documento

- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà di stato del gateway privato virtuale cambi `available` o `scada`.
- `aws:executeAwsApi`- Recupera una configurazione di gateway privato virtuale specificata.
- `aws:branch`- Rami basati sul `VpcAttachments` valore del parametro `.state`.
- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la proprietà `VpcAttachments .state` del gateway privato virtuale cambi `attached` o `scada`.
- `aws:executeAwsApi`- Accetta l'ID del gateway privato virtuale e l'ID di Amazon VPC come input e scollega il gateway privato virtuale da Amazon VPC.
- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale e attende che la `VpcAttachments` proprietà `.state` del gateway privato virtuale cambi o `scada`. `detached`
- `aws:executeAwsApi`- Accetta l'ID del gateway privato virtuale come input e lo elimina.
- `aws:waitForAwsResourceProperty`- Accetta l'ID del gateway privato virtuale come input e ne verifica l'eliminazione.

AWS-DisableIncomingSSHOnPort22

Descrizione

Il `AWS-DisableIncomingSSHOnPort22` runbook rimuove le regole che consentono il traffico SSH in entrata senza restrizioni sulla porta TCP 22 per i gruppi di sicurezza.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- SecurityGroupIds

Tipo: stringa

Descrizione: (Obbligatorio) Un elenco separato da virgole IDs dei gruppi di sicurezza per i quali si desidera limitare il traffico SSH.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupIngress

Fasi del documento

- aws:executeAwsApi- Rimuove tutte le regole che consentono il traffico SSH in entrata sulla porta TCP 22 dai gruppi di sicurezza specificati nel parametro. SecurityGroupIds

Output

DisableIncomingSSTemplate. RestrictedSecurityGroupIds - Un elenco dei gruppi IDs di sicurezza a cui sono state rimosse le regole SSH in entrata.

AWS-DisablePublicAccessForSecurityGroup

Descrizione

Questo runbook disabilita le porte SSH e RDP predefinite aperte a tutti gli indirizzi IP.

Important

Questo runbook fallisce con un `"InvalidPermission NotFound"` errore per i gruppi di sicurezza che soddisfano entrambi i seguenti criteri: 1) Il gruppo di sicurezza si trova in un VPC non predefinito; e 2) Le regole in entrata per il gruppo di sicurezza non specificano le porte aperte utilizzando tutti e quattro i seguenti schemi:

- `0.0.0.0/0`
- `::/0`
- `SSH or RDP port + 0.0.0.0/0`
- `SSH or RDP port + ::/0`

Note

Questo runbook non è disponibile Regioni AWS in Cina.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- GroupId

Tipo: stringa

Descrizione: (obbligatorio) ID del gruppo di sicurezza per il quale dovrebbero essere disabilitate le porte.

- IpAddressToBlock

Tipo: stringa

Descrizione: (Facoltativo) IPv4 Indirizzi aggiuntivi da cui bloccare l'accesso, nel formato. 1.2.3.4/32

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Descrizione

Il AWSConfigRemediation-DisableSubnetAutoAssignPublicIP runbook disabilita l'attributo IPv4 public address per la sottorete specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- SubnetId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della sottorete su cui si desidera disabilitare l'attributo di assegnazione automatica dell' IPv4 indirizzo pubblico.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSubnets
- ec2:ModifySubnetAttribute

Fasi del documento

- aws:executeAwsApi- Disattiva l'attributo di IPv4 indirizzo pubblico di assegnazione automatica per la sottorete specificata nel parametro. SubnetId
- aws:assertAwsResourceProperty- Verifica che l'attributo sia stato disabilitato.

AWSSupport-EnableVPCFlowLogs

Descrizione

Il AWSSupport-EnableVPCFlowLogs runbook crea log di flusso di Amazon Virtual Private Cloud (Amazon VPC) per sottoreti, interfacce di rete e nel tuo. VPCs Account AWS Se crei un log di flusso

per una sottorete o un VPC, viene monitorata ogni interfaccia di rete elastica in quella sottorete o Amazon VPC. I dati del log di flusso vengono pubblicati nel gruppo di log Amazon CloudWatch Logs o nel bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente. Per ulteriori informazioni sui log di flusso, consulta [VPC Flow Logs nella Amazon VPC User Guide](#).

 Important

I costi di inserimento e archiviazione dei dati per i log venduti si applicano quando si pubblicano i log di flusso su Logs CloudWatch o su Amazon S3. [Per ulteriori informazioni, consulta i prezzi di Flow Logs](#)

[Esegui questa automazione \(console\)](#)

 Note

Quando selezioni s3 come destinazione del log, assicurati che la policy del bucket consenta al servizio di consegna dei log di accedere al bucket. Per ulteriori informazioni, consulta le [autorizzazioni del bucket Amazon S3](#) per i log di flusso.

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux, macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- DeliverLogsPermissionArn

Tipo: stringa

Descrizione: (Facoltativo) L'ARN per il ruolo IAM che consente ad Amazon Elastic Compute Cloud (EC2Amazon) di pubblicare i log di flusso nel gruppo di log Logs CloudWatch del tuo account. Se specifichi il LogDestinationType parametro, non fornire un valore s3 per questo parametro. Per ulteriori informazioni, consulta [Publish flow logs to CloudWatch Logs](#) nella Amazon VPC User Guide.

- LogDestinationARN

Tipo: stringa

Descrizione: (Facoltativo) L'ARN della risorsa in cui vengono pubblicati i dati del log di flusso. Se cloud-watch-logs è specificato per il LogDestinationType parametro, fornisci l'ARN del gruppo di log CloudWatch Logs in cui desideri pubblicare i dati del log di flusso. In alternativa, utilizza LogGroupName. Se s3 è specificato per il LogDestinationType parametro, è necessario specificare l'ARN del bucket Amazon S3 in cui si desidera pubblicare i dati del log di flusso per questo parametro. Puoi anche specificare una cartella nel bucket.

 Important

Quando scegli s3 come bucket, assicurati che il bucket selezionato segua le [best practice di sicurezza di Amazon S3 Bucket](#) e che rispetti le leggi sulla privacy dei dati per la tua organizzazione e area geografica. LogDestinationType

- LogDestinationType

Tipo: stringa

Valori validi: | s3 cloud-watch-logs

Descrizione: (Obbligatorio) Determina dove vengono pubblicati i dati del log di flusso. Se specificate LogDestinationType ass3, non specificate DeliverLogsPermissionArn o LogGroupName.

- LogFormat

Tipo: stringa

Descrizione: (Facoltativo) I campi da includere nel log di flusso e l'ordine in cui devono apparire nel record. Per un elenco dei campi disponibili, consulta [Flow log records](#) nella Amazon VPC User Guide. Se non fornisci un valore per questo parametro, il log di flusso viene creato utilizzando il formato predefinito. Se specifichi questo parametro, è necessario specificare almeno un campo.

- LogGroupName

Tipo: stringa

Descrizione: (Facoltativo) Il nome del gruppo di log CloudWatch Logs in cui vengono pubblicati i dati del log di flusso. Se si specifica s3 il LogDestinationType parametro, non fornire un valore per questo parametro.

- ResourceIds

Tipo: StringList

Descrizione: (Obbligatorio) Un elenco separato da virgole delle IDs sottoreti, delle interfacce di rete elastiche o del VPC per cui si desidera creare un log di flusso.

- TrafficType

Tipo: stringa

Valori validi: ACCEPT | REJECT | ALL

Descrizione: (Obbligatorio) Il tipo di traffico da registrare. Puoi registrare il traffico che la risorsa accetta o rifiuta oppure tutto il traffico.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- 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`

Politica di esempio

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



```

    "Statement": [
      {
        "Sid": "SSM Execution Permissions",
        "Effect": "Allow",
        "Action": [
          "ssm:StartAutomationExecution",
          "ssm:GetAutomationExecution"
        ],
        "Resource": "*"
      },
      {
        "Sid": "EC2 FlowLogs Permissions",
        "Effect": "Allow",
        "Action": [
          "ec2:CreateFlowLogs",
          "ec2>DeleteFlowLogs",
          "ec2:DescribeFlowLogs"
        ],
        "Resource": "arn:{partition}:ec2:{region}:{account-id}:{instance|
subnet|vpc|transit-gateway|transit-gateway-attachment}/{resource ID}"
      },
      {
        "Sid": "IAM CreateRole Permissions",
        "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:{partition}:iam::{account-id}:role/{role name}",
          "arn:{partition}:iam::{account-id}:role/
AWSsupportCreateFlowLogsRole"
        ]
      }
    ],

```

```

        {
            "Sid": "CloudWatch Logs Permissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:CreateLogGroup",
                "logs>DeleteLogDelivery",
                "logs>DeleteLogGroup",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams"
            ],
            "Resource": [
                "arn:{partition}:logs:{region}:{account-id}:log-group:{log
group name}",
                "arn:{partition}:logs:{region}:{account-id}:log-group:{log
group name}:*"
            ]
        },
        {
            "Sid": "S3 Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketAcl",
                "s3:ListBucket",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:{partition}:s3:::{bucket name}",
                "arn:{partition}:s3:::{bucket name}/*"
            ]
        }
    ]
}

```

Fasi del documento

- `aws:branch`- Rami basati sul valore specificato per il `LogDestinationType` parametro.

- `aws:executeScript`- Verifica se l'Amazon Simple Storage Service (Amazon S3) di destinazione concede potenzialmente l'accesso in lettura o `public` scrittura ai suoi oggetti.
- `aws:executeScript`- Crea un gruppo di log se non viene specificato alcun valore per il `LogDestinationARN` parametro e `cloud-watch-logs` viene specificato per il `LogDestinationType` parametro.
- `aws:executeScript`- Crea registri di flusso in base ai valori specificati nei parametri del runbook.

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

Descrizione

Il `AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch` runbook sostituisce un log di flusso Amazon VPC esistente che pubblica i dati del log di flusso su Amazon Simple Storage Service (Amazon S3) con un log di flusso che pubblica i dati del log di flusso nel gruppo di log Amazon CloudWatch Logs (Logs) specificato. CloudWatch

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `DestinationLogGroup`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del gruppo di log CloudWatch Logs in cui desideri pubblicare i dati del log di flusso.

- DeliverLogsPermissionArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del ruolo AWS Identity and Access Management (IAM) che desideri utilizzare che fornisce ad Amazon Elastic Compute Cloud (Amazon EC2) le autorizzazioni necessarie per pubblicare i dati dei log di flusso su Logs. CloudWatch

- FlowLogId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del log di flusso pubblicato su Amazon S3 che desideri sostituire.

- MaxAggregationInterval

Tipo: integer

Valori validi: 60 | 600

Descrizione: (Facoltativo) L'intervallo di tempo massimo, in secondi, durante il quale un flusso di pacchetti viene acquisito e aggregato in un record del log di flusso.

- TrafficType

Tipo: stringa

Valori validi: ACCEPT | REJECT | ALL

Descrizione: (Obbligatorio) Il tipo di dati del registro di flusso che si desidera registrare e pubblicare.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2>DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie i dettagli sul tuo VPC dal valore specificato nel `FlowLogId` parametro.
- `aws:executeAwsApi`- Crea un log di flusso basato sui valori specificati per i parametri del runbook.
- `aws:assertAwsResourceProperty`- Verifica la pubblicazione del log di flusso appena creato su Logs. CloudWatch
- `aws:executeAwsApi`- Elimina il log di flusso pubblicato su Amazon S3.
- `aws:executeScript`- Conferma che il log di flusso pubblicato su Amazon S3 è stato eliminato.

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

Descrizione

Il `AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket` runbook sostituisce un log di flusso Amazon VPC esistente che pubblica i dati del log di flusso su Amazon CloudWatch Logs (CloudWatch Logs) con un log di flusso che pubblica i dati del log di flusso nel bucket Amazon Simple Storage Service (Amazon S3) specificato dall'utente.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- Destinazioni (3) BucketArn

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del bucket Amazon S3 in cui desideri pubblicare i dati del log di flusso.

- FlowLogId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del log di flusso che viene pubblicato nei log che desideri CloudWatch sostituire.

- MaxAggregationInterval

Tipo: integer

Valori validi: 60 | 600

Descrizione: (Facoltativo) L'intervallo di tempo massimo, in secondi, durante il quale un flusso di pacchetti viene acquisito e aggregato in un record del log di flusso.

- TrafficType

Tipo: stringa

Valori validi: ACCEPT | REJECT | ALL

Descrizione: (Obbligatorio) Il tipo di dati del registro di flusso che si desidera registrare e pubblicare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2>DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie i dettagli sul tuo VPC dal valore specificato nel `FlowLogId` parametro.
- `aws:executeAwsApi`- Crea un log di flusso basato sui valori specificati per i parametri del runbook.
- `aws:assertAwsResourceProperty`- Verifica la pubblicazione del log di flusso appena creato su Amazon S3.
- `aws:executeAwsApi`- Elimina il log di flusso che viene pubblicato su Logs. CloudWatch
- `aws:executeScript`- Conferma che il log di flusso pubblicato su CloudWatch Logs è stato eliminato.

AWS-ReleaseElasticIP

Descrizione

Rilascia l'indirizzo IP elastico specificato utilizzando ID allocazione.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AllocationId

Tipo: stringa

Descrizione: (obbligatorio) l'ID allocazione dell'indirizzo IP elastico.

AWS-RemoveNetworkACLUnrestrictedSSHRDP

Descrizione

Il AWS-RemoveNetworkACLUnrestrictedSSHRDP runbook rimuove tutte le regole dell'elenco di controllo degli accessi alla rete (ACL) dall'ACL di rete specificato che consentono l'ingresso del traffico da tutti gli indirizzi di origine alle porte SSH e RDP predefinite. Le regole che includono intervalli di porte che si sovrappongono alle porte SSH e RDP predefinite non vengono rimosse.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- NetworkAcId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ACL di rete da cui si desidera rimuovere le regole illimitate che consentono l'ingresso del traffico da tutti gli indirizzi di origine alle porte SSH e RDP predefinite.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkAclEntry
- ec2:DescribeNetworkAcls

Fasi del documento

- aws:executeScript- Rimuove tutte le regole di ingresso che consentono il traffico proveniente da tutti gli indirizzi di origine del gruppo di sicurezza specificato nel SecurityGroupId parametro.

Output

RemoveNACLEntriesAndVerify. VerificationMessage - Messaggi di verifica delle regole ACL di rete eliminate con successo.

RemoveNaclEntriesAndVerify. RulesDeletedAndApiResponses - Le regole ACL di rete che sono state eliminate e le risposte operative dell>DeleteNetworkAclEntryAPI.

AWSConfigRemediation- RemoveUnrestrictedSourceIngressRules

Descrizione

Il AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules runbook rimuove tutte le regole di ingresso dal gruppo di sicurezza specificato che consentono il traffico da tutti gli indirizzi di origine.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- SecurityGroupId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza da cui desideri rimuovere le regole di ingresso che consentono il traffico proveniente da tutti gli indirizzi di origine.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Fasi del documento

- `aws:executeScript`- Rimuove tutte le regole di ingresso che consentono il traffico proveniente da tutti gli indirizzi di origine del gruppo di sicurezza specificato nel `SecurityGroupId` parametro.

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

Descrizione

Il `AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` runbook rimuove tutte le regole dal gruppo di sicurezza predefinito del cloud privato virtuale (VPC) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- GroupId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gruppo di sicurezza da cui desideri rimuovere tutte le regole.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

Fasi del documento

- aws:assertAwsResourceProperty- Conferma che il gruppo di sicurezza specificato nel GroupId parametro è denominato default.
- aws:executeScript- Rimuove tutte le regole dal gruppo di sicurezza specificato nel GroupId parametro.

AWSSupport-SetupIPMonitoringFromVPC

Descrizione

AWSSupport-SetupIPMonitoringFromVPC crea un'istanza Amazon Elastic Compute Cloud (Amazon EC2) nella sottorete specificata e monitora la destinazione IPs (IPv4 o IPv6) selezionata eseguendo continuamente test ping, MTR, traceroute e tracertp. I risultati vengono archiviati nei

log di Amazon CloudWatch Logs e vengono applicati filtri metrici per visualizzare rapidamente le statistiche sulla latenza e sulla perdita di pacchetti in una dashboard. CloudWatch

Informazioni aggiuntive

I dati di CloudWatch Logs possono essere utilizzati per la risoluzione dei problemi di rete e l'analisi del raggiungimento di una soglia di latenza. pattern/trends. Additionally, you can configure CloudWatch alarms with Amazon SNS notifications when packet loss and/or I dati possono essere utilizzati anche per aprire un caso Supporto AWS, per aiutare a isolare rapidamente un problema e ridurre i tempi di risoluzione durante l'analisi di un problema di rete.

Note

Per ripulire le risorse create da `AWSSupport-SetupIPMonitoringFromVPC`, puoi usare il runbook. `AWSSupport-TerminateIPMonitoringFromVPC` Per ulteriori informazioni, consulta [AWSSupport-TerminateIPMonitoringFromVPC](#).

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo

conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- CloudWatchLogGroupNamePrefix

Tipo: stringa

Impostazione predefinita: /AWSSupport-SetupIPMonitoringFromVPC

Descrizione: (Facoltativo) Prefisso utilizzato per ogni gruppo di CloudWatch log creato per i risultati del test.

- CloudWatchLogGroupRetentionInDays

Tipo: stringa

Valori validi: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

Impostazione predefinita: 7

Descrizione: (facoltativo) numero di giorni che definisce l'intervallo di tempo durante il quale si desidera conservare i risultati del monitoraggio della rete.

- InstanceType

Tipo: stringa

Valori validi: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

Predefinito: t3.micro

Descrizione: (Facoltativo) Il tipo di EC2 istanza per l'istanza EC2 Rescue. Dimensione consigliata: t3.micro.

- SubnetId

Tipo: stringa

Descrizione: (obbligatorio) ID sottorete dell'istanza di monitoraggio. Tieni presente che se specifichi una sottorete privata, devi assicurarti che sia disponibile l'accesso a Internet per consentire all'istanza di monitoraggio di configurare il test (ovvero installare l'agente CloudWatch Logs, interagire con Systems Manager e CloudWatch).

- Obiettivo IPs

Tipo: stringa

Descrizione: (Obbligatorio) Elenco separato da virgole di IPv4s e/o IPv6s da monitorare. Gli spazi non sono consentiti. La dimensione massima è pari a 255 caratteri. Se si specifica un indirizzo IP non valido, l'automazione avrà esito negativo e verrà eseguito il rollback della configurazione dei test.

- `TestInstanceSecurityGroupId`

Tipo: stringa

Descrizione: (Facoltativo) L'ID del gruppo di sicurezza per l'istanza di test. Se non viene specificato, l'automazione ne crea uno durante la creazione dell'istanza. Assicurati che il gruppo di sicurezza consenta l'accesso in uscita al monitoraggio IPs.

- `TestInstanceProfileName`

Tipo: stringa

Descrizione: (Facoltativo) Il nome di un profilo di istanza IAM esistente per l'istanza di test. Se non viene specificato, l'automazione ne crea uno durante la creazione dell'istanza. Il ruolo deve avere le seguenti autorizzazioni: `logs:CreateLogStream`, `logs:DescribeLogGroups`, `logs:DescribeLogStreams`, `logs:PutLogEvents` e la AWS Managed Policy `AmazonSSMManagedInstanceCore`.

- `TestInterval`

Tipo: stringa

Descrizione: (Facoltativo) Il numero di minuti tra gli intervalli di test. Il valore predefinito è 1 minuto e il massimo è 10 minuti.

- `RetainDashboardAndLogsOnDeletion`

Tipo: stringa

Descrizione: (Facoltativo) `False` Specificare di eliminare la CloudWatch dashboard e i log di Amazon quando si elimina lo stack CloudFormation AWS. Il valore predefinito è `True`. Per impostazione predefinita, la dashboard e i log vengono conservati e dovranno essere eliminati manualmente quando non sono più necessari.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

 Warning

Si consiglia di passare `TestInstanceProfileName` parametri o garantire l'esistenza di protezioni di sicurezza per prevenire l'uso improprio delle autorizzazioni IAM mutabili.

Si consiglia di allegare all'utente che esegue l'automazione la policy gestita di Amazon SSMAutomation Role IAM. L'utente deve inoltre disporre della seguente policy associata al proprio account utente, gruppo o ruolo:

```
{
  "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:<partition>:iam:<account-id>:role/SetupIPMonitoringFromVPC*",
        "arn:<partition>:iam:<account-id>: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"
      }
    ]
  }
```

Se viene fornito il `TestInstanceProfileName` parametro, non sono necessarie le seguenti autorizzazioni IAM per eseguire il runbook:

- sono: `CreateRole`
- lo sono: `CreateInstanceProfile`
- lo sono: `DetachRolePolicy`
- lo sono: `AttachRolePolicy`
- lo sono: `AddRoleToInstanceProfile`
- lo sono: `RemoveRoleFromInstanceProfile`
- lo sono: `DeleteRole`
- lo sono: `DeleteRolePolicy`
- lo sono: `DeleteInstanceProfile`

Fasi del documento

1. **aws:executeAwsApi**- descrivi la sottorete fornita.
2. **aws:branch**- valuta l'IPs input di Target.

(IPv6) Se Target IPs contiene IPv6:

aws:assertAwsResourceProperty- verifica che la sottorete fornita abbia un IPv6 pool associato

3. **aws:executeScript**- ottieni l'architettura del tipo di istanza e il percorso dei parametri pubblici per la versione più recente di Amazon Linux 2 AMI.
4. **aws:executeAwsApi**- scarica la versione più recente di Amazon Linux 2 AMI da Parameter Store.
5. **aws:executeAwsApi**- creare un gruppo di sicurezza per il test nel VPC della sottorete.

(Pulizia) Se la creazione del gruppo di sicurezza ha esito negativo:

aws:executeAwsApi- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

6. **aws:executeAwsApi**- consentire tutto il traffico in uscita nel gruppo di sicurezza di test.

(Pulizia) Se la creazione della regola in uscita del gruppo di sicurezza ha esito negativo:

aws:executeAwsApi- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

7. **aws:executeAwsApi**- creare un ruolo IAM per l' EC2 istanza di test

(Pulizia) Se la creazione del ruolo ha esito negativo:

a. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione, se esiste.

b. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

8. **aws:executeAwsApi**- allega la politica SSMManged InstanceCore gestita da Amazon

(Pulizia) Se il collegamento della policy ha esito negativo:

a. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione, se allegato.

b. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.

c. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

9. **aws:executeAwsApi**- allega una politica in linea per consentire l'impostazione delle conservazioni dei gruppi di CloudWatch log e la creazione di una dashboard CloudWatch

(Pulizia) Se il collegamento della policy inline ha esito negativo:

a. **aws:executeAwsApi**- elimina la politica CloudWatch in linea dal ruolo creato dall'automazione, se creato.

b. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.

c. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.

d. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

10 **aws:executeAwsApi**- crea un profilo di istanza IAM.

(Pulizia) Se la creazione del profilo dell'istanza ha esito negativo:

a. **aws:executeAwsApi**- elimina il profilo di istanza IAM creato dall'automazione, se esiste.

b. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.

c. **aws:executeAwsApi**- elimina la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.

d. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.

e. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

11 **aws:executeAwsApi**- associare il profilo dell'istanza IAM al ruolo IAM.

(Pulizia) Se l'associazione tra profilo dell'istanza e ruolo ha esito negativo:

a. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo, se associato.

b. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.

c. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.

d. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.

f. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

12 **aws:sleep**- attendi che il profilo dell'istanza diventi disponibile.

13 **aws:runInstances**- crea l'istanza di test nella sottorete specificata e allegando il profilo di istanza creato in precedenza.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.

c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.

d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.

e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

14 **aws:branch**- valuta l'IPs input di Target.

(IPv6) Se Target IPs contiene IPv6:

aws:executeAwsApi- IPv6 assegna an all'istanza di test.

15 **aws:waitForAwsResourceProperty**- attendi che l'istanza di test diventi un'istanza gestita.

(Pulizia) Se la fase ha esito negativo:

a. **aws:changeInstanceState**- terminare l'istanza di test.

b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.

- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

16**aws:runCommand**- installa i prerequisiti di test:

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

17**aws:runCommand**- verificare che gli indirizzi forniti IPs siano sintatticamente corretti e/o che gli indirizzi siano corretti IPv4: IPv6

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

18**aws:runCommand**- definire il test MTR per ciascuno dei test forniti IPs.

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.

- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

19 **aws:runCommand**- definire il primo test di ping per ciascuno dei test forniti IPs.

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

20 **aws:runCommand**- definire il secondo test di ping per ciascuno dei test forniti IPs.

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

21 **aws:runCommand**- definire il test tracepath per ciascuno dei test forniti. IPs

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

22aws:runCommand- definire il test traceroute per ciascuno dei test forniti. IPs

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

23aws:runCommand- configurare CloudWatch i log.

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

24aws:runCommand- pianifica i cronjob per eseguire ogni test ogni minuto.

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

25**aws:sleep**- attendi che i test generino dei dati.

26**aws:runCommand**- imposta le conservazioni desiderate per i gruppi di CloudWatch log.

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- terminare l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.
- g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

27**aws:runCommand**- imposta i filtri metrici del gruppo di CloudWatch log.

(Pulizia) Se la fase ha esito negativo:

- a. **aws:changeInstanceState**- termina l'istanza di test.
- b. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.
- c. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.
- d. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
- e. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
- f. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.

g. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

28**aws:runCommand**- crea la CloudWatch dashboard.

(Pulizia) Se la fase ha esito negativo:

a. **aws:executeAwsApi**- elimina la CloudWatch dashboard, se esiste.

b. **aws:changeInstanceState**- terminare l'istanza di test.

c. **aws:executeAwsApi**- rimuove il profilo dell'istanza IAM dal ruolo.

d. **aws:executeAwsApi**- elimina il profilo dell'istanza IAM creato dall'automazione.

e. **aws:executeAwsApi**- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.

f. **aws:executeAwsApi**- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.

g. **aws:executeAwsApi**- elimina il ruolo IAM creato dall'automazione.

h. **aws:executeAwsApi**- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

Output

createCloudWatchDashboards.Output: l'URL della dashboard. CloudWatch

createManagedInstance. InstanceIds - l'ID dell'istanza di test.

AWSSupport-TerminateIPMonitoringFromVPC

Descrizione

AWSSupport-TerminateIPMonitoringFromVPCtermina un test di monitoraggio IP precedentemente avviato da. AWSSupport-SetupIPMonitoringFromVPC I dati relativi all'ID test specificato verranno eliminati.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- AutomationExecutionId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID di esecuzione dell'automazione utilizzato al momento dell'esecuzione precedente del `AWSSupport-SetupIPMonitoringFromVPC` runbook. Tutte le risorse associate a questo ID di esecuzione vengono eliminate.

- InstanceId

Tipo: stringa

Descrizione: (obbligatorio) ID istanza dell'istanza di monitoraggio.

- SubnetId

Tipo: stringa

Descrizione: (obbligatorio) ID sottorete dell'istanza di monitoraggio.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

Si consiglia di allegare all'utente che esegue l'automazione la policy gestita di Amazon `SSMAutomationRole` IAM. Inoltre, l'utente deve avere la seguente politica allegata al proprio utente, gruppo o ruolo:

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Action": [
      "iam:DetachRolePolicy",
      "iam:RemoveRoleFromInstanceProfile",
      "iam>DeleteRole",
      "iam>DeleteInstanceProfile",
      "iam>DeleteRolePolicy"
    ],
    "Resource": [
      "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport/
SetupIPMonitoringFromVPC_*",
      "arn:aws:iam::An-AWS-Account-ID:instance-profile/AWSSupport/
SetupIPMonitoringFromVPC_*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "iam:DetachRolePolicy"
    ],
    "Resource": [
      "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "cloudwatch:DeleteDashboards"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "ec2:DescribeTags",
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups",
      "ec2>DeleteSecurityGroup",
      "ec2:TerminateInstances",
      "ec2:DescribeInstanceStatus"
    ]
  }
]

```

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

Fasi del documento

1. `aws:assertAwsResourceProperty`- InstanceId controllano AutomationExecutionId e sono correlati allo stesso test.
2. `aws:assertAwsResourceProperty`- InstanceId controllano SubnetId e sono correlati allo stesso test.
3. `aws:executeAwsApi`- recupera il gruppo di sicurezza del test.
4. `aws:executeAwsApi`- elimina la CloudWatch dashboard.
5. `aws:changeInstanceState`- terminare l'istanza di test.
6. `aws:executeAwsApi`- rimuove il profilo dell'istanza IAM dal ruolo.
7. `aws:executeAwsApi`- elimina il profilo dell'istanza IAM creato dall'automazione.
8. `aws:executeAwsApi`- elimina la policy CloudWatch in linea dal ruolo creato dall'automazione.
9. `aws:executeAwsApi`- scollegare la policy SSMManged InstanceCore gestita da Amazon dal ruolo creato dall'automazione.
10. `aws:executeAwsApi`- elimina il ruolo IAM creato dall'automazione.
11. `aws:executeAwsApi`- elimina il gruppo di sicurezza creato dall'automazione, se esiste.

Output

Nessuno

AWS WAF

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS WAF Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-AddWAFRegionalRuleToRuleGroup](#)
- [AWS-AddWAFRegionalRuleToWebAcl](#)
- [AWSConfigRemediation-EnableWAFClassicLogging](#)
- [AWSConfigRemediation-EnableWAFClassicRegionalLogging](#)
- [AWSConfigRemediation-EnableWAFV2Logging](#)

AWS-AddWAFRegionalRuleToRuleGroup

Descrizione

Il `AWS-AddWAFRegionalRuleToRuleGroup` runbook aggiunge una regola AWS WAF regionale esistente a un gruppo di regole AWS WAF regionali. Sono supportati solo i gruppi di regole regionali AWS WAF classici. AWS WAF I gruppi di regole regionali classici possono avere un massimo di 10 regole.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- `RuleGroupId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del gruppo di regole che si desidera aggiornare.

- RulePriority

Tipo: integer

Descrizione: (Obbligatorio) La priorità per la nuova regola. La priorità delle regole determina l'ordine in cui vengono valutate le regole in un gruppo regionale. Le regole con un valore inferiore hanno una priorità maggiore rispetto alle regole con un valore più alto. Il valore deve essere un numero intero univoco. Se aggiungi più regole a un gruppo di regole regionali, i valori non devono essere consecutivi.

- RuleId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della regola che desideri aggiungere al gruppo di regole regionali.

- RuleAction

Tipo: stringa

Descrizione: (Obbligatorio) Specifica l' AWS WAF azione da eseguire quando una richiesta Web soddisfa le condizioni della regola.

Valori validi: ALLOW | BLOCK | COUNT

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- waf-regional:GetChangeToken
- waf-regional:GetChangeTokenStatus
- waf-regional:ListActivatedRulesInRuleGroup
- waf-regional:UpdateRuleGroup

Fasi del documento

- WAFChangeGet Token (aws:executeAwsApi) - Recupera un token di AWS WAF modifica per garantire che il runbook non invii richieste in conflitto al servizio.
- Aggiungi WAFRule a WAFRegional RuleGroup (aws:ExecuteScript) - Aggiunge la regola specificata al gruppo di regole regionali. AWS WAF
- VerifyChangeTokenPropagating (aws: waitForAwsResourceProperty) - Verifica che il token di modifica abbia lo stato o. PENDING INSYNC
- VerifyRuleAddedToRuleGroup (aws:ExecuteScript) - Verifica che la AWS WAF regola specificata sia stata aggiunta al gruppo di regole regionali di destinazione.

Output

- VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse - Risultato della fase di verifica dell'aggiunta della nuova regola al gruppo di regole regionali.
- VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse - Output dell'operazione ListActivatedRulesInRuleGroup API.

AWS-AddWAFRegionalRuleToWebAcl

Descrizione

Il AWS-AddWAFRegionalRuleToWebAcl runbook aggiunge una regola AWS WAF regionale, un gruppo di regole o una regola basata sulla tariffa esistente a una lista di controllo degli accessi Web (ACL) regionale AWS WAF classica. Questo runbook non aggiorna gli ACL web regionali AWS WAF classici esistenti gestiti da. AWS Firewall Manager

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Web ACLId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ACL Web che desideri aggiornare.

- ActivatedRulePriority

Tipo: integer

Descrizione: (Obbligatorio) La priorità per la nuova regola. La priorità delle regole determina l'ordine in cui vengono valutate le regole in un ACL Web. Le regole con un valore inferiore hanno una priorità maggiore rispetto alle regole con un valore più alto. Il valore deve essere un numero intero univoco. Se aggiungi più regole a un ACL web regionale, i valori non devono essere consecutivi.

- ActivatedRuleRuleId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della regola normale, della regola basata sulla tariffa o del gruppo che desideri aggiungere all'ACL web.

- ActivatedRuleAction

Tipo: stringa

Valori validi: ALLOW | BLOCK | COUNT

Descrizione: (Facoltativo) Specifica l' AWS WAF azione da eseguire quando una richiesta Web soddisfa le condizioni della regola.

- **ActivatedRuleType**

Tipo: stringa

Valori validi: REGULAR | RATE_BASED | GROUP

Predefinito: REGULAR

Descrizione: (Facoltativo) Il tipo di regola che stai aggiungendo all'ACL web. Sebbene questo campo sia facoltativo, tieni presente che se tenti di aggiungere una RATE_BASED regola a un ACL Web senza impostare il tipo, la richiesta ha esito negativo perché per impostazione predefinita la richiesta è una regola. REGULAR

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

Fasi del documento

- **DetermineWebACLNotIn FMSAnd RulePriority (AWS:ExecuteScript):** verifica se l'ACL AWS WAF Web rientra in una politica di sicurezza di Firewall Manager e verifica che l'ID di priorità non sia in conflitto con un ACL esistente.
- **AddRuleOrRuleGroupToWebACL (AWS:ExecuteScript):** aggiunge la regola specificata all'ACL Web. AWS WAF
- **VerifyRuleOrRuleGroupAddedToWebAcl (aws:ExecuteScript) -** Verifica che la regola specificata sia stata aggiunta all'ACL web di destinazione. AWS WAF

Output

- `DetermineWebACLNotNel.FMSAndRulePriorityPrereqResponse`: Uscita dalla `DetermineWebACLNotInFMSAndRulePriority` fase.
- `VerifyRuleOrRuleGroupAddedToWebAcl.VerifyRuleOrRuleGroupAddedToWebACLResponse`: Uscita dalla `AddRuleOrRuleGroupToWebACL` fase.
- `VerifyRuleOrRuleGroupAddedToWebAcl.ListActivatedRulesOrRuleGroupsInWebACLResponse`: Uscita del `VerifyRuleOrRuleGroupAddedToWebAcl` passo.

AWSConfigRemediation-EnableWAFCClassicLogging

Descrizione

Il `AWSConfigRemediation-EnableWAFCClassicLogging` runbook consente la registrazione su Amazon Data Firehose (Firehose) per AWS WAF la lista di controllo degli accessi Web (Web ACL) specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `DeliveryStreamName`

Tipo: stringa

Descrizione: (Obbligatorio) Il nome del flusso di distribuzione Firehose a cui si desidera inviare i log.

- Web ACLId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ACL AWS WAF Web a cui si desidera abilitare l'accesso.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

Fasi del documento

- `aws:executeAwsApi`- Conferma il flusso di consegna specificato in `DeliveryStreamName` exists.
- `aws:executeAwsApi`- Raccoglie l'ARN AWS WAF dell'ACL web specificato nel parametro. `WebACLId`
- `aws:executeAwsApi`- Abilita la registrazione per l'ACL web.
- `aws:assertAwsResourceProperty`- Verifica che la registrazione sia stata abilitata sull'ACL Web. AWS WAF

AWSConfigRemediation-EnableWAFClassicRegionalLogging

Descrizione

Il `AWSConfigRemediation-EnableWAFClassicRegionalLogging` runbook consente la registrazione su Amazon Data Firehose (Firehose) per la lista di controllo degli AWS WAF accessi Web (ACL) specificata.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `LogDestinationConfigs`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del flusso di distribuzione Firehose a cui desideri inviare i log.

- `Web ACLId`

Tipo: stringa

Descrizione: (Obbligatorio) L'ID dell'ACL AWS WAF Web a cui si desidera abilitare l'accesso.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie l'ARN AWS WAF dell'ACL web specificato nel parametro. `WebACLId`
- `aws:executeAwsApi`- Abilita la registrazione per l'ACL web.
- `aws:assertAwsResourceProperty`- Verifica che la registrazione sia stata abilitata sull'ACL Web. AWS WAF

AWSConfigRemediation-EnableWAFV2Logging

Descrizione

Il `AWSConfigRemediation-EnableWAFV2Logging` runbook consente la registrazione di una lista di controllo degli accessi Web AWS WAF (Web ACL) (AWS WAF V2) con il flusso di distribuzione Amazon Data Firehose (Firehose) specificato.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- LogDestinationConfigs

Tipo: stringa

Descrizione: (Obbligatorio) L'ARN del flusso di distribuzione Firehose che si desidera associare all'ACL Web.

Note

L'ARN del flusso di distribuzione Firehose deve iniziare con il prefisso `aws-waf-logs-`. Ad esempio, `aws-waf-logs-us-east-2-analytics`. Per ulteriori informazioni, consulta [Amazon Data Firehose](#).

- WebAclArn

Tipo: stringa

Descrizione: (Obbligatorio) ARN dell'ACL Web per il quale verrà abilitata la registrazione.

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`

- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

Fasi del documento

- `aws:executeScript`- Abilita la registrazione per l'ACL web AWS WAF V2 e verifica che la registrazione abbia la configurazione specificata.

Amazon WorkSpaces

AWS Systems Manager L'automazione fornisce runbook predefiniti per Amazon. WorkSpaces. Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWS-CreateWorkSpace](#)
- [AWSSupport-RecoverWorkSpace](#)

AWS-CreateWorkSpace

Descrizione

Il `AWS-CreateWorkSpace` runbook crea un nuovo desktop WorkSpaces virtuale Amazon, noto come a WorkSpace, in base ai valori specificati per i parametri di input. Per informazioni su WorkSpaces, consulta [What is Amazon WorkSpaces?](#) nella Amazon WorkSpaces Administration Guide.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

Linux macOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- BundleId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del pacchetto da utilizzare per. Workspace

- ComputeTypeName

Tipo: stringa

Valori validi: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

Descrizione: (Facoltativo) Il tipo di calcolo per il tuo. Workspace

- DirectoryId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID della directory a cui Workspace aggiungere il tuo.

- RootVolumeEncryptionEnabled

Tipo: Booleano

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (Facoltativo) Determina se il volume principale di Workspace è crittografato.

- RootVolumeSizeGib

Tipo: integer

Descrizione: (Obbligatorio) La dimensione del volume radice per Workspace.

- RunningMode

Tipo: stringa

Valori validi: ALWAYS_ON | AUTO_STOP

Descrizione: (Obbligatorio) La modalità di esecuzione di Workspace

- RunningModeAutoStopTimeoutInMinutes

Tipo: integer

Descrizione: (Facoltativo) Il tempo dopo che un utente si disconnette quando si WorkSpaces interrompe. Specificate un valore a intervalli di 60 minuti.

- Tag

Tipo: stringa

Descrizione: (Facoltativo) Tag che si desidera applicare a Workspace

- UserName

Tipo: stringa

Descrizione: (Obbligatorio) Il nome utente da associare a Workspace.

- UserVolumeEncryptionEnabled

Tipo: Booleano

Valori validi: true | false

Impostazione predefinita: false

Descrizione: (Facoltativo) Determina se il volume utente di Workspace è crittografato.

- UserVolumeSizeGib

Descrizione: (Obbligatorio) La dimensione del volume utente per Workspace.

- VolumeEncryptionKey

Tipo: stringa

Descrizione: (Facoltativo) La AWS Key Management Service chiave simmetrica che desideri utilizzare per crittografare i dati archiviati su. Workspace

Autorizzazioni IAM richieste

Il AutomationAssumeRole parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- workspaces:CreateWorkspaces
- workspaces:DescribeWorkspaces

Fasi del documento

- aws:executeScript- Crea un Workspace file basato sui valori specificati per i parametri di input.
- aws:waitForAwsResourceProperty- Verifica lo stato di Workspace isAVAILABLE.

Output

CreateWorkspace.WorkspaceId

AWSSupport-RecoverWorkspace

Descrizione

Il AWSSupport-RecoverWorkspace runbook esegue le fasi di ripristino sul desktop WorkSpaces virtuale Amazon, noto come a Workspace, specificato dall'utente. Il runbook riavvia e Workspace, se lo stato è fermoUNHEALTHY, lo ripristina o ricostruisce in Workspace base ai valori specificati per i parametri di input. Prima di utilizzare questo runbook, ti consigliamo di consultare la sezione [Troubleshooting WorkSpaces Issues](#) nella Amazon WorkSpaces Administration Guide.

⚠ Important

Il ripristino o la ricostruzione di un Workspace è un'azione potenzialmente distruttiva che può causare la perdita di dati. Questo perché Workspace viene ripristinato dall'ultima istantanea disponibile e i dati recuperati dalle istantanee possono durare fino a 12 ore.

L'opzione di ripristino ricrea sia il volume root che il volume utente in base alle istantanee più recenti. L'opzione rebuild ricrea il volume utente dall'istantanea più recente e ricrea quello Workspace dall'immagine associata al pacchetto da cui è stato creato. Workspace Le applicazioni installate o le impostazioni di sistema modificate dopo la Workspace creazione vengono perse. Per ulteriori informazioni sul ripristino e la ricostruzione WorkSpaces, consulta [Restore a Workspace e Rebuild a Workspace](#) nella Amazon WorkSpaces Administration Guide.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- AutomationAssumeRole

Tipo: stringa

Descrizione: (Facoltativo) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto. Se non viene specificato alcun ruolo, Systems Manager Automation utilizza le autorizzazioni dell'utente che avvia questo runbook.

- Riconoscere

Tipo: stringa

Valori validi: Sì

Descrizione: (Obbligatorio) Se si digita sì, si accetta che le azioni di ripristino e ricostruzione tenteranno di ripristinare l'istantanea più recente e che i dati ripristinati da queste istantanee possono durare fino a 12 ore. WorkSpace

- Riavvio

Tipo: stringa

Valori validi: Sì | No

Impostazione predefinita: Sì

Descrizione: (Obbligatorio) Determina se WorkSpace viene riavviato.

- Ricostruire

Tipo: stringa

Valori validi: Sì | No

Impostazione predefinita: No

Descrizione: (Obbligatorio) Determina se WorkSpace viene ricostruito.

- Ripristino

Tipo: stringa

Valori validi: Sì | No

Impostazione predefinita: No

Descrizione: (Obbligatorio) Determina se WorkSpace viene ripristinato.

- WorkSpaceId

Tipo: stringa

Descrizione: (Obbligatorio) L'ID del file che WorkSpace desideri ripristinare.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

Fasi del documento

- `aws:executeAwsApi`- Raccoglie lo stato `WorkSpace` specificato nel `WorkspaceId` parametro.
- `aws:assertAwsResourceProperty`- Verifica lo stato di `WorkSpace` `isAVAILABLE`, `ERRORIMPAIREDSTOPPED`, o `UNHEALTHY`
- `aws:branch`- Filiali in base allo stato del `WorkSpace`.
- `aws:executeAwsApi`- Avvia il `WorkSpace`.
- `aws:branch`- Rami basati sul valore specificato per il `Action` parametro.
- `aws:waitForAwsResourceProperty`- Attende lo `WorkSpace` stato dopo l'avvio.
- `aws:waitForAwsResourceProperty`- Attende che lo `WorkSpace` stato cambi in `AVAILABLE`, `ERRORIMPAIRED`, o `UNHEALTHY` dopo l'avvio.
- `aws:executeAwsApi`- Raccoglie lo stato di `WorkSpace` dopo l'avvio.
- `aws:branch`- Filiali in base allo stato del `WorkSpace` dopo l'avvio.
- `aws:executeAwsApi`- Raccoglie le istantanee disponibili per il ripristino o la ricostruzione di `WorkSpace`
- `aws:branch`- Rami basati sul valore specificato per il parametro. `Reboot`
- `aws:executeAwsApi`- Riavvia il `WorkSpace`
- `aws:executeAwsApi`- Raccoglie lo stato di `WorkSpace` dopo l'avvio.
- `aws:waitForAwsResourceProperty`- Attende che lo stato del `WorkSpace` cambi. `REBOOTING`

- `aws:waitForAwsResourceProperty`- Attende che lo WorkSpace stato cambi o UNHEALTHY dopo AVAILABLE il ERROR riavvio.
- `aws:executeAwsApi`- Raccoglie lo stato di dopo il riavvio. Workspace
- `aws:branch`- Rami in base allo stato del dopo il Workspace riavvio.
- `aws:branch`- Rami basati sul valore specificato per il Restore parametro.
- `aws:executeAwsApi`- Ripristina il. Workspace Se il ripristino fallisce, il runbook tenta di ricostruire il. Workspace
- `aws:waitForAwsResourceProperty`- Attende che lo stato Workspace di. RESTORING
- `aws:waitForAwsResourceProperty`- Attende che lo Workspace stato cambi a AVAILABLEERROR, o UNHEALTHY dopo essere stato ripristinato.
- `aws:executeAwsApi`- Raccoglie lo stato di Workspace dopo il ripristino.
- `aws:branch`- Rami in base allo stato dell'ambiente Workspace dopo il ripristino.
- `aws:branch`- Rami basati sul valore specificato per il Rebuild parametro.
- `aws:executeAwsApi`- Ricostruisce il. Workspace
- `aws:waitForAwsResourceProperty`- Attende che lo stato del cambi Workspace in. REBUILDING
- `aws:waitForAwsResourceProperty`- Attende che lo Workspace stato cambi a AVAILABLEERROR, o UNHEALTHY dopo essere stato ricostruito.
- `aws:executeAwsApi`- Raccoglie lo stato di Workspace dopo la ricostruzione.
- `aws:assertAwsResourceProperty`- Conferma lo stato di is. Workspace AVAILABLE

X-Ray

AWS Systems Manager L'automazione fornisce runbook predefiniti per. AWS X-Ray Per informazioni sull'uso dei runbook, consulta [Working with runbooks](#). Per informazioni su come visualizzare il contenuto dei runbook, consulta. [Visualizza il contenuto del runbook](#)

Argomenti

- [AWSConfigRemediation-UpdateXRayKMSKey](#)

AWSConfigRemediation-UpdateXRayKMSKey

Descrizione

Il `AWSConfigRemediation-UpdateXRayKMSKey` runbook abilita la crittografia AWS X-Ray dei dati utilizzando una chiave AWS Key Management Service (AWS KMS). Questo runbook deve essere usato solo come base per garantire che AWS X-Ray i dati siano crittografati secondo le migliori pratiche di sicurezza minime consigliate. Consigliamo di crittografare più set di dati con chiavi KMS diverse.

[Esegui questa automazione \(console\)](#)

Tipo di documento

Automazione

Proprietario

Amazon

Piattaforme

LinuxmacOS, Windows

Parametri

- `AutomationAssumeRole`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a Systems Manager Automation di eseguire le azioni per tuo conto.

- `KeyId`

Tipo: stringa

Descrizione: (Obbligatorio) L'Amazon Resource Name (ARN), l'ID della chiave o l'alias della chiave KMS che desideri utilizzare AWS X-Ray per crittografare i dati.

Autorizzazioni IAM richieste

Il `AutomationAssumeRole` parametro richiede le seguenti azioni per utilizzare correttamente il runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

Fasi del documento

- `aws:executeAwsApi`- Abilita la crittografia dei dati X-Ray utilizzando la chiave KMS specificata nel parametro. `KeyId`
- `aws:waitForAwsResourceProperty`- Attende lo stato di configurazione della crittografia del sistema X-Ray. `ACTIVE`
- `aws:executeAwsApi`- Raccoglie l'ARN della chiave specificata nel `KeyId` parametro.
- `aws:assertAwsResourceProperty`- Verifica che la crittografia sia stata abilitata sul sistema X-Ray.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.