



Guide de l'utilisateur

# AWS Systems Manager Guide de référence du manuel d'automatisation



# AWS Systems Manager Guide de référence du manuel d'automatisation: Guide de l'utilisateur

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

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

# Table of Contents

Référence du runbook Automation .....	1
Afficher le contenu du runbook .....	3
API Gateway .....	4
AWSConfigRemediation-DeleteAPIGatewayStage .....	4
AWSConfigRemediation-EnableAPIGatewayTracing .....	6
AWSConfigRemediation-UpdateAPIGatewayMethodCaching .....	7
AWS Batch .....	8
AWSSupport-TroubleshootAWSBatchJob .....	9
AWS CloudFormation .....	14
AWS-DeleteCloudFormationStack .....	15
AWS-EnableCloudFormationSNSNotification .....	16
AWS-RunCfnLint .....	18
AWSSupport-TroubleshootCFNCustomResource .....	20
AWS-UpdateCloudFormationStack .....	22
CloudFront .....	23
AWSConfigRemediation-EnableCloudFrontDefaultRootObject .....	23
AWSConfigRemediation-EnableCloudFrontAccessLogs .....	25
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity .....	27
AWSConfigRemediation-EnableCloudFrontOriginFailover .....	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-EnableCWAlarm .....	46
Amazon DocumentDB .....	49
AWS-EnableDocDbClusterBackupRetentionPeriod .....	49

CodeBuild .....	51
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMCMK .....	52
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject .....	53
AWS CodeDeploy .....	55
AWSSupport-TroubleshootCodeDeploy .....	55
AWS Config .....	57
AWSSupport-SetupConfig .....	57
Amazon Connect .....	60
AWSSupport-AssociatePhoneNumbersToConnectContactFlows .....	60
AWS Directory Service .....	69
AWS-CreateDSManagementInstance .....	69
AWSSupport-TroubleshootADConnectorConnectivity .....	74
AWSSupport-TroubleshootDirectoryTrust .....	77
AWS AppSync .....	81
AWS-EnableAppSyncGraphQLApiLogging .....	81
Amazon Athena .....	83
AWS-EnableAthenaWorkGroupEncryptionAtRest .....	84
DynamoDB .....	86
AWS-ChangeDDBRWCapacityMode .....	86
AWS-CreateDynamoDBBackup .....	89
AWS-DeleteDynamoDbBackup .....	90
AWSConfigRemediation-DeleteDynamoDbTable .....	91
AWS-DeleteDynamoDbTableBackups .....	92
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable .....	93
AWSConfigRemediation-EnablePITRForDynamoDbTable .....	95
AWS-EnableDynamoDbAutoscaling .....	96
AWS-RestoreDynamoDBTable .....	100
Amazon EBS .....	102
AWSSupport-AnalyzeEBSResourceUsage .....	103
AWS-ArchiveEBSSnapshots .....	109
AWS-AttachEBSVolume .....	112
AWSSupport-CalculateEBSPerformanceMetrics .....	113
AWS-CopySnapshot .....	119
AWS-CreateSnapshot .....	120
AWS-DeleteSnapshot .....	121
AWSConfigRemediation-DeleteUnusedEBSVolume .....	122

AWS-DeregisterAMIs .....	124
AWS-DetachEBSVolume .....	126
AWSConfigRemediation-EnableEbsEncryptionByDefault .....	127
AWS-ExtendEbsVolume .....	128
AWSSupport-ModifyEBSSnapshotPermission .....	130
AWSConfigRemediation-ModifyEBSVolumeType .....	133
Amazon EC2 .....	134
AWS-ASGEnterStandby .....	136
AWS-ASGExitStandby .....	137
AWS-CreateImage .....	138
AWS-DeleteImage .....	140
AWS-PatchAsgInstance .....	141
AWS-PatchInstanceWithRollback .....	144
AWS-QuarantineEC2Instance .....	146
AWS-ResizeInstance .....	148
AWS-RestartEC2Instance .....	149
AWS-SetupJupyter .....	150
AWS-StartEC2Instance .....	154
AWS-StopEC2Instance .....	155
AWS-TerminateEC2Instance .....	156
AWS-UpdateLinuxAmi .....	156
AWS-UpdateWindowsAmi .....	159
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck .....	163
AWSConfigRemediation-EnforceEC2InstanceIMDSv2 .....	164
AWSEC2-CloneInstanceAndUpgradeSQLServer .....	166
AWSEC2-CloneInstanceAndUpgradeWindows .....	170
AWSEC2-ConfigureSTIG .....	174
AWSEC2-PatchLoadBalancerInstance .....	202
AWSEC2-SQLServerDBRestore .....	204
AWSSupport-ActivateWindowsWithAmazonLicense .....	209
AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 .....	212
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD .....	217
AWSSupport-CheckXenToNitroMigrationRequirements .....	223
AWSSupport-ConfigureEC2Metadata .....	226
AWSSupport-CopyEC2Instance .....	230
AWSSupport-EnableWindowsEC2SerialConsole .....	235

AWSSupport-ExecuteEC2Rescue .....	244
AWSSupport-ListEC2Resources .....	247
AWSSupport-ManageRDPSettings .....	250
AWSSupport-ManageWindowsService .....	252
AWSSupport-MigrateEC2ClassicToVPC .....	254
AWSSupport-MigrateXenToNitroLinux .....	261
AWSSupport-ResetAccess .....	273
AWSSupport-ResetLinuxUserPassword .....	276
AWSPremiumSupport-ResizeNitroInstance .....	283
AWSSupport-RestoreEC2InstanceFromSnapshot .....	290
AWSSupport-SendLogBundleToS3Bucket .....	294
AWSSupport-StartEC2RescueWorkflow .....	296
AWSPremiumSupport-TroubleshootEC2DiskUsage .....	307
AWSSupport-TroubleshootEC2InstanceConnect .....	312
AWSSupport-TroubleshootRDP .....	318
AWSSupport-TroubleshootSSH .....	324
AWSSupport-TroubleshootSUSERegistration .....	327
AWSSupport-TroubleshootWindowsPerformance .....	329
AWSSupport-TroubleshootWindowsUpdate .....	337
AWSSupport-UpgradeWindowsAWSDrivers .....	344
Amazon ECS .....	348
AWSSupport-CollectECSInstanceLogs .....	348
AWS-InstallAmazonECSAgent .....	351
AWS-ECSRunTask .....	353
AWSSupport-TroubleshootECSContainerInstance .....	357
AWSSupport-TroubleshootECSTaskFailedToStart .....	359
AWS-UpdateAmazonECSAgent .....	363
Amazon EFS .....	365
AWSSupport-CheckAndMountEFS .....	365
Amazon EKS .....	368
AWSSupport-CollectEKSIInstanceLogs .....	369
AWS-CreateEKSClusterWithFargateProfile .....	371
AWS-CreateEKSClusterWithNodegroup .....	375
AWS-DeleteEKSCluster .....	378
AWS-MigrateToNewEKSSelfManagedNodeGroup .....	381
AWSPremiumSupport-TroubleshootEKSCluster .....	388

AWSSupport-TroubleshootEKSSelfManagedLinuxNodeGroups .....	392
AWS-UpdateEKSCluster .....	394
AWS-UpdateEKSMANAGEDNodeGroup .....	396
AWS-UpdateEKSSelfManagedLinuxNodeGroups .....	400
Elastic Beanstalk .....	404
AWSSupport-CollectElasticBeanstalkLogs .....	404
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ..	407
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications .....	409
AWSSupport-TroubleshootElasticBeanstalk .....	410
Elastic Load Balancing .....	413
AWSConfigRemediation-DropInvalidHeadersForALB .....	414
AWS-EnableCLBAccessLogs .....	415
AWS-EnableCLBConnectionDraining .....	417
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing .....	419
AWSConfigRemediation-EnableELBDeletionProtection .....	420
AWSConfigRemediation-EnableLoggingForALBAndCLB .....	422
AWSSupport-TroubleshootCLBConnectivity .....	423
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing .....	427
AWS UpdateALB DesyncMitigationMode .....	428
AWS UpdateCLB DesyncMitigationMode .....	430
Amazon EMR .....	432
AWSSupport-AnalyzeEMRLogs .....	432
Amazon OpenSearch Service .....	438
AWSConfigRemediation-DeleteOpenSearchDomain .....	439
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain .....	440
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups .....	442
AWSSupport-TroubleshootOpenSearchRedYellowCluster .....	443
AWSSupport-TroubleshootOpenSearchHighCPU .....	449
EventBridge .....	456
AWS-AddOpsItemDedupStringToEventBridgeRule .....	456
AWS-DisableEventBridgeRule .....	457
GuardDuty .....	459
AWSConfigRemediation-CreateGuardDutyDetector .....	459
IAM .....	460
AWS-AttachIAMToInstance .....	461
AWS-DeleteIAMInlinePolicy .....	463

AWSConfigRemediation-DeleteIAMRole .....	465
AWSConfigRemediation-DeleteIAMUser .....	466
AWSConfigRemediation-DeleteUnusedIAMGroup .....	469
AWSConfigRemediation-DeleteUnusedIAMPolicy .....	470
AWSConfigRemediation-DetachIAMPolicy .....	472
AWSConfigRemediation-EnableAccountAccessAnalyzer .....	473
AWSSupport-GrantPermissionsToIAMUser .....	474
AWSConfigRemediation-RemoveUserPolicies .....	480
AWSConfigRemediation-ReplaceIAMInlinePolicy .....	481
AWSConfigRemediation-RevokeUnusedIAMUserCredentials .....	483
AWSConfigRemediation-SetIAMPASSWORDPolicy .....	485
Amazon Kinesis Data Streams .....	488
AWS-EnableKinesisStreamEncryption .....	488
AWS KMS .....	490
AWSConfigRemediation-CancelKeyDeletion .....	490
AWSConfigRemediation-EnableKeyRotation .....	492
Lambda .....	493
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing .....	493
AWSConfigRemediation-DeleteLambdaFunction .....	495
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK .....	496
AWSConfigRemediation-MoveLambdaToVPC .....	498
AWSSupport-RemediateLambdaS3Event .....	500
AWSSupport-TroubleshootLambdaInternetAccess .....	502
AWSSupport-TroubleshootLambdaS3Event .....	506
Amazon Managed Workflows for Apache Airflow .....	508
AWSSupport-TroubleshootMWAAEnvironmentCreation .....	508
Neptune .....	515
AWS-EnableNeptuneDbAuditLogsToCloudWatch .....	515
AWS-EnableNeptuneDbBackupRetentionPeriod .....	517
AWS-EnableNeptuneClusterDeletionProtection .....	519
Amazon RDS .....	520
AWS-CreateEncryptedRdsSnapshot .....	521
AWS-CreateRdsSnapshot .....	524
AWSConfigRemediation-DeleteRDSCluster .....	525
AWSConfigRemediation-DeleteRDSClusterSnapshot .....	527
AWSConfigRemediation-DeleteRDSInstance .....	528



AWSConfigRemediation-DeleteRDSInstanceSnapshot .....	530
AWSConfigRemediation-DisablePublicAccessToRDSInstance .....	531
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster .....	533
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance .....	535
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance .....	537
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS .....	539
AWSConfigRemediation-EnableMultiAZOnRDSInstance .....	540
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance .....	542
AWSConfigRemediation-EnableRDSClusterDeletionProtection .....	544
AWSConfigRemediation-EnableRDSInstanceBackup .....	546
AWSConfigRemediation-EnableRDSInstanceDeletionProtection .....	548
AWSConfigRemediation-ModifyRDSInstancePortNumber .....	550
AWSSupport-ModifyRDSSnapshotPermission .....	551
AWSPremiumSupport-PostgreSQLWorkloadReview .....	554
AWS-RebootRdsInstance .....	570
AWSSupport-ShareRDSSnapshot .....	571
AWS-StartRdsInstance .....	575
AWS-StartStopAuroraCluster .....	576
AWS-StopRdsInstance .....	578
AWSSupport-TroubleshootConnectivityToRDS .....	579
AWSSupport-TroubleshootRDSIAMAuthentication .....	581
AWSSupport-ValidateRdsNetworkConfiguration .....	589
Amazon Redshift .....	595
AWSConfigRemediation-DeleteRedshiftCluster .....	595
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster .....	597
AWSConfigRemediation-EnableRedshiftClusterAuditLogging .....	598
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot .....	600
AWSConfigRemediation-EnableRedshiftClusterEncryption .....	601
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting .....	603
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster .....	604
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings .....	606
AWSConfigRemediation-ModifyRedshiftClusterNodeType .....	608
Amazon S3 .....	610
AWS-ArchiveS3BucketToIntelligentTiering .....	611
AWS-ConfigureS3BucketLogging .....	613
AWS-ConfigureS3BucketVersioning .....	615

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock .....	616
AWSConfigRemediation-ConfigureS3PublicAccessBlock .....	618
AWS-CreateS3PolicyToExpireMultipartUploads .....	621
AWS-DisableS3BucketPublicReadWrite .....	623
AWS-EnableS3BucketEncryption .....	624
AWS-EnableS3BucketKeys .....	625
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy .....	627
AWSConfigRemediation-RestrictBucketSSLRequestsOnly .....	628
AWSSupport-TroubleshootS3PublicRead .....	630
SageMaker .....	636
AWS-DisableSageMakerNotebookRootAccess .....	636
Secrets Manager .....	638
AWSConfigRemediation-DeleteSecret .....	638
AWSConfigRemediation-RotateSecret .....	640
Security Hub .....	641
AWSConfigRemediation-EnableSecurityHub .....	642
AWS Shield .....	643
AWSPremiumSupport-DDoSResiliencyAssessment .....	643
Amazon SNS .....	652
AWS-EnableSNSTopicDeliveryStatusLogging .....	653
AWSConfigRemediation-EncryptSNSTopic .....	655
AWS-PublishSNSNotification .....	657
Amazon SQS .....	658
AWS-EnableSQSEncryption .....	658
Step Functions .....	660
AWS-EnableStepFunctionsStateMachineLogging .....	661
Systems Manager .....	663
AWS-BulkDeleteAssociation .....	664
AWS-BulkEditOpsItems .....	665
AWS-BulkResolveOpsItems .....	668
AWS-ConfigureMaintenanceWindows .....	671
AWS-CreateManagedLinuxInstance .....	672
AWS-CreateManagedWindowsInstance .....	675
AWSConfigRemediation-EnableCWLoggingForSessionManager .....	677
AWS-ExportOpsDataToS3 .....	679
AWS-ExportPatchReportToS3 .....	680

AWS-SetupInventory .....	682
AWS-SetupManagedInstance .....	687
AWS-SetupManagedRoleOnEC2Instance .....	688
AWSSupport-TroubleshootManagedInstance .....	689
AWSSupport-TroubleshootPatchManagerLinux .....	692
AWSSupport-TroubleshootSessionManager .....	696
Tierce .....	701
AWS-CreateJiraIssue .....	702
AWS-CreateServiceNowIncident .....	704
AWS-RunPacker .....	706
Amazon VPC .....	708
AWS-CloseSecurityGroup .....	709
AWSSupport-ConfigureDNSQueryLogging .....	710
AWSSupport-ConfigureTrafficMirroring .....	713
AWSSupport-ConnectivityTroubleshooter .....	716
AWSSupport-TroubleshootVPN .....	720
AWSConfigRemediation-DeleteEgressOnlyInternetGateway .....	726
AWSConfigRemediation-DeleteUnusedENI .....	727
AWSConfigRemediation-DeleteUnusedSecurityGroup .....	728
AWSConfigRemediation-DeleteUnusedVPCNetworkACL .....	730
AWSConfigRemediation-DeleteVPCFlowLog .....	731
AWSConfigRemediation-DetachAndDeleteInternetGateway .....	732
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway .....	734
AWS-DisableIncomingSSHOnPort22 .....	736
AWS-DisablePublicAccessForSecurityGroup .....	738
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP .....	739
AWSSupport-EnableVPCFlowLogs .....	740
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch .....	744
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket .....	747
AWS-ReleaseElasticIP .....	749
AWS-RemoveNetworkACLUnrestrictedSSHRDP .....	750
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules .....	751
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules .....	753
AWSSupport-SetupIPMonitoringFromVPC .....	754
AWSSupport-TerminateIPMonitoringFromVPC .....	766
AWS WAF .....	769

---

AWS-AddWAFRegionalRuleToRuleGroup .....	770
AWS-AddWAFRegionalRuleToWebAcl .....	772
AWSConfigRemediation-EnableWAFClassicLogging .....	775
AWSConfigRemediation-EnableWAFClassicRegionalLogging .....	776
AWSConfigRemediation-EnableWAFV2Logging .....	778
Amazon WorkSpaces .....	780
AWS-CreateWorkSpace .....	780
AWSSupport-RecoverWorkSpace .....	783
X-Ray .....	787
AWSConfigRemediation-UpdateXRayKMSKey .....	787
.....	dccxc

# Référence du runbook Systems Manager Automation

Pour vous aider à démarrer rapidement, AWS Systems Manager fournit des runbooks prédéfinis. Ces runbooks sont gérés par Amazon Web Services AWS Support, et AWS Config. La référence des runbooks décrit chacun des runbooks prédéfinis fournis par Systems Manager AWS Support, et AWS Config

## Important

Si vous exécutez un flux de travail d'automatisation qui appelle d'autres services à l'aide d'un rôle de service AWS Identity and Access Management (IAM), le rôle de service doit être configuré avec l'autorisation d'appeler ces services. Cette exigence s'applique à tous les runbooks Automation d' AWS (runbooks AWS-\*) tels que les runbooks AWS-ConfigureS3BucketLogging, AWS-CreateDynamoDBBackup et AWS-RestartEC2Instance, par exemple. Cette exigence s'applique également à tous les runbooks d'automatisation personnalisés que vous créez et qui invoquent d'autres AWS services en utilisant des actions qui appellent d'autres services. Par exemple, si vous exécutez les actions `aws:executeAwsApi`, `aws:createStack` ou `aws:copyImage`, vous devez configurer la fonction du service avec l'autorisation de faire appel à ces services. Vous pouvez activer les autorisations d'accès à d'autres AWS services en ajoutant une politique IAM en ligne au rôle. Pour plus d'informations, voir [Ajouter une politique d'automatisation intégrée pour appeler d'autres AWS services](#).

Cette référence inclut des rubriques qui décrivent chacun des runbooks de Systems Manager détenus par AWS AWS Support, et AWS Config. Les runbooks sont organisés par personne concernée Service AWS. Chaque page fournit une explication des paramètres obligatoires et facultatifs que vous pouvez spécifier lors de l'utilisation du runbook. Chaque page répertorie également les étapes du runbook et le résultat de l'automatisation, le cas échéant.

Cette référence n'inclut pas de page distincte pour les runbooks qui nécessitent une approbation, comme le runbook `AWS-CreateManagedLinuxInstanceWithApproval` ou le `AWS-StopEC2InstanceWithApproval` runbook. Tout nom de runbook qui inclut `WithApproval`, signifie que le runbook inclut l'[aws:approve](#) action. Cette action interrompt temporairement une automatisation jusqu'à ce que les responsables désignés approuvent ou rejettent l'action. Une fois le nombre d'approbations requises atteint, l'automatisation reprend.

Pour plus d'informations sur l'exécution d'automatisations, voir [Exécution d'une automatisation simple](#). Pour plus d'informations sur l'exécution d'automatisations sur plusieurs cibles, voir [Exécution d'automatismes utilisant des cibles et des contrôles de débit](#).

## Rubriques

- [Afficher le contenu du runbook](#)
- [API Gateway](#)
- [AWS Batch](#)
- [AWS CloudFormation](#)
- [CloudFront](#)
- [CloudTrail](#)
- [CloudWatch](#)
- [Amazon DocumentDB](#)
- [CodeBuild](#)
- [AWS CodeDeploy](#)
- [AWS Config](#)
- [Amazon Connect](#)
- [AWS Directory Service](#)
- [AWS AppSync](#)
- [Amazon Athena](#)
- [DynamoDB](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [Amazon ECS](#)
- [Amazon EFS](#)
- [Amazon EKS](#)
- [Elastic Beanstalk](#)
- [Elastic Load Balancing](#)
- [Amazon EMR](#)
- [Amazon OpenSearch Service](#)
- [EventBridge](#)

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

## Afficher le contenu du runbook

Vous pouvez consulter le contenu des runbooks dans la console Systems Manager.

Pour afficher le contenu du runbook

1. Ouvrez la AWS Systems Manager console à l'[adresse https://console.aws.amazon.com/systems-manager/](https://console.aws.amazon.com/systems-manager/).

2. Dans le panneau de navigation, cliquez sur Documents.

-ou-

Si la page d' AWS Systems Manager accueil s'ouvre en premier, choisissez l'icône de menu



pour ouvrir le volet de navigation, puis choisissez Documents dans le volet de navigation.

3. Dans la section Catégories, sélectionnez Documents d'automatisation.

4. Sélectionnez un runbook, puis sélectionnez View details (Afficher les détails).

5. Sélectionnez l'onglet Contenu.

## API Gateway

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon API Gateway. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

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

## AWSConfigRemediation-DeleteAPIGatewayStage

### Description

Le AWSConfigRemediation-DeleteAPIGatewayStage runbook supprime un stage Amazon API Gateway (API Gateway). AWS Config doit être activé Région AWS là où vous exécutez cette automatisation.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire



## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- StageArn

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du stage API Gateway que vous souhaitez supprimer.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- aws:executeScript- Supprime le stage API Gateway spécifié dans le StageArn paramètre.

# AWSConfigRemediation-EnableAPIGatewayTracing

## Description

Le `AWSConfigRemediation-EnableAPIGatewayTracing` runbook permet le suivi sur un stage Amazon API Gateway (API Gateway). AWS Config doit être activé Région AWS là où vous exécutez cette automatisation.

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `StageArn`

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du stage API Gateway sur lequel vous souhaitez activer le suivi.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeScript`- Active le suivi sur le stage API Gateway spécifié dans le `StageArn` paramètre.

## AWSConfigRemediation-UpdateAPIGatewayMethodCaching

### Description

Le `AWSConfigRemediation-UpdateAPIGatewayMethodCaching` runbook met à jour le paramètre de méthode de cache pour une ressource de stage Amazon API Gateway.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `CachingAuthorizedMethods`

Type : `StringList`

Description : (Obligatoire) Méthodes autorisées pour activer la mise en cache. La liste doit être une combinaison de `DELETEGET`, `HEAD`, `OPTIONSPATCH`, `POST`, et `PUT`. La mise en cache est activée pour les méthodes sélectionnées et désactivée pour les méthodes non sélectionnées. La mise en cache est activée pour toutes les méthodes si elle `ANY` est sélectionnée et désactivée pour toutes les méthodes si elle `NONE` est sélectionnée.

- `StageArn`

Type : `String`

Description : (Obligatoire) L'ARN du stage API Gateway pour l'RESTAPI.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeScript`- Accepte l'ID de ressource du stage en tant qu'entrée, met à jour le paramètre de la méthode de cache pour un stage API Gateway à l'aide de l'action `UpdateStage API` et vérifie la mise à jour.

## AWS Batch

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Batch. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWSSupport-TroubleshootAWSBatchJob](#)

# AWSSupport - TroubleshootAWSBatchJob

## Description

Le `AWSSupport-TroubleshootAWSBatchJob` runbook vous aide à résoudre les problèmes qui empêchent une AWS Batch tâche de passer du statut au statut. `RUNNABLE STARTING`

## Comment fonctionne-t-il ?

Ce runbook effectue les vérifications suivantes :

- Si l'environnement de calcul est dans un `DISABLED` état `INVALID` ou.
- Si le `Max vCPU` paramètre de l'environnement de calcul est suffisamment important pour prendre en charge le volume des tâches dans la file d'attente des tâches.
- Si les tâches nécessitent plus de `vCPU` ou de ressources de mémoire que ce que les types d'instances de l'environnement de calcul peuvent fournir.
- Si les tâches doivent être exécutées sur des instances basées sur le GPU mais que l'environnement de calcul n'est pas configuré pour utiliser des instances basées sur le GPU.
- Si le groupe `Auto Scaling` de l'environnement de calcul n'a pas réussi à lancer les instances.
- [Si les instances lancées peuvent rejoindre le cluster Amazon Elastic Container Service \(Amazon ECS\) sous-jacent, sinon, il exécute `AWSSupport le runbook -TroubleShootECS. ContainerInstance`](#)
- Si un problème d'autorisation bloque des actions spécifiques requises pour exécuter le travail.

### Important

- Ce runbook doit être lancé dans la même AWS région que votre tâche dont le `RUNNABLE` statut est bloqué.
- Ce runbook peut être lancé pour des AWS Batch tâches planifiées sur des instances Amazon ECS AWS Fargate ou Amazon Elastic Compute Cloud (Amazon EC2). Si l'automatisation est initiée pour une AWS Batch tâche sur Amazon Elastic Kubernetes Service (Amazon EKS), le lancement s'arrête.

- Si des instances sont disponibles pour exécuter la tâche mais ne parviennent pas à enregistrer le cluster Amazon ECS, ce runbook lance le runbook [AWSSupport-TroubleshootECSContainerInstance](#) d'automatisation pour essayer de déterminer pourquoi. Pour plus d'informations, reportez-vous au manuel d'exécution [AWSSupport-TroubleshootECS ContainerInstance](#).

## [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- JobId

Type : chaîne

Description : (Obligatoire) L'ID du AWS Batch Job dont le RUNNABLE statut est bloqué.

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

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Instructions

1. Accédez à l'option [AWSSupport-Troubleshoot AWSBatchJob](#) dans la AWS Systems Manager console.
2. Sélectionnez Exécuter l'automatisation
3. Pour les paramètres d'entrée, entrez ce qui suit :
  - `AutomationAssumeRole` (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `JobId` (Obligatoire) :

L'ID du AWS Batch Job bloqué dans le RUNNABLE statut.

**Input parameters**

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

4. Sélectionnez Exécuter.
5. Notez que l'automatisation démarre.
6. Le document exécute les étapes suivantes :
  - `PreflightPermissionChecks`:



Effectue des vérifications d'autorisation IAM avant le vol par rapport à l'utilisateur/rôle initiateur. Si des autorisations sont manquantes, cette étape fournit les actions d'API manquantes dans la section de sortie globale.

- `ProceedOnlyIfUserHasPermission`:

Branches basées sur le fait que vous êtes autorisé à effectuer toutes les actions requises pour le runbook.

- `AWSBatchJobEvaluation`:

Effectue des vérifications par rapport au AWS Batch Job pour vérifier son existence et `RUNNABLE` son statut.

- `ProceedOnlyIfBatchJobExistsAndIsInRunnableState`:

Branches en fonction de l'existence et du `RUNNABLE` statut des emplois.

- `BatchComputeEnvironmentEvaluation`:

Effectue des vérifications par rapport à l'environnement AWS Batch informatique.

- `ProceedOnlyIfComputeEnvironmentChecksAreOK` :

Branches basées sur le succès des vérifications de l'environnement de calcul.

- `UnderlyingInfraEvaluation`:

Effectue des vérifications par rapport au groupe Auto Scaling ou à la demande de flotte Spot sous-jacents.

- `ProceedOnlyIfInstancesNotJoiningEcsCluster` :

Branches basées sur le fait que certaines instances ne rejoignent pas le cluster Amazon ECS.

- `EcsAutomationRunner`:

Exécute l'automatisation Amazon ECS pour les instances qui ne rejoignent pas le cluster.

- `ExecutionResults`:

Génère une sortie basée sur les étapes précédentes.

7. Une fois l'opération terminée, l'URI du fichier HTML du rapport d'évaluation est fourni :

Lien vers la console S3 et URI Amazon S3 pour le rapport sur l'exécution réussie du runbook

## ▼ Outputs

ExecutionResults.message

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

```

✔ [INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKn0EEWmt8eY":
❌ [ERROR]: Job "411[REDACTED]606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKn0EEWmt8eY" 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-egMKn0EEWmt8eY".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html
#####
❌ [ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.

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

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

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

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

✔ [INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKn0EEWmt8eY":
❌ [ERROR]: Job "411[REDACTED]606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKn0EEWmt8eY" 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-egMKn0EEWmt8eY".
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.
```

## Références

## Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

## AWS CloudFormation

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS CloudFormation. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

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

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

## AWS-DeleteCloudFormationStack

### Description

Supprimez une pile AWS CloudFormation.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- StackNameOrId

Type : String

Description : (Obligatoire) Nom ou identifiant unique de la CloudFormation pile à supprimer

# AWS-EnableCloudFormationSNSNotification

## Description

Le `AWS-EnableCloudFormationSNSNotification` runbook active les notifications Amazon Simple Notification Service (Amazon SNS) pour la pile AWS CloudFormation (AWS CloudFormation) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- StackArn

Type : chaîne

Description : (Obligatoire) L'ARN ou le nom de la AWS CloudFormation pile pour laquelle vous souhaitez activer les notifications Amazon SNS.

- NotificationArn

Type : chaîne

Description : (Obligatoire) L'ARN de la rubrique Amazon SNS que vous souhaitez associer à la AWS CloudFormation pile.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- SMS : `GetAutomationExecution`
- SMS : `StartAutomationExecution`
- formation des nuages : `DescribeStacks`
- formation des nuages : `UpdateStack`
- kms: `Decrypt`
- km : `GenerateDataKey`
- sns: `Publish`
- sqs : `GetQueueAttributes`

### Étapes de document

- `CheckCfnSnsLimits` (AWS:ExecuteScript) - Vérifie que le nombre maximum de sujets Amazon SNS n'a pas déjà été associé à la pile que vous spécifiez. AWS CloudFormation
- `EnableCfnSnsNotification` (aws :executeAwsApi) - Active les notifications Amazon SNS pour la AWS CloudFormation pile.
- `VerificationCfnSnsNotification` (AWS:ExecuteScript) - Vérifie que les notifications Amazon SNS ont été activées pour la pile. AWS CloudFormation

### Sorties

`CheckCfnSnsLimits`. `NotificationArnList` - Une liste des ARN qui reçoivent des notifications Amazon SNS pour AWS CloudFormation la pile.

`VerificationCfnSnsNotification`. `VerifySnsTopicsResponse` - Réponse de l'opération d'API confirmant que les notifications Amazon SNS ont été activées pour la AWS CloudFormation pile.

# AWS-RunCfnLint

## Description

Ce runbook utilise un [AWS CloudFormationLinter](#) (`cfn-python-lint`) pour valider les modèles YAML et JSON par rapport à la spécification de la AWS CloudFormation ressource. Le AWS-RunCfnLint runbook effectue des vérifications supplémentaires, notamment en s'assurant que des valeurs valides ont été saisies pour les propriétés des ressources. Si la validation échoue, l'étape RunCfnLintAgainstTemplate échoue et la sortie de l'outil linter est fournie dans un message d'erreur. Ce runbook utilise `cfn-lint v0.24.4`.

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- ConfigureRuleFlag

Type : String

Description : (Facultatif) Options de configuration d'une règle à transmettre au paramètre `--configure-rule`.

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

- FormatFlag

Type : String

Description : (Facultatif) Valeur à transmettre au paramètre `--format` pour spécifier le format de sortie.

Valeurs valides : Default | quiet | parseable | json

Par défaut : Default

- IgnoreChecksFlag

Type : String

Description : (Facultatif) ID des règles à transmettre au paramètre `--ignore-checks`. Ces règles ne sont pas vérifiées.

Exemple : E1001, E1003, W7001

- IncludeChecksFlag

Type : String

Description : (Facultatif) ID des règles à transmettre au paramètre `--include-checks`. Ces règles sont vérifiées.

Exemple : E1001, E1003, W7001

- InfoFlag

Type : String

Description : (Facultatif) Option du paramètre `--info`. Incluez l'option permettant d'activation des informations de journalisation supplémentaires sur le traitement du modèle.

Par défaut : faux

- TemplateFileName

Type : String

Description : Nom, ou clé, du fichier modèle dans le compartiment S3.

- **Modèles3 BucketName**

Type : String

Description : Nom du compartiment S3 contenant le modèle de packer.

- **RegionsFlag**

Type : String

Description : (Facultatif) Valeurs à transmettre au `--regions` paramètre for pour tester le modèle par rapport à la valeur spécifiée Régions AWS.

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

### Étapes de document

`RunCfnLintAgainstTemplate`— Exécute l'`cfn-python-lint` outil sur le AWS CloudFormation modèle spécifié.

### Sorties

`RunCfnLintAgainstTemplate.output` — La sortie standard de l'outil. `cfn-python-lint`

## **AWSSupport-TroubleshootCFNCustomResource**

### Description

Le `AWSSupport-TroubleshootCFNCustomResource` runbook permet de diagnostiquer les raisons pour lesquelles une AWS CloudFormation pile n'a pas réussi à créer, à mettre à jour ou à supprimer une ressource personnalisée. Le runbook vérifie le jeton de service utilisé pour la ressource personnalisée et le message d'erreur renvoyé. Après avoir examiné les détails de la ressource personnalisée, la sortie du runbook fournit une explication du comportement de la pile et des étapes de résolution des problèmes pour la ressource personnalisée.

[Exécutez cette automatisation \(console\)](#)

### Type de document

### Automatisation

### Propriétaire



## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- StackName

Type : String

Description : (Obligatoire) Le nom de la AWS CloudFormation pile dans laquelle la ressource personnalisée a échoué.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

## Étapes de document

- `validateCloudFormationStack`- Vérifie que la AWS CloudFormation pile existe dans la même bandeCompte AWS. Région AWS
- `checkCustomResource`- Analyse la AWS CloudFormation pile, vérifie la ressource personnalisée défailante et génère des informations sur la manière de résoudre les problèmes liés à la ressource personnalisée défailante.

## AWS-UpdateCloudFormationStack

### Description

Mettez à jour une AWS CloudFormation pile à l'aide d'un AWS CloudFormation modèle stocké dans un compartiment Amazon S3.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Linux, macOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- `LambdaAssumeRole`

Type : String

Description : (Obligatoire) L'ARN du rôle assumé par Lambda

- StackNameOrId

Type : String

Description : (Obligatoire) nom ou ID unique de la pile AWS CloudFormation à mettre à jour

- TemplateUrl

Type : String

Description : (Obligatoire) Emplacement du compartiment S3 qui contient le CloudFormation modèle mis à jour (par ex. `https://s3.amazonaws.com/doc-example-bucket/updated.template`)

## CloudFront

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon CloudFront. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

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

## AWSConfigRemediation-EnableCloudFrontDefaultRootObject

### Description

Le `AWSConfigRemediation-EnableCloudFrontDefaultRootObject` runbook configure l'objet racine par défaut pour la distribution Amazon CloudFront (CloudFront) que vous spécifiez.

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- CloudFrontDistributionId

Type : String

Description : (Obligatoire) ID de la CloudFront distribution pour laquelle vous souhaitez configurer l'objet racine par défaut.

- DefaultRootObject

Type : String

Description : (Obligatoire) Objet que vous CloudFront souhaitez renvoyer lorsqu'une requête d'utilisateur pointe vers votre URL racine.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

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

### Étapes de document

- `aws:executeScript`- Configure l'objet racine par défaut pour la CloudFront distribution que vous spécifiez dans le `CloudFrontDistributionId` paramètre.

## AWSConfigRemediation-EnableCloudFrontAccessLogs

### Description

Le `AWSConfigRemediation-EnableCloudFrontAccessLogs` runbook active la journalisation des accès pour la distribution Amazon CloudFront (CloudFront) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Linux,macOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `BucketName`

Type : chaîne

Description : (Obligatoire) Le nom du compartiment Amazon Simple Storage Service (Amazon S3) dans lequel vous souhaitez stocker les données d'accès se connecte. Les compartiments des répertoires `af-south-1`, `ap-east-1`, `eu-south-1` et `me-south-1` ne sont pas pris en charge. Région AWS

- `CloudFrontId`

Type : chaîne

Description : (Obligatoire) L'ID de la CloudFront distribution à laquelle vous souhaitez autoriser l'accès et la connexion.

- `IncludeCookies`

Type : booléen

Valeurs valides : `true` | `false`

Description : (Obligatoire) Définissez ce paramètre sur `true`, si vous souhaitez que les cookies soient inclus dans les journaux d'accès.

- `Préfixe`

Type : chaîne


Description : (Facultatif) Chaîne facultative que vous CloudFront souhaitez préfixer dans le journal `filenames` d'accès de votre distribution, `myprefix/` par exemple.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

- `s3:PutBucketAc1`

 Note

L'`s3:GetBucketLocationAPI` ne peut être utilisée que pour les compartiments S3 d'un même compte. Vous ne pouvez pas l'utiliser pour les compartiments S3 entre comptes.

## Étapes de document

- `aws:executeScript`- Active la journalisation des accès pour la CloudFront distribution que vous spécifiez dans le `CloudFrontDistributionId` paramètre.

# **AWSConfigRemediation- EnableCloudFrontOriginAccessIdentity**

## Description

Le `AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity` runbook active l'identité d'accès à l'origine pour la distribution Amazon CloudFront (CloudFront) que vous spécifiez. Cette automatisation attribue la même identité CloudFront d'accès à l'origine à toutes les origines du type d'origine Amazon Simple Storage Service (Amazon S3) sans identité d'accès à l'origine pour la CloudFront distribution que vous spécifiez. Cette automatisation n'accorde pas d'autorisation de lecture à l'identité d'accès d'origine CloudFront pour accéder aux objets de votre compartiment Amazon S3. Vous devez mettre à jour les autorisations de votre compartiment Amazon S3 pour autoriser l'accès.

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

## LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- CloudFrontDistributionId

Type : String

Description : (Obligatoire) L'ID de la CloudFront distribution sur laquelle vous souhaitez activer le basculement d'origine.

- OriginAccessIdentityId

Type : String

Description : (Obligatoire) L'ID de l'identité CloudFront d'accès à l'origine à associer à l'origine.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- aws:executeScript- Active l'identité d'accès d'origine pour la CloudFront distribution que vous spécifiez dans le CloudFrontDistributionId paramètre et vérifie que l'identité d'accès d'origine a été attribuée.



# AWSConfigRemediation-EnableCloudFrontOriginFailover

## Description

Le `AWSConfigRemediation-EnableCloudFrontOriginFailover` runbook active le basculement d'origine pour la distribution Amazon CloudFront (CloudFront) que vous spécifiez.

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- CloudFrontDistributionId

Type : String

Description : (Obligatoire) L'ID de la CloudFront distribution sur laquelle vous souhaitez activer le basculement d'origine.

- OriginGroupId

Type : String

Description : (Obligatoire) ID du groupe d'origine.

- PrimaryOriginId

Type : String

Description : (Obligatoire) L'identifiant de l'origine principale dans le groupe d'origine.

- SecondaryOriginId

Type : String

Description : (Obligatoire) L'identifiant de l'origine secondaire dans le groupe d'origine.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- aws:executeScript- Active le basculement d'origine pour la CloudFront distribution que vous spécifiez dans le CloudFrontDistributionId paramètre et vérifie que le basculement a été activé.

## **AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS**

### Description

Le AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS runbook active la politique de protocole d'affichage pour la distribution Amazon CloudFront (CloudFront) que vous spécifiez.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux, macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- CloudFrontDistributionId

Type : String

Description : (Obligatoire) L'ID de la CloudFront distribution sur laquelle vous souhaitez activer la politique de protocole du lecteur.

- ViewerProtocolPolicy

Type : String

Valeurs valides : https uniquement, redirect-to-https

Description : (Obligatoire) Protocole que les utilisateurs peuvent utiliser pour accéder aux fichiers d'origine.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

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

### Étapes de document

- `aws:executeScript`- Active la politique de protocole du visualiseur pour la CloudFront distribution que vous spécifiez dans le `CloudFrontDistributionId` paramètre et vérifie que la politique a été attribuée.

## CloudTrail

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS CloudTrail. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

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

## **AWSConfigRemediation-CreateCloudTrailMultiRegionTrail**

### Description

Le `AWSConfigRemediation-CreateCloudTrailMultiRegionTrail` runbook crée une trace AWS CloudTrail (CloudTrail) qui transmet les fichiers journaux de plusieurs utilisateurs Régions AWS au bucket Amazon Simple Storage Service (Amazon S3) de votre choix.

[Exécutez cette automatisation \(console\)](#)

### Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

Linux, macOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- BucketName

Type : String

Description : (Obligatoire) Le nom du compartiment Amazon S3 vers lequel vous souhaitez charger les journaux.

- KeyPrefix

Type : String

Description : (Facultatif) Le préfixe de clé Amazon S3 qui suit le nom du compartiment que vous avez désigné pour la livraison du fichier journal.

- TrailName

Type : String

Description : (Obligatoire) Le nom du CloudTrail parcouru à créer.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeAwsApi`- Accepte le nom du journal et le nom du compartiment Amazon S3 en tant qu'entrée et crée un CloudTrail journal.
- `aws:executeAwsApi`- Active la journalisation sur le journal créé et lance la livraison du journal vers le compartiment Amazon S3 que vous avez spécifié.
- `aws:assertAwsResourceProperty`- Vérifie que le CloudTrail parcours a été créé.

## AWS-EnableCloudTrail

### Description

Créez un suivi AWS CloudTrail et configurez la journalisation d'un compartiment S3.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- S3 BucketName

Type : String

Description : (obligatoire) nom du compartiment S3 désigné pour publier des fichiers journaux.

### Note

Le compartiment S3 doit exister et la stratégie de compartiment doit accorder à CloudTrail l'autorisation d'écrire dessus. Pour plus d'informations, consultez la [politique relative aux compartiments Amazon S3 pour CloudTrail](#).

- TrailName

Type : String

Description : (Obligatoire) nom du nouveau suivi.

## AWS-EnableCloudTrailCloudWatchLogs

### Description

Ce runbook met à jour la configuration d'un ou de plusieurs AWS CloudTrail sentiers pour envoyer des événements à un groupe de CloudWatch journaux Amazon Logs.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- CloudWatchLogsLogGroupArn

Type : chaîne

Description : (Obligatoire) L'ARN du groupe de CloudWatch journaux dans lequel les CloudTrail journaux seront livrés.

- CloudWatchLogsRoleArn

Type : chaîne

Description : (Obligatoire) L'ARN du rôle IAM CloudWatch Logs Logs suppose d'écrire dans le groupe de journaux spécifié.

- TrailNames

Type : StringList

Description : (Obligatoire) Liste séparée par des virgules des noms des CloudTrail sentiers dont vous souhaitez envoyer les événements à CloudWatch Logs.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.



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

### Étapes de document

- `aws:executeScript`- Met à jour les CloudTrail traces spécifiées pour transmettre les événements au groupe de CloudWatch journaux Logs spécifié.

## **AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS**

### Description

Le `AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS` runbook chiffre une trace AWS CloudTrail (CloudTrail) à l'aide de la clé gérée par le client AWS Key Management Service (AWS KMS) que vous spécifiez. Ce runbook ne doit être utilisé que comme base de référence pour garantir que vos CloudTrail traces sont cryptées conformément aux meilleures pratiques de sécurité minimales recommandées. Nous vous recommandons de crypter plusieurs pistes avec différentes clés KMS. CloudTrailles fichiers de résumé ne sont pas chiffrés. Si vous avez déjà défini le `EnableLogFileValidation` paramètre sur « true Pour le suivi », consultez la section « Utiliser le chiffrement côté serveur avec des clés AWS KMS gérées » de la rubrique [Meilleures pratiques de sécurité CloudTrail préventive](#) du Guide de l'AWS CloudTrailutilisateur pour plus d'informations.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- KMS KeyId

Type : String

Description : (Obligatoire) L'ARN, l'ID de clé ou l'alias de clé de la clé gérée par le client que vous souhaitez utiliser pour chiffrer le journal que vous spécifiez dans le `TrailName` paramètre.

- TrailName

Type : String

Description : (Obligatoire) L'ARN ou le nom du journal que vous souhaitez mettre à jour pour qu'il soit chiffré.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

## Étapes de document

- `aws:executeAwsApi`- Active le chiffrement sur la piste que vous spécifiez dans le `TrailName` paramètre.
- `aws:executeAwsApi`- Rassemble l'ARN de la clé gérée par le client que vous spécifiez dans le `KMSKeyId` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que le chiffrement a été activé sur la `CloudTrail` piste.

# AWS-EnableCloudTrailKmsEncryption

## Description

Ce runbook met à jour la configuration d'un ou de plusieurs AWS CloudTrail sentiers pour utiliser le chiffrement AWS Key Management Service (AWS KMS).

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- KMS KeyId

Type : chaîne

Description : (Obligatoire) L'ID de la clé gérée par le client que vous souhaitez utiliser pour chiffrer le suivi que vous spécifiez dans le `TrailName` paramètre. La valeur peut être un nom d'alias préfixé par « alias/ », un ARN entièrement spécifié pour un alias ou un ARN entièrement spécifié pour une clé.

- TrailNames

Type : StringList

Description : (Obligatoire) Liste séparée par des virgules des pistes que vous souhaitez mettre à jour pour qu'elles soient chiffrées.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeScript`- Active le AWS KMS chiffrement sur les pistes que vous spécifiez dans le `TrailName` paramètre.

## **AWSConfigRemediation-EnableCloudTrailLogFileValidation**

### Description

Le `AWSConfigRemediation-EnableCloudTrailLogFileValidation` runbook permet de valider le fichier journal de votre AWS CloudTrail parcours.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- **AutomationAssumeRole**

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- **TrailName**

Type : chaîne

Description : (Obligatoire) Le nom ou le nom de ressource Amazon (ARN) du journal pour lequel vous souhaitez activer la validation du journal.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

#### Étapes de document

- `aws:executeAwsApi`- Active la validation du journal pour le AWS CloudTrail parcours que vous spécifiez dans le `TrailName` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que la validation du journal est activée pour votre parcours.

## **AWS-EnableCloudTrailLogFileValidation**

### Description

Le `AWS-EnableCloudTrailLogFileValidation` runbook permet de valider le fichier journal pour les AWS CloudTrail sentiers que vous spécifiez.

## [Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- TrailNames

Type : StringList

Description : (Obligatoire) Liste séparée par des virgules des noms des CloudTrail sentiers pour lesquels vous souhaitez activer la validation du journal.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- cloudtrail:GetTrail
- cloudtrail:UpdateTrail

### Étapes de document

- `aws:executeScript`- Active la validation du journal pour les AWS CloudTrail sentiers que vous spécifiez dans le `TrailNames` paramètre.

## AWS-QueryCloudTrailLogs

### Description

Le `AWS-QueryCloudTrailLogs` runbook crée une table Amazon Athena à partir du compartiment Amazon Simple Storage Service (Amazon S3) de votre choix contenant des journaux AWS CloudTrail (CloudTrail). Après avoir créé la table, l'automatisation exécute les requêtes SQL que vous spécifiez, puis supprime la table.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- `Query`

Type : String

Description : (Obligatoire) La requête SQL que vous souhaitez exécuter.

- **SourceBucketPath**

Type : String

Description : (Obligatoire) Le nom du compartiment Amazon S3 contenant les fichiers CloudTrail journaux que vous souhaitez interroger.

- **TableName**

Type : String

Description : (Facultatif) Nom de la table Athena créée par l'automatisation.

Par défaut : cloudtrail\_logs

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`



## Étapes de document

- `aws:executeAwsApi`- Crée une table Athéna.
- `aws:executeAwsApi`- Exécute la chaîne de requête que vous avez spécifiée dans le Query paramètre.
- `aws:executeScript`- Sonde et attend que la requête soit terminée.
- `aws:executeAwsApi`- Obtient les résultats de la requête.
- `aws:executeAwsApi`- Supprime la table créée par l'automatisation.

## CloudWatch

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon CloudWatch. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

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

## AWS-ConfigureCloudWatchOnEC2Instance

### Description

Activez ou désactivez la surveillance CloudWatch détaillée d'Amazon sur les instances gérées.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux, macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance Amazon EC2 sur laquelle vous souhaitez activer la CloudWatch surveillance.

- propriétés

Type : String

Description : (Facultatif) Ce paramètre n'est pas pris en charge. Répertoire ici pour des raisons de compatibilité descendante.

- status

Valeurs valides : Activé | Désactivé

Description : (Facultatif) spécifie s'il convient d'activer ou de désactiver CloudWatch.

Par défaut : Enabled

## Étapes de document

configureCloudWatch- Configure CloudWatch sur l'instance Amazon EC2 avec le statut indiqué.

## Sorties

Cette automatisation n'a aucune sortie.

## **AWS-EnableCWAlarm**

### Description

Le `AWS-EnableCWAlarm` runbook crée des alarmes Amazon CloudWatch (CloudWatch) pour les AWS ressources de votre ordinateur Compte AWS qui n'en possèdent pas déjà une. CloudWatch des alarmes sont créées pour les AWS ressources suivantes :

- Instances Amazon Elastic Compute Cloud (Amazon EC2)
- Volumes Amazon Elastic Block Store (Amazon EBS)
- Compartiments Amazon Simple Storage Service (Amazon S3)
- Clusters Amazon Relational Database Service (Amazon RDS)

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `ComparisonOperator`

Type : chaîne

Valeurs valides : `GreaterThanOrEqualToThreshold` | `GreaterThanThreshold` | `GreaterThanUpperThreshold` | `LessThanLowerOrGreaterThanUpper Seuil` | `LessThanLowerThreshold` | `LessThanOrEqualToThreshold` `LessThanThreshold`

Description : (Obligatoire) Opération arithmétique à utiliser lors de la comparaison de la statistique et du seuil spécifiés.

- MetricName

Type : chaîne

Description : (Obligatoire) Nom de la métrique associée à l'alarme.

- Période

Type : entier

Valeurs valides : 10 | 30 | 60 | Un multiple de 60

Description : (Obligatoire) Période, en secondes, sur laquelle la statistique est appliquée.

- Arns relatifs aux ressources

Type : StringList

Description : (Obligatoire) Liste séparée par des virgules des ARN des ressources pour lesquelles créer une alarme CloudWatch

- Statistique

Type : chaîne

Valeurs valides : Moyenne | Maximum | Minimum | SampleCount | Somme

Description : (Obligatoire) La statistique de la métrique associée à l'alarme.

- Seuil

Type : entier

Description : (Obligatoire) La valeur à comparer avec la statistique spécifiée.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- cloudwatch:PutMetricAlarm

## Étapes de document

- `aws:executeScript`- Crée une CloudWatch alarme en fonction des valeurs spécifiées dans les paramètres du runbook pour les ressources que vous spécifiez dans le `ResourceARNs` paramètre.

## Sorties

Activez l'alarme. `FailedResources`: liste des ARN des ressources pour lesquelles aucune CloudWatch alarme n'a été créée et la raison de l'échec.

Activez l'alarme. `SuccessfulResources`: liste des ARN des ressources pour lesquelles une CloudWatch alarme a été créée avec succès.

# Amazon DocumentDB

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon DocumentDB (compatibles avec MongoDB). Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-EnableDocDbClusterBackupRetentionPeriod](#)

## AWS-EnableDocDbClusterBackupRetentionPeriod

### Description

Le `AWS-EnableDocDbClusterBackupRetentionPeriod` runbook active une période de conservation des sauvegardes pour le cluster Amazon DocumentDB que vous spécifiez. Cette fonctionnalité définit le nombre total de jours pendant lesquels une sauvegarde automatique est conservée. Pour modifier un cluster, celui-ci doit être dans l'état disponible avec un type de moteur `dedocdb`.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

## Amazon

### Plateformes

Linux macOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- DB ClusterResourceid

Type : chaîne

Description : (Obligatoire) L'ID de ressource du cluster Amazon DocumentDB pour lequel vous souhaitez activer la période de conservation des sauvegardes.

- BackupRetentionPeriod

Type : entier

Description : (Obligatoire) Nombre de jours pendant lesquels les sauvegardes automatisées sont conservées. Doit être une valeur comprise entre 7 et 35 jours.

- PreferredBackupWindow

Type : chaîne

Description : (Facultatif) Une plage horaire quotidienne en temps universel coordonné (UTC) au format hh24:mm-hh24:mm, par exemple 07:14-07:44. La valeur doit être d'au moins 30 minutes et ne doit pas entrer en conflit avec le créneau de maintenance préféré.

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

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

## Étapes de document

- `GetDocDbClusterIdentifier` (aws :executeAwsApi) - Renvoie l'identifiant du cluster Amazon DocumentDB à l'aide de l'ID de ressource fourni.
- `VerifyDocDbEngine` (aws : assertAwsResource Propriété) - Vérifie que le type de moteur Amazon DocumentDB `docdb` est destiné à empêcher toute modification involontaire d'autres types de moteurs Amazon RDS.
- `VerifyDocDbStatus` (aws : waitAwsResource Propriété) - Vérifie que l'état du cluster Amazon DocumentDB est `available`
- `ModifyDocDbRetentionPeriod` (aws :executeAwsApi) - Définit la période de rétention en utilisant les valeurs fournies pour le cluster Amazon DocumentDB spécifié.
- `VerifyDocDbBackupsEnabled` (AWS:ExecuteScript) - Vérifie que la période de rétention pour le cluster Amazon DocumentDB et que la fenêtre de sauvegarde préférée, si elle est spécifiée, ont été correctement définies.

## Sorties

`ModifyDocDbRetentionPeriod`. `ModifyDbClusterResponse` - Réponse de l'opération `ModifyDBCluster` API.

`VerifyDocDbBackupsEnabled`. `VerifyDbClusterBackupsEnabledResponse` - Résultat de l'`VerifyDocDbBackupsEnabled` étape de confirmation de la modification réussie du cluster Amazon DocumentDB.

## CodeBuild

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS CodeBuild. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK](#)

- [AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject](#)

## AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

### Description

Le AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK runbook chiffre les artefacts de construction d'un projet AWS CodeBuild (CodeBuild) à l'aide de la clé gérée par le client AWS Key Management Service (AWS KMS) que vous spécifiez. AWS Config doit être activé dans l' Région AWS endroit où vous exécutez cette automatisation.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Linux, macOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- KMS KeyId

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) de la clé gérée par le AWS KMS client que vous souhaitez utiliser pour chiffrer le CodeBuild projet que vous spécifiez dans le ProjectId paramètre.

- ProjectId



Type : chaîne

Description : (Obligatoire) L'ID du CodeBuild projet dont vous souhaitez chiffrer les artefacts de construction.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeAwsApi`- Regroupe le nom du CodeBuild projet à partir de l'identifiant du projet.
- `aws:executeAwsApi`- Active le chiffrement sur le CodeBuild projet que vous spécifiez dans le `ProjectId` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que le chiffrement a été activé sur le CodeBuild projet.

### Sorties

`UpdateLambdaConfig`. `UpdateFunctionConfigurationResponse` - Réponse de l'appel `UpdateFunctionConfiguration` d'API.

## **AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject**

### Description

Le `AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject` runbook supprime les variables d'`AWS_SECRET_ACCESS_KEY`environnement `AWS_ACCESS_KEY_ID` et du projet `AWS`

CodeBuild (CodeBuild) que vous spécifiez. AWS Config doit être activé Région AWS là où vous exécutez cette automatisation.

### [Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- ResourceId

Type : String

Description : (Obligatoire) L'ID du CodeBuild projet dont vous souhaitez supprimer les variables d'environnement clés d'accès.

Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

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

### Étapes de document

- `aws:executeScript`- Supprime les variables d'environnement de clé d'accès pour le CodeBuild projet spécifié dans le `ResourceId` paramètre.

## AWS CodeDeploy

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS CodeDeploy. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSSupport-TroubleshootCodeDeploy](#)

## AWSSupport - TroubleshootCodeDeploy

### Description

Le `AWSSupport-TroubleshootCodeDeploy` runbook permet de diagnostiquer les raisons de l'échec d'un AWS CodeDeploy déploiement sur une instance Amazon Elastic Compute Cloud (Amazon EC2). Le runbook indique les étapes à suivre pour vous aider à résoudre le problème ou à le résoudre davantage. Les meilleures pratiques pour CodeDeploy sont également fournies pour vous aider à éviter des problèmes similaires à l'avenir.

Ce runbook peut vous aider à résoudre les problèmes suivants :

- L'`CodeDeployAgent` n'est pas installé ou ne s'exécute pas sur l'instance Amazon EC2
- Aucun profil d'instance AWS Identity and Access Management (IAM) n'est associé à l'instance Amazon EC2
- Le profil d'instance IAM attaché à l'instance Amazon EC2 ne dispose pas des autorisations Amazon Simple Storage Service (Amazon S3) requises
- Une révision stockée dans Amazon S3 est manquante, ou le compartiment Amazon S3 utilisé se trouve dans une Région AWS instance différente de l'instance Amazon EC2

- Problèmes liés au fichier de spécification de l'application (AppSpec)
- Erreurs « Le fichier existe déjà à l'emplacement »
- Les crochets d'événements du cycle de vie CodeDeploy gérés ont échoué
- Échec des crochets d'événements du cycle de vie gérés par le
- Événements de mise à l'échelle pendant le déploiement

### [Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- DeploymentId

Type : String

Description : (Obligatoire) L'ID du déploiement qui a échoué.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance Amazon EC2 où le déploiement a échoué.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

## Étapes de document

- `aws:executeAwsApi`- Vérifie les valeurs fournies pour les `InstanceId` paramètres `DeploymentId` et.
- `aws:executeScript`- Recueille des informations à partir de l'instance Amazon EC2, telles que l'état de l'instance et les détails du profil de l'instance IAM.
- `aws:executeScript`- Examine le déploiement spécifié et renvoie une analyse expliquant pourquoi le déploiement a échoué.

## AWS Config

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Config. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSSupport-SetupConfig](#)

## AWSSupport-SetupConfig

### Description

Le `AWSSupport-SetupConfig` runbook crée un rôle lié à un service AWS Identity and Access Management (IAM), un enregistreur de configuration alimenté par AWS Config et un canal de distribution avec un bucket Amazon Simple Storage Service (Amazon S3) qui AWS Config envoie des instantanés de configuration et des fichiers d'historique de configuration. Si vous spécifiez des valeurs pour les `AggregatorAccountRegion` paramètres `AggregatorAccountId` et, le runbook

créé également des autorisations pour l'agrégation de données afin de collecter des données de AWS Config configuration et de conformité provenant de plusieurs et de plusieurs Comptes AWS. Régions AWS Pour en savoir plus sur l'agrégation des données provenant de plusieurs comptes et régions, consultez la section [Agrégation de données multicomptes et multirégions](#) dans le Guide du développeur. AWS Config

### [Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux macOS, Windows

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- AggregatorAccountId

Type : String

Description : (Facultatif) L'ID de l'Compte AWS endroit où un agrégateur sera ajouté pour agréger les données de AWS Config configuration et de conformité provenant de plusieurs comptes et Régions AWS. Ce compte est également utilisé par l'agrégateur pour autoriser les comptes sources.

- AggregatorAccountRegion

Type : String

Description : (Facultatif) Région dans laquelle un agrégateur sera ajouté pour agréger les données de AWS Config configuration et de conformité provenant de plusieurs comptes et régions.

- IncludeGlobalResourcesRegion

Type : String

Par défaut : us-east-1

Description : (Obligatoire) Pour éviter d'enregistrer des données de ressources globales dans chaque région, spécifiez une région à partir de laquelle enregistrer les données de ressources globales.

- Partition

Type : String

Par défaut : aws

Description : (Obligatoire) Partition à partir de laquelle vous souhaitez collecter des données de AWS Config configuration et de conformité.

- S3 BucketName

Type : String

Par défaut : aws-config-delivery-channel

Description : (Facultatif) Le nom que vous souhaitez appliquer au compartiment Amazon S3 créé pour le canal de livraison. L'identifiant du compte est ajouté à la fin du nom.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

- `aws:executeScript`- Crée un rôle IAM lié à un service AWS Config s'il n'en existe pas déjà un.
- `aws:executeScript`- Crée un enregistreur de configuration s'il n'en existe pas déjà un.
- `aws:executeScript`- Crée un compartiment Amazon S3 à utiliser par le canal de distribution s'il n'en existe pas déjà un.
- `aws:executeScript`- Crée un canal de distribution à l'aide des ressources créées par le runbook.
- `aws:executeAwsApi`- Démarre l'enregistreur de configuration.
- `aws:executeScript`- Si vous avez spécifié des valeurs pour les `AggregatorAccountRegion` paramètres `AggregatorAccountId` et, les autorisations pour l'agrégation de données multi-comptes et multirégions sont configurées.

## Amazon Connect

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Connect. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSSupport-AssociatePhoneNumbersToConnectContactFlows](#)

## AWSSupport-AssociatePhoneNumbersToConnectContactFlows

### Description



`AWSSupport-AssociatePhoneNumbersToConnectContactFlows` Cela vous permet d'associer des numéros de téléphone aux flux de contacts dans votre instance Amazon Connect. En fournissant les mappages des numéros de téléphone et des flux de contacts dans un fichier de valeurs séparées par des virgules (CSV) en entrée, le runbook associe autant de numéros de téléphone que possible aux flux de contacts en 14,5 minutes. Le runbook produit un fichier CSV contenant toutes les paires de numéros de téléphone et de flux de contacts qu'il n'a pas pu associer dans le délai imparti, afin que vous puissiez les saisir lors de la prochaine exécution.

Comment fonctionne-t-il ?

Le runbook `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` permet d'associer des numéros de téléphone aux flux de contacts de votre instance Amazon Connect à l'aide d'un fichier CSV contenant des données de mappage qui est stocké dans un bucket Amazon Simple Storage Service (Amazon S3). Le fichier CSV d'entrée doit être aligné sur le format suivant, avec des `PhoneNumber` valeurs au format [E.164](#).

Exemple de fichier CSV d'entrée

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

Le runbook d'automatisation crée également les fichiers suivants dans l'emplacement de destination spécifié dans le `DestinationFileBucket` et `DestinationFilePath`.

- **`automation:EXECUTION_ID/ResourceIdList.csv`**: fichier temporaire contenant les `ContactFlowId` paires `PhoneNumberId` et requises pour l'`AssociatePhoneNumberContactFlowAPI`.
- **`automation:EXECUTION_ID/ErrorResourceList.csv`**: fichier contenant les paires de numéros de téléphone et de flux de contacts qui n'ont pas pu être traitées en raison d'une erreur, par exemple `ResourceNotFoundException` au format `dePhoneNumber,ContactFlowName,ErrorMessage`.
- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`**: fichier contenant les paires de numéros de téléphone et de flux de contacts qui n'ont pas été traitées. Le runbook essaie de traiter autant de numéros de téléphone et de flux de contacts que possible dans un délai de 14,5 minutes (15 minutes d'expiration de la AWS Lambda fonction - 30 secondes de mémoire tampon). Si certains numéros de téléphone ou flux de contacts n'ont pas pu être traités en raison

de contraintes de temps, le runbook les inclut dans un fichier CSV à utiliser comme entrée pour la prochaine exécution du runbook.

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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"
    }
  ]
}
```

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez [AWSsupport-AssociatePhoneNumbersToConnectContactFlows](#) à Systems Manager sous Documents.
2. Sélectionnez Exécute automation (Exécuter l'automatisation).
3. Pour les paramètres d'entrée, entrez ce qui suit :

- AutomationAssumeRole (Facultatif)

Amazon Resource Name (ARN) du rôle AWS AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ConnectInstanceid (Obligatoire)

L'ID de votre instance Amazon Connect.

- SourceFileBucket (Obligatoire)

Le compartiment Amazon S3 qui stocke le fichier CSV contenant le numéro de téléphone et les paires de flux de contacts.

- SourceFilePath (Obligatoire)

La clé d'objet Amazon S3 du fichier CSV qui contient le numéro de téléphone et les paires de flux de contacts. Par exemple, path/to/input.csv.

- DestinationFileBucket (Obligatoire)

Le compartiment Amazon S3 dans lequel l'automatisation placera un fichier intermédiaire et un rapport de résultats.

- DestinationFilePath (Facultatif)

Le chemin de l'objet Amazon S3 `DestinationFileBucket` sous lequel un fichier intermédiaire et un rapport de résultats doivent être stockés. Par exemple, si vous le spécifiez `path/to/files/`, les fichiers sont stockés sous `s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`.

- `S3BucketOwnerAccount` (facultatif)

Numéro de AWS compte propriétaire du compartiment Amazon S3 dans lequel vous souhaitez télécharger le journal du flux de contacts. Si vous ne spécifiez pas ce paramètre, les runbooks utilisent l'ID de AWS compte de l'utilisateur ou du rôle dans lequel l'automatisation s'exécute.

- `S3BucketOwnerRoleArn` (facultatif)

L'ARN du rôle IAM autorisé à obtenir les paramètres d'accès public au compartiment Amazon S3 et au blocage du compte, à la configuration du chiffrement du compartiment, aux ACL du compartiment, à l'état de la politique du compartiment et au téléchargement d'objets dans le compartiment. Si ce paramètre n'est pas spécifié, le runbook utilise le `AutomationAssumeRole` (si spécifié) ou l'utilisateur qui démarre ce runbook (s'il n'`AutomationAssumeRole` est pas spécifié). Consultez la section relative aux autorisations requises dans la description du runbook.

Input parameters	
<p><b>AutomationAssumeRole</b> (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</p> <p>test-role</p>	<p><b>ConnectInstanceId</b> (Required) The ID of your Amazon Connect instance.</p> <p>01234567-89ab-cdef-0123-456789abcdef</p>
<p><b>SourceFileBucket</b> (Required) The Amazon S3 bucket name that stores the CSV file which contains the pairs of phone numbers and Contact Flows.</p> <p>[REDACTED]</p>	<p><b>SourceFilePath</b> (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".</p> <p>String</p>
<p><b>DestinationFileBucket</b> (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.</p> <p>[REDACTED]</p>	<p><b>DestinationFilePath</b> (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://&lt;DestinationFileBucket&gt;/path/to/files/&lt;automation:EXECUTION_ID&gt;".</p> <p>String</p>
<p><b>S3BucketOwnerAccount</b> (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.</p> <p>String</p>	<p><b>S3BucketOwnerRoleArn</b> (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.</p>

4. Sélectionnez Exécuter.
5. L'automatisation démarre.
6. Le document exécute les étapes suivantes :

- `CheckConnectInstanceExistence`

Vérifie si l'instance Amazon Connect fournie `ConnectInstanceId` existe.

- `Chèques 3 BucketPublicStatus`

Vérifie si les compartiments Amazon S3 spécifiés dans le `SourceFileBucket` et `DestinationFileBucket` autorisent des autorisations d'accès anonymes ou publiques en lecture ou en écriture.

- `CheckSourceFileExistenceAndSize`

Vérifie si le fichier CSV source spécifié dans le `SourceFilePath` existe et si la taille du fichier dépasse la limite de 25 Mo.

- `GenerateResourceIdMap`

Télécharge le fichier CSV source spécifié dans le `SourceFilePath` et identifie `PhoneNumberId` et `ContactFlowId` pour chaque ressource. Une fois cela fait, il télécharge un fichier CSV contenant `PhoneNumber`, `PhoneNumberIdContactFlowName`, et `ContactFlowId` dans le compartiment Amazon S3 de destination spécifié dans `DestinationFileBucket`. S'il `PhoneNumberId` n'est pas possible d'identifier un certain nombre, le fichier sera vide dans le fichier CSV.

- `AssociatePhoneNumbersToContactFlows`

Crée une AWS Lambda fonction dans votre compte à l'aide d'une AWS CloudFormation pile. La AWS Lambda fonction associe chaque numéro à un flux de contacts répertorié dans le fichier CSV source spécifié dans `SourceFileBucket` `SourceFilePath` et la AWS CloudFormation pile invoque la fonction. La AWS Lambda fonction associe autant de numéros de téléphone aux flux de contacts que possible avant l'expiration du délai (15 minutes). La liste des numéros de téléphone et des flux de contacts qui n'ont pas pu être traités en raison d'une erreur est importée `[automation:EXECUTION_ID]/ErrorResourceList.csv`. Les numéros qui n'ont pas pu être traités en raison d'un dépassement du nombre maximum de numéros de téléphone pouvant être traités en une seule exécution sont chargés dans `[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. Si cette étape échoue, elle passe à l'`DescribeCloudFormationErrorFromStackEvents` étape pour montrer pourquoi elle a échoué à cause d'événements de AWS CloudFormation pile.

- `WaitForPhoneNumberContactFlowAssociationCompletion`

Attend que la AWS Lambda fonction qui associe les numéros de téléphone aux flux de contacts soit créée et que la AWS CloudFormation pile termine son invocation.

- `GenerateReport`

Génère le rapport qui contient le nombre de numéros de téléphone mappés aux flux de contacts, ceux qui n'ont pas pu être traités en raison d'une erreur et ceux qui n'ont pas pu être traités en raison d'un dépassement du nombre maximum de numéros de téléphone pouvant être traités en une seule exécution. Le rapport indique également l'emplacement (URI Amazon S3 et URL de console Amazon S3) pour [automation:EXECUTION\_ID]/ErrorResourceList.csv ou [automation:EXECUTION\_ID]/NonProcessedResourceList.csv, le cas échéant.

- **DeleteCloudFormationStack**

Supprime la AWS CloudFormation pile, y compris la fonction Lambda pour le mappage.

- **DescribeCloudFormationErrorFromStackEvent**

Décrit les erreurs provenant de la AWS CloudFormation pile de l'AssociatePhoneNumbersToContactFlows étape.

7. Une fois terminé, consultez la section Sorties pour obtenir les résultats détaillés de l'exécution :

- **GenerateReport.OutputPayload**

Sortie des associations de numéros de téléphone et de flux de contacts. Ce rapport contient les informations suivantes :

- Le nombre de paires de numéros de téléphone et de flux de contacts répertoriées dans le fichier CSV d'entrée
- Le nombre de numéros de téléphone associés aux flux de contacts tel que spécifié dans le fichier CSV d'entrée
- Le nombre de numéros de téléphone qui n'ont pas pu être associés aux flux de contacts en raison d'une erreur
- Le nombre de numéros de téléphone qui n'ont pas été associés aux flux de contacts en raison de contraintes de temps
- L'emplacement (URI Amazon S3 et URL de console Amazon S3) du fichier CSV contenant le numéro de téléphone et les paires de flux de contacts qui n'ont pas pu être associées en raison d'une erreur
- L'emplacement (URI Amazon S3 et URL de console Amazon S3) du fichier CSV contenant le numéro de téléphone et les paires de flux de contacts qui n'ont pas été associées en raison d'une contrainte de temps
- **DescribeCloudFormationErrorFromStackEvents.Manifestations**

## Sortie qui affiche les événements de AWS CloudFormation pile en cas d'échec de l'AssociatePhoneNumbersToContactFlows étape.

### Résultat d'exécution avec un petit nombre de numéros de téléphone et de flux de contacts

```

▼ 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"
  }
}}

```

### Résultat d'exécution avec un grand nombre de numéros de téléphone et de flux de contacts et de numéros de téléphone non associés en raison d'une erreur ou d'une contrainte de temps

```

▼ 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.
}

```

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)



# AWS Directory Service

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Directory Service. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

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

## AWS-CreateDSManagementInstance

### Description

Le AWS-CreateDSManagementInstance runbook crée une instance Windows Amazon Elastic Compute Cloud (Amazon EC2) que vous pouvez utiliser pour gérer votre répertoire. AWS Directory Service L'instance de gestion ne peut pas être utilisée pour gérer les répertoires AD Connector.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- AMIID

Type : String

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

Description : (Obligatoire) L'ID du Amazon Machine Image (AMI) que vous souhaitez utiliser pour lancer l'instance de gestion.

- DirectoryId

Type : String

Description : (Obligatoire) L'ID du AWS Directory Service répertoire que vous souhaitez gérer. L'instance est jointe au répertoire que vous spécifiez.

- iamInstanceProfileName

Type : String

Description : (Obligatoire) Le nom que vous spécifiez est appliqué au profil d'instance IAM créé par l'automatisation et associé à l'instance de gestion.

- InstanceType

Type : String

Par défaut : t3.medium

Valeurs autorisées :

- 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

Description : (Obligatoire) Type d'instance que vous souhaitez lancer.

- KeyPairName

Type : String

Description : (Facultatif) La paire de clés à utiliser lors de la création de l'instance. Si vous ne spécifiez aucune valeur, aucune paire de clés n'est associée à l'instance.

- RemoteAccessCidr

Type : String

Description : (Obligatoire) Le bloc d'adresse CIDR à partir duquel vous souhaitez autoriser le trafic RDP (port 3389). Le bloc CIDR que vous spécifiez est appliqué à une règle entrante ajoutée au groupe de sécurité créé par l'automatisation.

- SecurityGroupName

Type : String

Description : (Obligatoire) Le nom que vous spécifiez est appliqué au groupe de sécurité créé par l'automatisation et associé à l'instance de gestion.

- Étiquettes

Type : MapList

Description : (Facultatif) Paire clé-valeur que vous souhaitez appliquer aux ressources créées par l'automatisation.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

- `aws:executeAwsApi`- Recueille des informations sur le répertoire que vous spécifiez dans le `DirectoryId` paramètre.
- `aws:executeAwsApi`- Obtient le bloc CIDR du cloud privé virtuel (VPC) où le répertoire a été lancé.
- `aws:executeAwsApi`- Crée un groupe de sécurité à l'aide de la valeur que vous spécifiez dans le `SecurityGroupName` paramètre.
- `aws:executeAwsApi`- Crée une règle entrante pour le groupe de sécurité nouvellement créé qui autorise le trafic RDP à partir du CIDR que vous spécifiez dans le paramètre. `RemoteAccessCidr`
- `aws:executeAwsApi`- Crée un rôle IAM et un profil d'instance à l'aide de la valeur que vous spécifiez dans le `IamInstanceProfileName` paramètre.
- `aws:executeAwsApi`- Lance une instance Amazon EC2 en fonction des valeurs que vous spécifiez dans les paramètres du runbook.
- `aws:executeAwsApi`- Crée un AWS Systems Manager document pour joindre l'instance nouvellement lancée à votre répertoire.
- `aws:runCommand`- Joint la nouvelle instance à votre répertoire.
- `aws:runCommand`- Installe les outils d'administration du serveur distant sur la nouvelle instance.

# AWSSupport-TroubleshootADConnectorConnectivity

## Description

Le AWSSupport-TroubleshootADConnectorConnectivity runbook vérifie les prérequis suivants pour un connecteur AD :

- Vérifie si le trafic requis est autorisé par le groupe de sécurité et les règles de la liste de contrôle d'accès réseau (ACL) associés à votre connecteur AD.
- Vérifie si les points de terminaison du VPC AWS Systems ManagerAWS Security Token Service,, et de l'CloudWatchinterface Amazon se trouvent dans le même cloud privé virtuel (VPC) que le connecteur AD.

Lorsque les vérifications préalables sont effectuées avec succès, le runbook lance deux instances Amazon Elastic Compute Cloud (Amazon EC2) Linux t2.micro dans les mêmes sous-réseaux que votre connecteur AD. Les tests de connectivité réseau sont ensuite effectués à l'aide netcat des nslookup utilitaires et.

[Exécutez cette automatisation \(console\)](#)

### Important

L'utilisation de ce runbook peut entraîner des frais supplémentaires Compte AWS pour les instances Amazon EC2, les volumes Amazon Elastic Block Store et Amazon Machine Image (AMI) créés lors de l'automatisation. Pour plus d'informations, consultez les [tarifs Amazon Elastic Compute Cloud](#) et [Amazon Elastic Block Store Pricing](#).

Si l'aws:deletestackétape échoue, accédez à la AWS CloudFormation console pour supprimer manuellement la pile. Le nom de la pile créée par ce runbook commence AWSSupport-TroubleshootADConnectorConnectivity par. Pour plus d'informations sur la suppression de AWS CloudFormation piles, consultez [la section Supprimer une pile](#) dans le Guide de l'AWS CloudFormationutilisateur.

Type de document

Automatisation

Propriétaire

## Amazon

### Plateformes

Linux, macOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- DirectoryId

Type : String

Description : (Obligatoire) L'ID du répertoire AD Connector auquel vous souhaitez résoudre les problèmes de connectivité.

- Ec2 InstanceProfile

Type : String

Nombre maximum de caractères : 128

Description : (Obligatoire) Le nom du profil d'instance que vous souhaitez attribuer aux instances lancées pour effectuer des tests de connectivité. Le profil d'instance que vous spécifiez doit être associé à la AmazonSSMManagedInstanceCore politique ou à des autorisations équivalentes.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

- `aws:assertAwsResourceProperty`- Confirme que le répertoire spécifié dans le `DirectoryId` paramètre est un connecteur AD.
- `aws:executeAwsApi`- Recueille des informations sur le connecteur AD.
- `aws:executeAwsApi`- Recueille des informations sur les groupes de sécurité associés au connecteur AD.
- `aws:executeAwsApi`- Recueille des informations sur les règles ACL réseau associées aux sous-réseaux du connecteur AD.
- `aws:executeScript`- Évalue les règles du groupe de sécurité AD Connector pour vérifier que le trafic sortant requis est autorisé.
- `aws:executeScript`- Évalue les règles ACL du réseau AD Connector pour vérifier que le trafic réseau sortant et entrant requis est autorisé.



- `aws:executeScript`- Vérifie si les AWS Systems Manager points de terminaison de CloudWatch l'interface AWS Security Token Service et Amazon se trouvent dans le même VPC que le connecteur AD.
- `aws:executeScript`- Compile les résultats des contrôles effectués lors des étapes précédentes.
- `aws:branch`- Branche l'automatisation en fonction du résultat des étapes précédentes. L'automatisation s'arrête là si les règles sortantes et entrantes requises sont absentes pour les groupes de sécurité et les ACL réseau.
- `aws:createStack`- Crée une AWS CloudFormation pile pour lancer des instances Amazon EC2 afin d'effectuer des tests de connectivité.
- `aws:executeAwsApi`- Rassemble les identifiants des instances Amazon EC2 récemment lancées.
- `aws:waitForAwsResourceProperty`- Attend que la première instance Amazon EC2 récemment lancée soit signalée comme étant gérée par. AWS Systems Manager
- `aws:waitForAwsResourceProperty`- Attend que la deuxième instance Amazon EC2 récemment lancée soit signalée comme étant gérée par. AWS Systems Manager
- `aws:runCommand`- Effectue des tests de connectivité réseau vers les adresses IP du serveur DNS local à partir de la première instance Amazon EC2.
- `aws:runCommand`- Effectue des tests de connectivité réseau vers les adresses IP du serveur DNS local à partir de la deuxième instance Amazon EC2.
- `aws:changeInstanceState`- Arrête les instances Amazon EC2 utilisées pour les tests de connectivité.
- `aws:deleteStack`- Supprime la AWS CloudFormation pile.
- `aws:executeScript`- Fournit des instructions sur la façon de supprimer manuellement la AWS CloudFormation pile si l'automatisation ne parvient pas à supprimer la pile.

## **AWSSupport-TroubleshootDirectoryTrust**

### Description

Le `AWSSupport-TroubleshootDirectoryTrust` runbook diagnostique les problèmes de création de confiance entre un AWS Managed Microsoft AD et Microsoft Active Directory. L'automatisation garantit que le type d'annuaire prend en charge les approbations, puis vérifie les règles de groupe de sécurité associées, les listes de contrôle d'accès réseau (liste ACL réseau) et les tables de routage pour détecter les problèmes de connectivité potentiels.

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- DirectoryId

Type : String

Modèle autorisé : `^d-[a-z0-9]{10}$`

Description : (Obligatoire) ID du AWS Managed Microsoft AD à dépanner.

- RemoteDomainCidrs

Type : StringList

Modèle autorisé : `^([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]|[1-9]))$`

Description : (Obligatoire) Le ou les CIDR du domaine distant avec lequel vous tentez d'établir une relation d'approbation. Vous pouvez ajouter plusieurs CIDR à l'aide de valeurs séparées par des virgules. Par exemple : 172.31.48.0/20, 192.168.1.10/32.

- RemoteDomainName

Type : String

Description : (Obligatoire) Nom de domaine complet du domaine distant avec lequel vous établissez une relation d'approbation.

- RequiredTrafficACL

Type : String

Description : (Obligatoire) Les exigences de ports par défaut pour AWS Managed Microsoft AD. Dans la plupart des cas, vous ne devez pas modifier la valeur par défaut.

Par défaut : {"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

Type : String

Description : (Obligatoire) Les exigences de ports par défaut pour AWS Managed Microsoft AD. Dans la plupart des cas, vous ne devez pas modifier la valeur par défaut.

Par défaut : {"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

Type : String

Description : (Facultatif) ID de la relation d'approbation à dépanner.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ds:DescribeConditionalForwarders
- ds:DescribeDirectories
- ds:DescribeTrusts

- `ds:ListIpRoutes`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`

## Étapes de document

- `aws:assertAwsResourceProperty`- Confirme que le type de répertoire est AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Obtient des informations sur le AWS Managed Microsoft AD.
- `aws:branch`- Automatisation des branches si une valeur est fournie pour le paramètre `TrustId` d'entrée.
- `aws:executeAwsApi`- Obtient des informations sur la relation de confiance.
- `aws:executeAwsApi`- Obtient les adresses IP DNS du redirecteur conditionnel pour `RemoteDomainName`
- `aws:executeAwsApi`- Obtient des informations sur les routes IP qui ont été ajoutées au AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Obtient les CIDR des AWS Managed Microsoft AD sous-réseaux.
- `aws:executeAwsApi`- Obtient des informations sur les groupes de sécurité associés au AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Obtient des informations sur les ACL réseau associées au AWS Managed Microsoft AD.
- `aws:executeScript`- Confirme que les valeurs `RemoteDomainCidrs` sont valides. Confirme qu'il AWS Managed Microsoft AD possède des redirecteurs conditionnels pour les `RemoteDomainCidrs` adresses IP et que les routes IP requises y ont été ajoutées AWS Managed Microsoft AD s'il s'agit d'adresses IP non conformes à la `RemoteDomainCidrs` RFC 1918.
- `aws:executeScript`- Évalue les règles des groupes de sécurité.
- `aws:executeScript`- Évalue les ACL du réseau.

## Sorties

`evalDirectorySecurityGroup.Output` : résultat de l'évaluation visant à déterminer si les règles du groupe de sécurité associées à AWS Managed Microsoft AD autorisent le trafic requis pour la création de rapports de confiance.

`evalAclEntries.output` : résultat de l'évaluation visant à déterminer si les ACL réseau associées à AWS Managed Microsoft AD autorisent le trafic requis pour la création de rapports de confiance.

`evaluateRemoteDomainCIDR.Output` - Résultat de l'évaluation de la validité `RemoteDomainCidrs` des valeurs. Confirme qu'il AWS Managed Microsoft AD possède des redirecteurs conditionnels pour les `RemoteDomainCidrs` adresses IP et que les routes IP requises y ont été ajoutées AWS Managed Microsoft AD s'il s'agit d'adresses IP non conformes à la `RemoteDomainCidrs` RFC 1918.

## AWS AppSync

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS AppSync. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

Rubriques

- [AWS-EnableAppSyncGraphQLApiLogging](#)

### AWS-EnableAppSyncGraphQLApiLogging

Description

Le `AWS-EnableAppSyncGraphQLApiLogging` runbook permet la journalisation au niveau du champ et la journalisation au niveau des demandes pour l'API AWS AppSync GraphQL que vous spécifiez. Le runbook appliquera les modifications à l'API GraphQL spécifiée même si la journalisation a déjà été activée.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux, macOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Apild

Type : chaîne

Description : (Obligatoire) L'ID de l'API pour laquelle vous souhaitez activer la journalisation.

- FieldLogLevel

Type : chaîne

Valeurs valides : ERROR | ALL

Description : (Obligatoire) Le niveau de journalisation du champ.

- CloudWatchLogsRoleArn

Type : chaîne

Description : (Obligatoire) L'ARN du rôle de service AWS AppSync censé publier sur Amazon CloudWatch Logs.

- ExcludeVerboseContent

Type : booléen

Par défaut : false

Description : (Facultatif) Définissez sur True pour exclure des informations telles que les en-têtes, le contexte et les modèles de mappage évalués, quel que soit le niveau de journalisation.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

## Étapes de document

- `aws : executeAwsApi` - Recueille le type d'authentification et les informations de configuration pertinentes pour le type d'authentification principal.
- `aws:branch` - Branches basées sur le type d'authentification.
- `aws : executeAwsApi` - Met à jour la configuration de journalisation pour l'API AWS AppSync GraphQL en fonction des valeurs spécifiées pour les paramètres d'entrée du runbook.

## Sorties

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Réponse à l'`UpdateGraphQLApi`appel.
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Réponse à l'`UpdateGraphQLApi`appel.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Réponse à l'`UpdateGraphQLApi`appel.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Réponse à l'`UpdateGraphQLApi`appel.

## Amazon Athena

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Athena. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-EnableAthenaWorkGroupEncryptionAtRest](#)

# AWS-EnableAthenaWorkGroupEncryptionAtRest

## Description

Le `AWS-EnableAthenaWorkGroupEncryptionAtRest` runbook active le chiffrement au repos pour le groupe de travail Amazon Athena que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- WorkGroup

Type : chaîne

Description : (Obligatoire) Le groupe de travail pour lequel vous souhaitez activer le chiffrement au repos.

- EncryptionOption

Type : chaîne

Valeurs valides : SSE\_S3 | SSE\_KMS | CSE\_KMS



Description : (Obligatoire) Spécifie l'option de chiffrement utilisée. Vous pouvez choisir le chiffrement côté serveur avec des clés gérées Amazon S3 (SSE\_S3), le chiffrement côté serveur avec des clés gérées (SSE\_KMS) ou le chiffrement côté AWS KMS client avec des clés gérées (CSE\_KMS). AWS KMS

- `KmsKeyId`

Type : chaîne

Description : (Facultatif) Si vous utilisez une option de AWS KMS chiffrement, spécifiez l'ARN de la clé, l'ID de clé ou l'alias de clé que vous souhaitez utiliser.

- `EnableMinimumEncryptionConfiguration`

Type : booléen

Valeur par défaut : `True`

Description : (Facultatif) Applique un niveau minimal de chiffrement au groupe de travail pour les résultats de requêtes et de calculs écrits sur Amazon S3. Lorsque cette option est activée, les utilisateurs du groupe de travail peuvent définir le chiffrement uniquement au niveau minimum défini par l'administrateur ou à un niveau supérieur lorsqu'ils soumettent des requêtes. Ce paramètre ne s'applique pas aux groupes de travail compatibles avec Spark.

- `EnforceWorkGroupConfiguration`

Type : booléen

Valeur par défaut : `True`

Description : (Facultatif) Si ce paramètre est défini sur `True`, les paramètres du groupe de travail remplacent les paramètres côté client. S'il est défini sur `False`, les paramètres côté client sont utilisés.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

- `athena:GetWorkGroup`
- `athena:UpdateWorkGroup`

## Étapes de document

- `aws:branch` - Branches basées sur l'option de chiffrement spécifiée dans le `EncryptionOption` paramètre.
- `aws : executeAwsApi` - Cette étape met à jour le groupe de travail Athena avec le paramètre de chiffrement spécifié.
- `aws : executeAwsApi` - Met à jour le groupe de travail Athena avec le paramètre de chiffrement spécifié.
- `aws : assertAwsResource Property` - Vérifie que le chiffrement du groupe de travail a été activé.

## DynamoDB

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon DynamoDB. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

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

## AWS - ChangeDDBRWCapacityMode

### Description

Le `AWS-ChangeDDBRWCapacityMode` runbook modifie le mode de capacité de lecture/écriture pour une ou plusieurs tables Amazon DynamoDB (DynamoDB) en mode à la demande ou en mode provisionné.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `CapacityMode`

Type : chaîne

Valeurs valides : `PROVISIONED | PAY_PER_REQUEST`

Description : (Obligatoire) Mode de capacité de lecture/écriture souhaité. Lors du passage d'une capacité à la demande (pay-per-request) à une capacité provisionnée, les valeurs de capacité provisionnée initiales doivent être définies. Les valeurs de capacité allouées initiales sont estimées en fonction de la capacité de lecture et d'écriture consommée par votre table et vos index secondaires globaux au cours des 30 dernières minutes.

- `ReadCapacityUnits`

Type : entier

Par défaut : 0

Description : (Facultatif) Nombre maximal de lectures hautement cohérentes consommées par seconde avant que DynamoDB ne renvoie une exception de limitation.

- TableNames

Type : chaîne

Description : (Obligatoire) Liste séparée par des virgules des noms de tables DynamoDB pour modifier le mode de capacité de lecture/écriture pour...

- WriteCapacityUnits

Type : entier

Par défaut : 0

Description : (Facultatif) Nombre maximal d'écritures consommées par seconde avant que DynamoDB ne renvoie une exception de limitation.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeScript`- Modifie le mode de capacité de lecture/écriture pour les tables DynamoDB spécifiées dans le paramètre. `TableNames`

### Sorties

DBRW modifié. `CapacityMode SuccessesTables` - Liste des noms de tables DynamoDB dont le mode de capacité a été correctement modifié

DBRW modifié. CapacityMode FailedTables - Liste des noms des tables DynamoDB pour lesquelles le changement du mode de capacité a échoué et pour quelle raison.

## AWS-CreateDynamoDBBackup

### Description

Créez une sauvegarde d'une table Amazon DynamoDB.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- BackupName

Type : String

Description : (Obligatoire) nom de la sauvegarde à créer.

- LambdaAssumeRole

Type : String

Description : (Facultatif) ARN du rôle qui autorise la fonction Lambda créée par Automation à effectuer des actions en votre nom. Si vous ne spécifiez pas cette valeur, un rôle transitoire est créé pour exécuter la fonction Lambda.

- TableName

Type : String

Description : (Obligatoire) nom de la table DynamoDB à analyser.

## AWS-DeleteDynamoDbBackup

Description

Supprimez la sauvegarde d'une table Amazon DynamoDB.

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- BackupArn

Type : String

Description : (Obligatoire) ARN de la sauvegarde de table DynamoDB à supprimer.

## **AWSConfigRemediation-DeleteDynamoDbTable**

### Description

Le `AWSConfigRemediation-DeleteDynamoDbTable` runbook supprime la table Amazon DynamoDB (DynamoDB) que vous avez spécifiée.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- TableName

Type : String

Description : (Obligatoire) Nom de la table DynamoDB que vous souhaitez supprimer.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

## Étapes de document

- `aws:executeScript`- Supprime la table DynamoDB spécifiée dans le paramètre. `TableName`
- `aws:executeScript`- Vérifie que la table DynamoDB a été supprimée.

## AWS-DeleteDynamoDbTableBackups

### Description

Supprimez les sauvegardes de tables DynamoDB en fonction du nombre de jours de rétention ou du nombre de jours.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `AutomationAssumeRole`



Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- LambdaAssumeRole

Type : String

Description : (Facultatif) ARN du rôle qui autorise la fonction Lambda créée par Automation à effectuer des actions en votre nom. Si vous ne spécifiez pas cette valeur, un rôle transitoire est créé pour exécuter la fonction Lambda.

- RetentionCount

Type : String

Par défaut: 10

Description : (Facultatif) nombre de sauvegardes à conserver pour la table. S'il existe plus que le nombre spécifié de sauvegardes, les sauvegardes les plus anciennes au-delà de ce nombre sont supprimées. L'un RetentionCount ou l'autre RetentionDays peut être utilisé, pas les deux.

- RetentionDays

Type : String

Description : (Facultatif) nombre de jours de conservation de sauvegardes pour la table. Les sauvegardes plus ancienne que le nombre de jours spécifié sont supprimées. L'un RetentionCount ou l'autre RetentionDays peut être utilisé, pas les deux.

- TableName

Type : String

Description : (Obligatoire) nom de la table DynamoDB à analyser.

## **AWSConfigRemediation-EnableEncryptionOnDynamoDbTable**

Description

Le `AWSConfigRemediation-EnableEncryptionOnDynamoDbTable` runbook chiffre une table Amazon DynamoDB (DynamoDB) à l'aide de la clé gérée par le client AWS KMS() que vous spécifiez pour AWS Key Management Service le paramètre. `KMSKeyId`

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `KMS KeyId`

Type : chaîne

Description : (Obligatoire) L'ARN de la clé gérée par le client que vous souhaitez utiliser pour chiffrer la table DynamoDB que vous spécifiez dans le paramètre. `TableName`

- `TableName`

Type : chaîne

Description : (Obligatoire) Nom de la table DynamoDB que vous souhaitez chiffrer.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeAwsApi`- Chiffre la table DynamoDB que vous spécifiez dans le paramètre. `TableName`
- `aws:waitForAwsResourceProperty`- Vérifie que la `Enabled` propriété de la table `SSESpecification` DynamoDB est définie sur. `true`
- `aws:assertAwsResourceProperty`- Vérifie que la table DynamoDB est chiffrée avec la clé gérée par le client spécifiée dans le paramètre. `KMSKeyId`

## **AWSConfigRemediation-EnablePITRForDynamoDbTable**

### Description

Le `AWSConfigRemediation-EnablePITRForDynamoDbTable` runbook active la point-in-time restauration (PITR) sur la table Amazon DynamoDB que vous avez spécifiée.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- **AutomationAssumeRole**

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- **TableName**

Type : String

Description : (Obligatoire) Nom de la table DynamoDB sur laquelle activer la point-in-time restauration.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeAwsApi`- Active la point-in-time restauration sur la table DynamoDB que vous spécifiez dans le `TableName` paramètre.
- `aws:assertAwsResourceProperty`- Confirme que point-in-time la restauration est activée dans la table DynamoDB.

## **AWS-EnableDynamoDbAutoscaling**

### Description

Le `AWS-EnableDynamoDbAutoscaling` runbook active Application Auto Scaling pour la table Amazon DynamoDB de capacité provisionnée que vous spécifiez. Application Auto Scaling

ajuste dynamiquement la capacité de débit allouée en fonction des modèles de trafic. Pour plus d'informations, consultez [la section Gestion automatique de la capacité de débit avec le dimensionnement automatique de DynamoDB dans le manuel du développeur Amazon DynamoDB](#).

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux, macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- TableName

Type : chaîne

Description : (Obligatoire) Nom de la table DynamoDB sur laquelle vous souhaitez activer Application Auto Scaling.

- MinReadCapacity

Type : entier

Description : (Obligatoire) Nombre minimal d'unités de capacité de lecture de débit allouées pour la table DynamoDB.

- MaxReadCapacity

Type : entier

Description : (Obligatoire) Nombre maximal d'unités de capacité de lecture de débit allouées pour la table DynamoDB.

- TargetReadCapacityUtilization

Type : entier

Description : (Obligatoire) L'utilisation de la capacité de lecture cible souhaitée. L'utilisation cible est le pourcentage du débit provisionné consommé à un moment donné. Vous pouvez définir les valeurs d'utilisation cibles de dimensionnement automatique entre 20 et 90 %.

- ReadScaleOutCooldown

Type : entier

Description : (Obligatoire) Durée en secondes pendant laquelle une précédente activité d'augmentation de la capacité de lecture prend effet.

- ReadScaleInCooldown

Type : entier

Description : (Obligatoire) Durée en secondes entre la fin d'une activité d'augmentation de la capacité de lecture et le début d'une autre activité d'extension.

- MinWriteCapacity

Type : entier

Description : (Obligatoire) Nombre minimal d'unités d'écriture de débit allouées pour la table DynamoDB.

- MaxWriteCapacity

Type : entier

Description : (Obligatoire) Nombre maximal d'unités d'écriture de débit allouées pour la table DynamoDB.

- TargetWriteCapacityUtilization

Type : entier

Description : (Obligatoire) L'utilisation de la capacité d'écriture cible souhaitée. L'utilisation cible est le pourcentage du débit provisionné consommé à un moment donné. Vous pouvez définir les valeurs d'utilisation cibles de dimensionnement automatique entre 20 et 90 %.

- WriteScaleOutCooldown

Type : entier

Description : (Obligatoire) Durée en secondes pendant laquelle une précédente activité d'augmentation de la capacité d'écriture prend effet.

- WriteScaleInCooldown

Type : entier

Description : (Obligatoire) Durée en secondes entre la fin d'une activité d'augmentation de la capacité d'écriture et le début d'une autre activité d'extension.

#### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- application-autoscaling:DescribeScalableTargets
- application-autoscaling:DescribeScalingPolicies
- application-autoscaling:PutScalingPolicy
- application-autoscaling:RegisterScalableTarget
- RegisterAppAutoscalingTargetWrite (aws :executeAwsApi) - Configure Application Auto Scaling sur la table DynamoDB que vous spécifiez.
- RegisterAppAutoscalingTargetWriteDelay (aws:sleep) - Se met en veille pour éviter le ralentissement de l'API.
- PutScalingPolicyWrite (aws :executeAwsApi) - Configure l'utilisation de la capacité d'écriture cible pour la table DynamoDB.
- PutScalingPolicyWriteDelay (aws:sleep) - Se met en veille pour éviter le ralentissement de l'API.

- RegisterAppAutoscalingTargetRead (aws :executeAwsApi) - Configure les unités de capacité de lecture minimale et maximale pour la table DynamoDB.
- RegisterAppAutoscalingTargetReadDelay (aws:sleep) - Se met en veille pour éviter le ralentissement de l'API.
- PutScalingPolicyRead (aws :executeAwsApi) - Configure l'utilisation de la capacité de lecture cible pour la table DynamoDB.
- VerifyDynamoDbAutoscalingEnabled (AWS:ExecuteScript) - Vérifie que Application Auto Scaling est activé pour la table DynamoDB en fonction des valeurs que vous spécifiez.

## Sorties

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

# AWS-RestoreDynamoDBTable

## Description

Le AWS-RestoreDynamoDBTable runbook restaure la table Amazon DynamoDB que vous avez spécifiée à l'aide de point-in-time recovery (PITR).

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres



- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- EnablePointInTimeRecoverAsNeeded

Type : booléen

Valeur par défaut : true

Description : (Facultatif) Détermine si l'automatisation active la point-in-time restauration selon les besoins pour restaurer la table.

- GlobalSecondaryIndexOverride

Type : String

Description : (Facultatif) Les nouveaux index secondaires globaux destinés à remplacer les index secondaires existants pour la nouvelle table.

- LocalSecondaryIndexOverride

Type : String

Description : (Facultatif) Les nouveaux index secondaires locaux destinés à remplacer les index secondaires existants pour la nouvelle table.

- RestoreDateTime

Type : String

Description : (Obligatoirepoint-in-time) Restauration vers laquelle vous souhaitez restaurer votre table au cours des 35 derniers jours. Spécifiez la date et l'heure en utilisant le format suivant : DD/MM/YYYY HH:MM:SS

- SourceTableArn

Type : String

Description : (Obligatoire) L'ARN de la table que vous souhaitez restaurer.

- `SseSpecificationOverride`

Type : String

Description : (Facultatif) Paramètres de chiffrement côté serveur à utiliser pour la nouvelle table.

- `TargetTableName`

Type : String

Description : (Obligatoire) Nom de la table à restaurer.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeScript`- Restaure la table DynamoDB que vous avez spécifiée dans le `TargetTableName` paramètre à l'aide point-in-time de la restauration.

## Amazon EBS

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Elastic Block Store. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [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

### Description

Le runbook `AWSSupport-AnalyzeEBSResourceUsage` d'automatisation est utilisé pour analyser l'utilisation des ressources sur Amazon Elastic Block Store (Amazon EBS). Il analyse l'utilisation des volumes et identifie les volumes, les images et les instantanés abandonnés dans une AWS région donnée.

### Comment fonctionne-t-il ?


Le runbook exécute les quatre tâches suivantes :

1. Vérifie l'existence d'un compartiment Amazon Simple Storage Service (Amazon S3) ou crée un nouveau compartiment Amazon S3.
2. Rassemble tous les volumes Amazon EBS dans leur état de disponibilité.
3. Regroupe tous les instantanés Amazon EBS pour lesquels le volume source a été supprimé.
4. Regroupe toutes les Amazon Machine Images (AMI) qui ne sont pas utilisées par des instances Amazon Elastic Compute Cloud (Amazon EC2) non résiliées.

Le runbook génère des rapports CSV et les stocke dans un compartiment Amazon S3 fourni par l'utilisateur. Le compartiment fourni doit être sécurisé conformément aux meilleures pratiques de AWS sécurité décrites à la fin. Si le compartiment Amazon S3 fourni par l'utilisateur n'existe pas dans le compte, le runbook crée un nouveau compartiment Amazon S3 au format de nom `<User-provided-name>-awssupport-YYYY-MM-DD`, chiffré avec une clé personnalisée AWS Key Management Service (AWS KMS), avec le versionnement des objets activé, bloqué l'accès public et nécessitant des demandes d'utilisation du protocole SSL/TLS.

Si vous souhaitez spécifier votre propre compartiment Amazon S3, assurez-vous qu'il est configuré conformément aux meilleures pratiques suivantes :

- Bloquez l'accès public au bucket (défini `IsPublic` sur `False`).
- Activez la journalisation des accès Amazon S3.
- [Autorisez uniquement les requêtes SSL vers votre compartiment.](#)
- Activez la gestion des versions des objets.
- Utilisez une clé AWS Key Management Service (AWS KMS) pour chiffrer votre compartiment.

 Important

L'utilisation de ce runbook peut entraîner des frais supplémentaires sur votre compte pour la création de buckets et d'objets Amazon S3. Consultez la [tarification d'Amazon S3](#) pour plus de détails sur les frais susceptibles d'être facturés.

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- S3 BucketName

Type : `AWS::S3::Bucket::Name`

Description : (Obligatoire) Le compartiment Amazon S3 de votre compte dans lequel vous souhaitez télécharger le rapport. Assurez-vous que la politique des compartiments n'accorde pas d'autorisations de lecture/écriture inutiles aux parties qui n'ont pas besoin d'accéder aux journaux collectés. Si le compartiment spécifié n'existe pas dans le compte, l'automatisation crée un nouveau compartiment dans la région où l'automatisation est lancée avec le format du nom `<User-provided-name>-awssupport-YYYY-MM-DD`, chiffré à l'aide d'une AWS KMS clé personnalisée.

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

- CustomerManagedKmsKeyArn

Type : chaîne

Description : (Facultatif) La AWS KMS clé personnalisée Amazon Resource Name (ARN) pour chiffrer le nouveau compartiment Amazon S3 qui sera créé si le compartiment spécifié n'existe pas dans le compte. L'automatisation échoue si la création du bucket est tentée sans spécifier un ARN de AWS KMS clé personnalisé.

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

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

Exemple de politique avec les autorisations IAM minimales requises pour exécuter ce 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:::awsexamplebucket1",
        "arn:aws:s3:::awsexamplebucket1/"
      ]
    }, {
      "Sid": "S3_Create_Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketLogging",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "*"
    }
  ]
}

```

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez au [AWSSupport-AnalyzeEBS ResourceUsage](#) dans la console. AWS Systems Manager
2. Pour les paramètres d'entrée, entrez ce qui suit :

- AutomationAssumeRole (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- S3 BucketName (obligatoire) :

Le compartiment Amazon S3 de votre compte dans lequel vous souhaitez télécharger le rapport.

- CustomerManagedKmsKeyArn (Facultatif) :

La AWS KMS clé personnalisée Amazon Resource Name (ARN) pour chiffrer le nouveau compartiment Amazon S3 qui sera créé si le compartiment spécifié n'existe pas dans le compte.

**Input parameters**

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

Enter the name of an existing S3 Bucket

S3 Bucket

Example: s3-bucket-name

**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

**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

3. Sélectionnez Exécuter.

4. L'automatisation démarre.

5. Le runbook d'automatisation exécute les étapes suivantes :

- Vérifiez la simultanéité :

Garantit qu'il n'y a qu'un seul lancement de ce runbook dans la Région. Si le runbook trouve une autre exécution en cours, il renvoie une erreur et se termine.

- verifyOrCreateSeau S3 :

Vérifie si le compartiment Amazon S3 existe. Dans le cas contraire, il crée un nouveau compartiment Amazon S3 dans la région où l'automatisation est lancée avec le format de nom <User-provided-name>-awssupport-YYYY-MM-DD, chiffré avec une AWS KMS clé personnalisée.



- **gatherAmiDetails:**

Recherche des AMI, qui ne sont utilisées par aucune instance Amazon EC2, génère le rapport au format `<region>-images.csv` de nom et le télécharge dans le compartiment Amazon S3.

- **gatherVolumeDetails:**

Vérifie l'état disponible des volumes Amazon EBS, génère le rapport au format `<region>-volume.csv` de nom et le télécharge dans un compartiment Amazon S3.

- **gatherSnapshotDetails:**

Recherche les instantanés Amazon EBS des volumes Amazon EBS déjà supprimés, génère le rapport avec le format `<region>-snapshot.csv` du nom et le télécharge dans le compartiment Amazon S3.

6. Une fois terminé, consultez la section Sorties pour connaître les résultats détaillés de l'exécution.

▼ 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.	

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

## AWS-ArchiveEBSSnapshots

### Description

Le `AWS-ArchiveEBSSnapshots` runbook vous permet d'archiver des instantanés pour les volumes Amazon Elastic Block Store (Amazon EBS) en spécifiant le tag que vous avez appliqué à vos instantanés. Vous pouvez également fournir l'ID d'un volume si vos instantanés ne sont pas balisés.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Description

Type : chaîne

Description : (Facultatif) Description de l'instantané Amazon EBS.

- DryRun

Type : chaîne

Valeurs valides : Oui | Non

Description : (Obligatoire) Vérifie si vous disposez des autorisations requises pour l'action, sans réellement faire la demande, et fournit une réponse d'erreur.

- RetentionCount

Type : chaîne

Description : (Facultatif) Nombre de clichés que vous souhaitez archiver. Ne spécifiez pas de valeur pour ce paramètre si vous spécifiez une valeur pour `RetentionDays`.

- `RetentionDays`

Type : chaîne

Description : (Facultatif) Le nombre de jours précédents de clichés que vous souhaitez archiver. Ne spécifiez pas de valeur pour ce paramètre si vous spécifiez une valeur pour `RetentionCount`.

- `SnapshotWithTag`

Type : chaîne

Valeurs valides : Oui | Non

Description : (Obligatoire) Spécifie si les instantanés que vous souhaitez archiver sont balisés.

- `TagKey`

Type : chaîne

Description : (Facultatif) La clé de la balise attribuée aux instantanés que vous souhaitez archiver.

- `TagValue`

Type : chaîne

Description : (Facultatif) La valeur de la balise attribuée aux instantanés que vous souhaitez archiver.

- `Volumeld`

Type : chaîne

Description : (Facultatif) ID du volume dont vous souhaitez archiver les instantanés. Utilisez ce paramètre si vos instantanés ne sont pas balisés.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ec2:ArchiveSnapshots`

- `ec2:DescribeSnapshots`

## Étapes de document

`aws:executeScript`- Archive les instantanés à l'aide de la balise que vous spécifiez à l'aide `TagValue` des paramètres `TagKey` et, ou du `VolumeId` paramètre.

# AWS-AttachEBSVolume

## Description

Associez un volume Amazon Elastic Block Store (Amazon EBS) à une instance Amazon Elastic Compute Cloud (Amazon EC2).

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `Appareil`

Type : chaîne

Description : (Obligatoire) Nom du périphérique (par exemple, /dev/sdh ou xvdh).

- InstanceId

Type : chaîne

Description : (Obligatoire) ID de l'instance à laquelle vous souhaitez attacher le volume.

- VolumeId

Type : chaîne

Description : (Obligatoire) L'ID du volume Amazon EBS. Le volume et l'instance doivent être dans la même zone de disponibilité.

## AWSSupport-CalculateEBSPerformanceMetrics

### Description

Le `AWSSupport-CalculateEBSPerformanceMetrics` runbook permet de diagnostiquer les problèmes de performances d'Amazon EBS en calculant et en publiant des indicateurs de performance sur un CloudWatch tableau de bord. Le tableau de bord affiche l'estimation des IOPS et du débit moyens pour un volume Amazon EBS cible ou pour tous les volumes attachés à l'instance Amazon Elastic Compute Cloud (Amazon EC2) cible. Pour les instances Amazon EC2, il indique également les IOPS et le débit moyens de l'instance. Le runbook affiche le lien vers le tableau de CloudWatch bord nouvellement créé qui affiche les CloudWatch mesures calculées pertinentes. Le CloudWatch tableau de bord est créé dans votre compte sous le nom `:AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>`.

### Comment fonctionne-t-il ?

Le runbook exécute les étapes suivantes :

- Garantit la validité des horodatages spécifiés.
- Valide si l'ID de ressource (volume Amazon EBS ou instance Amazon EC2) est valide.
- Lorsque vous fournissez un identifiant de ressource Amazon EC2, un tableau de CloudWatch bord est créé avec le nombre total d'IOPS/débit réel pour cette instance Amazon EC2 et un graphique d'IOPS/débit moyen estimé pour tous les volumes Amazon EBS attachés à une instance Amazon EC2.

- Lorsque vous fournissez un volume Amazon EBS en tant que ResourceID, un tableau de bord est créé avec CloudWatch un graphique d'IOPS/débit moyen estimé pour ce volume.
- Une fois le CloudWatch tableau de bord généré, si le débit moyen estimé par seconde ou le débit moyen estimé est supérieur au nombre maximal d'IOPS ou au débit maximal, le microbursting est possible pour le ou les volumes attachés à une instance Amazon EC2.

#### Note

Pour les volumes éclatables (gp2, sc2 et st1), le débit IOPS/débit maximal doit être pris en compte, jusqu'à ce que vous obteniez un équilibre en rafale. Une fois que la balance de rafale est complètement utilisée, c'est-à-dire qu'elle devient nulle, considérez les mesures de IOP/débit de base.

#### Important

La création du CloudWatch tableau de bord peut entraîner des frais supplémentaires sur votre compte. Pour plus d'informations, consultez le [guide de CloudWatch tarification Amazon](#).

### [Exécuter cette automatisation \(console\)](#)

#### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

#### Exemple de politique

```
{
```

```

    "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": "*"
      }
    ]
  }
}

```

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez [AWSsupport-CalculateEBSPerformanceMetrics](#) à Systems Manager sous Documents.

2. Sélectionnez Exécute automation (Exécuter l'automatisation).

3. Pour les paramètres d'entrée, entrez ce qui suit :

- AutomationAssumeRole (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ResourceID (obligatoire) :

L'ID de l'instance Amazon EC2 ou du volume Amazon EBS.

- Heure de début (obligatoire) :

Heure de début de l'affichage des données CloudWatch. L'heure doit être au format yyyy-mm-ddThh:mm:ss et en UTC.

- Heure de fin (obligatoire) :

Heure de fin d'affichage des données CloudWatch. L'heure doit être au format yyyy-mm-ddThh:mm:ss et en UTC.

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

4. Sélectionnez Exécuter.

5. L'automatisation démarre.

6. Le document exécute les étapes suivantes :

- CheckResourceIdAndTimeStamps:

Vérifie si l'heure de fin est supérieure à l'heure de début d'au moins une minute et si la ressource fournie existe.

- CreateCloudWatchDashboard:

Calcule les performances d'Amazon EBS et affiche un graphique basé sur votre identifiant de ressource. Si vous fournissez un identifiant de volume Amazon EBS pour le paramètre Resource ID, ce runbook crée un tableau de bord avec des estimations d'IOPS moyennes et un débit moyen estimé pour le volume Amazon EBS. Si vous fournissez un ID d'instance Amazon EC2 pour le paramètre Resource ID, ce runbook crée un CloudWatch tableau de bord avec le total moyen d'IOPS et le débit total moyen pour l'instance Amazon EC2, ainsi que les IOPS moyens estimés et le débit moyen estimé pour tous les volumes Amazon EBS attachés à l'instance Amazon EC2.

7. Une fois terminé, consultez la section Sorties pour obtenir les résultats détaillés de l'exécution :

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

Exemple CloudWatch de tableau de bord pour l'ID de ressource en tant qu'instance Amazon EC2



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

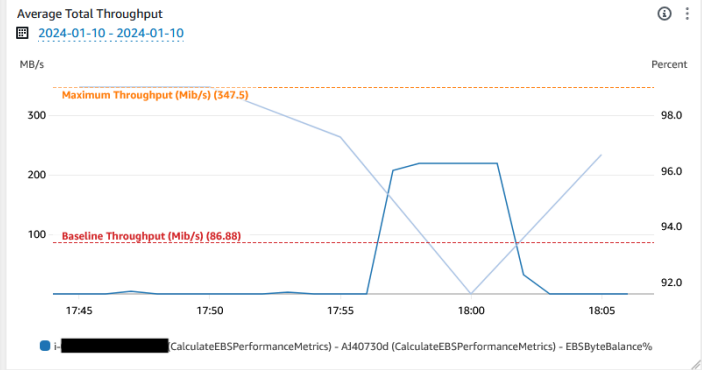
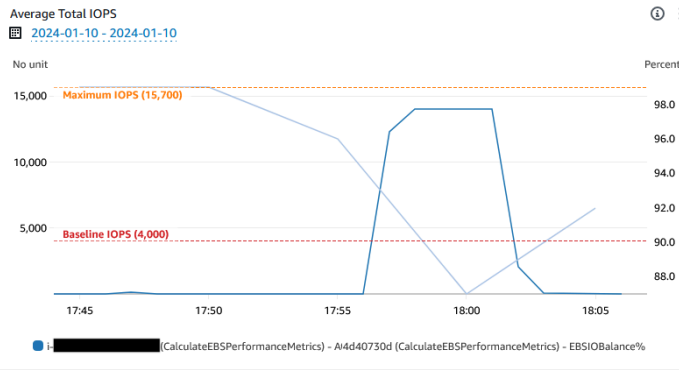
- Instance Type: t3.large
- EBS Optimized: True

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

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

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

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



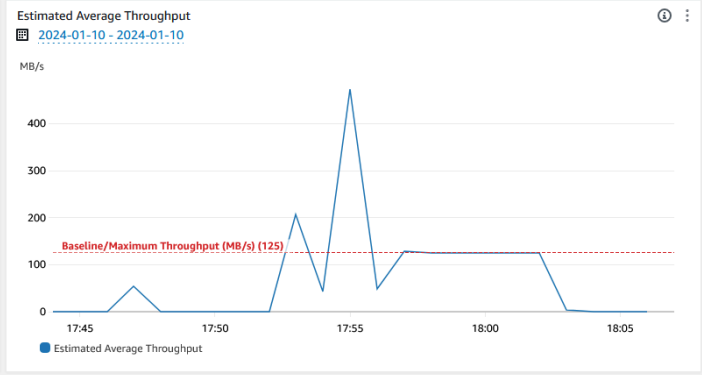
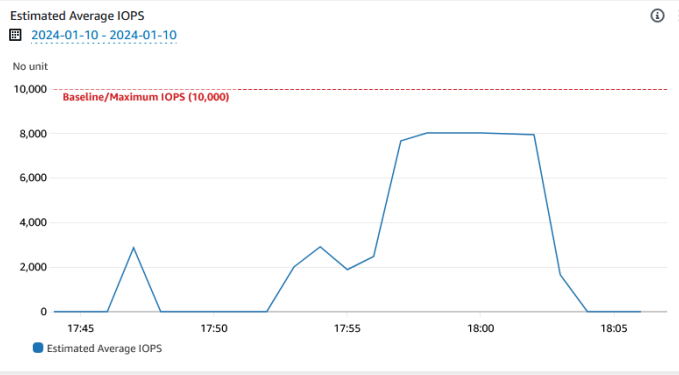
### EBS Volume(s) Metrics

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

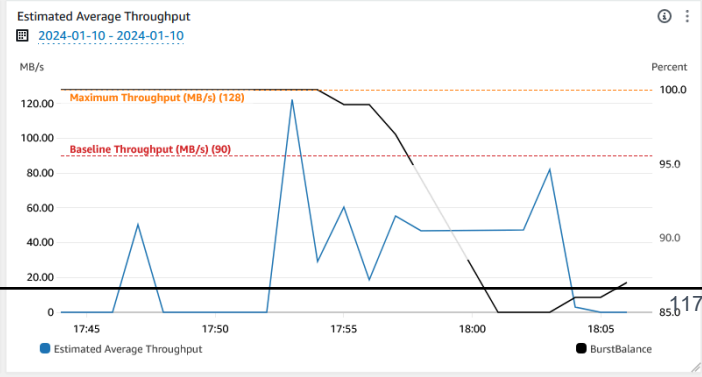
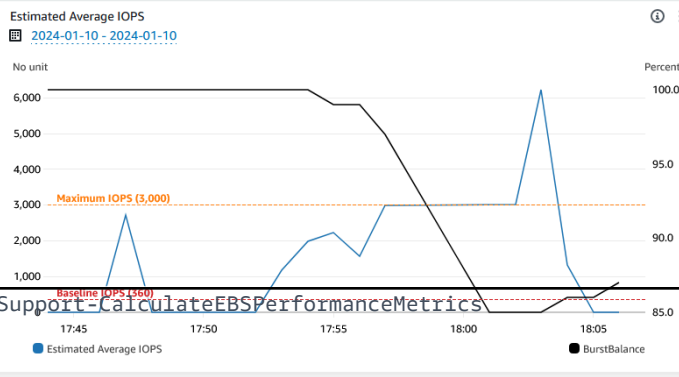
Note: If Estimated Average IOPS / Estimated Average Throughput is more than Maximum IOPS / Maximum Throughput, then microbursting is happening for that particular volume. Realtime analysis for Microbursting may vary, to confirm further you can use OS-level tool that has a finer granularity than CloudWatch.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

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

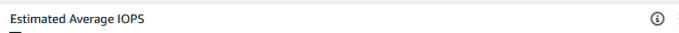
Volume: vol-[redacted] Type: gp3



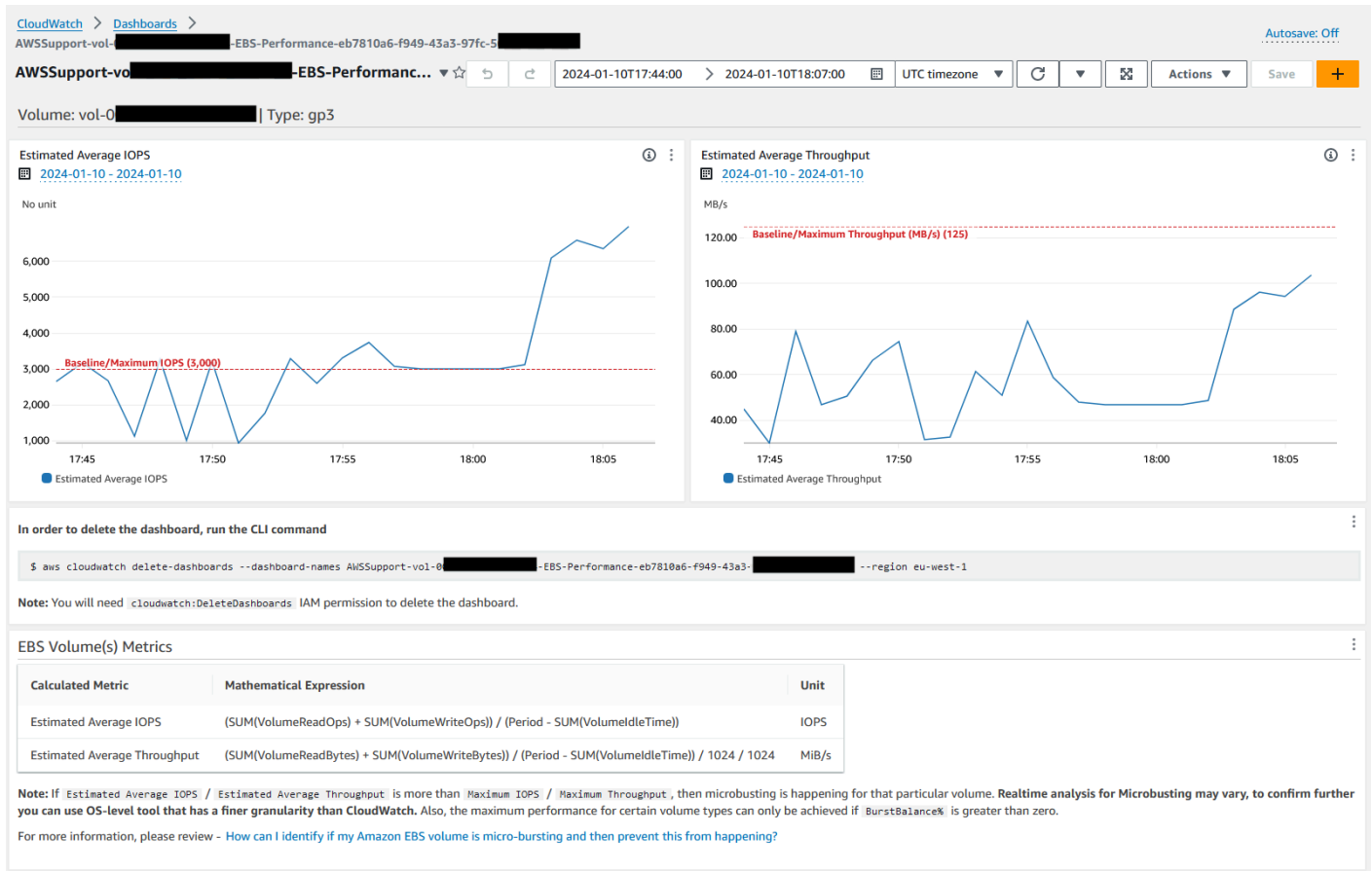
Volume: vol-[redacted] Type: gp2



Volume: vol-[redacted] Type: gp3



## Exemple CloudWatch de tableau de bord pour l'ID de ressource en tant qu'identifiant de volume Amazon EBS



## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

### AWSdocumentation de service

- [Comment puis-je déterminer si mon volume Amazon EBS est en microrafale et empêcher que cela ne se produise ?](#)

- [Comment puis-je consulter les mesures CloudWatch de performance agrégées d'Amazon EBS pour une instance EC2 ?](#)

## AWS - CopySnapshot

### Description

Copie un point-in-time instantané d'un volume Amazon Elastic Block Store (Amazon EBS). Vous pouvez copier l'instantané dans la même région Région AWS ou d'une région à l'autre. Les copies des instantanés Amazon EBS chiffrés restent chiffrées. Les copies des instantanés non chiffrés restent non chiffrées. Pour copier un instantané chiffré qui a été partagé depuis un autre compte, vous devez disposer des autorisations relatives à la clé KMS utilisée pour chiffrer le cliché. Les instantanés créés par l'action CopySnapshot ont un ID de volume arbitraire qui ne doit être utilisé en aucun cas.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Description

Type : chaîne

Description : (Facultatif) Description de l'instantané Amazon EBS.

- SnapshotId

Type : chaîne

Description : (Obligatoire) L'ID de l'instantané Amazon EBS à copier.

- SourceRegion

Type : chaîne

Description : (Obligatoire) région dans laquelle l'instantané source existe actuellement.

Étapes de document

CopySnapshot : copie un instantané d'un volume Amazon EBS.

Sorties

CopySnapshot. SnapshotId - L'ID du nouveau cliché.

## **AWS-CreateSnapshot**

Description

Créez un instantané d'un volume Amazon EBS.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Description

Type : chaîne

Description : (Facultatif) description de l'instantané

- Volumeld

Type : chaîne

Description : (Obligatoire) ID du volume.

## AWS-DeleteSnapshot

Description

Supprimez un instantané d'un volume Amazon EBS.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- SnapshotId

Type : chaîne

Description : (Obligatoire) ID de l'instantané EBS.

## AWSConfigRemediation-DeleteUnusedEBSVolume

### Description

Le AWSConfigRemediation-DeleteUnusedEBSVolume runbook supprime un volume Amazon Elastic Block Store (Amazon EBS) inutilisé.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `CreateSnapshot`

Type : booléen

Description : (Facultatif) Si ce paramètre est défini sur `true`, l'automatisation crée un instantané du volume Amazon EBS avant sa suppression.

- `VolumeId`

Type : chaîne

Description : (Obligatoire) L'ID du volume Amazon EBS que vous souhaitez supprimer.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

#### Étapes de document

- `aws:executeScript`- Vérifie que le volume Amazon EBS que vous spécifiez dans le `VolumeId` paramètre n'est pas utilisé et crée un instantané en fonction de la valeur que vous avez choisie pour le `CreateSnapshot` paramètre.
- `aws:branch`- Branches basées sur la valeur que vous avez choisie pour le `CreateSnapshot` paramètre.

- `aws:waitForAwsResourceProperty`- Attend que la capture d'écran soit terminée.
- `aws:executeAwsApi`- Supprime le cliché en cas d'échec de la création du cliché.
- `aws:executeAwsApi`- Supprime le volume Amazon EBS que vous spécifiez dans le `VolumeId` paramètre.
- `aws:executeScript`- Vérifie que le volume Amazon EBS a été supprimé.

## AWS-DeregisterAMIs

### Description

Le `AWS-DeregisterAMIs` runbook vous aide à vous désinscrire Amazon Machine Images (AMIs) en spécifiant le tag que vous avez appliqué à votre. AMIs

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `DryRun`



Type : chaîne

Valeurs valides : Oui | Non

Description : (Obligatoire) Vérifie si vous disposez des autorisations requises pour l'action, sans réellement faire la demande, et fournit une réponse d'erreur.

- RetainNumber

Type : chaîne

Description : (Facultatif) Le numéro AMIs que vous souhaitez conserver. Ne spécifiez pas de valeur pour ce paramètre si vous spécifiez une valeur pourAge.

- Age

Type : chaîne

Description : (Facultatif) Le nombre de jours précédents AMIs que vous souhaitez conserver. Ne spécifiez pas de valeur pour ce paramètre si vous spécifiez une valeur pourRetainNumber.

- TagKey

Type : chaîne

Description : (Obligatoire) La clé du tag attribué à celui AMIs que vous souhaitez désenregistrer.

- TagValue

Type : chaîne

Description : (Obligatoire) La valeur du tag attribué à celui AMIs que vous souhaitez désenregistrer.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ec2:DeregisterImage
- ec2:DescribeImages

## Étapes de document

- `aws:executeAwsApi`- Valide les valeurs que vous spécifiez pour les paramètres d'entrée du runbook.
- `aws:executeAwsApi`- Désenregistre à AMIs l'aide de la balise que vous avez spécifiée à l'`TagKey` aide des paramètres et. `TagValue`

## AWS-DetachEBSVolume

### Description

Détachez un volume Amazon EBS d'une instance Amazon Elastic Compute Cloud (Amazon EC2).

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `LambdaAssumeRole`

Type : chaîne

Description : (Facultatif) L'ARN du rôle assumé par Lambda

- Volumeld

Type : chaîne

Description : (Obligatoire) ID du volume EBS. Le volume et l'instance doivent être dans la même zone de disponibilité.

## **AWSConfigRemediation-EnableEbsEncryptionByDefault**

### Description

Le AWSConfigRemediation-EnableEbsEncryptionByDefault runbook permet le chiffrement de tous les nouveaux volumes Amazon Elastic Block Store (Amazon EBS) présents dans Compte AWS et sur Région AWS lesquels vous exécutez l'automatisation. Les volumes créés avant l'exécution de l'automatisation ne sont pas chiffrés.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeAwsApi`- Active le paramètre de chiffrement Amazon EBS par défaut dans le compte courant et la région.
- `aws:assertAwsResourceProperty`- Vérifie que le paramètre de chiffrement par défaut d'Amazon EBS a été activé.

## AWS-ExtendEbsVolume

### Description

Le `AWS-ExtendEbsVolume` runbook augmente la taille d'un volume Amazon EBS et étend le système de fichiers. Cette automatisation prend en charge les systèmes de fichiers `ext4` et `xfs`.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- DriveLetter

Type : chaîne

Description : (Facultatif) La lettre du lecteur dont vous souhaitez étendre le système de fichiers. Ce paramètre est obligatoire pour les Windows instances.

- InstanceId

Type : chaîne

Description : (Facultatif) L'ID de l'instance Amazon EC2 à laquelle le volume Amazon EBS que vous souhaitez étendre est attaché.

- KeepSnapshot

Type : booléen

Valeur par défaut : true

Description : (Facultatif) Détermine s'il faut conserver l'instantané créé avant d'augmenter la taille de votre volume Amazon EBS.

- MountPoint

Type : chaîne

Description : (Facultatif) Point de montage du lecteur dont vous souhaitez étendre le système de fichiers. Ce paramètre est obligatoire pour les instances Linux.

- SizeGib

Type : chaîne

Description : (Obligatoire) La taille en GiB à laquelle vous souhaitez modifier votre volume Amazon EBS.

- VolumeId

Type : chaîne

Description : (Obligatoire) L'ID du volume EBS que vous souhaitez étendre.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeScript`- Augmente la taille du volume jusqu'à la valeur que vous spécifiez dans le `VolumeId` paramètre et étend le système de fichiers.

## **AWSSupport-ModifyEBSSnapshotPermission**

### Description

Le `AWSSupport-ModifyEBSSnapshotPermission` runbook vous permet de modifier les autorisations pour plusieurs instantanés Amazon Elastic Block Store (Amazon EBS). À l'aide de ce runbook, vous pouvez créer des instantanés `Public` ou `Private` les partager avec d'autres. Comptes AWS Les instantanés chiffrés avec une clé KMS par défaut ne peuvent pas être partagés avec d'autres comptes utilisant ce runbook.

[Exécuter cette automatisation \(console\)](#)

### Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- AccountIds

Type : StringList

Par défaut: Aucun

Description : (Facultatif) Les identifiants des comptes avec lesquels vous souhaitez partager des instantanés. Ce paramètre est obligatoire si vous entrez No la valeur du Private paramètre.

- AccountPermissionOperation

Type : chaîne

Valeurs valides : ajouter | supprimer

Par défaut: Aucun

Description : (Facultatif) Type d'opération à effectuer.

- Privé

Type : chaîne

Valeurs valides : Oui | Non

Description : (Obligatoire) Entrez No la valeur si vous souhaitez partager des instantanés avec des comptes spécifiques.

- SnapshotIds

Type : StringList

Description : (Obligatoire) Les identifiants des instantanés Amazon EBS dont vous souhaitez modifier l'autorisation.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

## Étapes de document

1. `aws:executeScript`- Vérifie les identifiants des instantanés fournis dans le SnapshotIds paramètre. Après avoir vérifié les identifiants, le script recherche les instantanés chiffrés et affiche une liste s'ils sont trouvés.
2. `aws:branch`- Branche l'automatisation en fonction de la valeur que vous entrez pour le Private paramètre.
3. `aws:executeScript`- Modifie les autorisations des instantanés spécifiés pour les partager avec les comptes spécifiés.
4. `aws:executeScript`- Modifie les autorisations des instantanés pour les faire passer de Public à Private

## Sorties

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Résultat



MakePrivate.Résultat

MakePrivate.Commandes

## AWSConfigRemediation-ModifyEBSVolumeType

Description

Le AWSConfigRemediation-ModifyEBSVolumeType runbook modifie le type de volume d'un volume Amazon Elastic Block Store (Amazon EBS). Une fois le type de volume modifié, le volume entre dans un `optimizing` état. Pour plus d'informations sur le suivi de la progression des modifications de volume, consultez la section [Surveillance de la progression des modifications de volume](#) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- EbsVolumeld

Type : chaîne

Description : (Obligatoire) L'ID du volume Amazon EBS que vous souhaitez modifier.

- EbsVolumeType

Type : chaîne

Valeurs valides : standard | io1 | io2 | gp2 | gp3 | sc1 | st1

Description : le type de volume que vous souhaitez remplacer par le volume Amazon EBS. Pour plus d'informations sur les types de volumes Amazon EBS, consultez les types de [volumes Amazon EBS](#) dans le guide de l'utilisateur Amazon EC2 pour les instances Linux.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- aws:waitForAwsResourceProperty- Vérifie que l'état du volume est available ou in-use.
- aws:executeAwsApi- Modifie le volume Amazon EBS que vous spécifiez dans le EbsVolumeId paramètre.
- aws:waitForAwsResourceProperty- Vérifie que le type du volume a été modifié à la valeur que vous avez spécifiée dans le EbsVolumeType paramètre.

## Amazon EC2

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Elastic Compute Cloud. Les runbooks pour Amazon Elastic Block Store se trouvent dans la [Amazon EBS](#) section de référence des runbooks. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWS-ASGEnterStandby](#)

- [AWS-ASGExitStandby](#)
- [AWS-CreatelImage](#)
- [AWS-DeletelImage](#)
- [AWS-PatchAsgInstance](#)
- [AWS-PatchInstanceWithRollback](#)
- [AWS-QuarantineEC2Instance](#)
- [AWS-ResizeInstance](#)
- [AWS-RestartEC2Instance](#)
- [AWS-SetupJupyter](#)
- [AWS-StartEC2Instance](#)
- [AWS-StopEC2Instance](#)
- [AWS-TerminateEC2Instance](#)
- [AWS-UpdateLinuxAmi](#)
- [AWS-UpdateWindowsAmi](#)
- [AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck](#)
- [AWSConfigRemediation-EnforceEC2InstanceIMDSv2](#)
- [AWSEC2-CloneInstanceAndUpgradeSQLServer](#)
- [AWSEC2-CloneInstanceAndUpgradeWindows](#)
- [AWSEC2-ConfigureSTIG](#)
- [AWSEC2-PatchLoadBalancerInstance](#)
- [AWSEC2-SQLServerDBRestore](#)
- [AWSSupport-ActivateWindowsWithAmazonLicense](#)
- [AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2](#)
- [AWSPremiumSupport-ChangeInstanceTypeIntelToAMD](#)
- [AWSSupport-CheckXenToNitroMigrationRequirements](#)
- [AWSSupport-ConfigureEC2Metadata](#)
- [AWSSupport-CopyEC2Instance](#)
- [AWSSupport-EnableWindowsEC2SerialConsole](#)
- [AWSSupport-ExecuteEC2Rescue](#)
- [AWSSupport-ListEC2Resources](#)

- [AWSSupport-ManageRDPSettings](#)
- [AWSSupport-ManageWindowsService](#)
- [AWSSupport-MigrateEC2ClassicToVPC](#)
- [AWSSupport-MigrateXenToNitroLinux](#)
- [AWSSupport-ResetAccess](#)
- [AWSSupport-ResetLinuxUserPassword](#)
- [AWSPremiumSupport-ResizeNitroInstance](#)
- [AWSSupport-RestoreEC2InstanceFromSnapshot](#)
- [AWSSupport-SendLogBundleToS3Bucket](#)
- [AWSSupport-StartEC2RescueWorkflow](#)
- [AWSPremiumSupport-TroubleshootEC2DiskUsage](#)
- [AWSSupport-TroubleshootEC2InstanceConnect](#)
- [AWSSupport-TroubleshootRDP](#)
- [AWSSupport-TroubleshootSSH](#)
- [AWSSupport-TroubleshootSUSERegistration](#)
- [AWSSupport-TroubleshootWindowsPerformance](#)
- [AWSSupport-TroubleshootWindowsUpdate](#)
- [AWSSupport-UpgradeWindowsAWSDrivers](#)

## AWS-ASGEnterStandby

### Description

Modifiez l'état de veille d'une instance Amazon Elastic Compute Cloud (Amazon EC2) dans un groupe Auto Scaling.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) ID d'une instance Amazon EC2 pour laquelle vous souhaitez modifier l'état de veille au sein d'un groupe Auto Scaling.

- LambdaRoleArn

Type : String

Description : (Facultatif) ARN du rôle qui autorise la fonction Lambda créée par Automation à effectuer des actions en votre nom. Si vous ne spécifiez pas cette valeur, un rôle transitoire est créé pour exécuter la fonction Lambda.

## AWS-ASGExitStandby

### Description

Modifiez l'état de veille d'une instance Amazon Elastic Compute Cloud (Amazon EC2) dans un groupe Auto Scaling.

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) ID d'une instance EC2 dont vous souhaitez modifier l'état de veille au sein d'un groupe Auto Scaling.

- LambdaRoleArn

Type : String

Description : (Facultatif) ARN du rôle qui autorise la fonction Lambda créée par Automation à effectuer des actions en votre nom. Si vous ne spécifiez pas cette valeur, un rôle transitoire est créé pour exécuter la fonction Lambda.

## AWS-CreateImage

### Description

Créez un nouveau Amazon Machine Image (AMI) à partir d'une instance Amazon Elastic Compute Cloud (Amazon EC2).

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (obligatoire) ID de l'instance EC2.

- NoReboot

Type : booléen

Description : (Facultatif) ne redémarrez pas l'instance avant de créer l'image.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

```
        "Effect": "Allow",
        "Action": [
            "ec2:CreateImage",
            "ec2:DescribeImages"
        ],
        "Resource": [
            "*"
        ]
    }
]
}
```

## AWS-DeleteImage

### Description

Supprimez un Amazon Machine Image (AMI) et tous les instantanés associés.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- Imageld



Type : String

Description : (Obligatoire) ID de l'AMI.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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

### Description

Appliquez des correctifs aux instances Amazon Elastic Compute Cloud (Amazon EC2) dans un groupe Auto Scaling.

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

## Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) ID de l'instance à corriger. Ne spécifiez pas d'ID d'instance configuré pour s'exécuter pendant une fenêtre de maintenance.

- LambdaRoleArn

Type : String

Description : (Facultatif) L'ARN du rôle qui permet au Lambda créé par Automation d'effectuer les actions en votre nom. S'il n'est pas spécifié, un rôle transitoire sera créé pour exécuter la fonction Lambda.

- WaitForInstance

Type : String

Valeur par défaut : PT2M

Description : (Facultatif) Durée pendant laquelle l'automatisation doit rester en veille pour permettre à l'instance de revenir en service.

- WaitForReboot

Type : String

Valeur par défaut : PT5M

Description : (Facultatif) Durée pendant laquelle l'automatisation doit rester en veille pour permettre à une instance corrigée de redémarrer.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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

### Description

Met une instance EC2 en conformité avec la base de correctifs applicable. Réduit le volume racine en cas de panne.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Linux, macOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- `InstanceId`

Type : String

Description : (Obligatoire) EC2 InstanceId auquel nous appliquons le patch-baseline.

- `LambdaAssumeRole`

Type : String

Description : (Facultatif) ARN du rôle qui autorise la fonction Lambda créée par Automation à effectuer des actions en votre nom. Si vous ne spécifiez pas cette valeur, un rôle transitoire est créé pour exécuter la fonction Lambda.

- ReportS3Bucket

Type : String

Description : (Facultatif) Destination du compartiment Amazon S3 pour le rapport de conformité généré au cours du processus.

## Étapes de document

Numéro de l'étape	Nom de l'étape	Action Automation
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

Numéro de l'étape	Nom de l'étape	Action Automation
10	DeleteSnapshot	aws:invokeLambdaFunction
11	deleteCloudFormationModèle	aws:deleteStack

## Sorties

IdentifyRootVolume.Charge utile

PrePatchSnapshot. Sortie

SaveComplianceReportToS3. Charge utile

RestoreFromSnapshot.Charge utile

CheckCompliance.Charge utile

## AWS-QuarantineEC2Instance

### Description

Avec le AWS-QuarantineEC2Instance runbook, vous pouvez attribuer un groupe de sécurité à une instance Amazon Elastic Compute Cloud (Amazon EC2) qui n'autorise aucun trafic entrant ou sortant.

#### Important

Les modifications apportées aux paramètres RDP doivent être examinées attentivement avant d'exécuter ce runbook.

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) ID de l'instance chargée de gérer les paramètres RDP.

- IsolationSecurityGroup

Type : String

Description : (Obligatoire) Le nom du groupe de sécurité que vous souhaitez attribuer à l'instance pour empêcher le trafic entrant ou sortant.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

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

### Étapes de document

- `aws:executeAwsApi`- Recueille des informations sur l'instance.
- `aws:executeScript`- Vérifie que l'instance ne fait pas partie d'un groupe Auto Scaling.
- `aws:executeAwsApi`- Crée un instantané du volume racine attaché à l'instance.
- `aws:waitForAwsResourceProperty`- Attend que l'état du snapshot soit atteint. `completed`
- `aws:executeAwsApi`- Assigne le groupe de sécurité spécifié dans le `IsolationSecurityGroup` paramètre à votre instance.

### Sorties

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

## AWS-ResizeInstance

### Description

Modifiez le type d'instance d'une instance Amazon Elastic Compute Cloud (Amazon EC2).

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon



## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) ID de l'instance.

- InstanceType

Type : String

Description : (Obligatoire) type de l'instance.

- LambdaAssumeRole

Type : String

Description : (Facultatif) L'ARN du rôle assumé par Lambda.

## AWS-RestartEC2Instance

### Description

Redémarrez une ou plusieurs instances Amazon Elastic Compute Cloud (Amazon EC2).

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : StringList

Description : (Obligatoire) Les identifiants des instances Amazon EC2 à redémarrer.

## AWS-SetupJupyter

### Description

Le AWS-SetupJupyter runbook vous aide à configurer Jupyter Notebook sur une instance Amazon Elastic Compute Cloud (Amazon EC2). Vous pouvez soit spécifier une instance existante, soit fournir un ID Amazon Machine Image (AMI) pour que l'automatisation lance et configure une nouvelle instance. Avant de commencer, vous devez créer un SecureString paramètre dans Parameter Store à utiliser comme mot de passe pour Jupyter Notebook. Parameter Store est une fonctionnalité deAWS Systems Manager. Pour plus d'informations sur la création de paramètres, voir [Création de paramètres](#) dans le Guide de AWS Systems Manager l'utilisateur.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

## Propriétaire

Amazon

Plateformes

Linux

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- Amild

Type : String

Description : (Facultatif) L'identifiant AMI que vous souhaitez utiliser pour lancer une nouvelle instance et configurer Jupyter Notebook.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance sur laquelle vous souhaitez configurer Jupyter Notebook.

- InstanceType

Type : String

Par défaut : t3.medium

Description : (Facultatif) Si vous lancez une nouvelle instance pour configurer Jupyter Notebook, spécifiez le type d'instance que vous souhaitez utiliser.

- JupyterPasswordClé SSM

Type : String

Description : (Obligatoire) Le nom du SecureString paramètre dans Parameter Store que vous souhaitez utiliser comme mot de passe pour Jupyter Notebook.

- KeyPairName

Type : String

Description : (Facultatif) La paire de clés que vous souhaitez associer à l'instance récemment lancée.

- RemoteAccessCidr

Type : String

Par défaut : 0.0.0.0/0

Description : (Facultatif) La plage d'adresses CIDR à partir de laquelle vous souhaitez autoriser le trafic SSH.

- RoleName

Type : String

Par défaut : SSM ManagedInstanceProfileRole

Description : (Facultatif) Le nom du profil d'instance pour l'instance récemment lancée.

- StackName

Type : String

Par défaut : CreateManagedInstanceStack {{Automation:Execution\_ID}}

Description : (Facultatif) Le nom de la AWS CloudFormation pile que vous souhaitez que l'automatisation utilise.

- SubnetId

Type : String

Par défaut : Default

Description : (Facultatif) Le sous-réseau que vous souhaitez utiliser pour lancer la nouvelle instance.

- VpcId

Type : String

Par défaut : Default

Description : (Facultatif) L'ID du cloud privé virtuel (VPC) dans lequel vous souhaitez lancer la nouvelle instance.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

- `aws:executeScript`- Configure Jupyter Notebook sur l'instance que vous spécifiez, ou sur une instance récemment lancée, en utilisant les valeurs que vous spécifiez pour les paramètres d'entrée du runbook.

## AWS-StartEC2Instance

### Description

Démarrez une ou plusieurs instances Amazon Elastic Compute Cloud (Amazon EC2).

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : StringList

Description : (obligatoire) instances EC2 à démarrer.

## AWS-StopEC2Instance

Description

Arrête une ou plusieurs instances Amazon Elastic Compute Cloud (Amazon EC2).

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : StringList

Description : (Obligatoire) Instances EC2 à arrêter.

## AWS-TerminateEC2Instance

### Description

Mettez fin à une ou plusieurs instances Amazon Elastic Compute Cloud (Amazon EC2).

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : StringList

Description : (obligatoire) ID d'une ou de plusieurs instances EC2 à supprimer.

## AWS-UpdateLinuxAmi

### Description

Mettez à jour an Amazon Machine Image (AMI) avec les packages de distribution Linux et le logiciel Amazon.



[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ExcludePackages

Type : chaîne

Par défaut: Aucun

Description : (Facultatif) noms des packages spécifiques à exclure des mises à jour, sous toutes les conditions. Avec la valeur par défaut ("none"), aucun package n'est exclu.

- IamInstanceProfileName

Type : chaîne

Par défaut : ManagedInstanceProfile

Description : (Obligatoire) Le profil d'instance qui permet à Systems Manager de gérer l'instance.

- IncludePackages

Type : chaîne

Par défaut : all

Description : (Facultatif) mettez à jour uniquement ces packages nommés. Avec la valeur par défaut ("all"), toutes les mises à jour disponibles sont appliquées.

- InstanceType

Type : chaîne

Par défaut : t2.micro

Description : (Facultatif) type d'instance à lancer en tant qu'hôte d'espace de travail. Les types d'instances varient selon la région.

- MetadataOptions

Type : StringMap

Par défaut : {» HttpEndpoint « : « enabled », "HttpTokens« : « optional"}

Description : (Facultatif) Les options de métadonnées pour l'instance. Pour plus d'informations, consultez [InstanceMetadataOptionsRequest](#).

- PostUpdateScript

Type : chaîne

Par défaut: Aucun

Description : (Facultatif) URL d'un script à exécuter après l'application des mises à jour de package. La valeur par défaut ("none") implique la non-exécution d'un script.

- PreUpdateScript

Type : chaîne

Par défaut: Aucun

Description : (Facultatif) URL d'un script à exécuter avant l'application des mises à jour. La valeur par défaut ("none") implique la non-exécution d'un script.

- SourceAmild

Type : chaîne

Description : (Obligatoire) ID de l'Amazon Machine Image source.

- SubnetId

Type : chaîne

Description : (Facultatif) L'ID du sous-réseau dans lequel vous souhaitez lancer l'instance. Si vous avez supprimé votre VPC par défaut, ce paramètre est obligatoire.

- TargetAmiName

Type : chaîne

Par défaut : UpdateLinuxAmi \_from\_ {{SourceAmiId}} \_on\_ {{global:Date\_time}}

Description : (Facultatif) nom de l'AMI qui sera créée. La valeur par défaut est une chaîne générée par le système qui inclut l'ID de l'AMI source, et les date et heure de création.

## AWS-UpdateWindowsAmi

Description

Mettez à jour un Microsoft Windows Amazon Machine Image (AMI). Par défaut, ce runbook installe toutes les mises à jour Windows, les logiciels Amazon et les pilotes Amazon. Ensuite, il exécute Sysprep pour créer une AMI. Prend en charge Windows Server 2008 R2 ou version ultérieure.

### Important

Si vos instances se connectent à AWS Systems Manager l'aide de points de terminaison VPC, ce runbook échouera s'il n'est pas utilisé dans la région us-east-1. TLS 1.2 doit être activé sur les instances pour utiliser ce runbook.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

## Plateformes

### Windows

#### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Catégories

Type : chaîne

Description : (Facultatif) spécifiez une ou plusieurs catégories de mise à jour. Vous pouvez filtrer les catégories en utilisant des valeurs séparées par une virgule. Options : Application, connecteurs, CriticalUpdates, DefinitionUpdates, DeveloperKits, pilotes, FeaturePacks, conseils, Microsoft,, SecurityUpdates ServicePacks, outilsUpdateRollups, mises à jour. Les formats valides incluent une seule entrée, par exemple :CriticalUpdates. Vous pouvez également spécifier une liste séparée par des virgules :CriticalUpdates,SecurityUpdates. REMARQUE : n'ajoutez aucun espace autour des virgules.

- ExcludeKbs

Type : chaîne

Description : (Facultatif) spécifiez un ou plusieurs ID d'articles Microsoft Knowledge Base (KB) à exclure. Vous pouvez exclure plusieurs ID en utilisant des valeurs séparées par une virgule. Formats valides : KB9876543 ou 9876543.

- IamInstanceProfileName

Type : chaîne

Par défaut : ManagedInstanceProfile

Description : (Obligatoire) Le nom du rôle qui permet à Systems Manager de gérer l'instance.

- IncludeKbs

Type : chaîne

Description : (Facultatif) spécifiez un ou plusieurs ID d'articles Microsoft Knowledge Base (KB) à inclure. Vous pouvez installer plusieurs ID en utilisant des valeurs séparées par une virgule. Formats valides : KB9876543 ou 9876543.

- InstanceType

Type : chaîne

Par défaut : t2.medium

Description : (Facultatif) type d'instance à lancer en tant qu'hôte d'espace de travail. Les types d'instances varient selon la région. La valeur par défaut est t2.medium.

- MetadataOptions

Type : StringMap

Par défaut : { » HttpEndpoint « : « enabled », "HttpTokens« : « optional" }

Description : (Facultatif) Les options de métadonnées pour l'instance. Pour plus d'informations, consultez [InstanceMetadataOptionsRequest](#).

- PostUpdateScript

Type : chaîne

Description : (Facultatif) script fourni sous la forme d'une chaîne. Il est exécuté après l'installation des mises à jour du système d'exploitation.

- PreUpdateScript

Type : chaîne

Description : (Facultatif) script fourni sous la forme d'une chaîne. Il est exécuté avant l'installation des mises à jour du système d'exploitation.

- PublishedDateAfter

Type : chaîne

Description : (Facultatif) spécifiez la date après laquelle les mises à jour doivent être publiées. Par exemple, si 01/01/2017 est spécifié, toutes les mises à jour qui ont été trouvées pendant la recherche des mises à jour Windows qui ont été publiées après le 01/01/2017 sont renvoyées.

- `PublishedDateBefore`

Type : chaîne

Description : (Facultatif) spécifiez la date avant laquelle les mises à jour doivent être publiées. Par exemple, si 01/01/2017 est spécifié, toutes les mises à jour qui ont été trouvées pendant la recherche des mises à jour Windows qui ont été publiées avant le 01/01/2017 sont renvoyées.

- `PublishedDaysOld`

Type : chaîne

Description : (Facultatif) spécifiez le nombre de jours maximum qui se sont écoulés depuis la date de publication des mises à jour. Par exemple, si 10 est spécifié, toutes les mises à jour qui ont été trouvées pendant la recherche des mises à jour Windows il y a 10 jours ou plus sont renvoyées.

- `SeverityLevels`

Type : chaîne

Description : (Facultatif) spécifiez un ou plusieurs niveaux de sécurité MSRC associés à une mise à jour. Vous pouvez filtrer les niveaux de sécurité en utilisant des valeurs séparées par une virgule. Par défaut, les correctifs pour tous les niveaux de sécurité sont sélectionnés. Si cette valeur est fournie, la liste de mise à jour est filtrée en conséquence. Options : Critique, Important, Faible, Modéré ou Non précisé. Parmi les formats valides, on compte une seule entrée comme : Critique. Ou, vous pouvez spécifier une liste avec des éléments séparés par des virgules : Critique, Important, Faible.

- `SourceAmild`

Type : chaîne

Description : (Obligatoire) ID de l'Amazon Machine Image source.

- `SubnetId`

Type : chaîne

Description : (Facultatif) L'ID du sous-réseau dans lequel vous souhaitez lancer l'instance. Si vous avez supprimé votre VPC par défaut, ce paramètre est obligatoire.

- TargetAmiName

Type : chaîne

Par défaut : UpdateWindowsAmi \_from\_ {{SourceAmild}} \_on\_ {{global:Date\_time}}

Description : (Facultatif) nom de l'AMI qui sera créée. La valeur par défaut est une chaîne générée par le système qui inclut l'ID de l'AMI source, et les date et heure de création.

## **AWSConfigRemediation- EnableAutoScalingGroupELBHealthCheck**

Description

Le AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck runbook permet de vérifier l'état du groupe Amazon EC2 Auto Scaling (Auto Scaling) que vous avez spécifié.

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- AutoScalingGroupARN

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du groupe de mise à l'échelle automatique sur lequel vous souhaitez activer les contrôles de santé.

- HealthCheckGracePeriod

Type : entier

Par défaut : 300

Description : (Facultatif) Durée, en secondes, pendant laquelle Auto Scaling attend avant de vérifier l'état de santé d'une instance Amazon Elastic Compute Cloud (Amazon EC2) mise en service.

#### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

#### Étapes de document

- aws:executeScript- Active les vérifications de l'état du groupe Auto Scaling que vous spécifiez dans le AutoScalingGroupARN paramètre.

## **AWSConfigRemediation-EnforceEC2InstanceIMDSv2**

### Description



Le `AWSConfigRemediation-EnforceEC2InstanceIMDSv2` runbook nécessite l'instance Amazon Elastic Compute Cloud (Amazon EC2) que vous spécifiez pour utiliser le service de métadonnées d'instance version 2 (IMDSv2).

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `InstanceId`

Type : chaîne

Description : (Obligatoire) L'ID de l'instance Amazon EC2 dont vous souhaitez avoir besoin pour utiliser IMDSv2.

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `HttpPutResponseHopLimit`

Type : entier

Description : (Facultatif) Limite de réponse Hop entre le service IMDS et le demandeur. Défini sur 2 ou plus pour les instances EC2 hébergeant des conteneurs. Réglé sur 0 pour ne pas changer (valeur par défaut).

Schéma autorisé : `^[1-5]?\d|6[0-4])$`

Par défaut : 0

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

## Étapes de document

- `aws:executeScript`- Définit l'`HttpTokenOption required` sur l'instance Amazon EC2 que vous spécifiez dans le `InstanceId` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie qu'`IMDSv2` est requis sur l'instance Amazon EC2.

# AWSEC2-CloneInstanceAndUpgradeSQLServer

## Description

Créez un AMI à partir d'une instance EC2 pour Windows Server exécuter SQL Server 2008 ou version ultérieure, puis mettez à niveau l'AMI vers une version ultérieure de SQL Server.

Les chemins de mise à niveau suivants sont pris en charge :

- SQL Server 2008 vers SQL Server 2017, 2016 ou 2014
- SQL Server 2008 R2 vers SQL Server 2017, 2016 ou 2014
- SQL Server 2012 vers SQL Server 2019, 2017, 2016 ou 2014
- SQL Server 2014 vers SQL Server 2019, 2017 ou 2016
- SQL Server 2016 vers SQL Server 2019 ou 2017
- SQL Server 2017 vers SQL Server 2019

Si vous utilisez une version antérieure de Windows Server incompatible avec SQL Server 2019, le document d'automatisation doit mettre à niveau votre version de Windows Server vers 2016.

La mise à niveau est un processus en plusieurs étapes qui peut prendre 2 heures. L'automatisation crée l'AMI à partir de l'instance, puis lance une instance temporaire à partir de la nouvelle AMI instance spécifiée `SubnetID`. Les groupes de sécurité associés à votre instance d'origine sont appliqués à l'instance temporaire. L'automatisation effectue ensuite une mise à niveau `TargetSQLVersion` sur place de l'instance temporaire. Après la mise à niveau, l'automatisation crée une nouvelle instance AMI à partir de l'instance temporaire, puis met fin à l'instance temporaire.

Vous pouvez tester les fonctionnalités de l'application en lançant la nouvelle AMI dans votre VPC. Une fois que vous avez terminé le test et avant de procéder à une autre mise à niveau, planifiez les temps d'arrêt de l'application avant de passer complètement à l'instance mise à niveau.

#### Note

Si vous souhaitez modifier le nom de l'ordinateur de l'instance EC2 lancée à partir de la nouvelle AMI, voir [Renommer un ordinateur qui héberge une instance autonome de SQL Server](#).

### [Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Windows

Paramètres

Prérequis

- Version 1.2 du protocole TLS.

- L'instance EC2 doit utiliser une version Windows Server qui soit Windows Server 2008 R2 (ou version ultérieure) et SQL Server 2008 (ou version ultérieure).
- Vérifier que SSM Agent est installé sur votre instance. Pour plus d'informations, consultez [Installation et configuration de l'agent SSM sur des instances EC2 pour Windows Server](#).
- Configurez l'instance pour utiliser un rôle de profil d'instance AWS Identity and Access Management (IAM). Pour de plus amples informations, veuillez consulter [Créer un profil d'instance IAM pour Systems Manager](#).
- Vérifiez que l'instance a 20 Go d'espace disque libre dans le disque de démarrage.
- Pour les instances qui utilisent une version SQL Server avec apport de sa propre licence (BYOL), les prérequis supplémentaires suivants s'appliquent :
  - Fournissez un ID de snapshot EBS qui inclut le support d'installation cible de SQL Server. Pour cela :
    1. Vérifiez que l'instance EC2 exécute Windows Server 2008 R2 ou version ultérieure.
    2. Créez un volume EBS de 6 Go dans la même zone de disponibilité que celle où l'instance est en cours d'exécution. Attachez le volume à l'instance. Montez-la, par exemple, en tant que lecteur D.
    3. Cliquez avec le bouton droit de la souris sur le fichier ISO et montez-le sur une instance telle que le lecteur E.
    4. Copiez le contenu du fichier ISO depuis le lecteur E:\ vers le lecteur D:\.
    5. Créez un instantané EBS du volume de 6 Go créé à l'étape 2.

## Limites

- La mise à niveau peut uniquement être effectuée sur un serveur SQL à l'aide de l'authentification Windows.
- Vérifiez qu'il n'y a pas de correctifs et mises à jour de sécurité en attente sur les instances. Ouvrez le Panneau de configuration, puis choisissez Rechercher les mises à jour.
- Les déploiements SQL Server HA et le mode de mise en miroir ne sont pas pris en charge.

## Paramètres

- `IamInstanceProfile`

Type : String

Description : (Obligatoire) Le profil d'instance IAM.

- InstanceId

Type : String

Description : (obligatoire) L'instance exécutant Windows Server 2008 R2 (ou version ultérieure) ou SQL Server 2008 (ou version ultérieure).

- KeepPreUpgradedImageBackUp

Type : String

Description : (Facultatif) Si ce paramètre est défini sur `true`, l'automatisation ne supprime pas l'AMI créée à partir de l'instance avant la mise à niveau. Si ce paramètre est défini sur `true`, vous devez supprimer l'AMI. Par défaut, l'AMI sera supprimée.

- SubnetId

Type : String

Description : (Obligatoire) fournissez un sous-réseau pour le processus de mise à niveau. Vérifiez que le sous-réseau dispose d'une connectivité sortante vers les AWS services, Amazon S3 et Microsoft (pour télécharger des correctifs).

- SQL ServerSnapshotId

Type : String

Description : ID de snapshot (conditionnel) pour le support d'installation cible de SQL Server. Ce paramètre est obligatoire pour les instances qui utilisent une version BYOL de SQL Server. Ce paramètre est facultatif pour les instances SQL Server avec licence incluse (instances lancées à l'aide d'une Amazon Machine Image (AMI) fournie par AWS pour Microsoft Server avec Microsoft SQL Server).

- RebootInstanceBeforeTakingImage

Type : String

Description : (Facultatif) Si ce paramètre est défini sur `true`, l'automatisation redémarre l'instance avant de créer une AMI préalable à la mise à niveau. Par défaut, l'automatisation ne redémarre pas avant la mise à niveau.

- Version SQL cible

Type : String

Description : (Facultatif) Sélectionnez la version cible de SQL Server.

Cibles possibles :

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

Cible par défaut : SQL Server 2016

Sorties

AMIID : ID de l'AMI créée à partir de l'instance qui a été mise à niveau vers une version ultérieure de SQL Server.

## **AWSEC2-CloneInstanceAndUpgradeWindows**

Description

Créez une Amazon Machine Image (AMI) à partir d'une instance Windows Server 2008 R2, 2012 R2, 2016 ou 2019, puis mettez-la à niveau AMI vers Windows Server 2016, 2019 ou 2022. Les chemins de mise à niveau pris en charge sont les suivants.

- Windows Server2008 R2 à Windows Server 2016.
- Windows Server 2012 R2 vers Windows Server 2016.
- Windows Server 2012 R2 vers Windows Server 2019.
- Windows Server2012 R2 à Windows Server 2022.
- Windows Server 2016 vers Windows Server 2019.
- Windows Server2016 à Windows Server 2022.
- Windows Server2019 à Windows Server 2022.

L'opération de mise à niveau est un processus en plusieurs étapes qui peut prendre 2 heures. Nous recommandons d'effectuer une mise à niveau du système d'exploitation sur les instances avec au moins 2 vCPU et 4 Go de RAM. L'automatisation crée une AMI à partir de l'instance, puis lance une

instance temporaire à partir de l'AMI nouvellement créée dans celle SubnetId que vous spécifiez. Les groupes de sécurité associés à votre instance d'origine sont appliqués à l'instance temporaire. L'automatisation effectue ensuite une mise à niveau TargetWindowsVersion sur place vers l'instance temporaire. Pour mettre à niveau votre instance Windows Server 2008 R2 vers Windows Server 2016, 2019 ou 2022, une mise à niveau sur place est effectuée deux fois car la mise à niveau directe de Windows Server 2008 R2 vers Windows Server 2016, 2019 ou 2022 n'est pas prise en charge. L'automatisation met également à jour ou installe les AWS pilotes requis par l'instance temporaire. Après la mise à niveau, l'automatisation crée une nouvelle AMI à partir de l'instance temporaire, puis met fin à l'instance temporaire.

Vous pouvez tester les fonctionnalités de l'application en lançant une instance de test depuis l'AMI mise à niveau dans votre Amazon Virtual Private Cloud (Amazon VPC). Une fois que vous avez terminé le test et avant de procéder à une autre mise à niveau, planifiez les temps d'arrêt de l'application avant de passer complètement à l'AMI mise à niveau.

### [Exécuter cette automatisation \(console\)](#)

#### Types de document

Automatisation

Propriétaire

Amazon

Plateformes

Windows ServerÉditions Standard et Datacenter 2008 R2, 2012 R2, 2016 ou 2019

#### Prérequis

- Version 1.2 du protocole TLS.
- Vérifier que SSM Agent est installé sur votre instance. Pour plus d'informations, consultez [Installation et configuration de l'agent SSM sur les instances EC2 pour Windows Server](#).
- Windows PowerShell 3.0 ou version ultérieure doit être installé sur votre instance.
- Pour les instances qui sont jointes à un domaine Microsoft Active Directory, nous vous recommandons de spécifier un SubnetId qui n'a pas de connectivité à vos contrôleurs de domaine afin d'éviter les conflits de noms d'hôte.
- Le sous-réseau de l'instance doit disposer d'une connectivité sortante à Internet, qui permet d'accéder Services AWS à Amazon S3 et de télécharger des correctifs depuis Microsoft. Cette

exigence est satisfaite si le sous-réseau est un sous-réseau public et que l'instance possède une adresse IP publique, ou si le sous-réseau est un sous-réseau privé avec une route qui envoie le trafic Internet vers un périphérique NAT public.

- Cette automatisation fonctionne uniquement avec les instances Windows Server 2008 R2, 2012 R2, 2016 et 2019.
- Configurez l'instance Windows Server avec un profil d'instance AWS Identity and Access Management (IAM) fournissant les autorisations requises pour Systems Manager. Pour de plus amples informations, veuillez consulter [Créer un profil d'instance IAM pour Systems Manager](#).
- Vérifiez que l'instance a 20 Go d'espace disque libre dans le disque de démarrage.
- Si l'instance n'utilise pas de licence Windows AWS fournie, spécifiez un ID de snapshot Amazon EBS qui inclut le support d'installation Windows Server 2012 R2. Pour cela :
  - Vérifiez que l'instance EC2 exécute actuellement Windows Server 2012 ou version ultérieure.
  - Créez un volume EBS de 6 Go dans la même zone de disponibilité que celle où l'instance est en cours d'exécution. Attachez le volume à l'instance. Montez-la, par exemple, en tant que lecteur D.
  - Cliquez avec le bouton droit de la souris sur le fichier ISO et montez-le sur une instance telle que le lecteur E.
  - Copiez le contenu du fichier ISO depuis le lecteur E:\ vers le lecteur D:\.
  - Créez un instantané EBS de 6 Go comme à l'étape 2 ci-dessus.

## Limites

Cette procédure d'automatisation ne prend pas en charge la mise à niveau des contrôleurs de domaine Windows, les clusters ni les systèmes d'exploitation de bureau Windows. Elle ne prend pas non plus en charge les instances EC2 pour Windows Server avec les rôles suivants installés.

- Hôte de session des services Bureau à distance (RDSH)
- Broker de connexion des services Bureau à distance (RDCB)
- Hôte de virtualisation des services Bureau à distance (RDVH)
- Accès web des services Bureau à distance (RDWA)

## Paramètres

- `AlternativeKeyPairName`



Type : chaîne

Description : (Facultatif) Nom d'une paire de clés alternative à utiliser pendant le processus de mise à niveau. Cela est utile dans les situations où la paire de clés attribuée à l'instance d'origine n'est pas disponible. Si aucune paire de clés n'a été attribuée à l'instance d'origine, vous devez spécifier une valeur pour ce paramètre.

- PAR OL WindowsMediaSnapshotId

Type : chaîne

Description : (Facultatif) L'ID du snapshot Amazon EBS à copier qui inclut le support d'installation de Windows Server 2012R2. Obligatoire uniquement si vous mettez à niveau une instance BYOL.

- iamInstanceProfile

Type : chaîne

Description : (Obligatoire) Nom du profil d'instance IAM qui permet à Systems Manager de gérer l'instance.

- InstanceId

Type : chaîne

Description : (Obligatoire) L'instance EC2 exécutant Windows Server 2008 R2, 2012 R2, 2016 ou 2019.

- KeepPreUpgradeImageBackUp

Type : chaîne

Description : (Facultatif) Si ce paramètre est défini sur True, l'Automation ne supprime pas l'AMI créée à partir de l'instance EC2 avant la mise à niveau. S'il est défini sur True, vous devez supprimer l'AMI. Par défaut, l'AMI sera supprimée.

- SubnetId

Type : chaîne

Description : (Obligatoire) Il s'agit du sous-réseau pour le processus de mise à niveau et de l'emplacement de votre instance EC2 source. Vérifiez que le sous-réseau dispose d'une

connectivité sortante vers les AWS services, Amazon S3 et Microsoft (pour télécharger les correctifs).

- TargetWindowsVersion

Type : chaîne

Description : (Obligatoire) Sélectionnez la version cible de Windows.

Par défaut : 2022

- RebootInstanceBeforeTakingImage

Type : chaîne

Description : (Facultatif) Si ce paramètre est défini sur True, l'automatisation redémarre l'instance avant la création d'une l'AMI préalable à la mise à niveau. Par défaut, l'automatisation ne redémarre pas avant la mise à niveau.

## AWSEC2-ConfigureSTIG

Les guides de mise en œuvre technique de sécurité (STIG) sont des normes de renforcement de la configuration créées par la Defense Information Systems Agency (DISA) pour sécuriser les systèmes d'information et les logiciels. Pour rendre vos systèmes conformes aux normes STIG, vous devez installer, configurer et tester différents paramètres de sécurité.

Amazon EC2 fournit un runbook Systems ManagerAWSEC2-ConfigureSTIG, que vous pouvez utiliser pour appliquer les paramètres STIG à une instance. Ce document vous aide à créer rapidement des images conformes aux normes STIG. Le document STIG Systems Manager analyse les erreurs de configuration et exécute un script de correction. Il s'installe également InstallRoot depuis le ministère de la Défense (DoD) sur les AMI Windows pour installer et mettre à jour les certificats DoD et pour supprimer les certificats inutiles afin de garantir la conformité aux STIG. L'utilisation du document STIG Systems Manager est gratuite.

### Important

À quelques exceptions près, les composants de renforcement STIG que le document Systems Manager télécharge n'installent pas de packages tiers. Si des packages tiers sont déjà installés sur l'instance, et s'il existe des STIG connexes pris en charge par Amazon EC2 pour ce package, ces STIG sont appliqués.

Cette page répertorie tous les STIG pris en charge par Amazon EC2 et que les composants de renforcement STIG s'appliquent à votre instance EC2.

Vous pouvez choisir la catégorie de conformité STIG à appliquer.

### Niveaux de conformité

- Élevé (Catégorie I)

Risque le plus grave. Inclut toute vulnérabilité pouvant entraîner une perte de confidentialité, de disponibilité ou d'intégrité.

- Moyen (Catégorie II)

Inclut toute vulnérabilité susceptible d'entraîner une perte de confidentialité, de disponibilité ou d'intégrité, mais le risque peut être atténué.

- Faible (catégorie III)

Inclut toute vulnérabilité qui dégrade les mesures de protection contre la perte de confidentialité, de disponibilité ou d'intégrité.

### Rubriques

- [Téléchargements de composants de durcissement STIG](#)
- [Paramètres Windows STIG](#)
- [Historique des versions de Windows STIG](#)
- [Réglages STIG de Linux](#)
- [Historique des versions de Linux STIG](#)

## Téléchargements de composants de durcissement STIG

Amazon regroupe les composants de renforcement STIG dans des ensembles liés au système d'exploitation pour chaque version. Les ensembles sont des fichiers d'archive adaptés au système d'exploitation cible sur lequel ils sont téléchargés et exécutés. Les ensembles de composants Linux sont stockés sous forme de fichiers TAR (extension de fichier .tgz). Les ensembles de composants Windows sont stockés sous forme de fichiers ZIP (extension de fichier .zip).

Amazon stocke les ensembles de composants dans le compartiment Image Builder STIG S3 de chacun d'eux Région AWS. Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.

Les modèles et exemples de chemins de stockage des composants et de noms de fichiers de bundle sont les suivants :

Chemin de stockage des composants

`s3://aws-windows-downloads-<region>/STIG/<bundle file name>`

Variables de chemin des composants

region

Région AWS (Chaque région possède son propre compartiment de composants.)

bundle file name

Le format est `<os bundle name>_<YYYY>_Q<quarter>[_<release>].<file extension>`. Notez que le nom comporte des traits de soulignement entre les nœuds et non des points.

os bundle name

Le préfixe de nom standard du bundle de systèmes d'exploitation est `LinuxAWSConfigureSTIG` ou `AWSConfigureSTIG`. Pour garantir la rétrocompatibilité, le téléchargement pour Windows n'inclut pas de préfixe de plate-forme.

YYYY

Année à quatre chiffres de la sortie.

quarter

Identifie le trimestre de l'année : 1, 2, 3 ou 4.

release

Nombre incrémentiel qui commence à un et augmente d'un pour chaque nouvelle version. La version n'est pas incluse pour la première version d'un trimestre et n'est ajoutée que pour les versions suivantes.

file extension

Format de fichier compressé tgz (Linux) ou zip (Windows).

## Exemples de noms de fichiers groupés

- LinuxAWSConfigureSTIG\_2023\_Q1\_2.tgz
- AWSConfigureSTIG\_2022\_Q4.zip

## Paramètres Windows STIG

Les AMI Amazon EC2 Windows STIG et les composants de renforcement sont conçus pour les serveurs autonomes et appliquent une politique de groupe locale. Les composants conformes aux STIG sont installés InstallRoot depuis le ministère de la Défense (DoD) sur les AMI Windows pour télécharger, installer et mettre à jour les certificats DoD. Ils suppriment également les certificats inutiles pour maintenir la conformité aux STIG. Actuellement, Amazon EC2 prend en charge les lignes de base STIG pour les versions suivantes de Windows Server : 2012 R2, 2016, 2019 et 2022.

Cette section répertorie les paramètres STIG actuels pris en charge par Amazon EC2 pour votre infrastructure Windows, suivis d'un journal de l'historique des versions.

Vous pouvez appliquer des réglages STIG faibles, moyens ou élevés.

### Windows STIG Low (catégorie III)

La liste suivante contient les paramètres STIG qu'Amazon EC2 prend en charge pour votre infrastructure. Si un paramètre pris en charge n'est pas applicable à votre infrastructure, Amazon EC2 ignore ce paramètre et passe à autre chose. Par exemple, certains paramètres de renforcement STIG peuvent ne pas s'appliquer aux serveurs autonomes. Des politiques spécifiques de l'organisation peuvent également influencer les paramètres applicables, comme l'obligation pour les administrateurs de réviser les paramètres d'un document.

Pour obtenir la liste complète des paramètres STIG Windows, consultez la [Bibliothèque de documents STIG](#). Pour plus d'informations sur l'affichage de la liste complète, veuillez consulter la rubrique [Outils d'affichage STIG](#).

- Windows Server 2022 STIG version 1, version 1  
V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 et V-254481
- Windows Server 2019 STIG version 2 version 5  
V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 et V-205923
- Windows Server 2016 STIG version 2 version 5

V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 et V-225060

- Windows Server 2012 R2 MS STIG version 3 version 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 et V-225250

- Microsoft .NET Framework 4.0 STIG version 2, version 2

Aucun paramètre STIG ne s'applique au Microsoft .NET Framework pour les vulnérabilités de catégorie III.

- Pare-feu Windows STIG version 2, version 1

V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 et V-242008

- Internet Explorer 11 STIG version 2 version 3

V-46477, V-46629 et V-97527

- Microsoft Edge STIG version 1 version 6 (Windows Server 2022 uniquement)

V-235727, V-235731, V-235751, V-235752 et V-235765

## Windows STIG Medium (catégorie II)

La liste suivante contient les paramètres STIG qu'Amazon EC2 prend en charge pour votre infrastructure. Si un paramètre pris en charge n'est pas applicable à votre infrastructure, Amazon EC2 ignore ce paramètre et passe à autre chose. Par exemple, certains paramètres de renforcement STIG peuvent ne pas s'appliquer aux serveurs autonomes. Des politiques spécifiques de l'organisation peuvent également influencer les paramètres applicables, comme l'obligation pour les administrateurs de réviser les paramètres d'un document.

Pour obtenir la liste complète des paramètres STIG Windows, consultez la [Bibliothèque de documents STIG](#). Pour plus d'informations sur l'affichage de la liste complète, veuillez consulter la rubrique [Outils d'affichage STIG](#).

 Note

La catégorie Windows STIG Medium inclut tous les paramètres de renforcement STIG répertoriés qui s'appliquent à Windows STIG low (catégorie III), en plus des paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie II.

- Windows Server 2022 STIG version 1, version 1

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie III (faibles), ainsi que :

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-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-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254327, V-254328, V-254329, V-254330, V-254331, V-254332, V-254333, V-254334, V-254339, V-254341, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254358, V-254359, V-254360, V-254361, V-254364, V-254366, V-254367, V-254368, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254382, V-254383, V-254431, V-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-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-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 et V-254512

- Windows Server 2019 STIG version 2 version 5

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie III (faibles), ainsi que :

V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205636, V-205637, V-205638, V-205639, V-205643, V-205644, V-205648, V-205649, V-205650, V-205651, V-205652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205679, V-205680, V-205682, V-205683, V-205684, V-205685, V-205685, V-205686, V-205687, V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697,

V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205719, V-205716 5720, 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-205795, V-205796, V-205757 97, V-205798, V-205801, V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205826, V-205821 5827, V-205828, V-205830, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838, V-205839, V-205840, V-205841, V-205861, V-205863, V-205865, V-205866, 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 et V-236001

- Windows Server 2016 STIG version 2 version 5

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie III (faibles), ainsi que :

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-224882, V-224872 V-224883, V-224884, V-224885, 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-224902, V-224902, V-224898 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-224951, V-224947 52, 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-225022, V-225020 23, 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-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 et V-236000

- Windows Server 2012 R2 MS STIG version 3 version 5



Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie III (faibles), ainsi que :

V-225574, V-225573, V-225572, V-225571, V-225570, V-225569, V-225568, V-225567, V-225566, 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-225458, V-225457, V-225456, V-225455, V-225455, 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-225347, V-225346, V-225345, V-225344, V-225344, V-225344, V-225348 341, 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-225299, V-225298, V-225297, V-225296, V-225295, V-225294, V-225294, V-225298 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 et V-225259 239

- Microsoft .NET Framework STIG 4.0 version 2 version 2

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie III (faibles), ainsi que :

V-225238

- Pare-feu Windows STIG version 2, version 1

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie III (faibles), ainsi que :

V-241989, V-241990, V-241991, V-241993, V-241998 et V-242003

- Internet Explorer 11 STIG version 2 version 3

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie III (faibles), ainsi que :

V-46473, V-46475, V-46481, V-46483, V-46501, V-46507, V-46509, V-46511, V-46513, V-46515, V-46517, V-46521, V-46523, V-46525, V-46543, V-46545, V-46547, V-46549, V-46553, V-46555, V-46573, V-46575, V-46577, V-46579, V-46581, V-46583, V-46587, V-46589, V-46591, V-46593, V-46597, V-46599, V-46601, V-46603, V-46605, V-46607, V-46609, V-46615, V-46617, V-46619, V-46621, V-46625, V-46633, V-46635, V-46637, V-46639, V-46641, V-46643, V-46645, V-46647, V-46649, V-46653, V-46663, V-46665, V-46669, V-46681, V-46685, V-46689, V-46691, V-46693, V-46695, V-46701, V-46705, V-46709, V-46711, V-46713, V-46715, V-46717, V-46719, V-46721, V-46723, V-46725, V-46727, V-46729, V-46731, V-46733, V-46779, V-46781, V-46787, V-46789, V-46791, V-46797, V-46799, V-46801, V-46807, V-46811, V-46815, V-46819, V-46829, V-46841, V-46847, V-46849, V-46853, V-46857, V-46859, V-46861, V-46865, V-46869, V-46879, V-46883, V-46885, V-46889, V-46893, V-46895, V-46897, V-46903, V-46907, V-46921, V-46927, V-46939, V-46975, V-46981, V-46987, V-46995, V-46997, V-46999, V-47003, V-47005, V-47009, V-64711, V-64713, V-64715, V-64717, V-64719, V-64721, V-64723, V-64725, V-64729, V-72757, V-72759, V-72761, V-72763, V-75169 et V-75171

- Microsoft Edge STIG version 1 version 6 (Windows Server 2022 uniquement)

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 et V-246736

- Defender STIG version 2 version 4 (Windows Server 2022 uniquement)

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-213446, V-213447, V-213448, V-213448, V-213448, V-213448 V-213450, V-213451, V-213455, V-213464, V-213465 et V-213466

## Windows STIG High (catégorie I)

La liste suivante contient les paramètres STIG qu'Amazon EC2 prend en charge pour votre infrastructure. Si un paramètre pris en charge n'est pas applicable à votre infrastructure, Amazon EC2 ignore ce paramètre et passe à autre chose. Par exemple, certains paramètres de renforcement STIG peuvent ne pas s'appliquer aux serveurs autonomes. Des politiques spécifiques de l'organisation peuvent également influencer les paramètres applicables, comme l'obligation pour les administrateurs de réviser les paramètres d'un document.

Pour obtenir la liste complète des paramètres STIG Windows, consultez la [Bibliothèque de documents STIG](#). Pour plus d'informations sur l'affichage de la liste complète, veuillez consulter la rubrique [Outils d'affichage STIG](#).

### Note

La catégorie Windows STIG High inclut tous les paramètres de renforcement STIG répertoriés qui s'appliquent aux catégories Windows STIG Medium et Low, en plus des paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie I.

- Windows Server 2022 STIG version 1, version 1

V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475 et V-254500

- Windows Server 2019 STIG version 2 version 5

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles), ainsi que :

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 et V-205919

- Windows Server 2016 STIG version 2 version 5

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles), ainsi que :

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 et V-225079

- Windows Server 2012 R2 MS STIG version 3 version 5

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles), ainsi que :

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 et V-225274

- Microsoft .NET Framework STIG 4.0 version 2 version 2

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles) dans le Microsoft .NET Framework. Aucun paramètre STIG supplémentaire ne s'applique aux vulnérabilités de catégorie I.

- Pare-feu Windows STIG version 2, version 1

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles), ainsi que :

V-241992, V-241997 et V-242002

- Internet Explorer 11 STIG version 2 version 3

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles) dans Internet Explorer 11. Aucun paramètre STIG supplémentaire ne s'applique aux vulnérabilités de catégorie I.

- Microsoft Edge STIG version 1 version 6 (Windows Server 2022 uniquement)

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles), ainsi que :

V-235758 et V-235759

- Defender STIG version 2 version 4 (Windows Server 2022 uniquement)

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles), ainsi que :

V-213426, V-213452 et V-213453

## Historique des versions de Windows STIG

Cette section enregistre l'historique des versions des composants Windows pour les mises à jour trimestrielles de STIG. Pour voir les modifications et les versions publiées pendant un trimestre, choisissez le titre pour développer les informations.

Changements du premier trimestre 2024 - 23/02/2024 (aucun changement) :

Aucune modification n'a été apportée au composant Windows STIGS pour la version du premier trimestre 2024.

Changements du quatrième trimestre 2023 - 12/07/2023 (aucun changement) :

Aucune modification n'a été apportée au composant Windows STIGS pour la version du quatrième trimestre 2023.

Changements du troisième trimestre 2023 - 10/04/2023 (aucun changement) :

Aucune modification n'a été apportée au composant Windows STIGS pour la version du troisième trimestre 2023.

Changements du deuxième trimestre 2023 - 05/03/2023 (aucun changement) :

Aucune modification n'a été apportée au composant Windows STIGS pour la version du deuxième trimestre 2023.

Changements du premier trimestre 2023 - 27/03/2023 (aucun changement) :

Aucune modification n'a été apportée au composant Windows STIGS pour la version du premier trimestre 2023.

Changements du quatrième trimestre 2022 - 01/02/2023 :

Versions STIG mises à jour et STIGS appliquées pour la version du quatrième trimestre 2022 comme suit :

STIG-Build-Windows-Low version 2022.4.0

- Windows Server 2022 utilisant STIG version 1 sortie 1
- Windows Server 2019 utilisant STIG version 2 sortie 5
- Windows Server 2016 utilisant STIG version 2 sortie 5
- Windows Server 2012 R2 MS utilisant STIG version 3 sortie 5

- Microsoft .NET Framework 4.0 utilisant STIG version 2 sortie 2
- Pare-feu Windows utilisant STIG version 2 sortie 1
- Internet Explorer 11 utilisant STIG version 2 sortie 3
- Microsoft Edge STIG version 1 version 6 (Windows Server 2022 uniquement)

#### STIG-Build-Windows-Medium version 2022.4.0

- Windows Server 2022 utilisant STIG version 1 sortie 1
- Windows Server 2019 utilisant STIG version 2 sortie 5
- Windows Server 2016 utilisant STIG version 2 sortie 5
- Windows Server 2012 R2 MS utilisant STIG version 3 sortie 5
- Microsoft .NET Framework 4.0 utilisant STIG version 2 sortie 2
- Pare-feu Windows utilisant STIG version 2 sortie 1
- Internet Explorer 11 utilisant STIG version 2 sortie 3
- Microsoft Edge STIG version 1 version 6 (Windows Server 2022 uniquement)
- Defender STIG version 2 version 4 (Windows Server 2022 uniquement)

#### STIG-Build-Windows-HIGH version 2022.4.0

- Windows Server 2022 utilisant STIG version 1 sortie 1
- Windows Server 2019 utilisant STIG version 2 sortie 5
- Windows Server 2016 utilisant STIG version 2 sortie 5
- Windows Server 2012 R2 MS utilisant STIG version 3 sortie 5
- Microsoft .NET Framework 4.0 utilisant STIG version 2 sortie 2
- Pare-feu Windows utilisant STIG version 2 sortie 1
- Internet Explorer 11 utilisant STIG version 2 sortie 3
- Microsoft Edge STIG version 1 version 6 (Windows Server 2022 uniquement)
- Defender STIG version 2 version 4 (Windows Server 2022 uniquement)

Changements du troisième trimestre 2022 - 30/09/2022 (aucun changement) :

Aucune modification n'a été apportée au composant Windows STIGS pour la version du troisième trimestre 2022.

## Changements du deuxième trimestre 2022 - 08/02/2022 :

Versions STIG mises à jour et STIGS appliqués pour la version du deuxième trimestre 2022.

### STIG-Build-Windows-Low version 1.5.0

- Windows Server 2019 STIG version 2 version 4
- Windows Server 2016 STIG version 2 version 4
- Windows Server 2012 R2 MS STIG version 3 version 3
- Microsoft .NET Framework 4.0 STIG version 2 version 1
- Pare-feu Windows utilisant STIG version 2 sortie 1
- Internet Explorer 11 STIG version 1, version 19

### STIG-Build-Windows-Medium version 1.5.0

- Windows Server 2019 STIG version 2 version 4
- Windows Server 2016 STIG version 2 version 4
- Windows Server 2012 R2 MS STIG version 3 version 3
- Microsoft .NET Framework 4.0 STIG version 2 version 1
- Pare-feu Windows utilisant STIG version 2 sortie 1
- Internet Explorer 11 STIG version 1, version 19

### STIG-Build-Windows-High version 1.5.0

- Windows Server 2019 STIG version 2 version 4
- Windows Server 2016 STIG version 2 version 4
- Windows Server 2012 R2 MS STIG version 3 version 3
- Microsoft .NET Framework 4.0 STIG version 2 version 1
- Pare-feu Windows utilisant STIG version 2 sortie 1
- Internet Explorer 11 STIG version 1, version 19

## Changements du premier trimestre 2022 - 08/02/2022 (aucun changement) :

Aucune modification n'a été apportée au composant Windows STIGS pour la version du premier trimestre 2022.

## Changements du quatrième trimestre 2021 - 20/12/2021 :

Versions STIG mises à jour et STIGS appliquées pour la version du quatrième trimestre 2021.

### STIG-Build-Windows-Low version 1.5.0

- Windows Server 2019 STIG version 2 version 3
- Windows Server 2016 STIG version 2 version 3
- Windows Server 2012 R2 MS STIG version 3 version 3
- Microsoft .NET Framework 4.0 STIG version 2 version 1
- Pare-feu Windows utilisant STIG version 2 sortie 1
- Internet Explorer 11 STIG version 1, version 19

### STIG-Build-Windows-Medium version 1.5.0

- Windows Server 2019 STIG version 2 version 3
- Windows Server 2016 STIG version 2 version 3
- Windows Server 2012 R2 MS STIG version 3 version 3
- Microsoft .NET Framework 4.0 STIG version 2 version 1
- Pare-feu Windows utilisant STIG version 2 sortie 1
- Internet Explorer 11 STIG version 1, version 19

### STIG-Build-Windows-High version 1.5.0

- Windows Server 2019 STIG version 2 version 3
- Windows Server 2016 STIG version 2 version 3
- Windows Server 2012 R2 MS STIG version 3 version 3
- Microsoft .NET Framework 4.0 STIG version 2 version 1
- Pare-feu Windows utilisant STIG version 2 sortie 1
- Internet Explorer 11 STIG version 1, version 19

## Changements du troisième trimestre 2021 au 30/09/2021 :

Versions STIG mises à jour et STIGS appliquées pour la version du troisième trimestre 2021.



## STIG-Build-Windows-Low version 1.4.0

- Windows Server 2019 STIG version 2 version 2
- Windows Server 2016 STIG version 2 version 2
- Windows Server 2012 R2 MS STIG version 3 version 2
- Microsoft .NET Framework 4.0 STIG version 2 version 1
- Pare-feu Windows STIG version 1 version 7
- Internet Explorer 11 STIG version 1, version 19

## STIG-Build-Windows-Medium version 1.4.0

- Windows Server 2019 STIG version 2 version 2
- Windows Server 2016 STIG version 2 version 2
- Windows Server 2012 R2 MS STIG version 3 version 2
- Microsoft .NET Framework 4.0 STIG version 2 version 1
- Pare-feu Windows STIG version 1 version 7
- Internet Explorer 11 STIG version 1, version 19

## STIG-Build-Windows-High version 1.4.0

- Windows Server 2019 STIG version 2 version 2
- Windows Server 2016 STIG version 2 version 2
- Windows Server 2012 R2 MS STIG version 3 version 2
- Microsoft .NET Framework 4.0 STIG version 2 version 1
- Pare-feu Windows STIG version 1 version 7
- Internet Explorer 11 STIG version 1, version 19

## Réglages STIG de Linux

Cette section contient des informations sur les paramètres de renforcement de Linux STIG pris en charge par Amazon EC2, suivies d'un journal de l'historique des versions. Si la distribution Linux ne dispose pas de ses propres paramètres de renforcement STIG, Amazon EC2 utilise les paramètres RHEL. Les paramètres de renforcement STIG pris en charge s'appliquent aux AMI Linux Amazon EC2 et aux composants basés sur la distribution Linux, comme suit :

- Paramètres STIG de Red Hat Enterprise Linux (RHEL) 7
  - RHEL 7
  - CentOS 7
  - Amazon Linux 2 (AL2)
- Paramètres RHEL 8 STIG
  - RHEL 8
  - CentOS 8
  - Amazon Linux 2023 (AL 2023)

### Linux STIG Low (catégorie III)

La liste suivante contient les paramètres STIG qu'Amazon EC2 prend en charge pour votre infrastructure. Si un paramètre pris en charge n'est pas applicable à votre infrastructure, Amazon EC2 ignore ce paramètre et passe à autre chose. Par exemple, certains paramètres de renforcement STIG peuvent ne pas s'appliquer aux serveurs autonomes. Des politiques spécifiques de l'organisation peuvent également influencer les paramètres applicables, comme l'obligation pour les administrateurs de réviser les paramètres d'un document.

Pour obtenir une liste complète, veuillez consulter [STIGs Document Library](#). Pour plus d'informations sur l'affichage de la liste complète, veuillez consulter la rubrique [Outils d'affichage STIG](#).

### RHEL 7 STIG Version 3, version 14

- RHEL 7/CentOS 7  
V-204452, V-204576 et V-204605
- AL2  
V-204452, V-204576 et V-204605

### RHEL 8 STIG Version 1 Version 13

- RHEL 8/CentOS 8/AL 2023  
V-230241, V-244527, V-230269, V-230270, V-230285, V-230253, V-230346, V-230381, V-230395, V-230468, V-230469, V-230491, V-230485, V-230486, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499 et V-230281

## Ubuntu 18.04 STIG version 2, version 13

V-219172, V-219173, V-219174, V-219175, V-219210, V-219164, V-219165, V-219178, V-219180, V-219301, V-219163, V-219332, V-219327 et V-219333

## Ubuntu 20.04 STIG version 1 version 11

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 et V-238308

## Linux STIG Medium (catégorie II)

La liste suivante contient les paramètres STIG qu'Amazon EC2 prend en charge pour votre infrastructure. Si un paramètre pris en charge n'est pas applicable à votre infrastructure, Amazon EC2 ignore ce paramètre et passe à autre chose. Par exemple, certains paramètres de renforcement STIG peuvent ne pas s'appliquer aux serveurs autonomes. Des politiques spécifiques de l'organisation peuvent également influencer les paramètres applicables, comme l'obligation pour les administrateurs de réviser les paramètres d'un document.

Pour obtenir une liste complète, veuillez consulter [STIGs Document Library](#). Pour plus d'informations sur l'affichage de la liste complète, veuillez consulter la rubrique [Outils d'affichage STIG](#).

### Note

La catégorie Linux STIG Medium inclut tous les paramètres de renforcement STIG répertoriés qui s'appliquent à Linux STIG Low (catégorie III), en plus des paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie II.

## RHEL 7 STIG Version 3, version 14

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie III (faibles), ainsi que :

- RHEL 7/CentOS 7

V-204585, V-204490, V-204491, V-255928, V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204422, V-204423, V-204427, V-204416, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597,

V-204598, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204510, V-204511, V-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-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-204566, V-204567, V-204572, V-204584, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204450, V-204451, V-204619, V-2045, V-2045, V-204631, V-204633 et V-256970

- TOUS LES 2 :

V-204585, V-204490, V-204491, V-255928, V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204422, V-204423, V-204427, V-204416, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204510, V-204511, V-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-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-204566, V-204567, V-204572, V-204584, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204450, V-204451, V-204619, V-2045, V-2045, V-204631, V-204633 et V-256970

## RHEL 8 STIG Version 1 Version 13

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie III (faibles), ainsi que :

- RHEL 8/CentOS 8/AL 2023

V-230257, V-230258, V-230259, V-230550, V-230248, V-230249, V-230250, V-230245, V-230246, V-230247, V-230397, V-230399, V-230400, V-230401, V-230228, V-230298, V-230387, V-230231, V-230233, V-230324, V-230365, V-230370, V-230378, V-230383, V-230236, V-230314, V-230315, V-244523, V-230266, V-230267, V-230268, V-230280, V-230310, V-230311, V-230312, V-230502, V-230532, V-230535, V-230536, V-230538, V-230539, V-230540, V-230541, V-230542, V-230542,

V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230542, V-543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230549, V-244550, V-244551, V-244552, V-244553, V-244554, V-250317, V-251718, V-230237, V-230313, V-230356, V-230357, V-230358, V-230359, V-230360, V-230361, V-230362, V-230363, V-230368, V-230369, V-230375, V-230376, V-230377, V-244524, V-244533, V-251713, V-251717, V-251714, V-251715, V-251716, V-230332, V-230334, V-230336, V-230338, V-230340, V-230342, V-230344, V-230333, V-230335, V-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-230403, V-230404, V-230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, V-230418, V-230419, V-230421, V-230422, V-230423, V-230424, V-230425, V-230426, V-230427, V-230428, V-230429, V-230430, V-230431, V-230432, V-230433, V-230434, V-230435, V-230436, V-230437, V-230438, V-230439, V-230444, V-230446, V-230447, V-230448, V-230449, V-230455, V-230456, V-230462, V-230463, V-230465, V-230466, V-230467, V-230471, V-230472, V-230473, V-230474, V-230480, V-230483, V-244542, V-230503, V-230244, V-230286, V-230287, V-230288, V-230290, V-230291, V-230296, V-230330, V-230382, V-230526, V-230527, V-230555, V-230556, V-244526, V-244528, V-237642, V-237643, V-251711, V-230238, V-230239, V-230273, V-230275, V-230478, V-230488, V-230489, V-230559, V-230560, V-230560, V-230478 561, V-237640 et V-256974

#### Ubuntu 18.04 STIG version 2, version 13

V-219188, V-219190, V-219191, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219303, V-219326, V-219328, V-219330, V-219342, V-219189, V-219192, V-219193, V-219194, V-219315, V-219195, V-219196, V-219197, V-219213, V-219214, V-219215, V-219216, V-219217, V-219218, V-219220, V-219221, V-219222, V-219223, V-219224, 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-2194, 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-219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219297, V-219298, V-219299, V-219300, V-219309, V-219310, V-219311, V-219312, V-233779, V-233780, V-255906, V-219336, V-219338, V-219344, V-219181, V-219184, V-219186, V-219155, V-219156, V-219160, V-219306, V-219149, V-219166, V-219176, V-219339, V-219331, V-219337 et V-219335

#### Ubuntu 20.04 STIG version 1 version 11

V-238205, V-238207, V-238329, V-238337, V-238339, V-238340, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238350, V-238351, V-238352, V-238376, V-238377, V-238378, V-238209, V-238325, V-238330, V-238333, V-238369, V-238338, V-238341, V-238342, V-238343, V-238324, V-238353, V-238228, V-238225, V-238227, V-238299, V-238238, V-238240, V-238241, V-23824, V-23824, 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-238277772, 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-238211, V-238212, V-238213, V-238216, V-238220, V-255912, V-238355, V-238236, V-238303, V-238358, V-238356, V-238359, V-238370 et V-238334

### Linux STIG High (catégorie I)

La liste suivante contient les paramètres STIG qu'Amazon EC2 prend en charge pour votre infrastructure. Si un paramètre pris en charge n'est pas applicable à votre infrastructure, Amazon EC2 ignore ce paramètre et passe à autre chose. Par exemple, certains paramètres de renforcement STIG peuvent ne pas s'appliquer aux serveurs autonomes. Des politiques spécifiques de l'organisation peuvent également influencer les paramètres applicables, comme l'obligation pour les administrateurs de réviser les paramètres d'un document.

Pour obtenir une liste complète, veuillez consulter [STIGs Document Library](#). Pour plus d'informations sur l'affichage de la liste complète, veuillez consulter la rubrique [Outils d'affichage STIG](#).

#### Note

La catégorie Linux STIG High inclut tous les paramètres de renforcement STIG répertoriés qui s'appliquent aux catégories Linux STIG Medium et Low, en plus des paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégorie I.

### RHEL 7 STIG Version 3, version 14

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles), ainsi que :

- RHEL 7/CentOS 7

V-204425, V-204594, V-204455, V-204424, V-204442, V-204443, V-204447, V-204448, V-204502, V-204620 et V-204621

- TOUS LES 2 :

V-204425, V-204594, V-204455, V-204424, V-204442, V-204443, V-204447, V-204448, V-204502, V-204620 et V-204621

## RHEL 8 STIG Version 1 Version 13

Inclut tous les paramètres de renforcement STIG pris en charge par Amazon EC2 pour les vulnérabilités de catégories II et III (moyennes et faibles), ainsi que :

- RHEL 8/CentOS 8/AL 2023

V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533 et V-230558

## Ubuntu 18.04 STIG version 2, version 13

V-219157, V-219158, V-219177, V-219212 V-219308, V-219314, V-219316 et V-251507

## Ubuntu 20.04 STIG version 1 version 11

V-238218, V-238219, V-238201, V-238326, V-238327, V-238380 et V-251504

## Historique des versions de Linux STIG

Cette section enregistre l'historique des versions des composants Linux pour les mises à jour trimestrielles de STIG. Pour voir les modifications et les versions publiées pendant un trimestre, choisissez le titre pour développer les informations.

Changements du 1er trimestre 2024 - 02/06/2024 :

Versions STIG mises à jour et STIGS appliquées pour la version du premier trimestre 2024 comme suit :

### STIG-Build-Linux-Low version 2024.1.x

- RHEL 7 STIG Version 3, version 14
- RHEL 8 STIG Version 1 Version 13

- Ubuntu 18.04 STIG version 2, version 13
- Ubuntu 20.04 STIG version 1 version 11

#### STIG-Build-Linux-Medium version 2024.1.x

- RHEL 7 STIG Version 3, version 14
- RHEL 8 STIG Version 1 Version 13
- Ubuntu 18.04 STIG version 2, version 13
- Ubuntu 20.04 STIG version 1 version 11

#### STIG-Build-Linux-High version 2024.1.x

- RHEL 7 STIG Version 3, version 14
- RHEL 8 STIG Version 1 Version 13
- Ubuntu 18.04 STIG version 2, version 13
- Ubuntu 20.04 STIG version 1 version 11

Modifications apportées au quatrième trimestre 2023 - 07/12/2023 :

Versions STIG mises à jour et STIGS appliquées pour la version du quatrième trimestre 2023 comme suit :

#### Version 2023.4.x de STIG-Build-Linux-Low

- RHEL 7 STIG Version 3 Version 13
- RHEL 8 STIG Version 1 Version 12
- Ubuntu 18.04 STIG version 2 version 12
- Ubuntu 20.04 STIG version 1 version 10

#### STIG-Build-Linux-Medium version 2023.4.x

- RHEL 7 STIG Version 3 Version 13
- RHEL 8 STIG Version 1 Version 12
- Ubuntu 18.04 STIG version 2 version 12



- Ubuntu 20.04 STIG version 1 version 10

#### STIG-Build-Linux-High version 2023.4.x

- RHEL 7 STIG Version 3 Version 13
- RHEL 8 STIG Version 1 Version 12
- Ubuntu 18.04 STIG version 2 version 12
- Ubuntu 20.04 STIG version 1 version 10

#### Changements du troisième trimestre 2023 - 10/04/2023 :

Versions STIG mises à jour et STIGS appliquées pour la version du troisième trimestre 2023 comme suit :

#### Linux STIG Low (catégorie III)

- RHEL 7 STIG version 3 version 12
- RHEL 8 STIG Version 1 Version 11
- Ubuntu 18.04 STIG version 2 version 11
- Ubuntu 20.04 STIG version 1 version 9

#### Linux STIG Medium (catégorie II)

- RHEL 7 STIG version 3 version 12
- RHEL 8 STIG Version 1 Version 11
- Ubuntu 18.04 STIG version 2 version 11
- Ubuntu 20.04 STIG version 1 version 9

#### Linux STIG High (catégorie I)

- RHEL 7 STIG version 3 version 12
- RHEL 8 STIG Version 1 Version 11
- Ubuntu 18.04 STIG version 2 version 11
- Ubuntu 20.04 STIG version 1 version 9

## Changements du deuxième trimestre 2023 - 05/03/2023 :

Versions STIG mises à jour et STIGS appliquées pour la version du deuxième trimestre 2023 comme suit :

### Linux STIG Low (catégorie III)

- RHEL 7 STIG version 3 version 11
- RHEL 8 STIG Version 1 Version 10
- Ubuntu 18.04 STIG version 2 version 11
- Ubuntu 20.04 STIG version 1 version 8

### Linux STIG Medium (catégorie II)

- RHEL 7 STIG version 3 version 11
- RHEL 8 STIG Version 1 Version 10
- Ubuntu 18.04 STIG version 2 version 11
- Ubuntu 20.04 STIG version 1 version 8

### Linux STIG High (catégorie I)

- RHEL 7 STIG version 3 version 11
- RHEL 8 STIG Version 1 Version 10
- Ubuntu 18.04 STIG version 2 version 11
- Ubuntu 20.04 STIG version 1 version 8

## Changements du premier trimestre 2023 - 27/03/2023 :

Versions STIG mises à jour et STIGS appliquées pour la version du premier trimestre 2023 comme suit :

### Linux STIG Low (catégorie III)

- RHEL 7 STIG version 3 version 10
- RHEL 8 STIG Version 1 Version 9
- Ubuntu 18.04 STIG version 2 version 10

- Ubuntu 20.04 STIG version 1 version 7

#### Linux STIG Medium (catégorie II)

- RHEL 7 STIG version 3 version 10
- RHEL 8 STIG Version 1 Version 9
- Ubuntu 18.04 STIG version 2 version 10
- Ubuntu 20.04 STIG version 1 version 7

#### Linux STIG High (catégorie I)

- RHEL 7 STIG version 3 version 10
- RHEL 8 STIG Version 1 Version 9
- Ubuntu 18.04 STIG version 2 version 10
- Ubuntu 20.04 STIG version 1 version 7

Changements du quatrième trimestre 2022 - 01/02/2023 :

Versions STIG mises à jour et STIGS appliquées pour la version du quatrième trimestre 2022 comme suit :

#### Linux STIG Low (catégorie III)

- RHEL 7 STIG version 3, version 9
- RHEL 8 STIG Version 1 Version 8
- Ubuntu 18.04 STIG version 2 version 9
- Ubuntu 20.04 STIG version 1 version 6

#### Linux STIG Medium (catégorie II)

- RHEL 7 STIG version 3, version 9
- RHEL 8 STIG Version 1 Version 8
- Ubuntu 18.04 STIG version 2 version 9
- Ubuntu 20.04 STIG version 1 version 6

## Linux STIG High (catégorie I)

- RHEL 7 STIG version 3, version 9
- RHEL 8 STIG Version 1 Version 8
- Ubuntu 18.04 STIG version 2 version 9
- Ubuntu 20.04 STIG version 1 version 6

Changements du troisième trimestre 2022 - 30/09/2022 (aucun changement) :

Aucune modification n'a été apportée au composant Linux STIGS pour la version du troisième trimestre 2022.

Changements du deuxième trimestre 2022 - 08/02/2022 :

Nous avons introduit le support d'Ubuntu, mis à jour les versions de STIG et appliqué les STIGS pour la version du deuxième trimestre 2022 comme suit :

## Linux STIG Low (catégorie III)

- RHEL 7 STIG Version 3 Version 7
- RHEL 8 STIG Version 1 Version 6
- Ubuntu 18.04 STIG version 2, version 6 (nouveau)
- Ubuntu 20.04 STIG version 1, version 4 (nouveau)

## Linux STIG Medium (catégorie II)

- RHEL 7 STIG Version 3 Version 7
- RHEL 8 STIG Version 1 Version 6
- Ubuntu 18.04 STIG version 2, version 6 (nouveau)
- Ubuntu 20.04 STIG version 1, version 4 (nouveau)

## Linux STIG High (catégorie I)

- RHEL 7 STIG Version 3 Version 7
- RHEL 8 STIG Version 1 Version 6

- Ubuntu 18.04 STIG version 2, version 6 (nouveau)
- Ubuntu 20.04 STIG version 1, version 4 (nouveau)

Changements du premier trimestre 2022 - 26/04/2022 :

Refactorisé pour inclure un meilleur support pour les conteneurs. Combinaison du script AL2 précédent avec RHEL 7. Versions STIG mises à jour et STIGS appliquées pour la version du premier trimestre 2022 comme suit :

Linux STIG Low (catégorie III)

- RHEL 7 STIG Version 3 Version 6
- RHEL 8 STIG Version 1 Version 5

Linux STIG Medium (catégorie II)

- RHEL 7 STIG Version 3 Version 6
- RHEL 8 STIG Version 1 Version 5

Linux STIG High (catégorie I)

- RHEL 7 STIG Version 3 Version 6
- RHEL 8 STIG Version 1 Version 5

Changements du quatrième trimestre 2021 - 20/12/2021 :

Versions STIG mises à jour et STIGS appliquées pour la version du quatrième trimestre 2021 comme suit :

Linux STIG Low (catégorie III)

- RHEL 7 STIG version 3 version 5
- RHEL 8 STIG Version 1 Version 4

Linux STIG Medium (catégorie II)

- RHEL 7 STIG version 3 version 5

- RHEL 8 STIG Version 1 Version 4

#### Linux STIG High (catégorie I)

- RHEL 7 STIG version 3 version 5
- RHEL 8 STIG Version 1 Version 4

Changements du troisième trimestre 2021 au 30/09/2021 :

Versions STIG mises à jour et STIGS appliqués pour la version du troisième trimestre 2021 comme suit :

#### Linux STIG Low (catégorie III)

- RHEL 7 STIG version 3 version 4
- RHEL 8 STIG Version 1 Version 3

#### Linux STIG Medium (catégorie II)

- RHEL 7 STIG version 3 version 4
- RHEL 8 STIG Version 1 Version 3

#### Linux STIG High (catégorie I)

- RHEL 7 STIG version 3 version 4
- RHEL 8 STIG Version 1 Version 3

## **AWSEC2-PatchLoadBalancerInstance**

### Description

Mettez à niveau et corrigez une version mineure d'une instance Amazon EC2 (Windows ou Linux) connectée à n'importe quel équilibreur de charge (classique, ALB ou NLB). Le temps de vidange de connexion par défaut est appliqué avant que l'instance ne soit corrigée. Vous pouvez annuler le temps d'attente en saisissant votre temps de vidange personnalisé en minutes (1-59) pour le `ConnectionDrainTime` paramètre.

Le flux de travail d'automatisation est le suivant :

1. L'équilibreur de charge ou le groupe cible auquel l'instance est attachée est déterminé, et l'instance est vérifiée comme saine.
2. L'instance est supprimée de l'équilibreur de charge ou du groupe cible.
3. L'automatisation attend pendant la période spécifiée pour le temps de vidange de la connexion.
4. L'RunPatchBaselineautomatisation [AWS est](#) appelée pour appliquer un correctif à l'instance.
5. L'instance est rattachée à l'équilibreur de charge ou au groupe cible.

[Exécutez cette automatisation \(console\)](#)

Types de document

Automatisation

Propriétaire

Amazon

Prérequis

- Vérifier que SSM Agent est installé sur votre instance. Pour plus d'informations, consultez la section [Utilisation de l'agent SSM sur des instances EC2 pour Windows Server](#).

Paramètres

- InstanceId

Type : String

Description : ID (obligatoire) de l'instance à patcher associée à un équilibreur de charge (classique, ALB ou NLB).

- ConnectionDrainTime

Type : String

Description : (Facultatif) Durée d'expiration de la connexion de l'équilibreur de charge, en minutes (1-59).

# AWSEC2-SQLServerDBRestore

## Description

Le AWSEC2-SQLServerDBRestore runbook restaure les sauvegardes de bases de données Microsoft SQL Server stockées dans Amazon S3 vers SQL Server 2017 s'exécutant sur une instance Linux Amazon Elastic Compute Cloud (EC2). Vous pouvez fournir votre propre instance EC2 exécutant SQL Server 2017 Linux. Si aucune instance EC2 n'est fournie, l'automatisation lance et configure une nouvelle instance EC2 Ubuntu 16.04 avec SQL Server 2017. L'automatisation prend en charge la restauration des sauvegardes de journaux complètes, différentielles et transactionnelles. Cette instance d'Automatisation accepte plusieurs fichiers de sauvegarde de base de données et restaure automatiquement la dernière sauvegarde de chaque base de données valides dans les fichiers fournis.

Pour automatiser à la fois la sauvegarde et la restauration d'une base de données SQL Server locale sur une instance EC2 exécutant SQL Server 2017 Linux, vous pouvez utiliser le script AWS PowerShell -signed. [MigrateSQLServerToEC2Linux](#)

### Important

Ce runbook réinitialise le mot de passe utilisateur de l'administrateur (SA) du serveur SQL Server à chaque exécution de l'automatisation. Une fois l'automatisation terminée, vous devez redéfinir votre propre mot de passe utilisateur SA avant de vous connecter à l'instance SQL Server.

[Exécutez cette automatisation \(console\)](#)

Types de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux



## Prérequis

Pour exécuter cette automatisation, vous devez remplir les conditions préalables suivantes :

- L'utilisateur ou le rôle IAM qui exécute cette automatisation doit disposer d'une politique intégrée associée aux autorisations décrites dans [Autorisations IAM requises](#)
- Si vous fournissez votre propre instance EC2 :
  - L'instance EC2 que vous fournissez doit être une instance Linux exécutant Microsoft SQL Server 2017.
  - L'instance EC2 que vous fournissez doit être configurée avec un profil d'instance AWS Identity and Access Management (IAM) auquel est associée la politique AmazonSSMManagedInstanceCore gérée. Pour de plus amples informations, veuillez consulter [Créer un profil d'instance IAM pour Systems Manager](#).
  - L'agent SSM doit être installé sur votre instance EC2. Pour plus d'informations, consultez [Installation et configuration de l'agent SSM sur des instances EC2 pour Linux](#).
  - L'instance EC2 doit disposer de suffisamment d'espace disque disponible pour télécharger et restaurer les sauvegardes SQL Server.

## Limites

Cette instance d'Automation ne prend pas en charge la restauration vers SQL Server s'exécutant sur des instances EC2 pour Windows Server. Cette instance d'Automation ne restaure les sauvegardes de base de données qui sont compatibles avec SQL Server Linux 2017. Pour de plus amples informations, veuillez consulter [Fonctionnalités et éditions de SQL Server 2017 prises en charge sur Linux](#).

## Paramètres

Cette automatisation possède les paramètres suivants :

- DatabaseNames

Type : String

Description : (Facultatif) liste séparée par des virgules des noms des bases de données à restaurer.

- DataDirectorySize

Type : String

Description : (Facultatif) taille de volume (Gio) souhaitée du répertoire de données SQL Server pour la nouvelle instance EC2.

Valeur par défaut : 100

- KeyPair

Type : String

Description : (Facultatif) paire de clés à utiliser lors de la création de la nouvelle instance EC2.

- iamInstanceProfileName

Type : String

Description : (Facultatif) Le profil d'instance IAM à associer à la nouvelle instance EC2. La politique AmazonSSMManagedInstanceCore gérée doit être associée au profil d'instance IAM.

- InstanceId

Type : String

Description : (Facultatif) instance exécutant SQL Server 2017 sur Linux. Si la valeur non n'InstanceId est pas fournie, l'automatisation lance une nouvelle instance EC2 à l'aide du InstanceType et du SQL ServerEdition fournis.

- InstanceType

Type : String

Description : (Facultatif) type d'instance de l'instance EC2 à lancer.

- iSS3 PresignedUrl

Type : String

Description : (Facultatif) Si S3Input est une URL S3 pré-signée, indiquez-la. yes

Valeur par défaut : non

Valeurs valides : oui | non

- LogDirectorySize

Type : String

Description : (Facultatif) taille de volume (Gio) souhaitée du répertoire de journaux SQL Server pour la nouvelle instance EC2.

Valeur par défaut : 100

- Entrée S3

Type : String

Description : (Obligatoire) nom du compartiment S3, liste séparée par des virgules des clés d'objet S3, ou liste séparée par des virgules des URL S3 pré-signées contenant les fichiers de sauvegarde SQL à restaurer.

- SQL ServerEdition

Type : String

Description : (Facultatif) édition de SQL Server 2017 à installer sur l'instance EC2 qui vient d'être créée.

Valeurs valides : Standard | Enterprise | Web | Express

- SubnetId

Type : String

Description : (Facultatif) sous-réseau dans lequel lancer la nouvelle instance EC2. Le sous-réseau doit disposer d'une connectivité sortante aux services AWS. Si aucune valeur pour n'SubnetId est fournie, l'automatisation utilise le sous-réseau par défaut.

- TempDbDirectorySize

Type : String

Description : (Facultatif) taille de volume (Gio) souhaitée du répertoire TempDB SQL Server pour la nouvelle instance EC2.

Valeur par défaut : 100

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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"
    }
  ]
}
```

### Étapes de document

Pour utiliser cette automatisation, suivez les étapes qui s'appliquent à votre type d'instance :

Pour les nouvelles instances EC2 :

1. `aws:executeAwsApi`- Récupérez l'ID AMI pour SQL Server 2017 sur Ubuntu 16.04.
2. `aws:runInstances`- Lancez une nouvelle instance EC2 pour Linux.

3. `aws:waitForAwsResourceProperty`- Attendez que l'instance EC2 nouvellement créée soit prête.
4. `aws:executeAwsApi`- Redémarrez l'instance si elle n'est pas prête.
5. `aws:assertAwsResourceProperty`- Vérifiez que l'agent SSM est installé.
6. `aws:runCommand`- Exécutez le script de restauration de SQL Server dans PowerShell.

Pour les instances EC2 existantes :

1. `aws:waitForAwsResourceProperty`- Vérifiez que l'instance EC2 est prête.
2. `aws:executeAwsApi`- Redémarrez l'instance si elle n'est pas prête.
3. `aws:assertAwsResourceProperty`- Vérifiez que l'agent SSM est installé.
4. `aws:runCommand`- Exécutez le script de restauration de SQL Server dans PowerShell.

Sorties

`GetInstance.InstanceId`

`restoreToNewInstance.Sortie`

`restoreToExistingInstance.Sortie`

## **AWSSupport-ActivateWindowsWithAmazonLicense**

Description

Le `AWSSupport-ActivateWindowsWithAmazonLicense` runbook active une instance Amazon Elastic Compute Cloud (Amazon EC2) pour laquelle une licence est fournie Windows Server par Amazon. L'automatisation vérifie et configure les paramètres requis du système d'exploitation du service de gestion des clés et tente l'activation. Cela inclut les itinéraires du système d'exploitation vers les serveurs de gestion des clés d'Amazon et les paramètres du système d'exploitation du service de gestion des clés. La définition du paramètre `AllowOffline` sur `true` permet à l'automatisation de cibler avec succès les instances qui ne sont pas gérées par AWS Systems Manager, mais nécessite un arrêt et un démarrage de l'instance.

**Note**

Ce runbook ne peut pas être utilisé sur les instances du modèle Windows Server Bring Your Own License (BYOL). Pour plus d'informations sur l'utilisation de votre propre licence, consultez [Licences Microsoft sur AWS](#).

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Windows

Paramètres

- AllowOffline

Type : String

Valeurs valides : true | false

Par défaut : faux

Description : (Facultatif) Définissez-la sur `true` si vous autorisez une correction d'activation de Windows hors ligne en cas d'échec du dépannage en ligne ou si l'instance fournie n'est pas une instance gérée.

**Important**

Le mode hors connexion nécessite l'arrêt, puis le redémarrage de l'instance EC2. Les données stockées sur les volumes de stockage d'instance seront perdues. L'adresse IP publique change si vous n'utilisez pas une adresse IP Elastic.

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- ForceActivation

Type : String

Valeurs valides : true | false

Par défaut : faux

Description : (Facultatif) Réglez-la sur `true` si vous souhaitez continuer même si Windows est déjà activé.

- InstanceId

Type : String

Description : (obligatoire) ID de votre instance EC2 gérée pour Windows Server.

- SubnetId

Type : String

Par défaut : CreateNew VPC

Description : (Facultatif et hors connexion uniquement) ID de sous-réseau de l'instance EC2Rescue utilisé pour réaliser le dépannage hors connexion.

`SelectedInstanceSubnet` Utilisez-le pour utiliser le même sous-réseau que votre instance ou `CreateNewVPC` pour créer un nouveau VPC. IMPORTANT : Le sous-réseau doit se trouver dans la même zone de disponibilité que `InstanceId` les points de terminaison SSM et autoriser l'accès à ces derniers.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Nous recommandons que l'instance EC2 recevant la commande dispose d'un rôle IAM auquel est associée la politique gérée par ManagedInstanceCore Amazon d'AmazonSSM. Vous devez avoir au moins `ssm : StartAutomationExecution` et `ssm : SendCommand` pour exécuter l'automatisation et envoyer la commande à l'instance, plus `ssm : GetAutomationExecution` pour pouvoir lire la sortie de l'automatisation. Pour la correction hors ligne, consultez les autorisations requises par `AWSSupport-StartEC2RescueWorkflow`.

## Étapes de document

1. `aws:assertAwsResourceProperty`- Vérifiez que la plate-forme de l'instance fournie est Windows.
2. `aws:assertAwsResourceProperty`- Vérifiez que l'instance fournie est une instance gérée :
  - a. (Correctif d'activation en ligne) Si l'instance d'entrée est une instance gérée, exécutez `aws:runCommand` le PowerShell script afin de tenter de corriger l'activation de Windows.
  - b. (Correctif d'activation hors connexion) Si l'instance d'entrée n'est pas une instance gérée :
    - i. `aws:assertAwsResourceProperty`- Vérifie que le `AllowOffline` drapeau est réglé sur `true` Si tel est le cas, le correctif hors ligne démarre ; sinon, l'automatisation prend fin.
    - ii. `aws:executeAutomation`- Appelez à l'`AWSSupport-StartEC2RescueWorkflow` aide du script de correction hors ligne pour l'activation de Windows. Le script utilise `EC2Config` ou `EC2Launch`, selon la version du système d'exploitation.
    - iii. `aws:executeAwsApi`- Lisez le résultat à partir de `AWSSupport-StartEC2RescueWorkflow`.

## Sorties

`activateWindows.Output`

`getActivateWindowsOfflineResult`. Sortie

## **AWSSupport - AnalyzeAWSEndpointReachabilityFromEC2**

### Description

Le `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook analyse la connectivité entre une instance Amazon Elastic Compute Cloud (Amazon EC2) ou une interface Elastic Network Interface et un point de terminaison. Service AWS IPv6 n'est pas pris en charge. Le runbook utilise la valeur que vous spécifiez pour le `ServiceEndpoint` paramètre afin d'analyser la connectivité à un point de terminaison. Si aucun point de AWS PrivateLink terminaison n'est trouvé dans votre VPC,



le runbook utilise une adresse IP publique pour le service actuel. Région AWS Cette automatisation utilise Reachability Analyzer d'Amazon Virtual Private Cloud. Pour plus d'informations, voir [Qu'est-ce que Reachability Analyzer ?](#), dans Reachability Analyzer.

Cette automatisation vérifie les points suivants :

- Vérifie si votre cloud privé virtuel (VPC) est configuré pour utiliser le serveur DNS fourni par Amazon.
- Vérifie si un AWS PrivateLink point de terminaison existe dans le VPC pour Service AWS celui que vous spécifiez. Si un point de terminaison est détecté, l'automatisation vérifie que l'`privateDnsattribut` est activé.
- Vérifie si le AWS PrivateLink point de terminaison utilise la politique de point de terminaison par défaut.

### Considérations

- Vous êtes facturé par analyse effectuée entre une source et une destination. Pour de plus amples informations, veuillez consulter la [Tarification Amazon VPC](#).
- Au cours de l'automatisation, un chemin d'analyse du réseau et une analyse des informations du réseau sont créés. Si l'automatisation aboutit, le runbook supprime ces ressources. Si l'étape de nettoyage échoue, le chemin Network Insights n'est pas supprimé par le runbook et vous devrez le supprimer manuellement. Si vous ne supprimez pas le chemin d'accès aux informations sur le réseau manuellement, il continue à être pris en compte dans le quota de votre Compte AWS. Pour plus d'informations sur les quotas pour Reachability Analyzer, voir Quotas [pour Reachability Analyzer dans Reachability Analyzer](#).
- Les configurations au niveau du système d'exploitation, telles que l'utilisation d'un proxy, d'un résolveur DNS local ou d'un fichier d'hôtes, peuvent affecter la connectivité même si l'Analyzer de Reachability revient. PASS
- Passez en revue l'évaluation de tous les contrôles effectués par l'Analyzer de Reachability. Si l'un des contrôles renvoie un état deFAIL, cela peut affecter la connectivité même si le contrôle d'accessibilité global renvoie un statut de. PASS

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Source

Type : chaîne

Description : (Obligatoire) L'ID de l'instance Amazon EC2 ou de l'interface réseau à partir de laquelle vous souhaitez analyser l'accessibilité.

- ServiceEndpoint

Type : chaîne

Description : (Obligatoire) Le nom d'hôte du point de terminaison du service auquel vous souhaitez analyser l'accessibilité.

- RetainVpcReachabilityAnalysis

Type : chaîne

Valeur par défaut : false

Description : (Facultatif) Détermine si le chemin d'aperçu du réseau et l'analyse associée créés sont conservés. Par défaut, les ressources utilisées pour analyser l'accessibilité sont supprimées après une analyse réussie. Si vous choisissez de conserver l'analyse, le runbook ne la supprime pas et vous pouvez la visualiser dans la console Amazon VPC. Un lien vers la console est disponible dans la sortie d'automatisation.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

1. `aws:executeScript`: valide le point de terminaison du service en essayant de résoudre le nom d'hôte.
2. `aws:executeScript`: rassemble des informations sur le VPC et le sous-réseau.
3. `aws:executeScript`: Évalue la configuration DNS du VPC.
4. `aws:executeScript`: Évalue les vérifications des points de terminaison du VPC.
5. `aws:executeScript`: localise une passerelle Internet pour se connecter au point de terminaison du service public.

6. `aws:executeScript`: Détermine la destination à utiliser pour l'analyse d'accessibilité.
7. `aws:executeScript`: analyse l'accessibilité de la source au point de terminaison à l'aide de Reachability Analyzer et nettoie les ressources en cas de réussite de l'analyse.
8. `aws:executeScript`: Génère un rapport d'évaluation de l'accessibilité.
9. `aws:executeScript`: Génère la sortie au format JSON.

## Sorties

- `generateReport.EvalReport`- Les résultats des contrôles effectués par l'automatisation au format texte.
- `generateJsonOutput.Output`- Une version minimale des résultats au format JSON.

## AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

### Description

Le `AWSPremiumSupport-ChangeInstanceTypeIntelToAMD` runbook automatise les migrations depuis les instances Amazon Elastic Compute Cloud (Amazon EC2) alimentées par Intel vers les types d'instances AMD équivalents. Ce runbook prend en charge les instances à usage général (M), polyvalentes (T), optimisées pour le calcul (C) et optimisées pour la mémoire (R) créées sur le système Nitro. Ce runbook peut être utilisé sur des instances qui ne sont pas gérées par Systems Manager.

Pour réduire le risque potentiel de perte de données et d'indisponibilité, le runbook vérifie le comportement d'arrêt de l'instance, vérifie si l'instance fait partie d'un groupe Amazon EC2 Auto Scaling, son état de santé et vérifie qu'un type d'instance AMD équivalent est disponible dans la même zone de disponibilité. Par défaut, ce runbook ne changera pas le type d'instance si des volumes de stockage d'instance sont attachés ou si l'instance fait partie d'une AWS CloudFormation pile. Si vous souhaitez modifier ce comportement, spécifiez `yes` l'un des `AllowCloudFormationInstances` paramètres `AllowInstanceStoreInstances` et.

### Important

L'accès aux `AWSPremiumSupport-*` runbooks nécessite un abonnement Enterprise ou Business Support. Pour plus d'informations, consultez la section [Comparer AWS Support les plans](#).

## Considérations

- Nous vous recommandons de sauvegarder votre instance avant d'utiliser ce runbook.
- Pour modifier le type d'instance, le runbook doit arrêter votre instance. Lorsqu'une instance est arrêtée, toutes les données stockées dans la RAM ou dans les volumes de stockage d'instance sont perdues et l'adresse IPv4 publique automatique est libérée. Pour plus d'informations, consultez [Arrêt et démarrage de votre instance](#).
- Si vous ne spécifiez pas de valeur pour le TargetInstanceType paramètre, le runbook tente d'identifier l'instance AMD équivalente en termes de processeurs virtuels et de mémoire au sein de la même famille d'instances. Le runbook s'arrête s'il n'est pas en mesure d'identifier un type d'instance AMD équivalent.
- En utilisant DryRun cette option, vous pouvez capturer le type d'instance AMD équivalent et valider les exigences sans réellement modifier le type d'instance.

### [Exécutez cette automatisation \(console\)](#)

#### Type de document

Automatisation

#### Propriétaire

Amazon

#### Plateformes

LinuxmacOS, Windows

#### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- Reconnaître

Type : String

Description : (Obligatoire) Entrez `yes` pour confirmer que votre instance cible sera arrêtée si elle est en cours d'exécution.

- `InstanceId`

Type : String

Description : (Obligatoire) L'ID de l'instance Amazon EC2 dont vous souhaitez modifier le type.

- `TargetInstanceType`

Type : String

Par défaut : automatique

Description : (Facultatif) Le type d'instance AMD vers lequel vous souhaitez modifier votre instance. La valeur `automatic` par défaut utilise le type d'instance équivalent en termes de processeurs virtuels et de mémoire. Par exemple, un fichier `m5.large` serait remplacé par un fichier `m5a.large`.

- `AllowInstanceStoreInstances`

Type : String

Valeurs valides : `non` | `oui`

Par défaut : `non`

Description : (Facultatif) Si vous le spécifiez `yes`, le runbook s'exécute sur les instances auxquelles des volumes de stockage d'instance sont attachés.

- `AllowCloudFormationInstances`

Type : String

Valeurs valides : `non` | `oui`

Par défaut : `non`

Description : (Facultatif) Si ce paramètre est défini sur `yes`, le runbook s'exécute sur les instances faisant partie d'une AWS CloudFormation pile.

- AllowCrossGeneration

Type : String

Valeurs valides : non | oui

Par défaut : non

Description : (Facultatif) Si ce paramètre est défini sur yes, le runbook tente de trouver le type d'instance AMD équivalent le plus récent au sein de la même famille d'instances.

- DryRun

Type : String

Valeurs valides : non | oui

Par défaut : non

Description : (Facultatif) Si ce paramètre est défini sur yes, le runbook renvoie le type d'instance AMD équivalent et valide les exigences de migration sans modifier le type d'instance.

- SleepWait

Type : String

Par défaut : PT3S

Description : (Facultatif) Durée pendant laquelle le runbook doit attendre avant de démarrer une nouvelle automatisation. La valeur que vous fournissez pour ce paramètre doit correspondre à la norme ISO 8601. Pour plus d'informations sur la création de chaînes ISO 8601, voir [Formatage des chaînes de date et d'heure pour Systems Manager](#).

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

1. `aws:assertAwsResourceProperty`: confirme que l'état de l'instance Amazon EC2 cible est `running`, `pendingstopped`, ou `stopping`. Dans le cas contraire, l'automatisation prend fin.
2. `aws:executeAwsApi`: rassemble les propriétés de l'instance Amazon EC2 cible.
3. `aws:branch`: Branche l'automatisation en fonction de l'état de l'instance Amazon EC2.
  - a. Si tel `stopped` est le cas `stopping`, l'automatisation s'exécute `aws:waitForAwsResourceProperty` jusqu'à l'arrêt complet de l'instance Amazon EC2.
  - b. Si tel `running` est le cas `pending`, l'automatisation s'exécute `aws:waitForAwsResourceProperty` jusqu'à ce que l'instance Amazon EC2 passe les contrôles de statut.
4. `aws:assertAwsResourceProperty`: confirme que l'instance Amazon EC2 ne fait pas partie d'un groupe Auto Scaling en vérifiant si la `aws:autoscaling:groupName` balise est appliquée.
5. `aws:executeAwsApi`: rassemble les propriétés du type d'instance actuel pour trouver le type d'instance AMD équivalent.
6. `aws:assertAwsResourceProperty`: confirme qu'AWS Marketplace aucun code produit n'est associé à l'instance Amazon EC2. Certains produits ne sont pas disponibles sur tous les types d'instances.
7. `aws:branch`: Branche l'automatisation selon que vous souhaitez que l'automatisation vérifie si l'instance Amazon EC2 fait partie d'une pile AWS CloudFormation
  - a. Si la `aws:cloudformation:stack-name` balise est appliquée à l'instance, l'automatisation s'exécute `aws:assertAwsResourceProperty` pour confirmer que l'instance ne fait pas partie d'une AWS CloudFormation pile.

8. `aws:branch`: Branche l'automatisation selon que le type de volume racine de l'instance est Amazon Elastic Block Store (Amazon EBS).
9. `aws:assertAwsResourceProperty`: confirme que le comportement d'arrêt de l'instance est `stop` ou `nonterminate`.
10. `aws:executeScript`: confirme qu'il n'existe qu'une seule automatisation de ce runbook ciblant l'instance actuelle. Si une autre automatisation est déjà en cours et cible la même instance, elle renvoie une erreur et se termine.
11. `aws:executeAwsApi`: Renvoie la liste des types d'instances AMD dotés de la même quantité de mémoire et de processeurs virtuels.
12. `aws:executeScript`: vérifie si le type d'instance actuel est pris en charge et renvoie son type d'instance AMD équivalent. S'il n'y a pas d'équivalent, l'automatisation prend fin.
13. `aws:executeScript`: confirme que le type d'instance AMD est disponible dans la même zone de disponibilité et vérifie les autorisations IAM fournies.
14. `aws:branch`: Branche l'automatisation selon que la valeur du `DryRun` paramètre est ou non `yes`.
15. `aws:branch`: vérifie si le type d'instance d'origine et le type d'instance cible sont identiques. S'ils sont identiques, l'automatisation prend fin.
16. `aws:executeAwsApi`: obtient l'état actuel de l'instance.
17. `aws:changeInstanceState`: arrête l'instance Amazon EC2.
18. `aws:changeInstanceState`: force l'instance à s'arrêter si elle est bloquée à l'état d'arrêt.
19. `aws:executeAwsApi`: remplace le type d'instance par le type d'instance AMD cible.
20. `aws:sleep`: attend 3 secondes après avoir modifié le type d'instance pour une éventuelle cohérence.
21. `aws:branch`: Branche l'automatisation en fonction de l'état précédent de l'instance. Si tel est le cas `running`, l'instance est démarrée.
  - a. `aws:changeInstanceState`: démarre l'instance Amazon EC2 si elle était en cours d'exécution avant de modifier le type d'instance.
  - b. `aws:waitForAwsResourceProperty`: attend que l'instance Amazon EC2 passe les contrôles de statut. Si l'instance ne passe pas les contrôles d'état, elle revient à son type d'instance d'origine.
    - i. `aws:changeInstanceState`: arrête l'instance Amazon EC2 avant de la remplacer par son type d'instance d'origine.

- ii. `aws:changeInstanceState`: force l'instance Amazon EC2 à s'arrêter avant de la remplacer par son type d'instance d'origine au cas où elle resterait bloquée dans un état d'arrêt.
- iii. `aws:executeAwsApi`: rétablit le type d'origine de l'instance Amazon EC2.
- iv. `aws:sleep`: attend 3 secondes après avoir changé le type d'instance pour une éventuelle cohérence.
- v. `aws:changeInstanceState`: démarre l'instance Amazon EC2 si elle était en cours d'exécution avant de modifier le type d'instance.
- vi. `aws:waitForAwsResourceProperty`: attend que l'instance Amazon EC2 passe les contrôles de statut.

22.`aws:sleep`: Attend avant de terminer le runbook.

## AWSSupport-CheckXenToNitroMigrationRequirements

### Description

Le `AWSSupport-CheckXenToNitroMigrationRequirements` runbook vérifie qu'une instance Amazon Elastic Compute Cloud (Amazon EC2) répond aux conditions requises pour réussir à changer le type d'instance d'une instance de type Xen à un type d'instance basé sur Nitro. Cette automatisation vérifie les points suivants :

- Le périphérique racine est un volume Amazon Elastic Block Store (Amazon EBS).
- L'`enaSupport` attribut est activé.
- Le module ENA est installé sur l'instance.
- Le module NVMe est installé sur l'instance. Dans l'affirmative, le module est installé et un script vérifie que le module est chargé dans `initramfs` image.
- Analyse `/etc/fstab` et recherche les blocs de périphériques en cours de montage à l'aide de noms de périphériques.
- Détermine si le système d'exploitation (SE) utilise des noms d'interface réseau prévisibles par défaut.

Ce runbook prend en charge les systèmes d'exploitation suivants :

- Red Hat Enterprise Linux
- CentOS

- Amazon Linux 2
- Amazon Linux
- Debian Server
- Ubuntu Server
- SUSE Linux Enterprise Server15 SP2
- SUSE Linux Enterprise Server12 SP5

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Par défaut : faux

Description : (Obligatoire) L'ID de l'instance Amazon EC2 dont vous souhaitez vérifier les prérequis avant de migrer vers un type d'instance basé sur Nitro.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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:DescribeInstanceTypes`

## Étapes de document

- `aws:executeAwsApi`- Recueille des informations sur l'instance.
- `aws:executeAwsApi`- Recueille des informations sur l'hyperviseur de l'instance.
- `aws:branch`- Branches selon que l'instance cible exécute déjà ou non un type d'instance basé sur Nitro.
- `aws:branch`- Vérifie si le système d'exploitation de l'instance est pris en charge par les instances basées sur Nitro.
- `aws:assertAwsResourceProperty`- Vérifie que l'instance que vous avez spécifiée est gérée par Systems Manager et que son état est `Online`.

- `aws:branch`- Branches selon que le périphérique racine de l'instance est ou non un volume Amazon EBS.
- `aws:branch`- Branches selon que l'attribut ENA est activé ou non pour l'instance.
- `aws:runCommand`- Vérifie la présence de pilotes ENA sur l'instance.
- `aws:runCommand`- Vérifie la présence de pilotes NVMe sur l'instance.
- `aws:runCommand`- Vérifie que le `fstab` fichier ne contient pas de formats non reconnus.
- `aws:runCommand`- Vérifie si la configuration des noms d'interface sur l'instance est prévisible.
- `aws:executeScript`- Génère une sortie en fonction des étapes précédentes.

## Sorties

`FinalOutput.Output` - Les résultats des contrôles effectués par l'automatisation.

# AWSSupport-ConfigureEC2Metadata

## Description

Ce runbook vous aide à configurer les options du service de métadonnées d'instance (IMDS) pour les instances Amazon Elastic Compute Cloud (Amazon EC2). À l'aide de ce runbook, vous pouvez configurer les éléments suivants :

- Imposez l'utilisation des métadonnées IMDSv2 par exemple.
- Configurez la `HttpPutResponseHopLimit` valeur.
- Autorisez ou refusez l'accès aux métadonnées de l'instance.

Pour plus d'informations sur les métadonnées d'instance, consultez [la section Configuration du service de métadonnées d'instance](#) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- Appliquer IMDS v2

Type : String

Valeurs valides : obligatoires | facultatives

Par défaut : facultatif

Description : (Facultatif) Appliquez IMDSv2. Si vous le souhaitez `required`, l'instance Amazon EC2 utilisera uniquement IMDSv2. Si vous le souhaitez `optional`, vous pouvez choisir entre IMDSv1 et IMDSv2 pour l'accès aux métadonnées.

#### Important

Si vous appliquez IMDSv2, les applications qui utilisent IMDSv1 risquent de ne pas fonctionner correctement. Avant d'appliquer IMDSv2, assurez-vous que vos applications qui utilisent IMDS sont mises à niveau vers une version compatible avec IMDSv2. Pour plus d'informations sur le service de métadonnées d'instance version 2 (IMDSv2), consultez [la section Configuration du service de métadonnées d'instance](#) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

- HttpPutResponseHopLimit

Type : entier

Valeurs valides : 0-64

Par défaut : 0

Description : (Facultatif) La valeur limite de saut de réponse HTTP PUT souhaitée (1-64) pour les demandes de métadonnées d'instance. Cette valeur contrôle le nombre de sauts que la réponse PUT peut parcourir. Pour empêcher la réponse de sortir de l'instance, spécifiez 1 la valeur du paramètre.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance Amazon EC2 dont vous souhaitez configurer les paramètres de métadonnées.

- MetadataAccess

Type : String

Valeurs valides : activé | désactivé

Par défaut : activé

Description : (Facultatif) Autorisez ou refusez l'accès aux métadonnées de l'instance Amazon EC2. Si vous le spécifiez `disabled`, tous les autres paramètres seront ignorés et l'accès aux métadonnées sera refusé pour l'instance.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

## Étapes de document



1. `branchOnMetadataAccess` - Automatisation des branches en fonction de la valeur du `MetadataAccess` paramètre.
2. `disableMetadataAccess`- Appelle l'action de `ModifyInstanceMetadataOptionsAPI` pour désactiver l'accès au point de terminaison des métadonnées.
3. `branchOnHttpPutResponseHopLimit`- Automatisation des branches en fonction de la valeur du `HttpPutResponseHopLimit` paramètre.
4. `maintainHopLimitAndConfigureImdsVersion`- Si la valeur `HttpPutResponseHopLimit` est 0, la limite de sauts actuelle est maintenue et les autres options de métadonnées sont modifiées.
5. `waitBeforeAssertingIMDSv2State` - Attend 30 secondes avant d'affirmer le statut IMDSv2.
6. `setHopLimitAndConfigureImdsVersion`- S'il `HttpPutResponseHopLimit` est supérieur à 0, configure les options de métadonnées à l'aide des paramètres d'entrée donnés.
7. `waitBeforeAssertingHopLimit`- Patiente 30 secondes avant d'activer les options de métadonnées.
8. `assertHopLimit`- Affirme que la `HttpPutResponseHopLimit` propriété est définie sur la valeur que vous avez spécifiée.
9. `branchVerificationOnIMDSv2Option` - Vérification des branches basée sur la valeur du paramètre. `EnforceIMDSv2`
10. `AssertIMDSv2 IsOptional` - Affirme que `HttpTokens` la valeur est définie sur. `optional`
11. `AssertIMDSv2 IsEnforced` - Affirme que `HttpTokens` la valeur est définie sur. `required`
12. `waitBeforeAssertingMetadataState`- Patiente 30 secondes avant d'affirmer que l'état des métadonnées est désactivé.
13. `assertMetadataIsDésactivé` : affirme que les métadonnées sont `disabled`.
14. `describeMetadataOptions`- Obtient les options de métadonnées une fois que les modifications que vous avez spécifiées ont été appliquées.

## Sorties

`describeMetadataOptions`.État

`describeMetadataOptions`.`MetadataAccess`

`describeMetadataOptions`.`IMDS v2`

`describeMetadataOptions`.`HttpPutResponseHopLimit`

## AWSSupport-CopyEC2Instance

### Description

Le `AWSSupport-CopyEC2Instance` runbook fournit une solution automatisée pour la procédure décrite dans l'article du centre de connaissances [Comment déplacer mon instance EC2 vers un autre sous-réseau, une zone de disponibilité ou un VPC ?](#) Les branches d'automatisation dépendent des valeurs que vous spécifiez pour les `SubnetId` paramètres `Region` et.

Si vous spécifiez une valeur pour le `SubnetId` paramètre mais pas une valeur pour le `Region` paramètre, l'automatisation crée un Amazon Machine Image (AMI) de l'instance cible et lance une nouvelle instance à partir du AMI sous-réseau que vous avez spécifié.

Si vous spécifiez une valeur pour le `SubnetId` paramètre et le `Region` paramètre, l'automatisation crée une instance AMI de l'instance cible, copie l'instance AMI dans celle Région AWS que vous avez spécifiée et lance une nouvelle instance AMI à partir de l'instance du sous-réseau que vous avez spécifié.

Si vous spécifiez une valeur pour le `Region` paramètre mais pas une valeur pour le `SubnetId` paramètre, l'automatisation crée une instance AMI de l'instance cible, la AMI copie AMI dans la région que vous avez spécifiée et lance une nouvelle instance à partir du sous-réseau par défaut de votre cloud privé virtuel (VPC) dans la région de destination.

Si aucune valeur n'est spécifiée pour les `SubnetId` paramètres `Region` or, l'automatisation crée une instance AMI de l'instance cible et lance une nouvelle instance à partir du AMI sous-réseau par défaut de votre VPC.

Pour copier un AMI vers une autre région, vous devez fournir une valeur pour le `AutomationAssumeRole` paramètre. Si l'automatisation expire pendant `waitForAvailableDestinationAmi` étape, il se AMI peut que la copie soit toujours en cours. Dans ce cas, vous pouvez attendre que la copie soit terminée et lancer l'instance manuellement.


Avant d'exécuter cette automatisation, notez les points suivants :

- AMIs sont basés sur des instantanés Amazon Elastic Block Store (Amazon EBS). Pour les systèmes de fichiers volumineux sans capture instantanée préalable, AMI la création peut prendre plusieurs heures. Pour réduire le temps de AMI création, créez un instantané Amazon EBS avant de créer le AMI.
- Créer et AMI ne pas créer d'instantané pour les volumes de stockage de l'instance sur l'instance. Pour plus d'informations sur la sauvegarde des volumes de stockage d'instance sur Amazon EBS,

consultez [Comment sauvegarder un volume de stockage d'instance sur mon instance Amazon EC2 sur Amazon EBS ?](#)

- La nouvelle instance Amazon EC2 possède une adresse IP IPv4 privée ou IPv6 publique différente. Vous devez mettre à jour toutes les références aux anciennes adresses IP (par exemple, dans les entrées DNS) avec les nouvelles adresses IP attribuées à la nouvelle instance. Si vous utilisez une adresse IP Elastic sur votre instance source, veillez à l'associer à la nouvelle instance.
- Des problèmes de conflit avec l'identifiant de sécurité du domaine (SID) peuvent survenir lorsque la copie démarre et tente de contacter le domaine. Avant de capturer l'AMI, utilisez Sysprep ou supprimez l'instance jointe au domaine du domaine pour éviter les problèmes de conflit. Pour plus d'informations, voir [Comment utiliser Sysprep pour créer et installer des AMI Windows personnalisées réutilisables ?](#)

[Exécutez cette automatisation \(console\)](#)

 Important

Nous vous déconseillons d'utiliser ce runbook pour copier des instances du contrôleur de domaine Microsoft Active Directory.

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux, macOS, Windows

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance que vous souhaitez copier.

- KeyPair

Type : String

Description : (Facultatif) La paire de clés que vous souhaitez associer à la nouvelle instance copiée. Si vous copiez l'instance dans une autre région, assurez-vous que la paire de clés existe dans la région spécifiée.

- Région

Type : String

Description : (Facultatif) Région dans laquelle vous souhaitez copier l'instance. Si vous spécifiez une valeur pour ce paramètre, mais pas pour les SecurityGroupIds paramètres SubnetId et, l'automatisation tente de lancer l'instance dans le VPC par défaut avec le groupe de sécurité par défaut. Si EC2-Classic est activé dans la région de destination, le lancement échouera.

- SubnetId

Type : String

Description : (Facultatif) L'ID du sous-réseau sur lequel vous souhaitez copier l'instance. Si EC2-Classic est activé dans la région de destination, vous devez fournir une valeur pour ce paramètre.

- InstanceType

Type : String

Description : (Facultatif) Type d'instance sous lequel l'instance copiée doit être lancée. Si vous ne spécifiez pas de valeur pour ce paramètre, le type d'instance source est utilisé. Si le type d'instance source n'est pas pris en charge dans la région vers laquelle l'instance est copiée, l'automatisation échoue.

- SecurityGroupIds

Type : String

Description : (Facultatif) Liste séparée par des virgules des ID de groupes de sécurité que vous souhaitez associer à l'instance copiée. Si vous ne spécifiez aucune valeur pour ce paramètre et que l'instance n'est pas copiée vers une autre région, les groupes de sécurité associés à l'instance source sont utilisés. Si vous copiez l'instance vers une autre région, le groupe de sécurité par défaut du VPC par défaut de la région de destination est utilisé.

- KeepImageSourceRegion

Type : booléen

Valeurs valides : true | false

Valeur par défaut : true

Description : (Facultatif) Si vous spécifiez `true` ce paramètre, l'automatisation ne supprime pas AMI l'instance source. Si vous spécifiez `false` ce paramètre, l'automatisation annule l'enregistrement AMI et supprime les instantanés associés.

- KeepImageDestinationRegion

Type : booléen

Valeurs valides : true | false

Valeur par défaut : true

Description : (Facultatif) Si vous spécifiez `true` ce paramètre, l'automatisation ne supprime pas AMI celui qui est copié dans la région que vous avez spécifiée. Si vous spécifiez `false` ce paramètre, l'automatisation annule l'enregistrement AMI et supprime les instantanés associés.

- NoRebootInstanceBeforeTakingImage

Type : booléen

Valeurs valides : true | false

Par défaut : faux

Description : (Facultatif) Si vous spécifiez `true` ce paramètre, l'instance source ne sera pas redémarrée avant de créer le AMI. Une fois cette option utilisée, l'intégrité du système de fichiers sur l'image créée ne peut pas être garantie.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

Si vous copiez l'instance vers une autre région, vous aurez également besoin des autorisations suivantes.

- `ec2:CopyImage`

## Étapes de document

- `describeOriginalInstanceDetails` : rassemble les détails de l'instance à copier.
- `assertRootVolumeIsEbs`- Vérifie si le type de périphérique du volume racine est `etebs`, dans le cas contraire, met fin à l'automatisation.
- `evalInputParameters`- Évalue les valeurs fournies pour les paramètres d'entrée.
- `createLocalAmi`- Crée une instance AMI de l'instance source.
- `tagLocalAmi`- Marque ce qui AMI a été créé à l'étape précédente.
- `branchAssertRegionIsSame`- Branches selon que l'instance est copiée dans la même région ou dans une autre région.
- `branchAssertSameRegionWithKeyPair`- Branches selon qu'une valeur a été fournie ou non pour le `KeyPair` paramètre d'une instance copiée dans la même région.

- `sameRegionLaunchInstanceWithKeyPair`- Lance une instance Amazon EC2 à partir de l'instance source AMI du même sous-réseau ou du sous-réseau que vous avez spécifié à l'aide de la paire de clés que vous avez spécifiée.
- `sameRegionLaunchInstanceWithoutKeyPair`- Lance une instance Amazon EC2 à partir AMI de l'instance source du même sous-réseau ou du sous-réseau que vous spécifiez sans paire de clés.
- `copyAmiToRégion` : copie le dans AMI la région de destination.
- `waitForAvailableDestinationAmi`- Attend que l'AMI état copié devienne `available`.
- `destinationRegionLaunchInstance` : lance une instance Amazon EC2 à l'aide de la copie. AMI
- `branchAssertDestinationAmiToDelete`- Branches basées sur la valeur que vous avez fournie pour le `KeepImageDestinationRegion` paramètre.
- `deregisterDestinationAmiAndDeleteSnapshots`- Désenregistre les instantanés copiés AMI et supprime les instantanés associés.
- `branchAssertSourceAmiToDelete`- Branches basées sur la valeur que vous avez fournie pour le `KeepImageSourceRegion` paramètre.
- `deregisterSourceAmiAndDeleteSnapshots`- Annule l'enregistrement de l'instance AMI créée à partir de l'instance source et supprime les instantanés associés.
- `veille` : met en veille l'automatisation pendant 2 secondes. Il s'agit d'une étape terminale.

## Sorties

`sameRegionLaunchInstanceWithKeyPair.InstanceIds`

`sameRegionLaunchInstanceWithoutKeyPair.InstanceIds`

`destinationRegionLaunchInstance. DestinationInstanceId`

## **AWSSupport - EnableWindowsEC2SerialConsole**

### Description

Le runbook `AWSSupport-EnableWindowsEC2SerialConsole` permet d'activer la console série Amazon EC2, la console d'administration spéciale (SAC) et le menu de démarrage sur votre instance Windows Amazon EC2. Grâce à la fonctionnalité de console série Amazon Elastic Compute Cloud (Amazon EC2), vous avez accès au port série de votre instance Amazon EC2 pour résoudre les problèmes de démarrage, de configuration réseau et autres. Le runbook automatise les étapes nécessaires pour activer la fonctionnalité sur les instances en cours d'exécution et gérées par AWS Systems Manager, ainsi que sur celles en état arrêté ou non gérées par. AWS Systems Manager

## Comment fonctionne-t-il ?

Le manuel `AWSSupport-EnableWindowsEC2SerialConsole` d'automatisation permet d'activer le SAC et le menu de démarrage sur les instances Amazon EC2 exécutant Microsoft Windows Server. Pour les instances en cours d'exécution et gérées par AWS Systems Manager, le runbook exécute un PowerShell script AWS Systems Manager Run Command pour activer le SAC et le menu de démarrage. Pour les instances à l'état arrêté ou non gérées par AWS Systems Manager, le runbook utilise le paramètre [AWSSupport-StartEC2 RescueWorkflow](#) pour créer une instance Amazon EC2 temporaire afin d'effectuer les modifications requises hors ligne.

Pour plus d'informations, consultez la [console série Amazon EC2 pour les instances Windows](#).

### Important

- Si vous activez le SAC sur une instance, les services Amazon EC2 qui reposent sur la récupération du mot de passe ne fonctionneront pas depuis la console Amazon EC2. Pour plus d'informations, consultez [Utilisation de SAC pour dépanner votre instance Windows](#).
- Pour configurer l'accès à la console série, vous devez accorder l'accès à la console série au niveau du compte, puis configurer des politiques AWS Identity and Access Management (IAM) pour accorder l'accès à vos utilisateurs. Vous devez également configurer un utilisateur avec mot de passe sur chaque instance afin que vos utilisateurs puissent utiliser la console série pour le dépannage. Pour plus d'informations, consultez [Configurer l'accès à la console série Amazon EC2](#).
- Pour savoir si la console série est activée sur votre compte, voir [Afficher le statut d'accès du compte à la console série](#).
- L'accès à la console série n'est pris en charge que sur les instances virtualisées basées sur le système [Nitro](#).

[Pour plus d'informations, consultez les prérequis relatifs à la console série Amazon EC2.](#)

Type de document

Automatisation

Propriétaire

Amazon



## Plateformes

### Windows

### Paramètres

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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"
            ]
        }
    }
}
]
```

```
}
```

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez au `AWSSupport-EnableWindowsEC2SerialConsole` dans la AWS Systems Manager console.
2. Sélectionnez `Execute automation` (Exécuter l'automatisation).
3. Pour les paramètres d'entrée, entrez ce qui suit :

- `InstanceId`: (Obligatoire)

L'ID de l'instance Amazon EC2 sur laquelle vous souhaitez activer la console série Amazon EC2 (SAC) et le menu de démarrage.

- `AutomationAssumeRole`: (Facultatif)

L'Amazon Resource Name (ARN) du rôle IAM qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `HelperInstanceType`: (Conditionnel)

Type d'instance Amazon EC2 que le runbook fournit pour configurer la console série Amazon EC2 pour une instance hors ligne.

- `HelperInstanceProfileName`: (Conditionnel)

Nom d'un profil d'instance IAM existant pour l'instance d'assistance. Si vous activez le SAC et le menu de démarrage sur une instance arrêtée ou non gérée par AWS Systems Manager, cela est obligatoire. Si aucun profil d'instance IAM n'est spécifié, l'automatisation en crée un en votre nom.

- `SubnetId`: (Conditionnel)

ID de sous-réseau pour une instance d'assistance. Par défaut, il utilise le même sous-réseau que celui où réside l'instance fournie.

### ⚠ Important

Si vous fournissez un sous-réseau personnalisé, il doit se trouver dans la même zone de disponibilité que l'instance et les points de terminaison de Systems Manager et autoriser l'accès à ceux-ci. Cela n'est nécessaire que si l'instance cible est à l'état arrêté ou n'est pas gérée par AWS Systems Manager.

- `CreateInstanceBackupBeforeScriptExecution`: (Facultatif)

Spécifiez `True` pour créer une sauvegarde Amazon Machine Images (AMI) de l'instance Amazon EC2 avant d'activer le SAC et le menu de démarrage. L'AMI sera conservée une fois l'automatisation terminée. Il est de votre responsabilité de sécuriser l'accès à l'AMI ou de la supprimer.

- `BackupAmazonMachineImagePrefix`: (Conditionnel)

Préfixe pour l'Amazon Machine Image (AMI) créé si le `CreateInstanceBackupBeforeScriptExecution` paramètre est défini sur `True`

Input parameters	
<b>InstanceId</b> <small>(Required) The ID of Amazon EC2 instance that you want to enable EC2 serial console, Special Admin Console (SAC), and boot menu.</small> <input type="button" value="Show interactive instance picker"/> <input type="text" value="i-01234567890abcde0"/>	
<b>AutomationAssumeRole</b> <small>(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</small> <input type="text" value="EC2SerialConsole-MinimumRole-AutomationAssumeRole-7inoDR7gFLT"/>	<b>HelperInstanceType</b> <small>(Conditional) The type of Amazon EC2 instance that the runbook provisions to configure EC2 serial console for an offline instance.</small> <input type="text" value="t3.medium"/>
<b>SubnetId</b> <small>(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.</small> <input type="text" value="SelectedInstanceSubnet"/>	<b>HelperInstanceProfileName</b> <small>(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.</small> <input type="text" value="String"/>
<b>CreateInstanceBackupBeforeScriptExecution</b> <small>(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.</small> <input type="text" value="True"/>	<b>BackupAmazonMachineImagePrefix</b> <small>(Conditional) A prefix for the Amazon Machine Image (AMI) that is created if the "CreateInstanceBackupBeforeScriptExecution" parameter is set to "True".</small> <input type="text" value="AWSSupport"/>

#### 4. Sélectionnez Exécuter.

#### 5. L'automatisation démarre.

#### 6. Le document exécute les étapes suivantes :

- `CheckIfEc2 SerialConsoleAccessEnabled` :

Vérifie si l'accès à la console série Amazon EC2 est activé au niveau du compte. Remarque : L'accès à la console série n'est pas disponible par défaut. Pour plus d'informations, consultez [Configurer l'accès à la console série Amazon EC2](#).

- `CheckIfEc2 InstanceWindows` :

Indique si la plate-forme d'instance cible est Windows.

- `GetInstanceType`:

Récupère le type d'instance de l'instance cible.

- `CheckIfInstanceTypeIsNitro`:

Vérifie si l'hyperviseur de type d'instance est basé sur Nitro. L'accès à la console série n'est pris en charge que sur les instances virtualisées basées sur le système Nitro.

- `CheckIfInstanceIsInAutoScalingGroup` :

Vérifie si l'instance Amazon EC2 fait partie d'un groupe Amazon EC2 Auto Scaling en `DescribeAutoScalingInstances` appelant l'API. Si l'instance fait partie d'un groupe Amazon EC2 Auto Scaling, cela garantit que l'assistant de portage pour l'instance .NET est en état de veille.

- `WaitForEc2 InstanceStateStablized` :

Attend que l'instance soit en cours d'exécution ou arrêtée.

- `GetEc2 InstanceState` :

Obtient l'état actuel de l'instance.

- `BranchOnEc2 InstanceState` :

Branches basées sur l'état de l'instance récupéré à l'étape précédente. Si cet état d'instance est en cours d'exécution, il passe à `CheckIfEc2InstanceIsManagedBySSM` étape et sinon, il passe à `CheckIfHelperInstanceProfileIsProvided` étape.

- `CheckIfEc2 InstanceIsManagedBy SMS` :

Vérifie si l'instance est gérée par AWS Systems Manager. S'il est géré, le runbook active le SAC et le menu de démarrage à l'aide d'une commande d' PowerShell exécution.

- `BranchOnPreEC2 RescueBackup` :

Branches basées sur le paramètre `CreateInstanceBackupBeforeScriptExecution` d'entrée.

- `CreateAmazonMachineImageBackup`:

Crée une sauvegarde AMI de l'instance.

- Activez le SAC AndBootMenu :

Active le SAC et le menu de démarrage en exécutant un script PowerShell Run Command.

- `RebootInstance`:

Redémarre l'instance Amazon EC2 pour appliquer la configuration. Il s'agit de la dernière étape si l'instance est en ligne et est gérée par AWS Systems Manager.

- `CheckIfHelperInstanceProfileIsProvided`:

Vérifie si le paramètre `HelperInstanceProfileName` spécifié existe avant d'activer le SAC et le menu de démarrage hors ligne à l'aide d'une instance Amazon EC2 temporaire.

- `RunAutomationToInjectOfflineScriptForActivationAndBootMenu` du SAC :

Exécute le menu `AWSSupport-StartEC2RescueWorkflow` pour activer le SAC et le menu de démarrage lorsque l'instance est arrêtée ou n'est pas gérée par AWS Systems Manager.

- `GetExecutionDetails`:

Récupère l'ID d'image de la sauvegarde et de la sortie du script hors ligne.

7. Une fois terminé, consultez la section Sorties pour obtenir les résultats détaillés de l'exécution :

- Activer le SAC. Sortie `AndBootMenu` :

Résultat de l'exécution de la commande à l'`EnableSACAndBootMenu` étape.

- `GetExecutionDetails.OfflineScriptOutput`:

Sortie du script hors ligne exécuté à l'`RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` étape.

- `GetExecutionDetails.BackupBeforeScriptExecution`:

ID d'image de la sauvegarde AMI prise si le paramètre `CreateInstanceBackupBeforeScriptExecution` d'entrée est `True`.

Résultat de l'exécution sur une instance exécutée et gérée par AWS Systems Manager

Outputs	
<pre>GetExecutionDetails.BackupBeforeScriptExecution No output available yet because the step is not successfully executed  EnableSACAndBootMenu.Output The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully. The operation completed successfully.</pre>	<pre>GetExecutionDetails.OfflineScriptOutput No output available yet because the step is not successfully executed</pre>

Résultat de l'exécution sur une instance arrêtée ou non gérée par AWS Systems Manager

**Outputs**

```
EnableSACAndBootMenu.Output
No output available yet because the step is not successfully executed
GetExecutionDetails.OfflineScriptOutput
Device xvdf mapped to D
Offline Windows installation found in directory D:\Windows
Windows Server 2015 Datacenter (18.0.14393.6522)
BCD Store found in directory D:\Boot\BCD
Detecting installed drivers
EC2Rescue environment variables set
EC2Rescue script variables set
The operation completed successfully.
The operation completed successfully.
The operation completed successfully.
The operation completed successfully.
The operation completed successfully.
Volume successfully set offline
```

```
GetExecutionDetails.BackupBeforeScriptExecution
ami-09c33701932955dde
```

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

## AWSSupport - Exécute EC2Rescue

### Description

Ce runbook utilise cet EC2Rescue outil pour résoudre et, si possible, réparer les problèmes de connectivité courants liés à l'instance Amazon Elastic Compute Cloud (Amazon EC2) spécifiée pour Linux ou Windows Server. Les instances dont les volumes racine sont chiffrés ne sont pas prises en charge.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Linux, macOS, Windows

### Paramètres

- AutomationAssumeRole



Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- EC2 RescueInstanceType

Type : String

Valeurs valides : t2.small | t2.medium | t2.large

Par défaut : t2.small

Description : (Obligatoire) Type d'instance EC2 pour l'EC2Rescueinstance. Taille recommandée : t2.small

- LogDestination

Type : String


Description : (Facultatif) Nom du compartiment Amazon S3 de votre compte dans lequel vous souhaitez charger les journaux de résolution des problèmes. Assurez-vous que la stratégie de compartiment n'accorde pas des autorisations en lecture/écriture superflues pour les tiers qui n'ont pas besoin d'accéder aux journaux collectés.

- SubnetId

Type : String

Par défaut : CreateNew VPC

Description : (Facultatif) ID de sous-réseau de l'EC2Rescueinstance. Par défaut, AWS Systems Manager Automation crée un VPC. Vous pouvez également SelectedInstanceSubnet utiliser le même sous-réseau que votre instance ou spécifier un ID de sous-réseau personnalisé.


 Important

Le sous-réseau doit se trouver dans la même zone de disponibilité que les points de UnreachableInstanceId terminaison SSM et doit autoriser l'accès à ces derniers.

- `UnreachableInstanceId`

Type : String

Description : (Obligatoire) ID de votre instance EC2 inaccessible.

 Important

Systems Manager Automation arrête cette instance et crée une AMI avant de tenter toute opération. Les données stockées sur les volumes de stockage d'instance seront perdues. L'adresse IP publique changera si vous n'utilisez pas d'adresse IP Elastic.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Vous devez avoir au moins `ssm:StartAutomationExecution` et être `ssm:GetAutomationExecution` capable de lire le résultat de l'automatisation. Pour plus d'informations sur les autorisations requises, consultez [AWSSupport-StartEC2RescueWorkflow](#).

### Étapes de document

1. `aws:assertAwsResourceProperty`- Affirme si l'instance fournie est Windows Server :
  - a. (`EC2RescuepourWindows Server`) Si l'instance fournie est une Windows Server instance :
    - i. `aws:executeAutomation`- Appelle `AWSSupport-StartEC2RescueWorkflow` avec le script `EC2Rescue` pour Windows Server le mode hors connexion.
    - ii. `aws:executeAwsApi`- Récupère l'ID AMI de sauvegarde à partir de l'automatisation imbriquée.
    - iii. `aws:executeAwsApi`- Récupère le résumé d'`EC2Rescue` à partir de l'automatisation imbriquée.
  - b. (`EC2Rescuepour Linux`) Si l'instance fournie est une instance Linux :
    - i. `aws:executeAutomation`- Appelle `AWSSupport-StartEC2RescueWorkflow` avec les scripts hors ligne d'`EC2Rescue` pour Linux
    - ii. `aws:executeAwsApi`- Récupère l'ID AMI de sauvegarde à partir de l'automatisation imbriquée.

- iii. `aws:executeAwsApi`- Récupère le résumé d'EC2Rescue à partir de l'automatisation imbriquée.

## Sorties

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

## **AWSsupport-ListEC2Resources**

### Description

Le `AWSsupport-ListEC2Resources` runbook renvoie des informations sur les instances Amazon EC2 et les ressources associées telles que les volumes Amazon Elastic Block Store (Amazon EBS), les adresses IP Elastic et les groupes Amazon EC2 Auto Scaling à partir de ce que vous avez spécifié. Régions AWS Par défaut, les informations sont collectées dans toutes les régions et sont affichées dans les résultats de l'automatisation. Vous pouvez éventuellement spécifier un compartiment Amazon Simple Storage Service (Amazon S3) pour les informations à charger sous la forme d'un fichier de valeurs séparées par des virgules (.csv).

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- `Compartiment`

Type : String

Description : (Facultatif) Le nom du compartiment S3 vers lequel les informations collectées sont téléchargées.

- `DisplayResourceDeletionDocumentation`

Type : String

Valeur par défaut : true

Description : (Facultatif) Si cette option est définie sur `true`, l'automatisation crée des liens dans la sortie vers la documentation relative à la suppression de vos ressources.

- `RegionsToQuery`

Type : String

Par défaut : Tous

Description : (Facultatif) Les régions auprès desquelles vous souhaitez recueillir des informations relatives à Amazon EC2.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRegions`
- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

En outre, pour charger correctement les informations collectées dans le compartiment S3 que vous avez spécifié, vous `AutomationAssumeRole` devez effectuer les actions suivantes :

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

#### Étapes de document

- `aws:executeAwsApi`- Rassemble les régions activées pour le compte.
- `aws:executeScript`- Confirme que les régions activées pour le compte prennent en charge les régions spécifiées dans le `RegionsToQuery` paramètre.
- `aws:branch`- Si aucune région n'est activée pour le compte, l'automatisation prend fin.
- `aws:executeScript`- Répertorie toutes les instances EC2 pour le compte et les régions que vous spécifiez.
- `aws:executeScript`- Répertorie toutes les images Amazon Machine (AMI) pour le compte et les régions que vous spécifiez.
- `aws:executeScript`- Répertorie tous les volumes EBS pour le compte et les régions que vous spécifiez.
- `aws:executeScript`- Répertorie toutes les adresses IP Elastic pour le compte et les régions que vous spécifiez.
- `aws:executeScript`- Répertorie toutes les interfaces réseau élastiques pour le compte et les régions que vous spécifiez.
- `aws:executeScript`- Répertorie tous les groupes Auto Scaling pour le compte et les régions que vous spécifiez.

- `aws:executeScript`- Répertorie tous les équilibrateurs de charge pour le compte et les régions que vous spécifiez.
- `aws:executeScript`- Télécharge les informations collectées vers le compartiment S3 spécifié si vous fournissez une valeur pour le Bucket paramètre.

## AWSSupport-ManageRDPSettings

### Description

Le `AWSSupport-ManageRDPSettings` runbook permet à l'utilisateur de gérer les paramètres courants du protocole RDP (Remote Desktop Protocol), tels que le port RDP et l'authentification de la couche réseau (NLA). Par défaut, le runbook lit et affiche les valeurs des paramètres.

#### Important

Les modifications apportées aux paramètres RDP doivent être examinées attentivement avant d'exécuter ce runbook.

### [Exécutez cette automatisation \(console\)](#)

#### Type de document

Automatisation

#### Propriétaire

Amazon

#### Plateformes

Windows

#### Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre

nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) ID de l'instance chargée de gérer les paramètres RDP.

- NLA SettingAction

Type : String

Valeurs valides : Vérifier | Activer | Désactiver

Par défaut : Check

Description : (Obligatoire) action à effectuer au niveau du paramètre NLA : Check, Enable, Disable.

- RDPPort

Type : String

Par défaut: 3389

Description : (Facultatif) spécifiez le nouveau port RDP. Utilisé uniquement lorsque l'action est définie sur Modify. Le numéro de port doit être compris entre 1025 et 65535. Remarque : une fois que le port est modifié, le service RDP est redémarré.

- RDP PortAction

Type : String

Valeurs valides : Vérifier | Modifier

Par défaut : Check

Description : (Obligatoire) Action à appliquer au port RDP.

- RemoteConnections

Type : String

Valeurs valides : Vérifier | Activer | Désactiver

Par défaut : Check

Description : (Obligatoire) Action à exécuter sur le paramètre fDenytsConnections.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

L'instance EC2 qui reçoit la commande doit disposer d'un rôle IAM auquel doit être associée la politique gérée par ManagedInstanceCore Amazon d'AmazonSSM. L'utilisateur doit avoir au moins ssm : SendCommand pour envoyer la commande à l'instance, plus ssm : GetCommandInvocation pour pouvoir lire le résultat de la commande.

### Étapes de document

aws : runCommand- Exécutez le PowerShell script pour modifier ou vérifier les paramètres RDP sur l'instance cible.

### Sorties

manageRDPSettings.Output

## **AWSsupport-ManageWindowsService**

### Description

Le AWSsupport-ManageWindowsService runbook vous permet d'arrêter, de démarrer, de redémarrer, de suspendre ou de désactiver n'importe quel service Windows sur l'instance cible.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Windows



## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance gérée dont les services doivent être gérés.

- ServiceAction

Type : String

Valeurs valides : Vérifier | Redémarrer | Forcer le redémarrage | Démarrer | Arrêter | Forcer l'arrêt | Pause

Par défaut : Check

Description : (Obligatoire) Action à appliquer au service Windows. Notez que Force-Restart et Force-Stop peut être utilisé pour redémarrer et arrêter un service qui possède des services dépendants.

- StartupType

Type : String

Valeurs valides : Vérifier | Auto | Demander | Désactivé | DelayedAutoStart

Par défaut : Check

Description : (Obligatoire) Type de démarrage à appliquer au service Windows.

- WindowsServiceName

Type : String

Description : (Obligatoire) nom de service Windows valide.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Il est recommandé que l'instance EC2 recevant la commande dispose d'un rôle IAM auquel est associée la politique gérée par `ManagedInstanceCore` Amazon d'AmazonSSM. L'utilisateur doit avoir au moins `ssm : StartAutomationExecution` et `ssm : SendCommand` pour exécuter l'automatisation et envoyer la commande à l'instance, plus `ssm : GetAutomationExecution` pour pouvoir lire la sortie de l'automatisation.

## Étapes de document

`aws : runCommand`- Exécutez le PowerShell script pour appliquer la configuration souhaitée au service Windows sur l'instance cible.

## Sorties

`manageWindowsService`. Sortie

# AWSSupport-MigrateEC2ClassicToVPC

## Description

Le `AWSSupport-MigrateEC2ClassicToVPC` runbook migre une instance Amazon Elastic Compute Cloud (Amazon EC2) d'EC2-Classique vers un cloud privé virtuel (VPC). Ce runbook prend en charge la migration des instances Amazon EC2 du type de virtualisation de machine virtuelle matérielle (HVM) avec les volumes racines Amazon Elastic Block Store (Amazon EBS).

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

## Linux

### Paramètres

- AutomationAssumeRole

Type : String

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- Approuver IAM

Type : StringList

Description : (Facultatif) Les noms de ressources Amazon (ARN) des utilisateurs IAM qui peuvent approuver ou refuser l'action. Ce paramètre s'applique uniquement si vous spécifiez la `CutOver` valeur du `MigrationType` paramètre.

- DestinationSecurityGroupId

Type : StringList

Description : (Facultatif) L'ID du groupe de sécurité que vous souhaitez associer à l'instance Amazon EC2 lancée dans votre VPC. Si vous ne spécifiez pas de valeur pour ce paramètre, l'automatisation crée un groupe de sécurité dans votre VPC et copie les règles du groupe de sécurité dans EC2-Classic. Si les règles ne sont pas copiées vers le nouveau groupe de sécurité, le groupe de sécurité par défaut de votre VPC est associé à l'instance Amazon EC2.

- DestinationSubnetId

Type : String

Description : (Facultatif) L'ID du sous-réseau vers lequel vous souhaitez migrer votre instance Amazon EC2. Si vous ne spécifiez pas de valeur pour ce paramètre, l'automatisation choisit aléatoirement un sous-réseau de votre VPC.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance Amazon EC2 que vous souhaitez migrer.

- MigrationType

Type : String

Valeurs valides : CutOver | Test

Description : (Obligatoire) Type de migration que vous souhaitez effectuer.

L'option `CutOver` nécessite une approbation pour arrêter votre instance Amazon EC2 qui s'exécute dans EC2-Classic. Une fois cette action approuvée, l'instance Amazon EC2 est arrêtée et l'automatisation crée un Amazon Machine Image (AMI). Lorsque le statut de l'AMI est `available`, une nouvelle instance Amazon EC2 est lancée à partir de cet AMI dans le champ `DestinationSubnetId` que vous avez spécifié dans votre VPC. Si une adresse IP Elastic est associée à votre instance Amazon EC2 qui s'exécute dans EC2-Classic, l'instance sera déplacée vers l'instance Amazon EC2 nouvellement créée dans votre VPC. Si l'instance Amazon EC2 lancée dans votre VPC ne parvient pas à être créée pour une raison quelconque, elle est résiliée et une approbation est demandée pour démarrer votre instance Amazon EC2 dans EC2-Classic.

L'option `Test` crée une AMI instance Amazon EC2 qui s'exécute dans EC2-Classic sans redémarrer. Comme l'instance Amazon EC2 ne redémarre pas, nous ne pouvons pas garantir l'intégrité du système de fichiers de l'image créée. Lorsque le statut de l'AMI est `available`, une nouvelle instance Amazon EC2 est lancée à partir de cet AMI dans celui `DestinationSubnetId` que vous avez spécifié dans votre VPC. Si votre instance Amazon EC2 qui s'exécute dans EC2-Classic est associée à une adresse IP Elastic, l'automatisation vérifie que celle que `DestinationSubnetId` vous spécifiez est publique. Si l'instance Amazon EC2 lancée dans votre VPC ne parvient pas à être créée pour une raison quelconque, elle est arrêtée et l'automatisation prend fin.

- SNS Notification ARN `NforApproval`

Type : String

Description : (Facultatif) L'ARN de la rubrique Amazon Simple Notification Service (Amazon SNS) à laquelle vous souhaitez envoyer des demandes d'approbation. Ce paramètre s'applique uniquement si vous spécifiez la `CutOver` valeur du `MigrationType` paramètre.

- `TargetInstanceType`

Type : String

Par défaut : `t2.2xlarge`

Description : (Facultatif) Type d'instance Amazon EC2 que vous souhaitez lancer dans votre VPC. Seuls les types d'instances basés sur Xen, tels que T2, M4 ou C4, sont pris en charge.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

- `aws:executeAwsApi`- Recueille des informations sur l'instance Amazon EC2 que vous spécifiez dans le `InstanceId` paramètre.
- `aws:assertAwsResourceProperty`- Confirme que le type d'instance que vous spécifiez dans le `TargetInstanceType` paramètre est basé sur Xen.
- `aws:assertAwsResourceProperty`- Confirme que l'instance Amazon EC2 que vous spécifiez dans le `InstanceId` paramètre est du type de virtualisation HVM.
- `aws:assertAwsResourceProperty`- Confirme que l'instance Amazon EC2 que vous spécifiez dans le `InstanceId` paramètre possède un volume racine Amazon EBS.
- `aws:executeScript`- Crée un groupe de sécurité selon les besoins en fonction de la valeur que vous spécifiez pour le `DestinationSecurityGroupId` paramètre.
- `aws:branch`- Branches en fonction de la valeur que vous spécifiez dans le `DestinationSubnetId` paramètre.
- `aws:executeAwsApi`- Identifie le VPC par défaut dans Région AWS lequel vous exécutez cette automatisation.
- `aws:executeAwsApi`- Choisit de manière aléatoire l'ID d'un sous-réseau situé dans le VPC par défaut.
- `aws:createImage`- Crée une instance Amazon EC2 AMI sans redémarrer.
- `aws:branch`- Branches basées sur la valeur que vous spécifiez pour le `MigrationType` paramètre.
- `aws:branch`- Branches basées sur la valeur que vous spécifiez pour le `DestinationSubnetId` paramètre.
- `aws:runInstances`- Lance une nouvelle instance à partir de celle AMI créée sans redémarrer l'instance Amazon EC2 dans EC2-Classic.

- `aws:changeInstanceState`- Met fin à l'instance Amazon EC2 récemment lancée si l'étape précédente échoue pour une raison quelconque.
- `aws:runInstances`- Lance une nouvelle instance à partir de l'instance AMI créée sans redémarrer l'instance Amazon EC2 dans EC2-Classic si elle est fournie. `DestinationSubnetId`
- `aws:changeInstanceState`- Met fin à l'instance Amazon EC2 récemment lancée si l'étape précédente échoue pour une raison quelconque.
- `aws:assertAwsResourceProperty`- Confirme le comportement d'arrêt de l'instance Amazon EC2 exécutée dans EC2-Classic.
- `aws:approve`- Attend l'approbation pour arrêter l'instance Amazon EC2.
- `aws:changeInstanceState`- Arrête l'instance Amazon EC2 en cours d'exécution dans EC2-Classic.
- `aws:changeInstanceState`- Force l'arrêt de l'instance Amazon EC2 en cours d'exécution dans EC2-Classic si nécessaire.
- `aws:createImage`- Crée AMI une instance Amazon EC2 après son arrêt.
- `aws:branch`- Branches basées sur la valeur spécifiée pour le `DestinationSubnetId` paramètre.
- `aws:runInstances`- Lance une nouvelle instance à partir de l'instance Amazon EC2 AMI créée ou arrêtée dans EC2-Classic.
- `aws:approve`- Attend l'approbation pour mettre fin à l'instance nouvellement lancée et démarre l'instance Amazon EC2 dans EC2-Classic si l'étape précédente échoue pour une raison quelconque.
- `aws:changeInstanceState`- Met fin à l'instance Amazon EC2 récemment lancée.
- `aws:runInstances`- Lance une nouvelle instance à partir de l'instance Amazon EC2 AMI créée ou arrêtée dans EC2-Classic à partir du paramètre. `DestinationSubnetId`
- `aws:approve`- Attend l'approbation pour mettre fin à l'instance nouvellement lancée et démarre l'instance Amazon EC2 dans EC2-Classic si l'étape précédente échoue pour une raison quelconque.
- `aws:changeInstanceState`- Met fin à l'instance Amazon EC2 récemment lancée.
- `aws:changeInstanceState`- Démarre l'instance Amazon EC2 qui a été arrêtée dans EC2-Classic.
- `aws:branch`- Branches selon que l'instance Amazon EC2 possède ou non une adresse IP publique.
- `aws:executeAwsApi`- Vérifie si l'adresse IP publique est une adresse IP Elastic.

- `aws:branch`- Branches en fonction de la valeur que vous spécifiez dans le `MigrationType` paramètre.
- `aws:executeAwsApi`- Déplace l'adresse IP Elastic vers votre VPC.
- `aws:executeAwsApi`- Recueille l'ID d'allocation de l'adresse IP Elastic qui a été déplacée vers votre VPC.
- `aws:branch`- Branches en fonction du sous-réseau sur lequel l'instance Amazon EC2 exécutée dans votre VPC a été lancée.
- `aws:executeAwsApi`- Associe l'adresse IP Elastic à la nouvelle instance lancée dans votre VPC.
- `aws:executeScript`- Confirme que le sous-réseau que votre instance Amazon EC2 récemment lancée exécute dans votre VPC est public.

## Sorties

`getInstanceProperties.virtualizationType` - Le type de virtualisation de l'instance Amazon EC2 exécutée dans EC2-Classic.

`getInstanceProperties.rootDeviceType`- Le type de périphérique racine de l'instance Amazon EC2 exécutée dans EC2-Classic.

`createAMIWithoutReboot.ImageId`- L'ID de l'instance Amazon EC2 AMI créée sans redémarrer s'exécutant dans EC2-Classic.

`getDefaultVPC.VpcId`- L'ID du VPC par défaut sur lequel la nouvelle instance Amazon EC2 est lancée si aucune valeur n'est fournie pour le `DestinationSubnetId` paramètre.

`getSubnetIdInDefaultVPC.subnetIdFromDefaultVpc`- L'ID du sous-réseau du VPC par défaut où la nouvelle instance Amazon EC2 est lancée si aucune valeur n'est fournie pour le `DestinationSubnetId` paramètre.

`launchTestInstanceDefaultVPC.InstanceIds`- L'ID de l'instance Amazon EC2 récemment lancée dans votre VPC par défaut pendant le type de Test migration.

`launchTestInstanceProvidedSubnet.InstanceIds`- L'ID de l'instance Amazon EC2 récemment lancée dans celui `DestinationSubnetId` que vous avez spécifié lors du type de Test migration.

`createAMIAfterStoppingInstance.ImageId`- L'ID AMI créé après l'arrêt de l'instance Amazon EC2 exécutée dans EC2-Classic.



`launchCutOverInstanceProvidedSubnet.InstanceIds`- L'ID de l'instance Amazon EC2 récemment lancée dans celui `DestinationSubnetId` que vous avez spécifié lors du type de `CutOver` migration.

`launchCutOverInstanceDefaultVPC.InstanceIds`- L'ID de l'instance Amazon EC2 récemment lancée dans votre VPC par défaut pendant le type de `CutOver` migration.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`- Si le sous-réseau choisi par l'automatisation dans votre VPC par défaut est public.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`- Si le sous-réseau que vous avez spécifié dans le `DestinationSubnetId` est public.

## AWSSupport-MigrateXenToNitroLinux

### Description

[Le AWSSupport-MigrateXenToNitroLinux runbook clone, prépare et migre une instance Linux Xen Amazon Elastic Compute Cloud \(Amazon EC2\) vers un type d'instance Nitro](#) Ce runbook propose deux options pour les types d'opérations :

- `Clone&Migrate`— Le flux de travail de cette option comprend les vérifications préliminaires, les tests et les `Clone&Migrate` phases. Le flux de travail est exécuté à l'aide du `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro` runbook.
- `FullMigration`— Cette option exécute le `Clone&Migrate` flux de travail, puis exécute l'étape supplémentaire consistant à remplacer les volumes Amazon EBS racines.

#### Important

L'utilisation de ce runbook entraîne des coûts pour votre compte liés à la durée d'exécution des instances Amazon EC2, à la création de volumes Amazon Elastic Block Store (Amazon EBS) et. AMIs Pour en savoir plus, consultez les [tarifs Amazon EC2](#) et [Amazon EBS](#).

### Contrôles préliminaires

L'automatisation effectue les vérifications préliminaires suivantes avant de poursuivre la migration. Si l'une des vérifications échoue, l'automatisation prend fin. Cette phase ne représente qu'une partie du `Clone&Migrate` flux de travail.

- Vérifie si l'instance cible est déjà un type d'Nitroinstance.
- Vérifie si l'option d'achat d'instances Spot a été utilisée pour l'instance cible.
- Vérifie si les volumes de stockage d'instance sont attachés à l'instance cible.
- Vérifie que le système d'exploitation (SE) de l'instance cible est Linux.
- Vérifie si l'instance cible fait partie d'un groupe Amazon EC2 Auto Scaling. Si elle fait partie d'un groupe Auto Scaling, l'automatisation vérifie que l'instance est dans l'état standby.
- Vérifie que l'instance est gérée par AWS Systems Manager.

## Test

L'automatisation crée un Amazon Machine Image (AMI) à partir de l'instance cible et lance une instance de test à partir de l'instance nouvellement créée AMI. Cette phase fait uniquement partie du `Clone&Migrate` flux de travail.

Si l'instance de test passe avec succès tous les contrôles d'état, l'automatisation s'interrompt et l'approbation des responsables désignés est demandée via la notification Amazon Simple Notification Service (Amazon SNS). Si l'approbation est fournie, l'automatisation met fin à l'instance de test, arrête l'instance cible et poursuit la migration, tandis que l'instance nouvellement créée AMI est désenregistrée à la fin du flux de travail. `Clone&Migrate`

### Note

Avant de donner votre approbation, nous vous recommandons de vérifier que toutes les applications exécutées sur l'instance cible ont été fermées correctement.

## Cloner et migrer

L'automatisation en crée une autre AMI à partir de l'instance cible et lance une nouvelle instance pour passer à un type d'Nitroinstance. L'automatisation remplit les conditions préalables suivantes avant de poursuivre la migration. Si l'une des vérifications échoue, l'automatisation prend fin. Cette phase ne représente également qu'une partie du `Clone&Migrate` flux de travail.

- Active l'attribut Enhanced Networking (ENA).
- Installe la dernière version des pilotes ENA s'ils ne sont pas déjà installés, ou met à jour la version des pilotes ENA vers la dernière version. Pour garantir des performances réseau optimales, la

mise à jour vers la dernière version du pilote ENA est requise si le type d'Nitroinstance est de 6e génération.

- Vérifie que le module NVMe est installé. Si le module est installé, l'automatisation vérifie que le module est chargé. `initramfs`
- Analyse `/etc/fstab` et remplace les entrées par des noms de blocs d'appareils (`/dev/sd*` ou `/dev/xvd*`) par leurs UUID respectifs. Avant de modifier la configuration, l'automatisation crée une sauvegarde du fichier au niveau du chemin `/etc/fstab*`.
- Désactive la dénomination prévisible des interfaces en ajoutant l'`net.ifnames=0` option à la `GRUB_CMDLINE_LINUX` ligne du `/etc/default/grub` fichier si elle existe, ou au noyau dans `boot/grub/menu.lst`.
- Supprime le `/etc/udev/rules.d/70-persistent-net.rules` fichier s'il existe. Avant de supprimer le fichier, l'automatisation crée une sauvegarde du fichier au niveau du chemin `/etc/udev/rules.d/`.

Après avoir vérifié toutes les exigences, le type d'instance est remplacé Nitro par le type d'instance que vous avez spécifié. L'automatisation attend que l'instance nouvellement créée passe tous les contrôles d'état après avoir démarré en tant que type d'Nitroinstance. L'automatisation attend ensuite l'approbation des responsables désignés pour créer l'une AMI des instances lancées Nitro avec succès. Si l'approbation est refusée, l'automatisation prend fin, laissant l'instance nouvellement créée s'exécuter, et l'instance cible reste arrêtée.

### Remplacer le volume Amazon EBS racine

Si vous choisissez `FullMigration` l'`optionOperationType`, l'automatisation fait migrer l'instance Amazon EC2 cible vers le type d'Nitroinstance que vous spécifiez. L'automatisation demande l'approbation des responsables désignés pour remplacer le volume racine Amazon EBS de l'instance Amazon EC2 cible par le volume racine de l'instance Amazon EC2 clonée. Une fois la migration réussie, l'instance Amazon EC2 clonée est arrêtée. Si l'automatisation échoue, le volume racine Amazon EBS d'origine est attaché à l'instance Amazon EC2 cible. Si le volume Amazon EBS racine attaché à l'instance Amazon EC2 cible comporte des balises auxquelles le `aws:` préfixe est appliqué, l'`FullMigration` opération n'est pas prise en charge.

### Avant de commencer

L'instance cible doit disposer d'un accès Internet sortant. Cela permet d'accéder à des référentiels pour les pilotes et les dépendances tels que `kernel-develgcc`, `patch`, `rpm-build`, `wget`, `dracut` `makelinux-headers`, et. `unzip` Le gestionnaire de packages est utilisé si nécessaire.

Une rubrique Amazon SNS est requise pour envoyer des notifications concernant les approbations et les mises à jour. Pour plus d'informations sur la création d'une rubrique Amazon SNS, consultez la section [Création d'une rubrique Amazon SNS](#) dans le Guide du développeur Amazon Simple Notification Service.

Ce runbook prend en charge les systèmes d'exploitation suivants :

- RHEL7x - 8,5
- Amazon Linux (03/2018), Amazon Linux 2
- Debian Server
- Ubuntu Server 18.04 LTS, 20.04 LTS et 20.10 STR
- SUSE Linux Enterprise Server(SUSE 12 SP5, SUSE 15 SP2)

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- Reconnaissance

Type : String

Description : (Obligatoire) Lisez les détails complets des actions effectuées par ce runbook d'automatisation, puis saisissez-les **Yes, I understand and acknowledge** pour continuer à utiliser le runbook.

- Approver IAM

Type : String

Description : (Obligatoire) Les ARN des rôles, des utilisateurs ou des noms d'utilisateur IAM qui peuvent fournir des approbations à l'automatisation. Vous pouvez spécifier un maximum de 10 approbateurs.

- DeleteResourcesOnFailure

Type : booléen

Description : (Facultatif) Détermine si l'instance nouvellement créée et AMI destinée à la migration sont supprimées en cas d'échec de l'automatisation.

Valeurs valides : Vrai | Faux

Par défaut : VRAI

- MinimumRequiredApprovals

Type : String

Description : (Facultatif) Nombre minimum d'approbations requises pour continuer à exécuter l'automatisation lorsque des approbations sont demandées.

Valeurs valides : 1-10

Par défaut: 1

- NitroInstanceType

Type : String

Description : (Obligatoire) Le type d'Nitroinstance que vous souhaitez remplacer par l'instance. Les types d'instances pris en charge incluent M5, M6, C5, C6, R5, R6 et T3.

Par défaut : m5.xlarge

- **OperationType**

Type : String

Description : (Obligatoire) L'opération que vous souhaitez effectuer. L'`FullMigrationoption` exécute les mêmes tâches que le volume racine de votre instance cible `Clone&Migrate` et le remplace en outre. Le volume racine de l'instance cible est remplacé par le volume racine de l'instance nouvellement créée à la suite du processus de migration. L'opération `FullMigration` ne prend pas en charge les volumes racines définis par Logical Volume Manager (LVM).

Valeurs valides : `Clone&Migrate` | `FullMigration`

- **SNS TopicArn**

Type : String

Description : (Obligatoire) L'ARN de la rubrique Amazon SNS pour la notification d'approbation. La rubrique Amazon SNS est utilisée pour envoyer les notifications d'approbation requises lors de l'automatisation.

- **TargetInstanceid**

Type : String

Description : (Obligatoire) L'ID des instances Amazon EC2 à migrer.

## Flux de travail dans Clone&Migrate

### Autorisations IAM requises

Le paramètre `AutomationAssumeRole` nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

- `startOfPreliminaryChecksBranch`- Branches vers le flux de travail des contrôles préliminaires.
- `getTargetInstanceProperties`- Recueille les détails de l'instance cible.
- `checkIfNitroInstanceTypeIsSupportedInAZ`- Détermine si le type d'instance Amazon EC2 cible est pris en charge dans la même zone de disponibilité que l'instance cible.
- `getXenInstanceTypeInfo`- Recueille des informations sur le type d'instance source.
- `checkIfInstanceHypervisorIsNitroAlready`- Vérifie si l'instance cible est déjà en cours d'exécution en tant que type d'instance Nitro.

- `checkIfTargetInstanceLifecycleIsSpot`- Vérifie si l'option d'achat de l'instance cible est Spot.
- `checkIfOperatingSystemIsLinux`- Vérifie si le système d'exploitation de l'instance cible est Linux.
- `verifySSMConnectivityForTargetInstance`- Vérifie que l'instance cible est gérée par Systems Manager.
- `checkIfEphemeralVolumeAreSupported`- Vérifie si le type d'instance actuel de l'instance cible prend en charge les volumes de stockage d'instance.
- `verifyIfTargetInstanceHasEphemeralVolumesAttached`- Vérifie si des volumes de stockage d'instance sont attachés à l'instance cible.
- `checkIfRootVolumeIsEBS`- Vérifie si le type de volume racine de l'instance cible est EBS.
- `checkIfTargetInstanceIsInASG`- Vérifie si l'instance cible fait partie d'un groupe Auto Scaling.
- `endOfPreliminaryChecksBranch`- Fin de la branche des contrôles préliminaires.
- `startOfTestBranch`- Branches vers le flux de travail de test.
- `createTestImage`- Crée un test AMI de l'instance cible.
- `launchTestInstanceInSameSubnet`- Lance une instance de test à partir du test AMI en utilisant la même configuration que l'instance cible.
- `cleanupTestInstance`- Met fin à l'instance de test.
- `endOfTestBranch`- Fin de la branche Testing.
- `checkIfTestingBranchSucceeded`- Vérifie l'état de la branche Testing.
- `approvalToStopTargetInstance`- Attend l'approbation des responsables désignés pour arrêter l'instance cible.
- `stopTargetEC2Instance`- Arrête l'instance cible.
- `forceStopTargetEC2Instance`- Force arrête l'instance cible uniquement si l'étape précédente ne parvient pas à arrêter l'instance.
- `startOfCloneAndMigrateBranch`- Branches vers le Clone&Migrate flux de travail.
- `createBackupImage`- Crée une instance AMI de l'instance cible pour servir de sauvegarde.
- `launchInstanceInSameSubnet`- Lance une nouvelle instance à partir de la sauvegarde AMI en utilisant la même configuration que l'instance source.
- `waitForClonedInstanceToPassStatusChecks`- Attend que l'instance nouvellement créée passe tous les contrôles de statut.



- `verifySSMConnectivityForClonedInstance`- Vérifie que l'instance nouvellement créée est gérée par Systems Manager.
- `checkAndInstallENADrivers`- Vérifie si les pilotes ENA sont installés sur l'instance nouvellement créée et les installe si nécessaire.
- `checkAndAddNVMeDrivers`- Vérifie si les pilotes NVMe sont installés sur l'instance nouvellement créée et installe les pilotes si nécessaire.
- `checkAndModifyFSTABEntries`- Vérifie si des noms d'appareils sont utilisés `/etc/fstab` et les remplace par des UUID si nécessaire.
- `stopClonedInstance`- Arrête l'instance nouvellement créée.
- `forceStopClonedInstance`- Force arrête l'instance nouvellement créée uniquement si l'étape précédente ne parvient pas à arrêter l'instance.
- `checkENAAttributeForClonedInstance`- Vérifie si l'attribut réseau amélioré est activé pour l'instance nouvellement créée.
- `setNitroInstanceTypeForClonedInstance`- Remplace le type d'instance de l'instance nouvellement créée par le type d'Nitroinstance que vous avez spécifié.
- `startClonedInstance`- Démarre l'instance nouvellement créée dont vous avez modifié le type d'instance.
- `approvalForCreatingImageAfterDriversInstallation`- Si l'instance démarre correctement en tant que type d'Nitroinstance, l'automatisation attend l'approbation des responsables requis. Si l'approbation est fournie, un AMI est créé pour être utilisé comme un GoldenAMI.
- `createImageAfterDriversInstallation`- Crée un objet AMI à utiliser comme un GoldenAMI.
- `endOfCloneAndMigrateBranch`- Extrémité de Clone&Migrate la branche.
- `cleanupTestImage`- Désenregistre le fichier AMI créé pour les tests.
- `failureHandling`- Vérifie si vous avez choisi de mettre fin à des ressources en cas de défaillance.
- `onFailureTerminateClonedInstance`- Met fin à l'instance nouvellement créée en cas d'échec de l'automatisation.
- `onFailurecleanupTestImage`- Désenregistre le fichier AMI créé pour les tests.
- `onFailureApprovalToStartTargetInstance`- Si l'automatisation échoue, attend l'approbation des responsables désignés pour démarrer l'instance cible.

- `onFailureStartTargetInstance`- Si l'automatisation échoue, démarre l'instance cible.

## Flux de travail dans FullMigration

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

Le `FullMigration` flux de travail exécute les mêmes étapes que le `Clone&Migrate` flux de travail et exécute en outre les étapes suivantes :

- `checkConcurrency`- Vérifie qu'il n'existe qu'une seule automatisation de ce runbook ciblant l'instance Amazon EC2 que vous spécifiez. Si le runbook détecte une autre automatisation en cours ciblant la même instance, l'automatisation prend fin.
- `getTargetInstanceProperties`- Recueille les détails de l'instance cible.
- `checkRootVolumeTags`- Détermine si le volume racine de l'instance Amazon EC2 cible contient des balises AWS réservées.
- `cloneTargetInstanceAndMigrateToNitro`- Démarre une automatisation pour enfants à l'aide du `AWS-CloneXenInstanceToNitro` runbook.
- `branchOnTheOperationType`- Branches sur la valeur que vous avez spécifiée pour le `OperationType` paramètre.
- `getClonedInstanceId`- Récupère l'ID de l'instance nouvellement lancée à partir de l'automatisation enfant.
- `checkIfRootVolumeIsBasedOnLVM`- Détermine si la partition racine est gérée par LVM.
- `branchOnTheRootVolumeLVMStatus`- Si les approbations minimales requises sont reçues des principaux opérateurs, l'automatisation procède au remplacement du volume racine.
- `manualInstructionsInCaseOfLVM`- Si le volume racine est géré par LVM, l'automatisation envoie une sortie contenant des instructions sur la façon de remplacer manuellement les volumes racines.
- `startOfReplaceRootEBSVolumeBranch`- Lance le flux de travail de la branche `Replace Root EBS Volume`.

- `checkIfTargetInstanceIsManagedByCFN`- Détermine si l'instance cible est gérée par une AWS CloudFormation pile.
- `branchOnCFNStackStatus`- Branches en fonction de l'état de la CloudFormation pile.
- `approvalForRootVolumesReplacement(WithCFN)`- Si l'instance cible a été lancée par CloudFormation, l'automatisation attend d'être approuvée une fois que l'instance nouvellement lancée a correctement démarré en tant que type d'Nitroinstance. Lorsque les approbations sont fournies, les volumes Amazon EBS de l'instance cible sont remplacés par les volumes racines de l'instance récemment lancée.
- `approvalForRootVolumesReplacement`- Attend l'approbation après le démarrage réussi de l'instance nouvellement lancée en tant que type d'Nitroinstance. Lorsque les approbations sont fournies, les volumes Amazon EBS de l'instance cible sont remplacés par les volumes racines de l'instance récemment lancée.
- `assertIfTargetEC2InstanceIsStillStopped`- Vérifie que l'instance cible est dans un stopped état tel qu'il est avant de remplacer le volume racine.
- `stopTargetInstanceForRootVolumeReplacement`- Si l'instance cible est en cours d'exécution, l'automatisation arrête l'instance avant de remplacer le volume racine.
- `forceStopTargetInstanceForRootVolumeReplacement`- Force arrête l'instance cible en cas d'échec de l'étape précédente.
- `stopClonedInstanceForRootVolumeReplacement`- Arrête l'instance nouvellement créée avant de remplacer les volumes Amazon EBS.
- `forceStopClonedInstanceForRootVolumeReplacement`- Force arrête l'instance nouvellement créée si l'étape précédente échoue.
- `getBlockDeviceMappings`- Récupère les mappages des périphériques en mode bloc à la fois pour la cible et pour les instances nouvellement créées.
- `replaceRootEbsVolumes`- Remplace le volume racine de l'instance cible par le volume racine de l'instance nouvellement créée.
- `EndOfReplaceRootEBSVolumeBranch`- Fin du flux de travail de la branche Replace Root EBS Volume.
- `checkENAAttributeForTargetInstance`- Vérifie si l'attribut de mise en réseau améliorée (ENA) est activé pour l'instance Amazon EC2 cible.
- `enableENAAttributeForTargetInstance`- Active l'attribut ENA pour l'instance Amazon EC2 cible si nécessaire.
- `setNitroInstanceTypeForTargetInstance`- Remplace l'instance cible par le type d'Nitroinstance que vous avez spécifié.

- `replicateRootVolumeTags`- Réplique les balises sur le volume Amazon EBS racine à partir de l'instance Amazon EC2 cible.
- `startTargetInstance`- Démarre l'instance Amazon EC2 cible après avoir modifié le type d'instance.
- `onFailureStopTargetEC2Instance`- Arrête l'instance Amazon EC2 cible si elle ne démarre pas en tant que type d'Nitroinstance.
- `onFailureForceStopTargetEC2Instance`- Force l'arrêt de l'instance Amazon EC2 cible en cas d'échec de l'étape précédente.
- `OnFailureRevertOriginalInstanceType`- Rétablit le type d'instance d'origine de l'instance Amazon EC2 cible si l'instance cible ne démarre pas en tant que type d'Nitroinstance.
- `onFailureRollbackRootVolumeReplacement`- Annule toutes les modifications apportées par l'`replaceRootEbsVolumes` étape si nécessaire.
- `onFailureApprovalToStartTargetInstance`- Attend l'approbation du principal désigné pour démarrer l'instance Amazon EC2 cible après avoir annulé les modifications précédentes.
- `onFailureStartTargetInstance`- Démarre l'instance Amazon EC2 cible.
- `terminateClonedEC2Instance`- Met fin à l'instance Amazon EC2 clonée après avoir remplacé le volume Amazon EBS racine.

## AWSSupport-ResetAccess

### Description

Ce runbook utilisera l'outil EC2Rescue sur l'instance EC2 spécifiée pour réactiver le déchiffrement des mots de passe à l'aide de la console EC2 (Windows) ou pour générer et ajouter une nouvelle paire de clés SSH (Linux). Si vous avez oublié votre paire de clés, cette automatisation créera un mot de passe IAM que vous pourrez utiliser pour lancer une nouvelle instance EC2 avec une paire de clés qui vous appartient (Windows).

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- EC2 RescueInstanceType

Type : String

Valeurs valides : t2.small | t2.medium | t2.large

Par défaut : t2.small

Description : (Obligatoire) type d'instance EC2 pour l'instance EC2Rescue. Taille recommandée : t2.small.

- Instanceld

Type : String

Description : (Obligatoire) ID de l'instance EC2 pour laquelle vous souhaitez réinitialiser l'accès.

### Important


Systems Manager Automation arrête cette instance et crée une AMI avant de tenter toute opération. Les données stockées sur les volumes de stockage d'instance seront perdues. L'adresse IP publique change si vous n'utilisez pas une adresse IP Elastic.

- SubnetId

Type : String

Par défaut : CreateNew VPC

Description : (Facultatif) ID de sous-réseau pour l'instance EC2Rescue. Par défaut, Systems Manager Automation crée un nouveau VPC. Vous pouvez également SelectedInstanceSubnet utiliser le même sous-réseau que votre instance ou spécifier un ID de sous-réseau personnalisé.

 Important

Le sous-réseau doit se trouver dans la même zone de disponibilité que les points de InstanceId terminaison SSM et doit autoriser l'accès à ces derniers.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Vous devez avoir au moins ssm : StartAutomationExecution, ssm : GetParameter (pour récupérer le nom du paramètre clé SSH) et ssm : GetAutomationExecution pour pouvoir lire la sortie de l'automatisation. Pour plus d'informations sur les autorisations requises, consultez [AWSSupport-StartEC2RescueWorkflow](#).

## Étapes de document

1. aws:assertAwsResourceProperty- Affirme si l'instance fournie est Windows.
  - a. (EC2Rescue pour Windows) Si l'instance fournie est Windows :
    - i. aws:executeAutomation- Appelez AWSSupport-StartEC2RescueWorkflow avec le script de réinitialisation du mot de passe hors ligne EC2Rescue pour Windows
    - ii. aws:executeAwsApi- Récupérez l'ID AMI de sauvegarde depuis l'automatisation imbriquée
    - iii. aws:executeAwsApi- Récupérez l'ID AMI activé par mot de passe à partir de l'automatisation imbriquée
    - iv. aws:executeAwsApi- Récupérez le résumé d'EC2Rescue à partir de l'automatisation imbriquée
  - b. (EC2Rescue pour Linux) Si l'instance fournie est Linux :
    - i. aws:executeAutomation- Appelez AWSSupport-StartEC2RescueWorkflow avec le script d'injection de clé SSH hors ligne EC2Rescue pour Linux
    - ii. aws:executeAwsApi- Récupérez l'ID AMI de sauvegarde depuis l'automatisation imbriquée
    - iii. aws:executeAwsApi- Récupère le nom du paramètre SSM pour la clé SSH injectée

#### iv. `aws:executeAwsApi`- Récupérez le résumé d'EC2Rescue à partir de l'automatisation imbriquée

##### Sorties

`GetEC2RescueForWindowsResult`. Sortie

`getWindowsBackupAmi`. `ImageId`

`getWindowsPasswordEnabledAmi`. `ImageId`

`GetEC2RescueForLinuxResult`. Sortie

`getLinuxBackupAmi`. `ImageId`

`GetLinuxSSH`. `Nom KeyParameter`

## **AWSSupport-ResetLinuxUserPassword**

### Description

Le `AWSSupport-ResetLinuxUserPassword` runbook vous permet de réinitialiser le mot de passe d'un utilisateur du système d'exploitation (SE) local. Ce runbook est particulièrement utile pour les utilisateurs qui ont besoin d'accéder à leurs instances Amazon Elastic Compute Cloud (Amazon EC2) à l'aide de la console série. Le runbook crée une instance Amazon EC2 temporaire dans votre rôle Compte AWS et dans un rôle AWS Identity and Access Management (IAM) avec les autorisations nécessaires pour récupérer une valeur AWS Secrets Manager secrète contenant le mot de passe.

Le runbook arrête votre instance Amazon EC2 cible, détache le volume racine Amazon Elastic Block Store (Amazon EBS) et l'attache à l'instance Amazon EC2 temporaire. À l'aide de la commande `Exécuter la commande`, un script s'exécute sur l'instance temporaire pour définir le mot de passe de l'utilisateur du système d'exploitation que vous spécifiez. Le volume Amazon EBS racine est ensuite rattaché à votre instance cible. Le runbook fournit également une option permettant de créer un instantané du volume racine au début de l'automatisation.

### Avant de commencer

Créez un secret Secrets Manager avec la valeur du mot de passe que vous souhaitez attribuer à l'utilisateur de votre système d'exploitation. La valeur doit être en texte brut. Pour plus d'informations,



consultez [Créer un secret AWS Secrets Manager](#) dans le Guide de l'utilisateur AWS Secrets Manager.

## Considérations

- Nous vous recommandons de sauvegarder votre instance avant d'utiliser ce runbook. Envisagez de définir la valeur du `CreateSnapshot` paramètre comme **Yes**.
- Pour modifier le mot de passe de l'utilisateur local, le runbook doit arrêter votre instance. Lorsqu'une instance est arrêtée, toutes les données stockées en mémoire ou sur les volumes de stockage de l'instance sont perdues. De plus, toutes les adresses IPv4 publiques attribuées automatiquement sont publiées. Pour plus d'informations sur ce qui se passe lorsque vous arrêtez une instance, consultez [Arrêter et démarrer votre instance](#) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.
- Si les volumes Amazon EBS attachés à votre instance Amazon EC2 cible sont chiffrés à l'aide d'une clé gérée par le client AWS Key Management Service (AWS KMS), assurez-vous que cette AWS KMS clé ne l'est pas, de `Leted disabled` sinon votre instance ne démarrera pas.

## [Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux

Paramètres

- `AutomationAssumeRole`

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre

nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance Linux Amazon EC2 qui contient le mot de passe utilisateur du système d'exploitation que vous souhaitez réinitialiser.

- LinuxUserName

Type : String

Par défaut : ec2-user

Description : (Facultatif) Le compte utilisateur du système d'exploitation dont vous souhaitez réinitialiser le mot de passe.

- SecretArn

Type : String

Description : (Obligatoire) L'ARN du secret de votre gestionnaire de secrets contenant le nouveau mot de passe.

- SecurityGroupId

Type : String

Description : (Facultatif) L'ID du groupe de sécurité à associer à l'instance temporaire d'Amazon EC2. Si vous ne fournissez aucune valeur pour ce paramètre, le groupe de sécurité Amazon Virtual Private Cloud (Amazon VPC) par défaut est utilisé.

- SubnetId

Type : String

Description : (Facultatif) L'ID du sous-réseau dans lequel vous souhaitez lancer l'instance temporaire Amazon EC2. Par défaut, l'automatisation choisit le même sous-réseau que votre instance cible. Si vous choisissez de fournir un sous-réseau différent, celui-ci doit se trouver dans la même zone de disponibilité que l'instance cible et avoir accès aux points de terminaison de Systems Manager.

- CreateSnapshot

Type : String

Valeurs valides : Oui | Non

Par défaut : Oui

Description : (Facultatif) Détermine si un instantané du volume racine de votre instance Amazon EC2 cible est créé avant l'exécution de l'automatisation.

- StopConsent

Type : String

Valeurs valides : Oui | Non

Par défaut : Non

Description : Entrez **Yes** pour confirmer que votre instance Amazon EC2 cible sera arrêtée au cours de cette automatisation. Lorsque l'instance Amazon EC2 est arrêtée, toutes les données stockées dans la mémoire ou dans les volumes de stockage de l'instance sont perdues et l'adresse IPv4 publique automatique est libérée. Pour plus d'informations, veuillez consulter [Arrêt et démarrage de votre instance](#) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:DescribeInstanceInformation
- ssm:ListTagsForResource
- ssm:SendCommand
- ec2:AttachVolume
- ec2:CreateSnapshot
- ec2:CreateSnapshots
- ec2:CreateVolume
- ec2:DescribeImages
- ec2:DescribeInstances

- `ec2:DescribeInstanceStatus`
- `ec2:DescribeSnapshotAttribute`
- `ec2:DescribeSnapshots`
- `ec2:DescribeSnapshotTierStatus`
- `ec2:DescribeVolumes`
- `ec2:DescribeVolumeStatus`
- `ec2:DetachVolume`
- `ec2:RunInstances`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `ec2:TerminateInstances`
- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation>ListStacks`
- `logs:CreateLogDelivery`
- `logs:CreateLogGroup`
- `logs>DeleteLogDelivery`
- `logs>DeleteLogGroup`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:PutLogEvents`

## Étapes de document

1. `aws:branch`— Branches selon que vous avez ou non donné votre consentement à l'arrêt de l'instance Amazon EC2 cible.
2. `aws:assertAwsResourcePropertyGarantit` que l'état de l'instance Amazon EC2 est dans un `stopped` état `running` ou. Dans le cas contraire, l'automatisation prend fin.

3. `aws:executeAwsApi` Obtient les propriétés de l'instance Amazon EC2.
4. `aws:executeAwsApi` Obtient les propriétés du volume racine.
5. `aws:branch` Branche l'automatisation selon qu'un ID de sous-réseau a été fourni ou non pour l'instance temporaire Amazon EC2.
6. `aws:assertAwsResourceProperty` Garantit que le sous-réseau que vous spécifiez dans le `SubnetId` paramètre se trouve dans la même zone de disponibilité que l'instance Amazon EC2 cible.
7. `aws:assertAwsResourceProperty` Garantit que le volume racine de l'instance Amazon EC2 cible est un volume Amazon EBS.
8. `aws:assertAwsResourceProperty` Garantit que l'architecture de l'instance Amazon EC2 est `arm64` ou `x86_64`.
9. `aws:assertAwsResourceProperty` Garantit que le comportement d'arrêt de l'instance Amazon EC2 l'est `stop` ou `nonterminate`.
10. `aws:branch` Garantit que l'instance Amazon EC2 n'est pas une instance Spot. Dans le cas contraire, l'automatisation prend fin.
11. `aws:executeScript` Garantit que l'instance Amazon EC2 ne fait pas partie d'un groupe de mise à l'échelle automatique. Si l'instance fait partie d'un groupe de dimensionnement automatique, l'automatisation confirme que l'instance Amazon EC2 est dans un état de `Standby` cycle de vie.
12. `aws:createStack` Crée une instance Amazon EC2 temporaire qui est utilisée pour réinitialiser le mot de passe de l'utilisateur du système d'exploitation que vous spécifiez.
13. `aws:waitForAwsResourceProperty` Attend que l'instance temporaire Amazon EC2 récemment lancée soit en cours d'exécution.
14. `aws:executeAwsApi` Obtient l'ID de l'instance Amazon EC2 temporaire.
15. `aws:waitForAwsResourceProperty` Attend que l'instance temporaire Amazon EC2 génère un rapport tel que géré par Systems Manager.
16. `aws:changeInstanceState` Arrête l'instance Amazon EC2 cible.
17. `aws:changeInstanceStateForce` Force l'instance Amazon EC2 cible à s'arrêter au cas où elle serait bloquée dans un état d'arrêt.
18. `aws:branch` Branche l'automatisation selon qu'un instantané du volume racine de l'instance Amazon EC2 cible a été demandé ou non.
19. `aws:executeAwsApi` Crée un instantané du volume Amazon EBS racine de l'instance Amazon EC2 cible.

- 20 `aws:waitForAwsResourceProperty` Attend que l'instantané soit dans un `completed` état.
- 21 `aws:executeAwsApi` Détache le volume racine Amazon EBS de l'instance Amazon EC2 cible.
- 22 `aws:waitForAwsResourceProperty` Attend que le volume racine Amazon EBS soit détaché de l'instance Amazon EC2 cible.
- 23 `aws:executeAwsApi` Associe le volume Amazon EBS racine à l'instance Amazon EC2 temporaire.
- 24 `aws:waitForAwsResourceProperty` Attend que le volume racine Amazon EBS soit associé à l'instance Amazon EC2 temporaire.
- 25 `aws:runCommand` Réinitialise le mot de passe de l'utilisateur cible en exécutant un script shell à l'aide de `Run Command` sur l'instance temporaire Amazon EC2.
- 26 `aws:executeAwsApi` Détache le volume racine Amazon EBS de l'instance temporaire Amazon EC2.
- 27 `aws:waitForAwsResourceProperty` Attend que le volume racine Amazon EBS soit détaché de l'instance Amazon EC2 temporaire.
- 28 `aws:executeAwsApi` Détache le volume racine Amazon EBS de l'instance temporaire Amazon EC2 après une erreur.
- 29 `aws:waitForAwsResourceProperty` Attend que le volume racine Amazon EBS soit détaché de l'instance temporaire Amazon EC2 suite à une erreur.
- 30 `aws:branch` Branche l'automatisation selon qu'un instantané du volume racine a été demandé ou non pour déterminer le chemin de restauration en cas d'erreur.
- 31 `aws:executeAwsApi` Rattache le volume Amazon EBS racine à l'instance Amazon EC2 cible.
- 32 `aws:waitForAwsResourceProperty` Attend que le volume racine Amazon EBS soit associé à l'instance Amazon EC2.
- 33 `aws:executeAwsApi` Crée un nouveau volume Amazon EBS à partir de l'instantané du volume racine de l'instance Amazon EC2 cible.
- 34 `aws:waitForAwsResourceProperty` Attend que le nouveau volume Amazon EBS soit dans un `available` état défini.
- 35 `aws:executeAwsApi` Associe le nouveau volume Amazon EBS à l'instance cible en tant que volume racine.
- 36 `aws:waitForAwsResourceProperty` Attend que le volume Amazon EBS soit dans un `attached` état.
- 37 `aws:executeAwsApi` Décrit les événements de la AWS CloudFormation pile si les runbooks ne parviennent pas à créer ou à mettre à jour la AWS CloudFormation pile.

38. `aws:branch` Branche l'automatisation en fonction de l'état précédent de l'instance Amazon EC2. Si l'état était le cas `running`, l'instance est démarrée. S'il était en `stopped` état, l'automatisation se poursuit.
39. `aws:changeInstanceState` Démarre l'instance Amazon EC2 si nécessaire.
40. `aws:waitForAwsResourceProperty` Attend que la AWS CloudFormation pile passe à l'état de terminal avant de la supprimer.
41. `aws:executeAwsApi` Supprime la AWS CloudFormation pile, y compris l'instance temporaire Amazon EC2.

## AWSPremiumSupport-ResizeNitroInstance

### Description

Le `AWSPremiumSupport-ResizeNitroInstance` runbook fournit une solution automatisée pour redimensionner les instances Amazon Elastic Compute Cloud (Amazon EC2) créées sur le système Nitro.

Pour réduire le risque potentiel de perte de données et d'interruption de service, le runbook vérifie les points suivants :

- Comportement d'arrêt de l'instance.
- Si l'instance fait partie d'un groupe Amazon EC2 Auto Scaling, et en `standby` mode.
- État de l'instance et location.
- Le type d'instance que vous souhaitez modifier prend en charge le nombre d'interfaces réseau actuellement attachées à votre instance.
- L'architecture du processeur et le type de virtualisation du type d'instance actuel et du type d'instance cible sont identiques.
- Si l'instance est en cours d'exécution, elle passe avec succès tous les contrôles d'état.
- Le type d'instance vers lequel vous souhaitez passer est disponible dans la même zone de disponibilité.

Si Amazon EC2 ne passe pas les contrôles d'état après avoir modifié le type d'instance, le runbook revient automatiquement au type d'instance précédent.

Par défaut, ce runbook ne changera pas le type d'instance s'il est en cours d'exécution et si des volumes de stockage d'instance sont attachés. Le runbook ne changera pas non plus le type

d'instance si l'instance fait partie d'une AWS CloudFormation pile. Si vous souhaitez modifier l'un de ces comportements, spécifiez yes les `AllowCloudFormationInstances` paramètres `AllowInstanceStoreInstances` et.

Le runbook propose deux méthodes différentes pour spécifier le type d'instance que vous souhaitez modifier :

- Pour les automatisations simples ciblant une seule instance, spécifiez le type d'instance que vous souhaitez modifier à l'aide du `TargetInstanceTypeFromParameter` paramètre.
- Pour exécuter des automatisations à grande échelle afin de modifier le type d'instance de plusieurs instances, spécifiez le type d'instance à l'aide du `TargetInstanceTypeFromTagValue` paramètre. Pour plus d'informations sur l'exécution d'automatisations à grande échelle, voir [Exécuter des automatisations à grande échelle](#).

Si vous ne spécifiez aucune valeur pour aucun des paramètres, l'automatisation échoue.

#### Important

L'accès aux `AWSPremiumSupport-*` runbooks nécessite un abonnement Enterprise ou Business Support. Pour plus d'informations, consultez la section [Comparer AWS Support les plans](#).

## Considérations

- Nous vous recommandons de sauvegarder votre instance avant d'utiliser ce runbook.
- Pour plus d'informations sur la compatibilité pour la modification des types d'instance, consultez la section [Compatibilité pour la modification du type d'instance](#).
- Si l'automatisation échoue et revient au type d'instance d'origine, voir [Résolution des problèmes liés à la modification du type d'instance](#).
- Pour modifier le type d'instance, le runbook doit arrêter votre instance. Lorsqu'une instance est arrêtée, toutes les données stockées en mémoire ou sur les volumes de stockage de l'instance sont perdues. De plus, toutes les adresses IPv4 publiques attribuées automatiquement sont publiées. Pour plus d'informations sur ce qui se passe lorsque vous arrêtez une instance, consultez [Arrêter et démarrer votre instance](#).
- À l'aide de `SkipInstancesWithTagKey` ce paramètre, vous pouvez ignorer les instances auxquelles une clé de balise Amazon EC2 spécifique est appliquée.



[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- Reconnaître

Type : String

Description : (Obligatoire) Entrez **yes** pour confirmer que votre instance sera arrêtée si elle est en cours d'exécution.

- AllowInstanceStoreInstances

Type : String

Valeurs valides : non | oui

Par défaut : non

Description : (Facultatif) Si vous le spécifiez **yes**, vous autorisez le runbook à s'exécuter sur des instances auxquelles des volumes de stockage d'instance sont attachés.

- AllowCloudFormationInstances

Type : String

Valeurs valides : non | oui

Par défaut : non

Description : (Facultatif) Si vous le spécifiez, le runbook s'exécute sur des instances faisant partie d'une AWS CloudFormation pile.

- DryRun

Type : String

Valeurs valides : non | oui

Par défaut : non

Description : (Facultatif) Si vous le spécifiez, le runbook valide les exigences de redimensionnement sans modifier le type d'instance.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance Amazon EC2 dont vous souhaitez modifier le type.

- SkipInstancesWithTagKey

Type : String

Description : (Facultatif) L'automatisation ignore une instance cible si la clé de balise que vous spécifiez est appliquée à l'instance.

- SleepTime

Type : String

Par défaut : 3

Description : (Facultatif) Le nombre de secondes pendant lesquelles ce runbook doit rester en veille une fois terminé.

- TagInstance

Type : String

Description : (Facultatif) Marquez les instances avec la clé et la valeur de votre choix en utilisant le format suivant : *Clé=ChangingType, Valeur=True*. Cette option vous permet de suivre les instances qui ont été ciblées par ce runbook. Les clés et valeurs de balise sont sensibles à la casse.

- TargetInstanceTypeFromParameter

Type : String

Description : (Facultatif) Le type d'instance vers lequel vous souhaitez modifier votre instance. Laissez ce paramètre vide si vous souhaitez utiliser la valeur de la clé de balise fournie dans le TargetInstanceTypeFromTagValue paramètre.

- TargetInstanceTypeFromTagValue

Type : String

Description : (Facultatif) La clé de balise appliquée à vos instances cibles dont la valeur contient le type d'instance vers lequel vous souhaitez passer. Si vous spécifiez une valeur pour le TargetInstanceTypeFromParameter paramètre, elle remplace toute valeur que vous avez spécifiée pour ce paramètre.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

1. `aws:assertAwsResourceProperty`: garantit que l'instance Amazon EC2 n'est pas balisée avec la clé de balise de ressource spécifiée dans le `SkipInstancesWithTagKey` paramètre. Si la clé de balise est trouvée appliquée à l'instance, l'étape échoue et l'automatisation prend fin.
2. `aws:assertAwsResourceProperty`: confirme que l'état de l'instance Amazon EC2 cible `estrunning`, `pendingstopped`, ou `stopping`. Dans le cas contraire, l'automatisation prend fin.
3. `aws:executeAwsApi`: rassemble les propriétés de l'instance Amazon EC2.
4. `aws:executeAwsApi`: recueille des informations sur le type d'instance Amazon EC2 actuel.
5. `aws:branch`: vérifie si le type d'instance actuel et le type d'instance spécifié dans le `TargetInstanceTypeFromParameter` paramètre sont identiques. Si tel est le cas, l'automatisation prend fin.
6. `aws:assertAwsResourceProperty`: vérifie que l'instance s'exécute sur le système Nitro.
7. `aws:branch`: garantit que le type de volume racine de l'instance Amazon EC2 est un volume Amazon Elastic Block Store (Amazon EBS).
8. `aws:assertAwsResourceProperty`: confirme que le comportement d'arrêt de l'instance est `stop` ou `nonterminate`.
9. `aws:branch`: garantit que l'instance Amazon EC2 n'est pas une instance Spot.
10. `aws:branch`: garantit que la location de l'instance Amazon EC2 est celle par défaut et qu'il ne s'agit pas d'un hôte dédié ou d'une instance dédiée.
11. `aws:executeScript`: confirme qu'il n'existe qu'une seule automatisation de ce runbook ciblant l'ID d'instance actuel. Si une autre automatisation est déjà en cours et cible la même instance, elle renvoie une erreur et se termine.
12. `aws:branch`: Branche l'automatisation en fonction de l'état de l'instance Amazon EC2.
  - a. Si tel `stopped` est le cas `stopping`, l'automatisation s'exécute `aws:waitForAwsResourceProperty` jusqu'à l'arrêt complet de l'instance Amazon EC2.
  - b. Si tel `running` est le cas `pending`, l'automatisation s'exécute `aws:waitForAwsResourceProperty` jusqu'à ce que l'instance Amazon EC2 passe les contrôles de statut.

- 13 `aws:assertAwsResourceProperty`: confirme que l'instance Amazon EC2 ne fait pas partie d'un groupe Auto Scaling en appelant l'opération `DescribeAutoScalingInstances` d'API. Si l'instance fait partie d'un groupe Auto Scaling, assurez-vous que l'instance Amazon EC2 est en standby mode.
- 14 `aws:branch`: Branche l'automatisation selon que vous souhaitez que l'automatisation vérifie si l'instance Amazon EC2 fait partie d'une AWS CloudFormation pile :
- `aws:executeScript` Assurez-vous que l'instance Amazon EC2 ne fait pas partie d'une AWS CloudFormation pile en appelant l'opération `DescribeStackResources` d'API.
- 15 `aws:executeAwsApi`: renvoie une liste de types d'instances ayant le même type d'architecture de processeur et de virtualisation, et qui prennent en charge le nombre d'interfaces réseau actuellement attachées à l'instance cible.
- 16 `aws:executeAwsApi`: obtient la valeur du type d'instance cible à partir de la clé de balise spécifiée dans le `TargetInstanceTypeFromTagValue` paramètre.
- 17 `aws:executeScript`: confirme que les types d'instances actuels et cibles sont compatibles. Garantit que le type d'instance cible est disponible dans le même sous-réseau. Vérifie que le principal qui a lancé le runbook est autorisé à modifier le type d'instance et à arrêter et démarrer l'instance si elle était en cours d'exécution.
- 18 `aws:branch`: Branche l'automatisation selon que la valeur du `DryRun` paramètre est définie ou non sur yes. Si c'est le cas yes, l'automatisation prend fin.
- 19 `aws:branch`: vérifie si le type d'instance d'origine et le type d'instance cible sont identiques. S'ils sont identiques, l'automatisation prend fin.
- 20 `aws:executeAwsApi`: obtient l'état actuel de l'instance.
- 21 `aws:changeInstanceState`: arrête l'instance Amazon EC2.
- 22 `aws:changeInstanceState`: force l'instance à s'arrêter si elle est bloquée dans stopping cet état.
- 23 `aws:executeAwsApi`: remplace le type d'instance par le type d'instance cible.
- 24 `aws:sleep`: attend 3 secondes après avoir modifié le type d'instance pour une éventuelle cohérence.
- 25 `aws:branch`: Branche l'automatisation en fonction de l'état précédent de l'instance. Si tel est le cas `running`, l'instance est démarrée.
- `aws:changeInstanceState`: démarre l'instance Amazon EC2 si elle était en cours d'exécution avant de modifier le type d'instance.

- b. `aws:waitForAwsResourceProperty`: attend que l'instance Amazon EC2 passe les contrôles de statut. Si l'instance ne passe pas les contrôles d'état, elle revient à son type d'instance d'origine.
  - i. `aws:changeInstanceState`: arrête l'instance Amazon EC2 avant de la remplacer par son type d'instance d'origine.
  - ii. `aws:changeInstanceState`: force l'instance Amazon EC2 à s'arrêter avant de la remplacer par son type d'instance d'origine au cas où elle resterait bloquée dans un état d'arrêt.
  - iii. `aws:executeAwsApi`: rétablit le type d'origine de l'instance Amazon EC2.
  - iv. `aws:sleep`: attend 3 secondes après avoir modifié le type d'instance pour une éventuelle cohérence.
  - v. `aws:changeInstanceState`: démarre l'instance Amazon EC2 si elle était en cours d'exécution avant de modifier le type d'instance.
  - vi. `aws:waitForAwsResourceProperty`: attend que l'instance Amazon EC2 passe les contrôles de statut.

26 `aws:sleep`: Attend avant de terminer le runbook.

## AWSSupport-RestoreEC2InstanceFromSnapshot

### Description

Le `AWSSupport-RestoreEC2InstanceFromSnapshot` runbook vous aide à identifier et à restaurer une instance Amazon Elastic Compute Cloud (Amazon EC2) à partir d'un instantané Amazon Elastic Block Store (Amazon EBS) fonctionnel du volume racine.

[Exécutez cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- EndDate

Type : String

Description : (Facultatif) La dernière date à laquelle vous souhaitez que l'automatisation recherche un instantané.

- InplaceSwap

Type : booléen

Valeurs valides : true | false

Description : (Facultatif) Si la valeur de ce paramètre est définie sur `true`, le volume nouvellement créé à partir du snapshot remplace le volume racine existant attaché à votre instance.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance que vous souhaitez restaurer à partir d'un instantané.

- LookForInstanceStatusCheck

Type : booléen

Valeurs valides : true | false

Valeur par défaut : true

Description : (Facultatif) Si la valeur de ce paramètre est définie sur `true`, l'automatisation vérifie si les vérifications de l'état des instances échouent sur les instances de test lancées à partir des instantanés.

- SkipSnapshotsBy

Type : String

Description : (Facultatif) Intervalle auquel les instantanés sont ignorés lorsque vous recherchez des instantanés pour restaurer votre instance. Par exemple, si 100 instantanés sont disponibles et que vous spécifiez une valeur de 2 pour ce paramètre, un instantané sur trois est examiné.

Par défaut : 0

- SnapshotId

Type : String

Description : (Facultatif) L'ID d'un instantané à partir duquel vous souhaitez restaurer l'instance.

- StartDate

Type : String

Description : (Facultatif) La première date à laquelle vous souhaitez que l'automatisation recherche un instantané.

- TotalSnapshotsToLook

Type : String

Description : (Facultatif) Nombre d'instantanés examinés par l'automatisation.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

1. `aws:executeAwsApi`- Recueille des informations sur l'instance cible.
2. `aws:assertAwsResourceProperty`- Vérifie que l'instance cible existe.
3. `aws:assertAwsResourceProperty`- Vérifie que le volume racine est un volume Amazon EBS.
4. `aws:assertAwsResourceProperty`- Vérifie qu'aucune autre automatisation n'est déjà en cours d'exécution pour cibler cette instance.
5. `aws:executeAwsApi`- Marque l'instance cible.
6. `aws:executeAwsApi`- Crée une AMI de l'instance.
7. `aws:executeAwsApi`- Recueille des détails sur ce qui AMI a été créé à l'étape précédente.
8. `aws:waitForAwsResourceProperty`- Attend que l'AMI État le devienne disponible avant de continuer.
9. `aws:executeScript`- Lance une nouvelle instance à partir de celle qui vient d'être créée AMI.
10. `aws:assertAwsResourceProperty`- Vérifie que l'état de l'instance est disponible.
11. `aws:executeAwsApi`- Recueille des informations sur l'instance récemment lancée.
12. `aws:branch`- Branches selon que vous avez fourni ou non une valeur pour le `SnapshotId` paramètre.

- 13 `aws:executeScript`- Renvoie une liste d'instantanés au cours de la période spécifiée.
- 14 `aws:executeAwsApi`- Arrête l'instance.
- 15 `aws:waitForAwsResourceProperty`- Attend que l'état du volume soit atteint. `available`
- 16 `aws:waitForAwsResourceProperty`- Attend que l'état de l'instance soit atteint. `stopped`
- 17 `aws:executeAwsApi`- Détache le volume racine.
- 18 `aws:waitForAwsResourceProperty`- Attend que le volume racinaire se détache.
- 19 `aws:executeAwsApi`- Attache le nouveau volume de racine.
- 20 `aws:waitForAwsResourceProperty`- Attend que le nouveau volume soit attaché.
- 21 `aws:executeAwsApi`- Démarre l'instance.
- 22 `aws:waitForAwsResourceProperty`- Attend que l'état de l'instance soit atteint. `available`
- 23 `aws:waitForAwsResourceProperty`- Attend que les contrôles d'état du système et de l'instance soient réussis pour l'instance.
- 24 `aws:executeScript`- Exécute un script pour trouver un instantané qui peut être utilisé pour créer un volume avec succès.
- 25 `aws:executeScript`- Exécute un script pour récupérer l'instance en utilisant le volume nouvellement créé à partir de l'instantané identifié par l'automatisation, ou en utilisant le volume créé à partir de l'instantané que vous avez spécifié dans le `SnapshotId` paramètre.
- 26 `aws:executeScript`- Supprime les ressources créées par l'automatisation.

## Sorties

`launchCloneInstance.InstanceIds`

`ListSnapshotByDate`. Instantanés finaux

`ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange`

`findWorkingSnapshot`. Instantané de travail

`InstanceRecovery`. résultat

## **AWSsupport - SendLogBundleToS3Bucket**

### Description

Le `AWSsupport - SendLogBundleToS3Bucket` runbook télécharge un bundle de journaux généré par l'outil `EC2Rescue` depuis l'instance cible vers le compartiment S3 spécifié. Le runbook installe

la version spécifique à la plate-forme d'EC2Rescue en fonction de la plate-forme de l'instance cible. EC2Rescue est ensuite utilisé pour collecter tous les journaux de système d'exploitation (SE).

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux, macOS, Windows

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) ID de l'instance gérée Windows ou Linux à partir de laquelle vous souhaitez collecter les journaux.

- S3 BucketName

Type : String

Description : (Obligatoire) compartiment S3 dans lequel charger les journaux.

- S3Path

Type : String

Par défaut : `AWSSupport-SendLogBundleToS3Bucket/`

Description : (Facultatif) chemin S3 des journaux collectés.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Il est recommandé que l'instance EC2 recevant la commande dispose d'un rôle IAM auquel est associée la politique gérée par `ManagedInstanceCore` Amazon d'AmazonSSM. L'utilisateur doit avoir au moins `ssm : StartAutomationExecution` et `ssm : SendCommand` pour exécuter l'automatisation et envoyer la commande à l'instance, plus `ssm : GetAutomationExecution` pour pouvoir lire la sortie de l'automatisation.

## Étapes de document

1. `aws:runCommand`- Installez EC2Rescue via. `AWS-ConfigureAWSPackage`
2. `aws:runCommand`- Exécutez le PowerShell script pour collecter les journaux de dépannage de Windows avec EC2Rescue.
3. `aws:runCommand`- Exécutez le script bash pour collecter les journaux de dépannage de Linux avec EC2Rescue.

## Sorties

`collectAndUploadWindowsLogBundle`. Sortie

`collectAndUploadLinuxLogBundle`. Sortie

## **AWSsupport-StartEC2RescueWorkflow**

### Description

Le `AWSsupport-StartEC2RescueWorkflow` runbook exécute le script encodé en base64 fourni (Bash ou Powershell) sur une instance d'assistance créée pour sauver votre instance. Le volume racine de votre instance est attaché et monté sur l'instance d'assistant, également connu sous le nom d'instance EC2Rescue. Si votre instance est basée sur Windows, fournissez un script Powershell. Dans le cas contraire, utilisez Bash. Le runbook définit certaines variables d'environnement que vous pouvez utiliser dans votre script. Les variables d'environnement contiennent des informations sur l'entrée que vous avez fournie, ainsi que des informations sur le volume racine hors connexion. Le

volume hors connexion est déjà monté et prêt à être utilisé. Par exemple, vous pouvez enregistrer un fichier Desired State Configuration dans un volume racine Windows hors connexion ou exécuter une commande chroot pour un volume racine Linux hors connexion et effectuer une correction hors connexion.

### [Exécutez cette automatisation \(console\)](#)

#### Important

Les instances Amazon EC2 créées à partir des AMI (Amazon Machine Images) de Marketplace ne sont pas prises en charge par cette automatisation.

### Informations supplémentaires

Pour coder un script en base64, vous pouvez utiliser Powershell ou Bash. PowerShell :

```
[System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes([System.IO.File]::ReadAllText("path_to_file.txt")))
```

Bash :

```
base64 PATH_TO_FILE
```

Voici une liste des variables d'environnement que vous pouvez utiliser dans vos scripts hors connexion, en fonction du système d'exploitation cible

Windows :

Variable	Description	Exemple de valeur
\$env:EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
\$env:EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
\$env:EC2RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
\$env:EC2RESCUE_EC2_RW_DIR	Chemin d'installation d'EC2Rescue pour Windows	C:\Program Files\Amazon\EC2Rescue

Variable	Description	Exemple de valeur
\$env:EC2RESCUE_EC2RW_DIR	Chemin d'installation d'EC2Rescue pour Windows	C:\Program Files\Amazon\EC2Rescue
\$env:EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
\$env:EC2RESCUE_OFFLINE_CURRENT_CONTROL_SET	Chemin de l'ensemble de contrôles Windows hors connexion	HKLM:\AWSTempSystem\ControlSet001
\$env:EC2RESCUE_OFFLINE_DRIVE	Lecteur Windows hors connexion	D:\
\$env:EC2RESCUE_OFFLINE_EBS_DEVICE	Périphérique EBS de volume racine hors connexion	xvdf
\$env:EC2RESCUE_OFFLINE_KERNEL_VER	Version de noyau Windows hors connexion	6.1.7601.24214
\$env:EC2RESCUE_OFFLINE_OS_ARCHITECTURE	Architecture Windows hors connexion	AMD64
\$env:EC2RESCUE_OFFLINE_OS_CAPTION	Légende Windows hors connexion	Windows Server 2008 R2 Datacenter
\$env:EC2RESCUE_OFFLINE_OS_TYPE	Type de système d'exploitation Windows hors connexion	de bases de données
\$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR	Chemin de répertoire de fichiers de programme Windows hors connexion	D:\Program Files
\$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	Chemin de répertoire de fichiers de programme x86 hors connexion	D:\Program Files (x86)

Variable	Description	Exemple de valeur
<code>\$env:EC2RESCUE_OFFLINE_REGISTRY_DIR</code>	Chemin de répertoire de registre Windows hors connexion	D:\Windows\System32\config
<code>\$env:EC2RESCUE_OFFLINE_SYSTEM_ROOT</code>	Chemin de répertoire racine du système Windows hors connexion	D:\Windows
<code>\$env:EC2RESCUE_REGION</code>	{{ global:REGION }}	us-west-1
<code>\$env:EC2RESCUE_S3_BUCKET</code>	{{ S3BucketName }}	mybucket
<code>\$env:EC2RESCUE_S3_PREFIX</code>	{{ S3Prefix }}	myprefix/
<code>\$env:EC2RESCUE_SOURCE_INSTANCE</code>	{{ InstanceId }}	i-abcdefgh123456789
<code>\$script:EC2RESCUE_OFFLINE_WINDOWS_INSTALL</code>	Métadonnées d'installation Windows hors connexion	Objet Powershell client

## Linux :

Variable	Description	Exemple de valeur
<code>EC2RESCUE_ACCOUNT_ID</code>	{{ global:ACCOUNT_ID }}	123456789012
<code>EC2RESCUE_DATE</code>	{{ global:DATE }}	2018-09-07
<code>EC2RESCUE_DATE_TIME</code>	{{ global:DATE_TIME }}	2018-09-07_18.09.59
<code>EC2RESCUE_EC2RL_DIR</code>	Chemin d'installation d'EC2Rescue pour Linux	/usr/local/ec2rl-1.1.3

Variable	Description	Exemple de valeur
EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_DEVICE	Nom du périphérique hors connexion	/dev/xvdf1
EC2RESCUE_OFFLINE_EBS_DEVICE	Périphérique EBS de volume racine hors connexion	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	Point de montage du volume racine hors connexion	/mnt/mount
EC2RESCUE_PYTHON	Version Python	python2.7
EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	mybucket
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AMIPrefix

Type : String



Par défaut : `AWSSupport-EC2Rescue`

Description : (Facultatif) préfixe pour le nom AMI de secours.

- `AutomationAssumeRole`

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- `CreatePostEC2 RescueBackup`

Type : String

Valeurs valides : `true` | `false`

Par défaut : `faux`

Description : (Facultatif) Réglez-la `true` sur pour créer une AMI ou InstanceId après avoir exécuté le script, avant de le démarrer. L'AMI sera conservée une fois l'automatisation terminée. Vous devez sécuriser l'accès à l'AMI ou le supprimer.

- `CreatePreEC2 RescueBackup`

Type : String

Valeurs valides : `true` | `false`

Par défaut : `faux`

Description : (Facultatif) `true` Définissez-la sur pour créer une AMI InstanceId avant d'exécuter le script. L'AMI sera conservée une fois l'automatisation terminée. Vous devez sécuriser l'accès à l'AMI ou le supprimer.

- `EC2 RescueInstanceType`

Type : String

Valeurs valides : `t2.small` | `t2.medium` | `t2.large`

Par défaut : `t2.small`

Description : (Facultatif) type d'instance EC2 pour l'instance EC2Rescue.

- InstanceId

Type : String

Description : (Obligatoire) ID de votre instance EC2. IMPORTANT : AWS Systems Manager Automation arrête cette instance. Les données stockées sur les volumes de stockage d'instance seront perdues. L'adresse IP publique change si vous n'utilisez pas une adresse IP Elastic.

- OfflineScript

Type : String

Description : (Obligatoire) script codé en Base64 à exécuter sur l'instance d'assistant. Utilisez Bash si votre instance source est Linux et PowerShell Windows.

- S3 BucketName

Type : String

Description : (Facultatif) nom du compartiment S3 de votre compte dans lequel vous souhaitez charger les journaux de dépannage. Assurez-vous que la stratégie de compartiment n'accorde pas des autorisations en lecture/écriture superflues pour les tiers qui n'ont pas besoin d'accéder aux journaux collectés.

- S3Prefix

Type : String

Par défaut : `AWSSupport-EC2Rescue`

Description : (Facultatif) préfixe pour les journaux S3.

- SubnetId

Type : String

Par défaut : `SelectedInstanceSubnet`

Description : (Facultatif) ID de sous-réseau pour l'instance EC2Rescue. Par défaut, le même sous-réseau dans lequel l'instance réside est utilisé. IMPORTANT : Si vous fournissez un sous-réseau personnalisé, il doit se trouver dans la même zone de disponibilité que les points de InstanceId terminaison SSM et autoriser l'accès à ces derniers.

- UniqueId

Type : String

Par défaut : {{ automation:EXECUTION\_ID }}

Description : (Facultatif) Un identifiant unique pour l'automatisation.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Il est recommandé à l'utilisateur qui exécute l'automatisation d'associer la politique de gestion AmazonSSM AutomationRole IAM. En plus de cette stratégie, l'utilisateur doit avoir :

```
{
  "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"
      }
    ]
  }

```

## Étapes de document

1. `aws:executeAwsApi`- Décrivez l'instance fournie
2. `aws:executeAwsApi`- Décrivez le volume racine de l'instance fournie
3. `aws:assertAwsResourceProperty`- Vérifiez que le type de périphérique du volume racine est EBS
4. `aws:assertAwsResourceProperty`- Vérifiez que le volume racine n'est pas crypté
5. `aws:assertAwsResourceProperty`- Vérifiez l'ID de sous-réseau fourni
  - a. (Utiliser le sous-réseau de l'instance actuelle) - Si `* SubnetId = SelectedInstanceSubnet *`, exécutez `aws:createStack` pour déployer la pile EC2Rescue CloudFormation
  - b. (Créer un nouveau VPC) - Si `* SubnetId = CreateNew VPC*`, exécutez `aws:createStack` pour déployer la pile EC2Rescue CloudFormation
  - c. (Utiliser un sous-réseau personnalisé) - Dans tous les autres cas :
 

`aws:assertAwsResourceProperty`- Vérifiez que le sous-réseau fourni se trouve dans la même zone de disponibilité que l'instance fournie

`aws:createStack`- Déployez la pile EC2Rescue CloudFormation
6. `aws:invokeLambdaFunction`- Effectuer une validation d'entrée supplémentaire
7. `aws:executeAwsApi`- Mettez à jour la CloudFormation pile EC2Rescue pour créer l'instance d'assistance EC2Rescue
8. `aws:waitForAwsResourceProperty`- Attendez la fin de la mise à jour de la CloudFormation pile EC2Rescue
9. `aws:executeAwsApi`- Décrivez la sortie de la CloudFormation pile EC2Rescue pour obtenir l'ID de l'instance d'assistance EC2Rescue
10. `aws:waitForAwsResourceProperty`- Attendez que l'instance d'assistance EC2Rescue devienne une instance gérée
11. `aws:changeInstanceState`- Arrête l'instance fournie
12. `aws:changeInstanceState`- Arrête l'instance fournie
13. `aws:changeInstanceState`- Arrêt forcé de l'instance fournie

- 14 `aws:assertAwsResourceProperty`- Vérifiez la valeur `RescueBackup` d'entrée `CreatePre EC2`
- (Créer une sauvegarde avant `EC2Rescue`) - Si `EC2 = vrai` `CreatePre RescueBackup`
  - `aws:executeAwsApi`- Crée une sauvegarde AMI de l'instance fournie
  - `aws:createTags`- Marquez la sauvegarde de l'AMI
- 15 `aws:runCommand`- Installez `EC2Rescue` sur l'instance d'assistance `EC2Rescue`
- 16 `aws:executeAwsApi`- Détache le volume racine de l'instance fournie
- 17 `aws:assertAwsResourceProperty`- Vérifiez la plateforme d'instance fournie
- (Instance Windows) :
    - `aws:executeAwsApi`- Attachez le volume racine à l'instance d'assistance `EC2Rescue` sous la forme `*xvdf*`
    - `aws:sleep`- Dormez 10 secondes
    - `aws:runCommand`- Exécute le script hors ligne fourni dans Powershell
  - (Instance Linux) :
    - `aws:executeAwsApi`- Attachez le volume racine à l'instance d'assistance `EC2Rescue` en tant que `*/dev/sdf*`
    - `aws:sleep`- Dormez 10 secondes
    - `aws:runCommand`- Exécute le script hors ligne fourni dans Bash
- 18 `aws:changeInstanceState`- Arrêtez l'instance d'assistance `EC2Rescue`
- 19 `aws:changeInstanceState`- Arrêt forcé de l'instance d'assistance `EC2Rescue`
- 20 `aws:executeAwsApi`- Détache le volume racine de l'instance d'assistance `EC2Rescue`
- 21 `aws:executeAwsApi`- Rattachez le volume racine à l'instance fournie
- 22 `aws:assertAwsResourceProperty`- Vérifiez la valeur `RescueBackup` d'entrée `CreatePost EC2`
- (Créer une sauvegarde après `EC2Rescue`) - Si `EC2 = vrai` `CreatePost RescueBackup`
  - `aws:executeAwsApi`- Crée une sauvegarde AMI de l'instance fournie
  - `aws:createTags`- Marquez la sauvegarde de l'AMI
- 23 `aws:executeAwsApi`- Restaure l'état initial de suppression à la fin du volume racine de l'instance fournie
- 24 `aws:changeInstanceState`- Restaure l'état initial de l'instance fournie (en cours d'exécution/arrêtée)

## 25.aws:deleteStack- Supprimer la pile EC2Rescue CloudFormation

### Sorties

runScriptForLinux. Sortie

runScriptForWindows.Sortie

preScriptBackup.Imageld

postScriptBackup.Imageld

## **AWSPremiumSupport - TroubleshootEC2DiskUsage**

### Description

Le `AWSPremiumSupport-TroubleshootEC2DiskUsage` runbook vous aide à étudier et éventuellement à résoudre les problèmes liés à l'utilisation des disques root et non root de l'instance Amazon Elastic Compute Cloud (Amazon EC2). Si possible, le runbook tente de résoudre les problèmes en étendant le volume et son système de fichiers. Pour effectuer ces tâches, ce runbook orchestre l'exécution de plusieurs runbooks en fonction du système d'exploitation de l'instance concernée.

Le premier runbook, `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` ou `AWSPremiumSupport-DiagnoseDiskUsageOnLinux`, détermine si les problèmes de disque peuvent être atténués en augmentant le volume.

Le second runbook, `AWSPremiumSupport-ExtendVolumesOnWindows` ou `AWSPremiumSupport-ExtendVolumesOnLinux`, utilise la sortie du premier runbook pour exécuter du code Python qui modifie le volume. Une fois le volume modifié, le runbook étend la partition et le système de fichiers des volumes concernés.

#### Important

L'accès aux `AWSPremiumSupport-*` runbooks nécessite un abonnement Enterprise ou Business Support. Pour plus d'informations, consultez la section [Comparer AWS Support les plans](#).

Ce document a été élaboré en collaboration avec AWS Managed Services (AMS). AMS vous aide à gérer votre AWS infrastructure de manière plus efficace et sécurisée. AMS fournit également une

flexibilité opérationnelle, une sécurité et une conformité améliorées, une optimisation des capacités et une identification des économies de coûts. Pour plus d'informations, veuillez consulter [AWS Managed Services](#).

### [Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux, Windows

Paramètres

- InstanceId

Type : String

Valeurs autorisées : `^i-[a-z0-9]{8,17}$`

Description : ID (obligatoire) de votre instance Amazon EC2.

- VolumeExpansionEnabled

Type : booléen

Description : (Facultatif) Indicateur permettant de contrôler si le document va étendre les volumes et les partitions concernés.

Valeur par défaut : true

- VolumeExpansionUsageTrigger

Type : String

Description : (Facultatif) Utilisation minimale de l'espace de partition requise pour déclencher l'extension (en pourcentage).

Valeurs autorisées : `^[0-9]{1,2}$`



Par défaut : 85

- VolumeExpansionCapSize

Type : String

Description : (Facultatif) Taille maximale à laquelle le volume Amazon Elastic Block Store (Amazon EBS) sera augmenté (en GiB).

Valeurs autorisées :  $^ [0-9] \{1,4\} \$$

Par défaut : 2048

- VolumeExpansionGibIncrease

Type : String

Description : (Facultatif) Augmentation en GiB du volume. La plus forte augmentation nette entre VolumeExpansionGibIncrease et VolumeExpansionPercentageIncrease sera utilisée.

Valeurs autorisées :  $^ [0-9] \{1,4\} \$$

Par défaut : 20

- VolumeExpansionPercentageIncrease

Type : String

Description : (Facultatif) Augmentation en pourcentage du volume. La plus forte augmentation nette entre VolumeExpansionGibIncrease et VolumeExpansionPercentageIncrease sera utilisée.

Valeurs autorisées :  $^ [0-9] \{1,2\} \$$

Par défaut : 20

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

1. `aws:assertAwsResourceProperty`- Vérifiez si l'instance est gérée par Systems Manager
2. `aws:executeAwsApi`- Décrit l'instance permettant d'accéder à la plateforme.
3. `aws:branch`- Automatisation des branches en fonction de la plateforme de l'instance.
  - a. Si l'instance est Windows :
    - i. `aws:executeAutomation`- Exécutez le `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` runbook afin de diagnostiquer les problèmes d'utilisation du disque sur l'instance.

- ii. `aws:executeAwsApi`- Obtient le résultat de l'automatisation précédente.
- iii. `aws:branch`- Branches en fonction des résultats des diagnostics et de la possibilité d'étendre certains volumes pour atténuer l'alerte.
  - A. Aucun volume n'a besoin d'être étendu : mettez fin à l'automatisation.
  - B. Certains volumes doivent être étendus :
    - I. `aws:executeAwsApi`- Créez un Amazon Machine Image (AMI) de l'instance.
    - II. `aws:waitForAwsResourceProperty`- Il attend que l'AMI État le soit. `available`
    - III. `aws:executeAutomation`- Exécutez le `AWSPremiumSupport-ExtendVolumesOnWindows` runbook afin d'effectuer la modification du volume ainsi que les étapes requises dans le système d'exploitation (OS) pour rendre le nouvel espace disponible.
- b. (La plate-forme n'est pas Windows) Si l'instance d'entrée n'est pas Windows :
  - i. `aws:executeAutomation`- Exécutez le `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` runbook afin de diagnostiquer les problèmes d'utilisation du disque sur l'instance.
  - ii. `aws:executeAwsApi`- Obtient le résultat de l'automatisation précédente.
  - iii. `aws:branch`- Branches en fonction des résultats des diagnostics et de la possibilité d'étendre certains volumes pour atténuer l'alerte.
    - A. Aucun volume n'a besoin d'être étendu : mettez fin à l'automatisation.
    - B. Certains volumes doivent être étendus :
      - I. `aws:executeAwsApi`- Créez AMI une instance.
      - II. `aws:waitForAwsResourceProperty`- Il attend que l'AMI État le soit. `available`
      - III. `aws:executeAutomation`- Exécutez le `AWSPremiumSupport-ExtendVolumesOnLinux` runbook afin d'effectuer la modification du volume ainsi que les étapes requises dans le système d'exploitation pour rendre le nouvel espace disponible.

## Sorties

`diagnoseDiskUsageAlertOnWindows`. Sortie

`extendVolumesOnWindows`. Sortie

`diagnoseDiskUsageAlertOnLinux`. Sortie

AWSPremiumSupport-TroubleshootEC2DiskUsage

`extendVolumesOnLinux`. Sortie

Sauvegardez AMI Linux. `ImageId`

Sauvegardez les fenêtres d'AMI. `ImageId`

## **AWSsupport-TroubleshootEC2InstanceConnect**

### Description

`AWSsupport-TroubleshootEC2InstanceConnect` l'automatisation permet d'analyser et de détecter les erreurs empêchant la connexion à une instance Amazon Elastic Compute Cloud (Amazon EC2) à l'aide d'Amazon EC2 [Instance Connect](#). Il identifie les problèmes liés à une Amazon Machine Image (AMI) non prise en charge, à une installation ou à une configuration de package manquantes au niveau du système d'exploitation, à des autorisations AWS Identity and Access Management (IAM) manquantes ou à des problèmes de configuration réseau.

Comment fonctionne-t-il ?

Le runbook prend l'ID de l'instance Amazon EC2, le nom d'utilisateur, le mode de connexion, l'adresse IP source CIDR, le port SSH et le nom de ressource Amazon (ARN) du rôle IAM ou de l'utilisateur rencontrant des problèmes avec Amazon EC2 Instance Connect. Il vérifie ensuite les [conditions requises](#) pour se connecter à une instance Amazon EC2 à l'aide d'Amazon EC2 Instance Connect :

- L'instance est en cours d'exécution et en bon état.
- L'instance est située dans une AWS région prise en charge par Amazon EC2 Instance Connect.
- L'AMI de l'instance est prise en charge par Amazon EC2 Instance Connect.
- L'instance peut accéder au service de métadonnées d'instance (IMDSv2).
- Le package Amazon EC2 Instance Connect est correctement installé et configuré au niveau du système d'exploitation.
- La configuration réseau (groupes de sécurité, ACL réseau et règles de table de routage) permet la connexion à l'instance via Amazon EC2 Instance Connect.
- Le rôle ou l'utilisateur IAM utilisé pour tirer parti d'Amazon EC2 Instance Connect a accès aux touches push de l'instance Amazon EC2.

**⚠ Important**

- Pour vérifier l'AMI de l'instance, l'accessibilité d'IMDSv2 et l'installation du package Amazon EC2 Instance Connect, l'instance doit être gérée par SSM. Dans le cas contraire, il ignore ces étapes. Pour plus d'informations, consultez [Pourquoi mon instance Amazon EC2 ne s'affiche-t-elle pas en tant que nœud géré ?](#)
- La vérification du réseau détecte uniquement si le groupe de sécurité et les règles ACL du réseau bloquent le trafic lorsque le SourceIP CIDR est fourni en tant que paramètre d'entrée. Dans le cas contraire, seules les règles liées au SSH seront affichées.
- Les connexions utilisant le point de [terminaison Amazon EC2 Instance Connect](#) ne sont pas validées dans ce runbook.
- Pour les connexions privées, l'automatisation ne vérifie pas si le client SSH est installé sur la machine source et s'il peut atteindre l'adresse IP privée de l'instance.

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux

Paramètres

Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`

- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez au [AWSSupport-TroubleshootEC2InstanceConnect](#) dans la AWS Systems Manager console.
2. Sélectionnez Exécute automation (Exécuter l'automatisation).
3. Pour les paramètres d'entrée, entrez ce qui suit :

- `InstanceId` (Obligatoire) :

L'ID de l'instance Amazon EC2 cible à laquelle vous n'avez pas pu vous connecter à l'aide d'Amazon EC2 Instance Connect.

- `AutomationAssumeRole` (Facultatif) :

L'ARN du rôle IAM qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `UserName` (obligatoire) :

Le nom d'utilisateur utilisé pour se connecter à l'instance Amazon EC2 à l'aide d'Amazon EC2 Instance Connect. Il est utilisé pour évaluer si l'accès IAM est accordé à cet utilisateur en particulier.

- `EC2InstanceConnectRoleOrUser` (obligatoire) :

L'ARN du rôle ou de l'utilisateur IAM qui utilise Amazon EC2 Instance Connect pour appuyer sur les touches de l'instance.

- `SSHport` (facultatif) :

Le port SSH configuré sur l'instance Amazon EC2. La valeur par défaut est 22. Le numéro de port doit être compris entre 1-65535.

- **SourceNetworkType (Facultatif) :**

Méthode d'accès réseau à l'instance Amazon EC2 :

- **Navigateur :** vous vous connectez depuis la console AWS de gestion.
- **Public :** vous vous connectez à l'instance située dans un sous-réseau public via Internet (par exemple, votre ordinateur local).
- **Privé :** vous vous connectez via l'adresse IP privée de l'instance.
- **SourceIpCIDR (facultatif) :**

Le CIDR source qui inclut l'adresse IP de l'appareil (tel que votre ordinateur local) à partir duquel vous vous connecterez à l'aide d'Amazon EC2 Instance Connect. Exemple : 172.31.48.6/32. Si aucune valeur n'est fournie avec le mode d'accès public ou privé, le runbook n'évaluera pas si le groupe de sécurité des instances Amazon EC2 et les règles ACL du réseau autorisent le trafic SSH. Il affichera plutôt les règles liées au 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'.

**SourceIpCIDR**  
(Optional) The source CIDR that includes the IP address of the device you will be logging from using EC2 Instance Connect (such as your local computer). Example: 172.31.48.0/20.

4. Sélectionnez Exécuter.

5. L'automatisation démarre.

6. Le document exécute les étapes suivantes :

- **AssertInitialState:**

Garantit que le statut de l'instance Amazon EC2 est en cours d'exécution. Dans le cas contraire, l'automatisation prend fin.

- **GetInstanceProperties:**

Obtient les propriétés actuelles de l'instance Amazon EC2 (PlatformDetails, PublicIpAddress VpId, SubnetId et MetadataHttpEndpoint).

- **GatherInstanceInformationFromSMS :**

Obtient l'état du ping de l'instance Systems Manager et les détails du système d'exploitation si l'instance est gérée par SSM.

- `CheckIfAWSRegionSupported`:

Vérifie si l'instance Amazon EC2 se trouve dans une région prise en charge par Amazon EC2 Instance ConnectAWS.

- `BranchOnIfAWSRegionSupported`:

Poursuit l'exécution si la AWS région est prise en charge par Amazon EC2 Instance Connect. Sinon, il crée la sortie et quitte l'automatisation.

- `CheckIfInstanceAMI IsSupported` :

Vérifie si l'AMI associée à l'instance est prise en charge par Amazon EC2 Instance Connect.

- `BranchOnIfInstanceAMI IsSupported` :

Si l'AMI d'instance est prise en charge, elle effectue les vérifications au niveau du système d'exploitation, telles que l'accessibilité des métadonnées et l'installation et la configuration du package Amazon EC2 Instance Connect. Sinon, il vérifie si les métadonnées HTTP sont activées à l'aide de l'AWSAPI, puis passe à l'étape de vérification du réseau.

- Vérifiez les `IMD ReachabilityFromOs` :

Exécute un script Bash sur l'instance Linux Amazon EC2 cible pour vérifier si elle est capable d'atteindre l'IMDSv2.

- Vérifiez `EIC : PackageInstallation`

Exécute un script Bash sur l'instance Linux Amazon EC2 cible pour vérifier si le package Amazon EC2 Instance Connect est correctement installé et configuré.

- Vérifiez `SSH ConfigFromOs` :

Exécute un script Bash sur l'instance Linux Amazon EC2 cible pour vérifier si le port SSH configuré correspond au paramètre d'entrée ``SSHport.``

- `CheckMetadataHTTP EndpointIsEnabled` :

Vérifie si le point de terminaison HTTP du service de métadonnées d'instance est activé.

- Vérifiez `EIC : NetworkAccess`



Vérifiez si la configuration réseau (groupes de sécurité, ACL réseau et règles de table de routage) autorise la connexion à l'instance via Amazon EC2 Instance Connect.

- Vérifiez que je suis RoleOrUserPermissions :

Vérifiez si le rôle ou l'utilisateur IAM utilisé pour tirer parti d'Amazon EC2 Instance Connect a accès aux touches push de l'instance Amazon EC2 à l'aide du nom d'utilisateur fourni.

- MakeFinalOutput:

Consolide le résultat de toutes les étapes précédentes.

7. Une fois terminé, consultez la section Sorties pour obtenir les résultats détaillés de l'exécution :

Exécution lorsque l'instance cible possède tous les prérequis requis :

```

▼ 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

```

Exécution lorsque l'AMI de l'instance cible n'est pas prise en charge :

```

▼ 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

```

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)

- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

AWSdocumentation de service

- [Comment résoudre les problèmes de connexion à mon instance Amazon EC2 à l'aide d'Amazon EC2 Instance Connect ?](#)

## AWSSupport-TroubleshootRDP

Description

Le AWSSupport-TroubleshootRDP runbook permet à l'utilisateur de vérifier ou de modifier les paramètres courants de l'instance cible qui peuvent avoir un impact sur les connexions RDP (Remote Desktop Protocol), tels que le port RDP, l'authentification de la couche réseau (NLA) et les profils du pare-feu Windows. Le cas échéant, les modifications peuvent être appliquées hors connexion par l'arrêt et le redémarrage de l'instance, si l'utilisateur autorise explicitement la correction hors connexion. Par défaut, le runbook lit et affiche les valeurs des paramètres.

### Important

Les modifications apportées aux paramètres RDP, au service RDP et aux profils du pare-feu Windows doivent être examinées attentivement avant d'utiliser ce runbook.

[Exécutez cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Windows

Paramètres

- Action

Type : String

Valeurs valides : CheckAll | FixAll | Personnalisé

Par défaut : Custom

Description : (Facultatif) [Personnalisé] Utilisez les valeurs du pare-feu, du RDP, du RDPServiceStartupType, du RDP ServiceActionPortAction, du NLA SettingAction et RemoteConnections pour gérer les paramètres. [CheckAll] Lisez les valeurs des paramètres sans les modifier. [FixAll] Restaurez les paramètres par défaut du protocole RDP et désactivez le pare-feu Windows.

- AllowOffline

Type : String

Valeurs valides : true | false

Par défaut : faux

Description : (Facultatif) Fix only - définissez cette valeur sur true si vous autorisez la correction RDP hors connexion dans le cas où le dépannage en ligne échouerait ou dans le cas où l'instance fournie ne serait pas une instance gérée. Remarque : pour la correction hors connexion, SSM Automation arrête l'instance et crée une AMI avant de tenter toute opération.

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- Pare-feu

Type : String

Valeurs valides : Vérifier | Désactiver

Par défaut : Check

Description : (Facultatif) vérifiez ou désactivez le pare-feu Windows (tous les profils).

- InstanceId

Type : String

Description : (Obligatoire) ID de l'instance pour laquelle les paramètres RDP doivent être dépannés.

- NLA SettingAction

Type : String

Valeurs valides : Vérifier | Désactiver

Par défaut : Check

Description : (Facultatif) vérifiez ou désactivez l'authentification NLA (Network Layer Authentication).

- RDP PortAction

Type : String

Valeurs valides : Vérifier | Modifier

Par défaut : Check

Description : (Facultatif) vérifiez le port utilisé pour les connexions RDP ou remplacez le port RDP par 3389 et redémarrez le service.

- RDP ServiceAction

Type : String

Valeurs valides : Vérifier | Démarrer | Redémarrer | Force-Restart

Par défaut : Check

Description : (Facultatif) Vérifiez, démarrez, redémarrez ou forcez le redémarrage du service RDP (). TermService

- RDP ServiceStartupType

Type : String

Valeurs valides : Check | Auto

Par défaut : Check

Description : (Facultatif) vérifiez ou définissez le service RDP pour commencer automatiquement au démarrage de Windows.

- RemoteConnections

Type : String

Valeurs valides : Vérifier | Activer

Par défaut : Check

Description : (Obligatoire) action à effectuer au niveau du paramètre fDenyTSConnections : Check, Enable.

- S3 BucketName

Type : String

Description : (Facultatif) hors connexion uniquement - nom du compartiment S3 de votre compte dans lequel vous souhaitez charger les journaux de dépannage. Assurez-vous que la stratégie de compartiment n'accorde pas des autorisations en lecture/écriture superflues pour les tiers qui n'ont pas besoin d'accéder aux journaux collectés.

- SubnetId

Type : String

Par défaut : SelectedInstanceSubnet

Description : (Facultatif et hors connexion uniquement) ID de sous-réseau de l'instance EC2Rescue utilisé pour réaliser le dépannage hors connexion. Si aucun ID de sous-réseau n'est spécifié, AWS Systems Manager Automation crée un VPC. IMPORTANT : Le sous-réseau doit se trouver dans la même zone de disponibilité que InstanceId les points de terminaison SSM et autoriser l'accès à ces derniers.

## Autorisations IAM requises

Le paramètre `AutomationAssumeRole` nécessite les actions suivantes pour utiliser correctement le runbook.

Il est recommandé que l'instance EC2 recevant la commande dispose d'un rôle IAM auquel est associée la politique gérée par `ManagedInstanceCore` Amazon d'AmazonSSM. Pour la correction en ligne, l'utilisateur doit disposer au minimum de `ssm : DescribeInstanceInformation`, `ssm : StartAutomationExecution` et `ssm : SendCommand` pour exécuter l'automatisation et envoyer la commande à l'instance, ainsi que de `ssm : GetAutomationExecution` pour pouvoir lire le résultat de l'automatisation. Pour la correction hors ligne, l'utilisateur doit disposer au moins de `ssm : DescribeInstanceInformation`, `ssm :`, `ec2 : StartAutomationExecution` `DescribeInstances`, plus `ssm : GetAutomationExecution` pour pouvoir lire le résultat de l'automatisation. `AWSsupport-TroubleshootRDP` appelle `AWSsupport-ExecuteEC2Rescue` pour effectuer la correction hors ligne : veuillez vérifier les autorisations pour vous `AWSsupport-ExecuteEC2Rescue` assurer que vous pouvez exécuter l'automatisation correctement.

### Étapes de document

1. `aws:assertAwsResourceProperty`- Vérifie si l'instance est une Windows Server instance
2. `aws:assertAwsResourceProperty`- Vérifiez si l'instance est une instance gérée
3. (Dépannage en ligne) S'il s'agit d'une instance gérée :

a. `aws:assertAwsResourceProperty`- Vérifiez la valeur d'action fournie

b. (Vérification en ligne) Si l'action = `CheckAll`, alors :

`aws:runPowerShellScript`- Exécute le PowerShell script pour obtenir l'état des profils du pare-feu Windows.

`aws:executeAutomation`- Appels `AWSsupport-ManageWindowsService` pour obtenir l'état du service RDP.

`aws:executeAutomation`- Appels `AWSsupport-ManageRDPSettings` pour obtenir les paramètres RDP.

c. (Correctif en ligne) Si l'action = `FixAll`, alors :

`aws:runPowerShellScript`- Exécute le PowerShell script pour désactiver tous les profils du pare-feu Windows.

`aws:executeAutomation`- Appels `AWSsupport-ManageWindowsService` pour démarrer le service RDP.

`aws:executeAutomation-Appels AWSSupport-ManageRDPSettings` pour activer les connexions à distance et désactiver le NLA.

d. (Gestion en ligne) Si Action = Custom :

`aws:runPowerShellScript`- Exécute le PowerShell script pour gérer les profils du pare-feu Windows.

`aws:executeAutomation-Appels AWSSupport-ManageWindowsService` pour gérer le service RDP.

`aws:executeAutomation-Appels AWSSupport-ManageRDPSettings` pour gérer les paramètres RDP.

4. (Correction hors connexion) Si l'instance n'est pas une instance gérée :

a. `aws:assertAwsResourceProperty`- Affirmer AllowOffline= vrai

b. `aws:assertAwsResourceProperty`- Affirmer une action = FixAll

c. `aws:assertAwsResourceProperty`- Affirmer la valeur de SubnetId

(Utilisez le sous-réseau de l'instance fournie) S'il s'agit de `SELECTED_INSTANCE_SUBNET`

`aws:executeAwsApi`- Récupère le sous-réseau de l'instance en cours.

`aws:executeAutomation-Exécuter AWSSupport-ExecuteEC2Rescue` avec le sous-réseau de l'instance fournie.

d. (Utilisez le sous-réseau personnalisé fourni) S'il n'y a pas `SELECTED_INSTANCE_SUBNET`

`aws:executeAutomation-Exécuter AWSSupport-ExecuteEC2Rescue` avec SubnetId la valeur fournie.

## Sorties

`manageFirewallProfiles`. Sortie

`Manager DPServiceSettings`. Sortie

`manageRDPSettings.Output`

checkFirewallProfiles. Sortie

Vérifiez RDP. Output ServiceSettings

checkRDPSettings.Output

disableFirewallProfiles. Sortie

Restaurer ServiceSettings le RDP par défaut. Sortie

restoreDefaultRDPSettings.Output

troubleshootRDPOffline.Output

Résoudre les problèmes liés à RDP. Output OfflineWithSubnetId

## **AWSSupport - TroubleshootSSH**

### Description

Le `AWSSupport - TroubleshootSSH` runbook installe l'outil Amazon EC2Rescue pour Linux, puis utilise l'outil EC2Rescue pour vérifier ou tenter de résoudre les problèmes courants qui empêchent une connexion à distance à la machine Linux via SSH. Le cas échéant, les modifications peuvent être appliquées hors connexion par l'arrêt et le redémarrage de l'instance, si l'utilisateur autorise explicitement la correction hors connexion. Par défaut, le runbook fonctionne en mode lecture seule.

[Exécutez cette automatisation \(console\)](#)

Pour plus d'informations sur l'utilisation du `AWSSupport - TroubleshootSSH` runbook, consultez cette [rubrique de AWSSupport - TroubleshootSSH résolution des problèmes](#) du support AWS Premium.

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes



## Linux

### Paramètres

- Action

Type : String

Valeurs valides : CheckAll | FixAll

Par défaut : CheckAll

Description : (Obligatoire) spécifiez si vous souhaitez vérifier les problèmes sans les corriger ou vérifier et corriger automatiquement les problèmes détectés.

- AllowOffline

Type : String

Valeurs valides : true | false

Par défaut : faux

Description : (Facultatif) Fix only - définissez cette valeur sur true si vous autorisez la correction SSH hors connexion dans le cas où le dépannage en ligne échouerait ou dans le cas où l'instance fournie ne serait pas une instance gérée. Remarque : pour la correction hors connexion, SSM Automation arrête l'instance et crée une AMI avant de tenter toute opération.

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (obligatoire) ID de votre instance EC2 pour Linux.

- S3 BucketName

Type : String


Description : (Facultatif) hors connexion uniquement - nom du compartiment S3 de votre compte dans lequel vous souhaitez charger les journaux de dépannage. Assurez-vous que la stratégie de compartiment n'accorde pas des autorisations en lecture/écriture superflues pour les tiers qui n'ont pas besoin d'accéder aux journaux collectés.

- SubnetId

Type : String

Par défaut : SelectedInstanceSubnet

Description : (Facultatif et hors connexion uniquement) ID de sous-réseau de l'instance EC2Rescue utilisé pour réaliser le dépannage hors connexion. Si aucun ID de sous-réseau n'est spécifié, AWS Systems Manager Automation crée un VPC.

 Important

Le sous-réseau doit se trouver dans la même zone de disponibilité que les points de InstanceId terminaison SSM et doit autoriser l'accès à ces derniers.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Il est recommandé que l'instance EC2 recevant la commande dispose d'un rôle IAM auquel est associée la politique gérée par ManagedInstanceCore Amazon d'AmazonSSM. Pour la correction en ligne, l'utilisateur doit disposer au minimum de ssm : DescribeInstanceInformation, ssm : StartAutomationExecution et ssm : SendCommand pour exécuter l'automatisation et envoyer la commande à l'instance, ainsi que de ssm : GetAutomationExecution pour pouvoir lire le résultat de l'automatisation. Pour la correction hors ligne, l'utilisateur doit disposer au moins de ssm : DescribeInstanceInformation, ssm :, ec2 : StartAutomationExecution DescribeInstances, plus ssm : GetAutomationExecution pour pouvoir lire le résultat de l'automatisation. AWSSupport-TroubleshootSSHappels AWSSupport-ExecuteEC2Rescue pour effectuer la correction hors ligne : veuillez vérifier les autorisations pour vous AWSSupport-ExecuteEC2Rescue assurer que vous pouvez exécuter l'automatisation correctement.

## Étapes de document

1. `aws:assertAwsResourceProperty`- Vérifiez si l'instance est une instance gérée
  - a. (Correction en ligne) Si l'instance est une instance gérée :
    - i. `aws:configurePackage`- Installez EC2Rescue pour Linux via. AWS-ConfigureAWSPackage
    - ii. `aws:runCommand`- Exécutez le script bash pour exécuter EC2Rescue pour Linux.
  - b. (Correction hors connexion) Si l'instance n'est pas une instance gérée :
    - i. `aws:assertAwsResourceProperty`- Affirmer AllowOffline= vrai
    - ii. `aws:assertAwsResourceProperty`- Affirmer une action = FixAll
    - iii. `aws:assertAwsResourceProperty`- Affirmer la valeur de SubnetId
    - iv. (Utiliser le sous-réseau de l'instance fournie) C'SubnetId est SelectedInstanceSubnet  
`aws:executeAutomation` à utiliser AWSSupport-ExecuteEC2Rescue avec le sous-réseau de l'instance fournie.
    - v. (Utilisez le sous-réseau personnalisé fourni) SubnetId Il n'est pas SelectedInstanceSubnet utilisé `aws:executeAutomation` pour exécuter AWSSupport-ExecuteEC2Rescue avec SubnetId la valeur fournie.

## Sorties

troubleshootSSH.Output

troubleshootSSHOffline.Output

Résolution des problèmes liés à la sortie SSH OfflineWithSubnetId

## AWSSupport-TroubleshootSUSERegistration

### Description

Le `AWSSupport-TroubleshootSUSERegistration` runbook vous aide à identifier pourquoi l'enregistrement d'une SUSE Linux Enterprise Server instance Amazon Elastic Compute Cloud (Amazon EC2) auprès de SUSE Update Infrastructure a échoué. La sortie d'automatisation fournit des étapes pour résoudre le problème ou vous aide à le résoudre. Si l'instance passe tous les contrôles lors de l'automatisation, elle est enregistrée auprès de SUSE Update Infrastructure.

[Exécutez cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux

Paramètres

- AutomationAssumeRole

Type : String

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui démarre ce runbook.

- InstanceId

Type : String

Description : (Obligatoire) L'ID de l'instance Amazon EC2 que vous souhaitez dépanner.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:DescribeInstanceProperties
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:SendCommand
- ssm:ListCommands

## Étapes de document

- `aws:assertAwsResourceProperty`- Vérifie si l'instance Amazon EC2 est gérée parAWS Systems Manager.
- `aws:runCommand`- Vérifie si la plateforme d'instance Amazon EC2 l'estSLES.
- `aws:runCommand`- Vérifie si la `cloud-regionsrv-client` version du package est supérieure ou égale à la version requise 9.0.10.
- `aws:runCommand`- Vérifie si le lien symbolique du produit de base est rompu et corrige le lien s'il est rompu.
- `aws:runCommand`- Vérifie si le fichier `hosts (/etc/hosts)` contient des enregistrements pour `smt-ec2-susecloud.net`. L'automatisation supprime les doublons.
- `aws:runCommand`- Vérifie si la `curl` commande est installée.
- `aws:runCommand`- Vérifie si l'instance Amazon EC2 peut accéder à l'adresse 169.254.169.254 du service de métadonnées d'instance (IMDS).
- `aws:runCommand`- Vérifie si l'instance Amazon EC2 possède un code de facturation ou un code AWS Marketplace produit.
- `aws:runCommand`- Vérifie si l'instance Amazon EC2 peut accéder à au moins un serveur régional via HTTPS.
- `aws:runCommand`- Vérifie si l'instance Amazon EC2 peut accéder aux serveurs de l'outil de gestion des abonnements (SMT) via HTTP.
- `aws:runCommand`- Vérifie si l'instance Amazon EC2 peut accéder aux serveurs de l'outil de gestion des abonnements (SMT) via HTTPS.
- `aws:runCommand`- Vérifie si l'instance Amazon EC2 peut accéder à l'`smt-ec2.susecloud.net`adresse via HTTPS.
- `aws:runCommand`- Enregistre l'instance Amazon EC2 auprès de SUSE Update Infrastructure.
- `aws:executeScript`- Rassemble et produit les résultats de toutes les étapes précédentes.

## AWSSupport-TroubleshootWindowsPerformance

### Description

Le runbook `AWSSupport-TroubleshootWindowsPerformance` permet de résoudre les problèmes de performances récurrents sur l'instance Windows Amazon Elastic Compute Cloud (Amazon EC2). Le runbook capture les journaux de l'instance cible et analyse les indicateurs

de performance du processeur, de la mémoire, du disque et du réseau. L'automatisation peut éventuellement capturer un vidage du processus pour vous aider à déterminer la cause potentielle de la dégradation des performances. L'automatisation capture également les journaux des événements et du système à l'aide de l'[EC2Rescue](#) outil le plus récent, si vous autorisez ce runbook à l'installer.

Comment fonctionne-t-il ?

Le runbook exécute les étapes suivantes :

- Vérifie les prérequis de l'instance Amazon EC2.
- Génère des journaux de performance sur le disque racine de l'instance Windows Amazon EC2
- Stocke les journaux capturés dans un dossier `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Si un compartiment Amazon Simple Storage Service (Amazon S3) est fourni et que le rôle d'automatisation assume les autorisations requises, les journaux capturés sont chargés dans le compartiment Amazon S3.
- Installe le dernier EC2Rescue outil sur l'instance Windows Amazon EC2 pour capturer les événements et les journaux système si vous choisissez de l'installer, mais il n'analyse pas le vidage du processus ni les journaux capturés par EC2Rescue

#### Important

- Pour exécuter ce runbook, l'instance Windows Amazon EC2 doit être gérée par AWS Systems Manager. Pour plus d'informations, consultez [Pourquoi mon instance Amazon EC2 ne s'affiche-t-elle pas en tant que nœud géré ?](#)
- Pour exécuter ce runbook, l'instance Windows Amazon EC2 doit être exécutée sur les versions Windows 8.1/Windows Server 2012 R2 (6.3) ou plus récentes, 4.0 ou PowerShell supérieures. Pour plus d'informations, voir [Version du système d'exploitation Windows](#).
- Pour générer des journaux de performance, au moins 10 Go d'espace libre sur le périphérique racine sont nécessaires. Si la taille du disque racine est supérieure à 100 Go, l'espace libre doit être supérieur à 10 % de la taille du disque. Si vous videz un processus en cours d'exécution, l'espace libre doit être supérieur à 10 Go plus la taille de mémoire totale consommée par le processus lorsque celui-ci consomme plus de 10 Go de mémoire.
- Les journaux générés sur le périphérique racine ne sont pas supprimés automatiquement.

- Le runbook ne désinstalle pas l'EC2Rescueoutil. Pour plus d'informations, consultez la section [Utiliser EC2Rescue pour Windows Server](#).
- Il est recommandé d'exécuter cette automatisation en cas d'impact sur les performances. Vous pouvez également l'exécuter périodiquement à l'aide d'une association AWS Systems Manager State Manager ou en planifiant des fenêtres de AWS Systems Manager maintenance.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Windows

Paramètres

Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

(Facultatif) Le rôle IAM attaché au profil d'instance ou l'utilisateur IAM configuré sur l'instance nécessite les actions suivantes pour télécharger les journaux dans le compartiment Amazon S3 spécifié pour le paramètre : *LogUploadBucketName*

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez [AWSsupport-TroubleshootWindowsPerformance](#) à Systems Manager sous Documents.
2. Sélectionnez Exécute automation (Exécuter l'automatisation).
3. Pour les paramètres d'entrée, entrez ce qui suit :

- `AutomationAssumeRole` (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `InstanceId` (Obligatoire) :

L'ID de l'instance Windows Amazon EC2 cible sur laquelle vous souhaitez exécuter l'automatisation. L'instance doit être gérée par Systems Manager pour exécuter l'automatisation.

- `CaptureProcessDump` (Facultatif) :

Type de vidage du processus à capturer. L'automatisation peut capturer un vidage du processus susceptible d'avoir un impact sur les performances au début de l'automatisation. Le volume racine de l'instance nécessite au moins 10 Go d'espace libre (plus de 10 % de la taille du



disque lorsque la taille du volume racine est supérieure à 100 Go, et 10 Go plus la taille de mémoire totale consommée par le processus lorsque le processus consomme plus de 10 Go de mémoire).

- LogCaptureDuration (Facultatif) :

Le nombre de minutes, entre 1 et 15, pendant lesquelles cette automatisation capturera les journaux tant que le problème persiste. La valeur par défaut est 5.

- LogUploadBucketName (Facultatif) :

Le compartiment Amazon S3 de votre compte dans lequel vous souhaitez télécharger les journaux. Le compartiment doit être configuré avec le chiffrement côté serveur (SSE), et la politique du compartiment ne doit pas accorder d'autorisations de lecture/écriture inutiles aux parties qui n'ont pas besoin d'accéder aux journaux capturés. L'instance Windows Amazon EC2 doit avoir accès au compartiment Amazon S3.

- Installez EC2 RescueTool (facultatif) :

Définissez ce paramètre Yes sur pour permettre au runbook d'installer la dernière version de l'EC2Rescueoutil permettant de capturer les événements Windows et les journaux système. La valeur par défaut est No.

- Reconnaissance (obligatoire) :

Lisez les détails complets des actions effectuées par ce manuel d'automatisation et, si vous êtes d'accord, tapez 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. Sélectionnez Exécuter.

5. L'automatisation démarre.

6. Le document exécute les étapes suivantes :

- **CheckConcurrency:**

Garantit qu'il n'y a qu'une seule exécution de ce runbook ciblant l'instance. Si le runbook trouve une autre exécution ciblant la même instance, il renvoie une erreur et se termine.

- **AssertInstanceIsWindows:**

Affirme que l'instance Amazon EC2 s'exécute sur le système d'exploitation Windows. Dans le cas contraire, l'automatisation prend fin.

- **AssertInstanceIsManagedInstance:**

Affirme que l'instance Amazon EC2 est gérée par AWS Systems Manager. Dans le cas contraire, l'automatisation prend fin.

- **VerifyPrerequisites:**

Vérifie la PowerShell version sur le système d'exploitation de l'instance et garantit que l'instance peut être connectée via Systems Manager pour exécuter des PowerShell commandes. Cette automatisation prend en charge les versions PowerShell 4.0 et supérieures exécutées sur les versions Windows 8.1 /Server 2012 R2 (6.3) ou plus récentes. Si la version est plus ancienne, l'automatisation échoue. Lorsque vous choisissez de télécharger des journaux dans le compartiment Amazon S3, cette automatisation vérifie que le PowerShell module AWS Tools for est disponible. Dans le cas contraire, l'automatisation prend fin.

- **BranchOnProcessDump:**

Branches basées sur le fait que vous l'avez configuré pour capturer le vidage des processus ayant un impact sur les performances.

- **CaptureProcessDump:**

Vérifie si l'instance dispose de suffisamment d'espace pour exécuter cette automatisation (lorsque vous choisissez Highest CPU/Memory).

- **CapturePerformanceLogs:**

Vérifie à nouveau l'espace disque et exécute le PowerShell script sur l'instance pour créer des compteurs de performances et démarrer la journalisation de Performance Monitor et Windows Performance Recorder. Le script s'arrête une fois que la valeur définie LogCaptureDuration est atteinte.

- **SummarizePerformanceLogs:**

Résume le rapport XML généré à l'étape précédente `CapturePerformanceLogs`, pour trouver le processus responsable consommant le plus de `WorkingSet 64` (mémoire) et le % de temps processeur (CPU) indiqués en sortie sur l'automatisation. Il génère des informations similaires pour l'utilisation de l'interface réseau `LogicalDisk`, de la mémoire, de `TCPv4`, `IPv4` et `UDPv4` et les enregistre dans le dossier de `analysis_output.log` sortie.

- **BranchOnInstallEC2Rescue:**

Branches si vous le configurez pour installer le dernier `EC2Rescue` outil dans l'instance Amazon EC2.

- **InstallEC2RescueTool:**

Installe l'`EC2Rescue` outil dans le système d'exploitation de l'instance pour capturer les `EC2Rescue` journaux à l'aide `AWS-ConfigureAWSPackage` de.

- **RunEC2RescueTool:**

Exécute l'`EC2Rescue` outil dans le système d'exploitation de l'instance pour capturer tous les journaux nécessaires. `EC2Rescue` capture uniquement les journaux nécessaires pour économiser de l'espace.

- **BranchOnIfS3BucketProvided:**

Branches basées sur les informations saisies par l'utilisateur `LogUploadBucketName` pour voir s'il existe un nom de compartiment disponible pour le téléchargement des journaux.

- **GetS3BucketPublicStatus:**

Détermine si un compartiment Amazon S3 est fourni et, dans l'affirmative, confirme que le compartiment Amazon S3 n'est pas public et qu'il est configuré avec SSE.

- **UploadLogResult:**

Télécharge les journaux dans le compartiment Amazon S3 fourni. Si la `PowerShell` version est 5.0 ou supérieure, elle compresse les journaux dans une archive ZIP et les télécharge. Il supprime le fichier ZIP une fois le téléchargement terminé. Si la `PowerShell` version est inférieure à 5.0, elle télécharge les fichiers directement dans un dossier.

- **CleanUpLogsOnFailure:**

Nettoie tous les journaux générés par l'`CapturePerformanceLogs` étape en cas d'échec. L'`CleanUpLogsOnFailure` étape peut échouer ou expirer si l'agent SSM ne fonctionne pas correctement ou si le système Windows ne répond pas.

## 7. Une fois terminé, consultez la section Sorties pour obtenir les résultats détaillés de l'exécution :

### Exécution lorsque l'instance cible possède tous les prérequis requis.

**▼ 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 [redacted] was not found.  
Attempting to create Performance monitor Data Collector Set TroubleshootWindowsPerformance [redacted].....  
Data Collector Set TroubleshootWindowsPerformance [redacted] created successfully.  
Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance [redacted].....  
Data Collector Set TroubleshootWindowsPerformance [redacted] 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 [redacted] is currently generating logs.  
The Data Collector Set TroubleshootWindowsPerformance [redacted] has finished generating logs and is currently in 'Stopped' state.  
Attempting to delete Data Collector Set TroubleshootWindowsPerformance [redacted].....  
Data Collector Set TroubleshootWindowsPerformance [redacted] deleted successfully.

[PASSED] Performance logs are captured successfully inside the folder: C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance [redacted]  
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 [redacted]\_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 %
sppsvr	Processor	0.00	106.00	9.00
WmiPrvSE#2	Processor	0.00	90.00	2.00
MsMpEng	Processor	0.00	38.00	0.75
GenVclObj	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

### Exécution lorsque l'instance cible se trouve sur une plate-forme Linux et que l'exécution a échoué. Vous devez sélectionner l'ID de l'étape pour voir les détails de l'échec.

**▼ Outputs**

CapturePerformanceLogs.Output  
No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output  
No output available yet because the step is not successfully executed

SummarizePerformanceLogs.Output  
No output available yet because the step is not successfully executed

VerifyPrerequisites.Output  
No output available yet because the step is not successfully executed

CaptureProcessDump.Output  
No output available yet because the step is not successfully executed

RunEC2RescueTool.Output  
No output available yet because the step is not successfully executed

UploadLogResult.Output  
No output available yet because the step is not successfully executed

**Execution status**

Overall status	All executed steps	# Succeeded
Failed	2	1
# Failed	# Cancelled	# TimedOut
1	0	0


**Executed steps (2)**

Find Steps

Step ID	Step #	Step name	Action	Status	Start time	End time
[redacted]	1	CheckConcurrency	aws:executeScript	Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT
[redacted]0a3a9	2	AssertInstanceIsWindows	aws:assertAwsResourceProperty	Failed	Tue, 19 Mar 2024 16:15:00 GMT	Tue, 19 Mar 2024 16:15:01 GMT

### Les détails de l'échec de l'étape AssertInstanceIsWindows.

**Failure details**

 **Failure message**  
Step fails when it is Execute/Canceling action. Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows']. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

FailureType	FailureStage
Verification	Invocation
VerificationErrorMessage	
Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows'].	

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

## AWSSupport-TroubleshootWindowsUpdate

### Description

Le AWSSupport-TroubleshootWindowsUpdate runbook est utilisé pour identifier les problèmes susceptibles d'échouer lors des mises à jour Windows pour les instances Windows Amazon Elastic Compute Cloud (Amazon EC2).

### Comment fonctionne-t-il ?

Le runbook exécute les étapes suivantes :

- Vérifie si l'instance Amazon EC2 cible est gérée par. AWS Systems Manager
- Vérifie si les versions de l' AWS Systems Manager agent (agent SSM) et de Windows Server sont prises en charge pour les opérations de correction de Systems Manager.
- Vérifie l'espace disque disponible recommandé pour les mises à jour Windows et vérifie si un redémarrage est en attente. Un redémarrage en attente indique généralement que des mises à jour sont en attente et qu'un redémarrage est nécessaire avant d'effectuer des mises à jour supplémentaires.
- Configure les paramètres du proxy au niveau du système d'exploitation, ce qui peut aider à résoudre les problèmes de connectivité.

- Effectue un test de connectivité des terminaux Amazon Simple Storage Service (Amazon S3) et appelle [GetDeployablePatchSnapshotForInstance](#) l'opération API pour récupérer l'instantané actuel de la ligne de base de correctifs utilisée par le nœud géré.
- Si la connexion échoue, offre la possibilité d'exécuter le `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook pour analyser la connectivité de l'instance aux points de terminaison Amazon S3.
- Valide la configuration des mises à jour Windows et teste Windows Server Update Services (WSUS) (le cas échéant).

#### Important

- Les contrôleurs de domaine Active Directory ne sont pas pris en charge.
- Windows Server version 2008 R2 ou les versions antérieures ne sont pas prises en charge.
- Les versions 1.2.371 ou antérieures de l'agent SSM ne sont pas prises en charge.
- Le `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook permet [VPC Reachability Analyzer](#) d'analyser la connectivité réseau entre une source et un point de terminaison de service. Vous êtes facturé par analyse effectuée entre une source et une destination. Pour plus de détails, consultez la section [Tarification d'Amazon VPC](#).
- Le `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook n'est pas disponible dans toutes les régions où Systems Manager est pris en charge.

#### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Windows

Paramètres

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

### Note

Pour exécuter le runbook `enfantAWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`, ajoutez les autorisations répertoriées dans [ce document](#).

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez à [AWSSupport-TroubleshootWindowsUpdate](#) à Systems Manager sous Documents.
2. Sélectionnez `Execute automation` (Exécuter l'automatisation).
3. Pour les paramètres d'entrée, entrez ce qui suit :
  - `AutomationAssumeRole` (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `InstanceId` (Obligatoire) :

Entrez l'ID de l'instance Amazon EC2 sur laquelle la mise à jour Windows a échoué.

- `RunVpcReachabilityAnalyzer`(Facultatif) :

Spécifiez `true` l'exécution de l'`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` automatisation si un problème réseau est déterminé par les vérifications étendues ou si l'ID d'instance spécifié n'est pas une instance gérée. Pour plus d'informations sur cette automatisation des enfants, consultez la [documentation](#). La valeur par défaut est `false`.

- `RetainVpcReachabilityAnalysis`(Facultatif) :

Pertinent uniquement si `RunVpcReachabilityAnalyzer` c'est le `true`. Spécifiez `true` pour conserver le chemin d'aperçu du réseau et les analyses associées créées par `Reachability Analyzer`. Par défaut, ces ressources sont supprimées après une analyse réussie. Si vous choisissez de conserver l'analyse, le runbook enfant ne la supprime pas et vous pouvez la visualiser dans la console Amazon VPC. Le lien vers la console sera disponible dans la sortie d'automatisation de l'enfant. La valeur par défaut `false`.

**Input parameters**

---

**InstanceId**  
(Required) The ID of the Amazon EC2 instance.

Show interactive instance picker

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

**RunVpcReachabilityAnalyzer**  
(Optional) Specify 'true' to run the 'AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2' automation if a network issue is determined by the extended checks, or if the instance ID specified is not a managed instance. For more information on this child automation, please refer to the documentation above. This parameter defaults to 'false'.

**RetainVpcReachabilityAnalysis**  
(Optional) Only relevant if 'RunVpcReachabilityAnalyzer' is true. Specify 'true' to retain the network insight path and related analyses created by VPC Reachability Analyzer. By default, those resources are deleted after successful analysis. If you choose to retain the analysis, the child runbook does not delete the analysis and you can visualize it in the VPC console. The console link will be available in the child automation output. This parameter defaults to 'false'.

4. Sélectionnez Exécuter.

5. L'automatisation démarre.

6. Le document exécute les étapes suivantes :

- **`getWindowsServerAndSSMAgentVersion` :**

Vérifie que l'instance cible est gérée par AWS Systems Manager et obtient des informations sur la version de l'agent SSM et la version de Windows.

- **`assertIfInstanceIsSsmManaged` :**

Garantit que l'instance Amazon EC2 est gérée par AWS Systems Manager (SSM), sinon l'automatisation prend fin.



- **CheckProxy:**

Vérifie tous les types de proxy pour l'instance Windows.

- **CheckPrerequisites:**

Obtient la version de l'agent SSM et la version de Windows, et détermine s'il s'agit d'un contrôleur de domaine Active Directory (DC). Si l'instance est un contrôleur de domaine ou si la version de l'agent SSM ou de Windows n'est pas prise en charge, le runbook s'arrête.

- **CheckDiskSpace:**

Obtient et valide l'espace disque disponible sur l'instance Windows s'il est suffisant pour effectuer la mise à jour Windows.

- **CheckPendingReboot:**

Vérifie s'il y a un redémarrage en attente sur l'instance Windows.

- **CheckS3Connectivity:**

Vérifie si l'instance peut atteindre les points de terminaison Amazon S3 pour `Patchbaseline`.

- **branchOnRunVpcReachabilityAnalyzer:**

Si `RunVpcReachabilityAnalyzer` c'est vrai, il branche l'automatisation pour effectuer une analyse plus approfondie pour le débogage de la connectivité Amazon S3.

- **GenerateEndpoints:**

Génère un point de terminaison pour effectuer un contrôle de connectivité étendu pour le point de terminaison Amazon S3.

- **analyzeAwsEndpointReachabilityFromEC2:**

Appelle le runbook d'automatisation, `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`. pour vérifier l'accessibilité de l'instance sélectionnée aux points de terminaison requis.

- **CheckWindowsUpdateServices:**

Vérifie l'état du service Windows Update et le type de démarrage.

- **CheckWindowsUpdateSettings:**

Vérifie les politiques Windows Update configurées sur l'instance Windows.

- **CheckWSUSSettings:**

Vérifie si la mise à jour Windows est configurée avec WSUS ou Microsoft Update Catalog et vérifie la connectivité.

- **CheckWUGlobalSettings:**

Vérifie les paramètres globaux de Windows Update configurés sur l'instance Windows.

- **GenerateLogs:**

Télécharge les journaux Windows Update et les journaux CBS sur le bureau de l'instance et vérifie les erreurs dans les journaux d'événements Windows.

- **FinalReport:**

Génère un rapport complet de toutes les étapes.

7. Une fois terminé, consultez la section Sorties pour obtenir les résultats détaillés de l'exécution :

```

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
"

```

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)

- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

Documentation relative au AWS service

- Reportez-vous à l'article [Troubleshoot Windows Update](#) pour plus d'informations.

## AWSSupport-UpgradeWindowsAWSDrivers

### Description

Le `AWSSupport-UpgradeWindowsAWSDrivers` runbook met à niveau ou répare le stockage et AWS les pilotes réseau sur l'instance EC2 spécifiée. Le runbook tente d'installer les dernières versions des AWS pilotes en ligne en appelant l'agent SSM. Si l'agent SSM n'est pas joignable, le runbook peut effectuer une installation hors ligne des AWS pilotes si cela est explicitement demandé.

#### Note

La mise à niveau en ligne et hors ligne créera une AMI avant toute tentative d'opération, qui persistera une fois l'automatisation terminée. Vous devez sécuriser l'accès à l'AMI ou le supprimer. La méthode en ligne redémarre l'instance dans le cadre du processus de mise à niveau, tandis que la méthode hors connexion nécessite l'arrêt, puis le redémarrage de l'instance EC2 fournie.

#### Important

Si vos instances se connectent à AWS Systems Manager l'aide de points de terminaison VPC, ce runbook échouera s'il n'est pas utilisé dans la région us-east-1. Ce runbook échouera également sur un contrôleur de domaine. Pour mettre à jour les pilotes AWS PV sur un contrôleur de domaine, veuillez consulter [Mise à niveau d'un contrôleur de domaine \(Mise à niveau d'AWS PV\)](#).

[Exécuter cette automatisation \(console\)](#)

Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AllowOffline

Type : chaîne

Valeurs valides : true | false

Valeur par défaut : false

Description : (Facultatif) Définissez ce paramètre sur true si vous autorisez la mise à niveau des pilotes hors connexion si l'installation en ligne ne peut pas être effectuée. Remarque : le mode hors connexion nécessite l'arrêt, puis le redémarrage de l'instance EC2. Les données stockées sur les volumes de stockage d'instance seront perdues. L'adresse IP publique change si vous n'utilisez pas une adresse IP Elastic.

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ForceUpgrade

Type : chaîne

Valeurs valides : true | false

Valeur par défaut : false

Description : (Facultatif et hors connexion uniquement) définissez ce paramètre sur true si vous autorisez la mise à niveau des pilotes hors connexion même si les derniers pilotes sont déjà installés sur votre instance.

- InstanceId

Type : chaîne

Description : (obligatoire) ID de votre instance EC2 pour Windows Server.

- SubnetId

Type : chaîne

Par défaut : SelectedInstanceSubnet

Description : (Facultatif et hors connexion uniquement) ID de sous-réseau de l'instance EC2Rescue utilisé pour réaliser les mises à niveau de pilotes hors connexion. Si aucun ID de sous-réseau n'est spécifié, Systems Manager Automation créera un nouveau VPC.

#### Important

Le sous-réseau doit se trouver dans la même zone de disponibilité que les points de terminaison SSM InstanceId, et il doit autoriser l'accès à ceux-ci.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

L'instance EC2 recevant la commande doit au minimum avoir un rôle IAM qui inclut des autorisations pour ssm : StartAutomationExecution et ssm : SendCommand pour exécuter l'automatisation et envoyer la commande à l'instance, plus ssm : GetAutomationExecution pour pouvoir lire le résultat de l'automatisation. Vous pouvez joindre la stratégie gérée par AmazonSSMManagedInstanceCore Amazon à votre rôle IAM pour fournir ces autorisations. Nous vous recommandons toutefois d'utiliser le rôle IAM Automation AmazonSSMAutomationRole à cette fin. Pour plus d'informations, consultez [Utiliser IAM pour configurer les rôles pour l'automatisation](#).

Si vous effectuez une mise à niveau hors connexion, veuillez consulter les autorisations requises par [AWSSupport-StartEC2RescueWorkflow](#).

## Étapes de document

1. `aws:assertAwsResourceProperty`- Vérifie que l'instance d'entrée est Windows.
2. `aws:assertAwsResourceProperty`- Vérifie que l'instance d'entrée est une instance gérée. Si tel est le cas, la mise à niveau en ligne démarre. Dans le cas contraire, la mise à niveau hors connexion est évaluée.
  - a. (Mise à niveau en ligne) Si l'instance d'entrée est une instance gérée :
    - i. `aws:createImage`- Crée une sauvegarde AMI.
    - ii. `aws:createTags`- Marque la sauvegarde de l'AMI.
    - iii. `aws:runCommand`- Installe le pilote réseau ENA via `AWS-ConfigureAWSPackage`.
    - iv. `aws:runCommand`- Installe le pilote NVMe via `AWS-ConfigureAWSPackage`.
    - v. `aws:runCommand`- Installe le pilote AWS PV via `AWS-ConfigureAWSPackage`.
  - b. (Mise à niveau hors connexion) Si l'instance d'entrée n'est pas une instance gérée :
    - i. `aws:assertAwsResourceProperty`- Vérifie que le `AllowOffline` drapeau est réglé sur `true`. Dans ce cas, la mise à niveau hors ligne démarre, sinon l'automatisation prend fin.
    - ii. `aws:changeInstanceState`- Arrêtez l'instance source.
    - iii. `aws:changeInstanceState`- Arrêtez de force l'instance source.
    - iv. `aws:createImage`- Créez une sauvegarde AMI de l'instance source.
    - v. `aws:createTags`- Marquez la sauvegarde AMI de l'instance source.
    - vi. `aws:executeAwsApi`- Activez l'ENA pour l'instance.
    - vii. `aws:assertAwsResourceProperty`- Affirmez le `ForceUpgrade` drapeau.
    - viii. Forcer la mise à niveau hors ligne) Si `ForceUpgrade = true`, exécutez `aws:executeAutomation` pour appeler le script de mise à niveau forcée `AWSSupport-StartEC2RescueWorkflow` avec les pilotes. Cette opération installe les pilotes quelle que soit la version actuelle qui est installée.
    - ix. (Mise à niveau hors ligne) Si `ForceUpgrade = false`, exécutez `aws:executeAutomation` pour appeler `AWSSupport-StartEC2RescueWorkflow` avec le script de mise à niveau des pilotes.

## Sorties

`preUpgradeBackup.ImgId`

`preOfflineUpgradeBackup.ImgId`

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

`upgradeDriversOffline.Sortie`

`forceUpgradeDriversHors ligne. Sortie`

## Amazon ECS

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Elastic Container Service. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSSupport-CollectECSInstanceLogs](#)
- [AWS-InstallAmazonECSAgent](#)
- [AWS-ECSRunTask](#)
- [AWSSupport-TroubleshootECSContainerInstance](#)
- [AWSSupport-TroubleshootECSTaskFailedToStart](#)
- [AWS-UpdateAmazonECSAgent](#)

## AWSSupport-CollectECSInstanceLogs

### Description

Le `AWSSupport-CollectECSInstanceLogs` runbook collecte les fichiers journaux relatifs au système d'exploitation et à Amazon Elastic Container Service (Amazon ECS) à partir d'une instance Amazon Elastic Compute Cloud (Amazon EC2) afin de vous aider à résoudre les problèmes courants liés à Amazon ECS. Pendant que l'automatisation collecte les fichiers journaux associés, des modifications sont apportées au système de fichiers. Ces modifications incluent la création de répertoires temporaires et d'un répertoire de journaux, la copie de fichiers journaux dans ces répertoires et la compression des fichiers journaux dans une archive.



Si vous spécifiez une valeur pour le `LogDestination` paramètre, l'automatisation évalue l'état de la politique du bucket Amazon Simple Storage Service (Amazon S3) que vous spécifiez. Pour renforcer la sécurité des journaux collectés depuis votre instance Amazon EC2, si le statut de la politique `isPublic` est défini sur `true`, ou si la liste de contrôle d'accès (ACL) accorde des `READ` | `WRITE` autorisations au groupe prédéfini `All Users Amazon S3`, les journaux ne sont pas chargés. De plus, si le bucket fourni n'est pas disponible dans votre compte, les journaux ne sont pas chargés. Pour plus d'informations sur les groupes prédéfinis Amazon S3, consultez les [groupes prédéfinis Amazon S3](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

### [Exécuter cette automatisation \(console\)](#)

#### Type de document

Automatisation

#### Propriétaire

Amazon

#### Plateformes

Linux, Windows

#### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `ECS InstanceId`

Type : chaîne

Description : (Obligatoire) L'ID de l'instance à partir de laquelle vous souhaitez collecter des journaux. L'instance que vous spécifiez doit être gérée par Systems Manager.

- `LogDestination`

Type : chaîne

Description : (Facultatif) Le compartiment Amazon S3 dans lequel vous Compte AWS souhaitez télécharger les journaux archivés.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`

Nous recommandons que l'instance Amazon EC2 que vous spécifiez dans le `ECSInstanceId` paramètre possède un rôle IAM auquel est attachée la politique gérée par `AmazonSSMManagedInstanceCore` Amazon. Pour télécharger l'archive du journal dans le compartiment Amazon S3 que vous spécifiez dans le `LogDestination` paramètre, vous devez ajouter les autorisations suivantes :

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

### Étapes de document

- `assertInstanceIsManaged`- Vérifie si l'instance que vous spécifiez dans le `ECSInstanceId` paramètre est gérée par Systems Manager.
- `getInstancePlatform`- Obtient des informations sur la plate-forme du système d'exploitation (OS) de l'instance spécifiée dans le `ECSInstanceId` paramètre.
- `verifyInstancePlatform`- Branche l'automatisation en fonction de la plate-forme du système d'exploitation.

- `runLogCollectionScriptOnLinux`- Rassemble les fichiers journaux liés au système d'exploitation et à Amazon ECS sur les instances Linux et crée un fichier d'archive dans le `/var/log/collectECSlogs` répertoire.
- `runLogCollectionScriptOnWindows`- Rassemble les fichiers journaux liés au système d'exploitation et à Amazon ECS sur les instances Windows et crée un fichier d'archive dans le `C:\ProgramData\collectECSlogs` répertoire.
- `verifyIfS3BucketProvided`- Vérifie si une valeur a été spécifiée pour le `LogDestination` paramètre.
- `runUploadScript`- Branche l'étape d'automatisation en fonction de la plate-forme du système d'exploitation.
- `runUploadScriptOnLinux`- Télécharge l'archive du journal dans le compartiment Amazon S3 spécifié dans le `LogDestination` paramètre et supprime le fichier journal archivé du système d'exploitation.
- `runUploadScriptOnWindows`- Télécharge l'archive du journal dans le compartiment Amazon S3 spécifié dans le `LogDestination` paramètre et supprime le fichier journal archivé du système d'exploitation.

## AWS-InstallAmazonECSAgent

### Description

Le `AWS-InstallAmazonECSAgent` runbook installe l'agent Amazon Elastic Container Service (Amazon ECS) sur l'instance Amazon Elastic Compute Cloud (Amazon EC2) que vous spécifiez. Ce runbook ne prend en charge que les instances Amazon Linux et Amazon Linux 2.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- InstanceIds

Type : StringList

Description : (Obligatoire) Les identifiants des instances Amazon EC2 sur lesquelles vous souhaitez installer l'agent Amazon ECS.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances

### Étapes de document

aws:executeScript- Installe l'agent Amazon ECS sur les instances Amazon EC2 que vous spécifiez dans InstanceIds le paramètre.

### Sorties

InstallAmazonAgent ECS. SuccessfulInstances - L'ID de l'instance où l'installation de l'agent Amazon ECS a réussi.

InstallAmazonAgent ECS. FailedInstances - L'ID de l'instance sur laquelle l'installation de l'agent Amazon ECS a échoué.

InstallAmazonAgent ECS. InProgressInstances - L'ID de l'instance sur laquelle l'installation de l'agent Amazon ECS est en cours.

## AWS-ECSRunTask

### Description

Le AWS-ECSRunTask runbook exécute la tâche Amazon Elastic Container Service (Amazon ECS) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Linux

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- capacityProviderStrategy

Type : chaîne

Description : (Facultatif) La stratégie du fournisseur de capacité à utiliser pour la tâche.

- `cluster`

Type : chaîne

Description : (Facultatif) Nom abrégé ou ARN du cluster sur lequel exécuter votre tâche. Si vous ne spécifiez aucun cluster, le cluster par défaut est utilisé.

- `count`

Type : chaîne

Description : (Facultatif) Nombre d'instanciations de la tâche spécifiée à placer sur votre cluster. Vous pouvez spécifier jusqu'à 10 tâches pour chaque demande.

- `Activez l'ECS ManagedTags`

Type : booléen

Description : (Facultatif) Spécifie s'il faut utiliser les balises gérées par Amazon ECS pour la tâche. Pour plus d'informations, veuillez consulter la rubrique [Balisage de vos ressources Amazon ECS](#) dans le Guide du développeur Amazon Elastic Container Service.

- `enableExecuteCommand`

Type : booléen

Description : (Facultatif) Détermine s'il faut activer la fonctionnalité d'exécution de commande pour les conteneurs de cette tâche. Si cela est vrai, cela active la fonctionnalité d'exécution de commande sur tous les conteneurs de la tâche.

- `groupe`

Type : chaîne

Description : (Facultatif) Nom du groupe de tâches à associer à la tâche. La valeur par défaut est le nom de famille de la définition de tâche. Par exemple, `family:my-family-name`.

- `Type de lancement`

Type : chaîne

Valeurs valides : `EC2` | `FARGATE` | `EXTERNAL`

Description : (Facultatif) L'infrastructure sur laquelle exécuter votre tâche autonome.

- `networkConfiguration`

**Type : chaîne**

Description : (Facultatif) Configuration réseau de la tâche. Ce paramètre est obligatoire pour les définitions de tâches qui utilisent le mode `aws_vpc` réseau pour recevoir leur propre interface réseau Elastic, et il n'est pas pris en charge pour les autres modes réseau.

- `replacements`

**Type : chaîne**

Description : (Facultatif) Liste de remplacements de conteneurs au format JSON qui spécifie le nom d'un conteneur dans la définition de tâche spécifiée et les remplacements qu'il doit recevoir. Vous pouvez remplacer la commande par défaut d'un conteneur spécifiée dans la définition de la tâche ou dans l'image Docker par une commande de remplacement. Vous pouvez également remplacer les variables d'environnement existantes spécifiées dans la définition de la tâche ou dans l'image Docker d'un conteneur. En outre, vous pouvez ajouter de nouvelles variables d'environnement avec une dérogation d'environnement.

- `Contraintes de placement`

**Type : chaîne**

Description : (Facultatif) Tableau d'objets de contrainte de placement à utiliser pour la tâche. Vous pouvez définir jusqu'à 10 contraintes pour chaque tâche, y compris les contraintes dans la définition de la tâche et celles spécifiées lors de l'exécution.

- `Stratégie de placement`

**Type : chaîne**

Description : (Facultatif) Les objets de stratégie de placement à utiliser pour la tâche. Vous pouvez définir un maximum de 5 règles de stratégie pour chaque tâche.

- `platformVersion`

**Type : chaîne**

Description : (Facultatif) Version de plate-forme utilisée par la tâche. Une version de plateforme n'est spécifiée que pour les tâches hébergées sur Fargate. Si vous ne spécifiez aucune version de plateforme, la version LATEST est utilisée.

- `propagateTags`

Type : chaîne

Description : (Facultatif) Détermine si les balises se propagent de la définition de la tâche à la tâche. Si aucune valeur n'est spécifiée, les balises ne sont pas propagées. Les balises ne peuvent être propagées à la tâche que lors de la création de tâche.

- `referenceId`

Type : chaîne

Description : (Facultatif) L'ID de référence à utiliser pour la tâche. L'ID de référence peut avoir une longueur maximale de 1024 caractères.

- `Commencé par`

Type : chaîne

Description : (Facultatif) Balise facultative spécifiée lors du démarrage d'une tâche. Cela vous permet d'identifier les tâches qui appartiennent à une tâche spécifique en filtrant les résultats d'une opération d'`ListTasksAPI`. Jusqu'à 36 lettres (majuscules et minuscules), chiffres, tirets (-) et traits de soulignement (\_) sont autorisés.

- `balises`

Type : chaîne

Description : (Facultatif) Métadonnées que vous souhaitez appliquer à la tâche pour vous aider à classer et à organiser les tâches. Chaque balise est composée d'une clé et d'une valeur définies par l'utilisateur.

- `Définition de la tâche`

Type : chaîne

Description : (Facultatif) Le `family` et `revision` (`family:revision`) ou l'ARN complet de la définition de tâche à exécuter. Si aucune révision n'est spécifiée, la dernière ACTIVE révision est utilisée.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le `runbook`.



- `ecs:RunTask`

## Étapes de document

`aws:executeScript`- Exécute la tâche Amazon ECS en fonction des valeurs que vous spécifiez pour les paramètres d'entrée du runbook.

# AWSSupport-TroubleshootECSTainerInstance

## Description

Le `AWSSupport-TroubleshootECSTainerInstance` runbook vous aide à dépanner une instance Amazon Elastic Compute Cloud (Amazon EC2) qui ne parvient pas à s'enregistrer auprès d'un cluster Amazon ECS. Cette automatisation vérifie si les données utilisateur de l'instance contiennent les informations de cluster correctes, si le profil de l'instance contient les autorisations requises et vérifie les problèmes de configuration réseau.

### Important

Pour exécuter correctement cette automatisation, l'état de votre instance Amazon EC2 doit être `running`, et l'état du cluster Amazon ECS doit l'être. `ACTIVE`

## [Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterName

Type : chaîne

Description : (Obligatoire) Nom du cluster Amazon ECS auprès duquel l'instance n'a pas pu être enregistrée.

- InstanceId

Type : chaîne

Description : (Obligatoire) L'ID de l'instance Amazon EC2 que vous souhaitez dépanner.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

AWS:ExecuteScript : vérifie si l'instance Amazon EC2 répond aux conditions requises pour s'enregistrer auprès d'un cluster Amazon ECS.

# AWSSupport-TroubleshootECSTaskFailedToStart

## Description

Le `AWSSupport-TroubleshootECSTaskFailedToStart` runbook vous aide à résoudre les problèmes liés à l'échec du démarrage d'une tâche Amazon Elastic Container Service (Amazon ECS) dans un cluster Amazon ECS. Vous devez exécuter ce runbook en même temps Région AWS que votre tâche qui n'a pas pu démarrer. Le runbook analyse les problèmes courants suivants qui peuvent empêcher le démarrage d'une tâche :

- Connectivité réseau avec le registre de conteneurs configuré
- Autorisations IAM manquantes requises par le rôle d'exécution de la tâche
- Connectivité des terminaux VPC
- Configuration des règles du groupe de sécurité
- AWS Secrets Manager références secrètes
- Configuration de journalisation

### Note

Si l'analyse détermine que la connectivité réseau doit être testée, une fonction Lambda et le rôle IAM requis sont créés dans votre compte. Ces ressources sont utilisées pour simuler la connectivité réseau de votre tâche ayant échoué. L'automatisation supprime ces ressources lorsqu'elles ne sont plus nécessaires. Toutefois, si l'automatisation ne parvient pas à supprimer les ressources, vous devez le faire manuellement.

[Exécuter cette automatisation \(console\)](#)

## Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterName

Type : chaîne

Description : (Obligatoire) Nom du cluster Amazon ECS dans lequel la tâche n'a pas pu démarrer.

- CloudwatchRetentionPeriod

Type : entier

Description : (Facultatif) Période de conservation, en jours, des journaux des fonctions Lambda à stocker dans Amazon CloudWatch Logs. Cela n'est nécessaire que si l'analyse détermine que la connectivité réseau doit être testée.

Valeurs valides : 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

Valeur par défaut : 30

- TaskId

Type : chaîne

Description : (Obligatoire) L'ID de la tâche ayant échoué. Utilisez la dernière tâche ayant échoué.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

- `aws:executeScript`- Vérifie que l'utilisateur ou le rôle qui a lancé l'automatisation dispose des autorisations IAM requises. Si vous ne disposez pas des autorisations suffisantes pour utiliser ce runbook, les autorisations requises manquantes sont incluses dans le résultat de l'automatisation.
- `aws:branch`- Branches selon que vous êtes autorisé à effectuer toutes les actions requises pour le runbook.
- `aws:executeScript`- Crée une fonction Lambda dans votre VPC si l'analyse détermine que la connectivité réseau doit être testée.
- `aws:branch`- Branches basées sur les résultats de l'étape précédente.
- `aws:executeScript`- Analyse les causes possibles de l'échec du démarrage de votre tâche.
- `aws:executeScript`- Supprime les ressources créées par cette automatisation.
- `aws:executeScript`- Formate la sortie de l'automatisation pour renvoyer les résultats de l'analyse à la console. Vous pouvez revoir l'analyse après cette étape avant que l'automatisation ne soit terminée.
- `aws:branch`- Branches selon que la fonction Lambda et les ressources associées ont été créées et doivent être supprimées.

- `aws:sleep`- Sort pendant 30 minutes afin que l'interface Elastic network de la fonction Lambda puisse être supprimée.
- `aws:executeScript`- Supprime l'interface réseau de la fonction Lambda.
- `aws:executeScript`- Formate la sortie de l'étape de suppression de l'interface réseau de la fonction Lambda.

## AWS-UpdateAmazonECSAgent

### Description

Le AWS-UpdateAmazonECSAgent runbook met à jour l'agent Amazon Elastic Container Service (Amazon ECS) sur l'instance Amazon Elastic Compute Cloud (Amazon EC2) que vous spécifiez. Ce runbook ne prend en charge que les instances Amazon Linux et Amazon Linux 2.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Linux

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ARN du cluster

Type : StringList

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du cluster Amazon ECS auprès duquel vos instances de conteneur sont enregistrées.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

`aws:executeScript`- Met à jour l'agent Amazon ECS sur le cluster Amazon ECS que vous spécifiez dans les `ClusterARN` paramètres.

### Sorties

`UpdateAmazonAgent ECS`. `UpdatedContainers` - L'ID de l'instance où la mise à jour de l'agent Amazon ECS a réussi.

`UpdateAmazonAgent ECS`. `FailedContainers` - L'ID de l'instance où la mise à jour de l'agent Amazon ECS a échoué.



UpdateAmazonAgent ECS. InProgressContainers - L'ID de l'instance où la mise à jour de l'agent Amazon ECS est en cours.

## Amazon EFS

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Elastic File System. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

Rubriques

- [AWSSupport-CheckAndMountEFS](#)

### **AWSSupport - CheckAndMountEFS**

Description

Le AWSSupport-CheckAndMountEFS runbook vérifie les conditions requises pour monter votre système de fichiers Amazon Elastic File System (Amazon EFS) et monte le système de fichiers sur l'instance Amazon Elastic Compute Cloud (Amazon EC2) que vous spécifiez. Ce runbook prend en charge le montage de votre système de fichiers Amazon EFS à l'aide du nom DNS ou de l'adresse IP de la cible de montage.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Action

Type : chaîne

Valeurs valides : Vérifiez | CheckAndMount

Description : (Obligatoire) Détermine si le runbook vérifie les prérequis ou vérifie les prérequis et monte le système de fichiers.

- EfsId

Type : chaîne

Description : (Obligatoire) L'ID du système de fichiers que vous souhaitez monter.

- InstanceId

Type : chaîne

Description : (Obligatoire) L'ID de l'instance Amazon EC2 sur laquelle vous souhaitez monter le système de fichiers.

- MountOptions

Type : chaîne

Description : (Facultatif) Les options prises en charge par l'assistant de montage Amazon EFS que vous souhaitez utiliser lors du montage du système de fichiers. Si vous spécifiez `tls` cette option, vérifiez que `Stunnel` a été mis à niveau sur l'instance cible.

- MountPoint

Type : chaîne

Description : (Facultatif) Le répertoire dans lequel vous souhaitez monter le système de fichiers. Si vous spécifiez la `Check` valeur du `Action` paramètre, celui-ci ne doit pas être spécifié.

- MountTargetIP

Type : chaîne

Description : (Facultatif) Adresse IP de la cible de montage. Le montage par adresse IP fonctionne dans les environnements où le DNS est désactivé, tels que les clouds privés virtuels (VPC) dont les noms d'hôte DNS sont désactivés. Vous pouvez également utiliser cette option si votre environnement utilise un fournisseur DNS autre qu'Amazon Route 53 (Route 53).

- Région

Type : chaîne

Description : (Obligatoire) L' Région AWS emplacement de l'instance Amazon EC2 et du système de fichiers.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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:*`

## Étapes de document

- `aws:executeScript`- Recueille des informations sur l'instance Amazon EC2 que vous spécifiez dans `InstanceId` le paramètre.
- `aws:executeScript`- Rassemble des informations sur le système de fichiers que vous spécifiez dans le `EfsId` paramètre.
- `aws:executeScript`- Vérifie que le groupe de sécurité associé au système de fichiers autorise le trafic sur le port 2049 depuis l'instance Amazon EC2 que vous spécifiez dans le paramètre. `InstanceId`
- `aws:assertAwsResourceProperty`- Vérifie que l'instance Amazon EC2 que vous spécifiez dans `InstanceId` le paramètre est gérée par Systems Manager et que son statut est correct. `Online`
- `aws:branch`- Branches basées sur la valeur que vous spécifiez pour le `Action` paramètre.
- `aws:runCommand`- Vérifie les conditions requises pour le montage du système de fichiers que vous spécifiez dans le `EfsId` paramètre.
- `aws:runCommand`- Vérifie les conditions requises pour le montage du système de fichiers que vous spécifiez dans le `EfsId` paramètre, et monte le système de fichiers sur l'instance Amazon EC2 que vous spécifiez dans le paramètre. `InstanceId`

## Amazon EKS

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Elastic Kubernetes Service. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSSupport-CollectEKSIInstanceLogs](#)
- [AWS-CreateEKSClusterWithFargateProfile](#)
- [AWS-CreateEKSClusterWithNodegroup](#)

- [AWS-DeleteEKSCluster](#)
- [AWS-MigrateToNewEKSSelfManagedNodeGroup](#)
- [AWSPremiumSupport-TroubleshootEKSCluster](#)
- [AWSSupport-TroubleshootEKSWorkerNode](#)
- [AWS-UpdateEKSCluster](#)
- [AWS-UpdateEKSMangedNodeGroup](#)
- [AWS-UpdateEKSSelfManagedLinuxNodeGroups](#)

## AWSSupport-CollectEKSIInstanceLogs

### Description

Le `AWSSupport-CollectEKSIInstanceLogs` runbook rassemble les fichiers journaux relatifs au système d'exploitation et à Amazon Elastic Kubernetes Service (Amazon EKS) à partir d'une instance Amazon Elastic Compute Cloud (Amazon EC2) afin de vous aider à résoudre les problèmes courants. Pendant que l'automatisation collecte les fichiers journaux associés, des modifications sont apportées à la structure du système de fichiers, notamment la création de répertoires temporaires, la copie des fichiers journaux dans les répertoires temporaires et la compression des fichiers journaux dans une archive. Cette activité peut entraîner une augmentation de `CPUUtilization` l'instance EC2. Pour plus d'informations `CPUUtilization`, consultez la section [Mesures relatives aux instances](#) dans le guide de CloudWatch l'utilisateur Amazon.

Si vous spécifiez une valeur pour le `LogDestination` paramètre, l'automatisation évalue l'état de la politique du bucket Amazon Simple Storage Service (Amazon S3) que vous spécifiez. Pour renforcer la sécurité des journaux collectés depuis votre instance EC2, si le statut de la politique `isPublic` est défini sur `true`, ou si la liste de contrôle d'accès (ACL) accorde des `READ|WRITE` autorisations au groupe prédéfini `All Users Amazon S3`, les journaux ne sont pas chargés. Pour plus d'informations sur les groupes prédéfinis Amazon S3, consultez les [groupes prédéfinis Amazon S3](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

#### Note

Cette automatisation nécessite au moins 10 % de l'espace disque disponible sur le volume racine Amazon Elastic Block Store (Amazon EBS) attaché à votre instance EC2. Si l'espace disque disponible sur le volume racine est insuffisant, l'automatisation s'arrête.

## [Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Linux

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- EKS InstanceId

Type : chaîne

Description : ID (obligatoire) de l'instance Amazon EKS EC2 à partir de laquelle vous souhaitez collecter des journaux.

- LogDestination

Type : chaîne

Description : (Facultatif) Le compartiment S3 de votre compte dans lequel vous souhaitez télécharger les journaux archivés.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

Nous recommandons que l'instance EC2 recevant la commande ait un rôle IAM associé à la politique gérée par `ManagedInstanceCore` Amazon Amazon. Pour télécharger l'archive du journal dans le compartiment S3 que vous spécifiez dans le `LogDestination` paramètre, vous devez ajouter `s3:PutObject` autorisation.

### Étapes de document

- `aws:assertAwsResourceProperty`- Confirme que le système d'exploitation de la valeur spécifiée dans le `EKSInstanceId` paramètre est Linux.
- `aws:runCommand`- Rassemble les fichiers journaux liés au système d'exploitation et à Amazon EKS, en les compressant dans une archive dans le `/var/log` répertoire.
- `aws:branch`- Confirme si une valeur a été spécifiée pour le `LogDestination` paramètre.
- `aws:runCommand`- Télécharge l'archive du journal dans le compartiment S3 que vous spécifiez dans le `LogDestination` paramètre.

## AWS-CreateEKSClusterWithFargateProfile

### Description

Le `AWS-CreateEKSClusterWithFargateProfile` runbook crée un cluster Amazon Elastic Kubernetes Service (Amazon EKS) à l'aide d'un. AWS Fargate

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

## LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterName

Type : chaîne

Description : (Obligatoire) Nom unique pour le cluster.

- ClusterRoleArn

Type : chaîne

Description : (Obligatoire) L'ARN du rôle IAM qui autorise le plan de contrôle Kubernetes à effectuer des appels aux opérations d' AWS API en votre nom.

- FargateProfileName

Type : chaîne

Description : (Obligatoire) Nom du profil Fargate.

- FargateProfileRoleArn

Type : chaîne

Description : (Obligatoire) L'ARN du rôle IAM d'exécution du Pod Amazon EKS.

- FargateProfileSelectors

Type : chaîne

Description : (Obligatoire) Les sélecteurs permettant de faire correspondre les pods au profil Fargate.

- SubnetIds



Type : `StringList`

Description : (Obligatoire) Les identifiants des sous-réseaux que vous souhaitez utiliser pour votre cluster Amazon EKS. Amazon EKS crée des interfaces réseau élastiques dans ces sous-réseaux pour la communication entre vos nœuds et le plan de contrôle Kubernetes. Vous devez spécifier au moins deux ID de sous-réseau.

- `EKS EndpointPrivateAccess`

Type : booléen

Valeur par défaut : `True`

Description : (Facultatif) Définissez cette valeur sur `True` pour autoriser l'accès privé `True` au point de terminaison du serveur d'API Kubernetes de votre cluster. Si vous activez l'accès privé, les demandes d'API Kubernetes en provenance du VPC de votre cluster utilisent un point de terminaison d'un VPC privé. Si vous désactivez l'accès privé et que le cluster contient des nœuds ou AWS Fargate des pods, assurez-vous qu'ils `publicAccessCidrs` incluent les blocs CIDR nécessaires à la communication avec les nœuds ou les pods Fargate.

- `EKS EndpointPublicAccess`

Type : booléen

Par défaut : `false`

Description : (Facultatif) Définissez cette valeur sur `False` pour désactiver l'accès public `False` au point de terminaison du serveur d'API Kubernetes de votre cluster. Si vous désactivez l'accès public, le serveur d'API Kubernetes de votre cluster ne peut recevoir des demandes que depuis le VPC où il a été lancé.

- `PublicAccessCIDR`

Type : `StringList`

Description : (Facultatif) Les blocs CIDR autorisés à accéder au point de terminaison public du serveur d'API Kubernetes de votre cluster. La communication vers le point de terminaison à partir d'adresses situées en dehors des blocs d'adresse CIDR que vous spécifiez est refusée. Si vous avez désactivé l'accès privé aux terminaux et que le cluster contient des nœuds ou des pods Fargate, assurez-vous de spécifier les blocs d'adresse CIDR nécessaires.

- `SecurityGroupIds`

Type : StringList

Description : (Facultatif) Spécifiez un ou plusieurs groupes de sécurité à associer aux interfaces réseau élastiques créées dans votre compte par Amazon EKS.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

- `CreateEKSCluster` (`aws :executeAwsApi`) - Crée un cluster Amazon EKS.
- `VerifyEks ClusterIsActive` (`aws :waitForAwsResourceProperty`) - Vérifie que l'état du cluster est. ACTIVE
- `CreateFargateProfile` (`aws :executeAwsApi`) - Crée un Fargate pour le cluster.
- `VerifyFargateProfileIsActive` (`aws :waitForAwsResourceProperty`) - Vérifie que l'état du profil Fargate est. ACTIVE

## Sorties

### `CreateEKSCluster.CreateClusterResponse`

Description : réponse reçue à la suite de l'appel d'`CreateClusterAPI`.

### `CreateFargateProfile.CreateFargateProfileResponse`

Description : réponse reçue à la suite de l'appel d'`CreateFargateProfileAPI`.

## **AWS-CreateEKSClusterWithNodegroup**

### Description

Le `AWS-CreateEKSClusterWithNodegroup` runbook crée un cluster Amazon Elastic Kubernetes Service (Amazon EKS) en utilisant un groupe de nœuds pour la capacité.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `ClusterName`

Type : chaîne

Description : (Obligatoire) Nom unique pour le cluster.

- ClusterRoleArn

Type : chaîne

Description : (Obligatoire) L'ARN du rôle IAM qui autorise le plan de contrôle Kubernetes à effectuer des appels aux opérations d' AWS API en votre nom.

- NodegroupName

Type : chaîne

Description : (Obligatoire) Nom unique pour le groupe de nœuds.

- NodegroupRoleArn

Type : chaîne

Description : (Obligatoire) L'ARN du rôle IAM à associer à votre groupe de nœuds. Le démon kubelet du nœud de travail Amazon EKS passe des appels aux AWS API en votre nom. Les nœuds reçoivent l'autorisation pour ces appels d'API via un profil d'instance IAM et les politiques associées. Avant de pouvoir lancer les nœuds et les enregistrer dans un cluster, vous devez créer un rôle IAM qui sera utilisé par ces nœuds lors de leur lancement.

- SubnetIds

Type : StringList

Description : (Obligatoire) Les identifiants des sous-réseaux que vous souhaitez utiliser pour votre cluster Amazon EKS. Amazon EKS crée des interfaces réseau élastiques dans ces sous-réseaux pour la communication entre vos nœuds et le plan de contrôle Kubernetes. Vous devez spécifier au moins deux ID de sous-réseau.

- EKSEndpointPrivateAccess

Type : booléen

Valeur par défaut : True

Description : (Facultatif) Définissez cette valeur sur `True` pour autoriser l'accès privé au point de terminaison du serveur d'API Kubernetes de votre cluster. Si vous activez l'accès privé,

les demandes d'API Kubernetes en provenance du VPC de votre cluster utilisent un point de terminaison d'un VPC privé. Si vous désactivez l'accès privé et que le cluster contient des nœuds ou AWS Fargate des pods, assurez-vous qu'ils `publicAccessCidrs` incluent les blocs CIDR nécessaires à la communication avec les nœuds ou les pods Fargate.

- `EKS EndpointPublicAccess`

Type : booléen

Par défaut : `false`

Description : (Facultatif) Définissez cette valeur sur `false` pour désactiver l'accès public au point de terminaison du serveur d'API Kubernetes de votre cluster. Si vous désactivez l'accès public, le serveur d'API Kubernetes de votre cluster ne peut recevoir des demandes que depuis le VPC où il a été lancé.

- `PublicAccessCIDR`

Type : `StringList`

Description : (Facultatif) Les blocs CIDR autorisés à accéder au point de terminaison public du serveur d'API Kubernetes de votre cluster. La communication vers le point de terminaison à partir d'adresses situées en dehors des blocs d'adresse CIDR que vous spécifiez est refusée. Si vous avez désactivé l'accès privé aux terminaux et que le cluster contient des nœuds ou des pods Fargate, assurez-vous de spécifier les blocs d'adresse CIDR nécessaires.

- `SecurityGroupIds`

Type : `StringList`

Description : (Facultatif) Spécifiez un ou plusieurs groupes de sécurité à associer aux interfaces réseau élastiques créées dans votre compte par Amazon EKS.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam>ListAttachedRolePolicies`
- `iam:PassRole`

### Étapes de document

- `CreateEKSCluster` (`aws :executeAwsApi`) - Crée un cluster Amazon EKS.
- `VerifyEksClusterIsActive` (`aws :waitForAwsResourceProperty`) - Vérifie que l'état du cluster est `ACTIVE`
- `CreateNodegroup` (`aws :executeAwsApi`) - Crée un groupe de nœuds pour le cluster.
- `VerifyNodegroupIsActive` (`aws :waitForAwsResourceProperty`) - Vérifie que l'état du groupe de nœuds est `ACTIVE`.

### Sorties

- `CreateEKSCluster.CreateClusterResponse`: réponse reçue à la suite de l'appel d'`CreateClusterAPI`.
- `CreateNodegroup.CreateNodegroupResponse`: réponse reçue à la suite de l'appel d'`CreateNodegroupAPI`.

## AWS-DeleteEKSCluster

### Description

Ce runbook supprime les ressources associées à un cluster Amazon EKS, notamment les groupes de nœuds et les profils Fargate. Vous pouvez éventuellement choisir de supprimer tous les nœuds autogérés, les AWS CloudFormation piles utilisées pour créer les nœuds et la CloudFormation pile VPC de votre cluster. Pour plus d'informations sur la suppression d'un cluster, consultez [Supprimer un cluster](#) dans le guide de l'utilisateur Amazon EKS.

**Note**

Si votre cluster comporte des services actifs associés à un équilibreur de charge, vous devez supprimer ces services avant de supprimer le cluster. Dans le cas contraire, le système ne pourra pas supprimer les équilibreurs de charge. Suivez la procédure ci-dessous pour rechercher et supprimer des services avant d'exécuter le `AWS-DeleteEKSCluster` runbook.

Pour localiser et supprimer des services dans votre cluster

1. Installez l'utilitaire de ligne de commande Kubernetes, `kubectl`. Pour plus d'informations, consultez la section [Installation de kubectl](#) dans le guide de l'utilisateur Amazon EKS.
2. Exécutez la commande suivante pour répertorier tous les services exécutés dans votre cluster.

```
kubectl get svc --all-namespaces
```

3. Exécutez la commande suivante pour supprimer tous les services associés à une valeur `EXTERNAL-IP`. Ces services sont dirigés par un équilibreur de charge, et vous devez les supprimer dans Kubernetes pour permettre à l'équilibreur de charge et aux ressources associées d'être correctement libérés.

```
kubectl delete svc  
service-name
```

Vous pouvez maintenant exécuter le `AWS-DeleteEKSCluster` runbook.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

## LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- EKS ClusterName

Type : chaîne

Description : (Obligatoire) Nom du cluster Amazon EKS à supprimer.

- VPC CloudFormationStack

Type : chaîne

Description : nom de AWS CloudFormation pile (facultatif) pour le VPC du cluster EKS en cours de suppression. Cela supprime la AWS CloudFormation pile pour VPC et toutes les ressources créées par la pile.

- VPC CloudFormationStackRole

Type : chaîne

Description : (Facultatif) L'ARN d'un rôle IAM AWS CloudFormation censé supprimer la pile CloudFormation VPC. AWS CloudFormation utilise les informations d'identification du rôle pour passer des appels en votre nom.

- SelfManagedNodeStacks

Type : chaîne

Description : (Facultatif) Liste de noms de AWS CloudFormation pile séparés par des virgules pour les nœuds autogérés. Cela supprimera les AWS CloudFormation piles pour les nœuds autogérés.

- SelfManagedNodeStacksRole

Type : chaîne



Description : (Facultatif) L'ARN d'un rôle IAM censé AWS CloudFormation supprimer les piles de nœuds autogérées. AWS CloudFormation utilise les informations d'identification du rôle pour passer des appels en votre nom.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- sts:AssumeRole
- eks:ListNodegroups
- eks>DeleteNodegroup
- eks>ListFargateProfiles
- eks>DeleteFargateProfile
- eks>DeleteCluster
- cfn:DescribeStacks
- cfn>DeleteStack

### Étapes de document

- aws:executeScript- DeleteNodeGroups : Recherchez et supprimez tous les groupes de nœuds du cluster EKS.
- aws:executeScript- DeleteFargateProfiles : Recherchez et supprimez tous les profils Fargate dans le cluster EKS.
- aws:executeScript- DeleteSelfManagedNodes : Supprimez tous les nœuds autogérés et les CloudFormation piles utilisées pour créer les nœuds.
- aws:executeScript- DeleteEksCluster : Supprime le cluster EKS.
- aws:executeScript- DeleteVPC CloudFormationStack : supprimez la pile de VPC. CloudFormation

## **AWS-MigrateToNewEKSSelfManagedNodeGroup**

### Description

Le `AWS-MigrateToNewEKSSelfManagedNodeGroup` runbook vous aide à créer un nouveau groupe de nœuds Linux Amazon Elastic Kubernetes Service (Amazon EKS) vers lequel migrer votre application existante. Pour plus d'informations, consultez la section [Migration vers un nouveau groupe de nœuds](#) dans le guide de l'utilisateur Amazon EKS.

### [Exécuter cette automatisation \(console\)](#)

#### Type de document

Automatisation

#### Propriétaire

Amazon

#### Plateformes

Linux

#### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- OldStackName

Type : chaîne

Description : (Obligatoire) Le nom ou l'ID de pile de votre AWS CloudFormation pile existante.

- NewStackName

Type : chaîne

Description : (Facultatif) Le nom de la nouvelle AWS CloudFormation pile créée pour votre nouveau groupe de nœuds. Si vous ne spécifiez aucune valeur pour ce paramètre, le nom de la pile est créé au format :`NewNodeGroup-ClusterName-AutomationExecutionID`.

- `ClusterControlPlaneSecurityGroup`

Type : chaîne

Description : (Facultatif) L'ID du groupe de sécurité que vous souhaitez que les nœuds utilisent pour communiquer avec le plan de contrôle Amazon EKS. Si vous ne spécifiez aucune valeur pour ce paramètre, le groupe de sécurité spécifié dans votre AWS CloudFormation pile existante est utilisé.

- `NodeInstanceType`

Type : chaîne

Description : (Facultatif) Type d'instance que vous souhaitez utiliser pour le nouveau groupe de nœuds. Si vous ne spécifiez aucune valeur pour ce paramètre, le type d'instance spécifié dans votre AWS CloudFormation pile existante est utilisé.

- `NodeGroupName`

Type : chaîne

Description : (Facultatif) Le nom de votre nouveau groupe de nœuds. Si vous ne spécifiez aucune valeur pour ce paramètre, le nom du groupe de nœuds spécifié dans votre AWS CloudFormation pile existante est utilisé.

- `NodeAutoScalingGroupDesiredCapacity`

Type : chaîne

Description : (Facultatif) Le nombre de nœuds souhaité à atteindre lors de la création de votre nouvelle pile. Ce nombre doit être supérieur ou égal à la `NodeAutoScalingGroupMinSize` valeur et inférieur ou égal à `NodeAutoScalingGroupMaxSize`. Si vous ne spécifiez aucune valeur pour ce paramètre, la capacité souhaitée du groupe de nœuds spécifiée dans votre AWS CloudFormation pile existante est utilisée.

- `NodeAutoScalingGroupMaxSize`

Type : chaîne

Description : (Facultatif) Le nombre maximum de nœuds que votre groupe de nœuds peut atteindre. Si vous ne spécifiez aucune valeur pour ce paramètre, la taille maximale du groupe de nœuds spécifiée dans votre AWS CloudFormation pile existante est utilisée.

- `NodeAutoScalingGroupMinSize`

Type : chaîne

Description : (Facultatif) Le nombre minimum de nœuds que votre groupe de nœuds peut atteindre. Si vous ne spécifiez aucune valeur pour ce paramètre, la taille minimale du groupe de nœuds spécifiée dans votre AWS CloudFormation pile existante est utilisée.

- NodeImageId

Type : chaîne

Description : (Facultatif) L'ID du Amazon Machine Image (AMI) que vous souhaitez que le groupe de nœuds utilise.

- NodeImageIdParamètre SSM

Type : chaîne

Description : (Facultatif) Le paramètre public de Systems Manager AMI que vous souhaitez que le groupe de nœuds utilise.

- NodeVolumeSize

Type : chaîne

Description : (Facultatif) Taille du volume racine de vos nœuds en GiB. Si vous ne spécifiez aucune valeur pour ce paramètre, la taille du volume du nœud spécifiée dans votre AWS CloudFormation pile existante est utilisée.

- NodeVolumeType

Type : chaîne

Description : (Facultatif) Type de volume Amazon EBS que vous souhaitez utiliser pour le volume racine de vos nœuds. Si vous ne spécifiez aucune valeur pour ce paramètre, le type de volume spécifié dans votre AWS CloudFormation pile existante est utilisé.

- KeyName

Type : chaîne

Description : (Facultatif) La paire de clés que vous souhaitez attribuer à vos nœuds. Si vous ne spécifiez aucune valeur pour ce paramètre, la paire de clés spécifiée dans votre AWS CloudFormation pile existante est utilisée.

- **Sous-réseaux**

Type : StringList

Description : (Facultatif) Liste séparée par des virgules des ID de sous-réseau que vous souhaitez utiliser pour votre nouveau groupe de nœuds. Si vous ne spécifiez aucune valeur pour ce paramètre, les sous-réseaux spécifiés dans votre AWS CloudFormation pile existante sont utilisés.

- **Désactiver IMDS V1**

Type : booléen

Description : (Facultatif) Spécifiez `true` la désactivation du service de métadonnées d'instance version 1 (IMDSv1). Par défaut, les nœuds prennent en charge IMDSv1 et IMDSv2.

- **BootstrapArguments**

Type : chaîne

Description : (Facultatif) Arguments supplémentaires que vous souhaitez transmettre au script bootstrap du nœud.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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:DescribeInstanceState`
- `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`

## Étapes de document

- `DetermineParameterValuesForNewNodeGroup` (AWS:ExecuteScript) - Rassemble les valeurs des paramètres à utiliser pour le nouveau groupe de nœuds.
- `CreateStack` (AWS:CreateStack) - Crée la AWS CloudFormation pile pour le nouveau groupe de nœuds.
- `GetNewStackNodeInstanceRole` (aws :executeAwsApi) - Obtient le rôle d'instance du nœud.
- `GetNewStackSecurityGroup` (aws :executeAwsApi) - L'étape obtient le groupe de sécurité du nœud.
- `AddIngressRulesToNewNodeSecurityGroup` (aws :executeAwsApi) - Ajoute des règles d'entrée au groupe de sécurité nouvellement créé afin qu'il puisse accepter le trafic provenant de celui attribué à votre groupe de nœuds précédent.
- `AddIngressRulesToOldNodeSecurityGroup` (aws :executeAwsApi) - Ajoute des règles d'entrée au groupe de sécurité précédent afin qu'il puisse accepter le trafic provenant de celui attribué à votre nouveau groupe de nœuds.
- `VerifyStackComplete` (aws : assertAwsResource Property) - Vérifie que le nouveau statut de la pile est `CREATE_COMPLETE`.

## Sorties

`DetermineParameterValuesForNewNodeGroup`. `NewStackParameters` - Les paramètres utilisés pour créer la nouvelle pile.

`GetNewStackNodeInstanceRole`. `NewNodeInstanceRole` - Le rôle d'instance de nœud pour le nouveau groupe de nœuds.

`GetNewStackSecurityGroup`. `NewNodeSecurityGroup` - L'ID du groupe de sécurité pour le nouveau groupe de nœuds.

DetermineParameterValuesForNewNodeGroup. NewStackName - Le nom de la AWS CloudFormation pile pour le nouveau groupe de nœuds.

CreateStack. StackId - L'ID de AWS CloudFormation pile du nouveau groupe de nœuds.

## AWSPremiumSupport-TroubleshootEKSCluster

### Description

Le AWSPremiumSupport-TroubleshootEKSCluster runbook diagnostique les problèmes courants liés à un cluster Amazon Elastic Kubernetes Service (Amazon EKS) et à l'infrastructure sous-jacente, et propose des mesures correctives recommandées.

#### Important

L'accès aux AWSPremiumSupport- \* runbooks nécessite un abonnement Enterprise ou Business Support. Pour plus d'informations, consultez la section [Comparer les plans de AWS support](#).

Si vous spécifiez une valeur pour le S3BucketName paramètre, l'automatisation évalue l'état de la politique du bucket Amazon Simple Storage Service (Amazon S3) que vous spécifiez. Pour renforcer la sécurité des journaux collectés depuis votre instance EC2, si le statut de la politique isPublic est défini sur true, ou si la liste de contrôle d'accès (ACL) accorde des READ|WRITE autorisations au groupe prédéfini All Users Amazon S3, les journaux ne sont pas chargés. Pour plus d'informations sur les groupes prédéfinis Amazon S3, consultez les [groupes prédéfinis Amazon S3](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes



## LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterName

Type : chaîne

Description : (Obligatoire) Nom du cluster Amazon EKS que vous souhaitez dépanner.

- S3 BucketName

Type : chaîne

Description : (Facultatif) Le nom du compartiment privé Amazon S3 dans lequel le rapport généré par le runbook doit être chargé.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

En outre, la politique AWS Identity and Access Management (IAM) attachée à l'utilisateur ou au rôle qui lance l'automatisation doit autoriser l'`ssm:GetParameter` opération selon les AWS Systems Manager paramètres publics suivants afin d'obtenir le dernier Amazon EKS Amazon Machine Image (AMI) recommandé pour les nœuds de travail.

- `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`

Pour télécharger le rapport généré par le runbook dans un compartiment Amazon S3, les autorisations suivantes sont requises pour le compartiment Amazon S3 que vous spécifiez.

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

Étapes de document

- `aws:executeAwsApi`- Rassemble les informations relatives au cluster Amazon EKS spécifié.
- `aws:executeScript`- Recueille des informations sur les instances Amazon Elastic Compute Cloud (Amazon EC2), les groupes Auto Scaling AMI et les types d'instances graphiques de GPU Amazon EC2.
- `aws:executeScript`- Recueille des informations sur le cloud privé virtuel (VPC), les sous-réseaux, les passerelles de traduction d'adresses réseau (NAT), les routes de sous-réseau, les groupes de sécurité et les listes de contrôle d'accès réseau (ACL) du cluster Amazon EKS.
- `aws:executeScript`- Rassemble les détails des profils d'instance IAM attachés et des politiques de rôle.
- `aws:executeScript`- Rassemble les détails du compartiment Amazon S3 que vous spécifiez dans le `S3BucketName` paramètre.
- `aws:executeScript`- Classifie les sous-réseaux Amazon VPC comme publics ou privés.
- `aws:executeScript`- Vérifie les sous-réseaux Amazon VPC pour détecter les balises requises dans le cadre d'un cluster Amazon EKS.
- `aws:executeScript`- Vérifie dans les sous-réseaux Amazon VPC les balises requises pour les sous-réseaux Elastic Load Balancing.
- `aws:executeScript`- Vérifie si les instances Amazon EC2 du nœud de travail utilisent les dernières versions optimisées d'Amazon EKS AMI
- `aws:executeScript`- Vérifie si les groupes de sécurité Amazon VPC attachés aux nœuds de travail contiennent les balises requises.
- `aws:executeScript`- Vérifie que les règles du groupe de sécurité Amazon VPC du cluster Amazon EKS et du nœud de travail sont conformes aux règles d'entrée recommandées dans le cluster Amazon EKS.
- `aws:executeScript`- Vérifie les règles du groupe de sécurité Amazon EKS du cluster Amazon EKS et du nœud de travail Amazon VPC pour vérifier les règles de sortie recommandées depuis le cluster Amazon EKS.
- `aws:executeScript`- Vérifie la configuration réseau ACL des sous-réseaux Amazon VPC.
- `aws:executeScript`- Vérifie si les instances Amazon EC2 du nœud de travail disposent des politiques gérées requises.
- `aws:executeScript`- Vérifie si les groupes Auto Scaling possèdent les balises nécessaires à l'autoscaling des clusters.
- `aws:executeScript`- Vérifie si les instances Amazon EC2 du nœud de travail sont connectées à Internet.

- `aws:executeScript`- Génère un rapport basé sur les résultats des étapes précédentes. Si une valeur est spécifiée pour le `S3BucketName` paramètre, le rapport généré est chargé dans le compartiment Amazon S3.

## AWSSupport-TroubleshootEKSWorkerNode

### Description

Le `AWSSupport-TroubleshootEKSWorkerNode` runbook analyse un nœud de travail Amazon Elastic Compute Cloud (Amazon EC2) et un cluster Amazon Elastic Kubernetes Service (Amazon EKS) pour vous aider à identifier et à résoudre les causes courantes qui empêchent les nœuds de travail de rejoindre un cluster. Le runbook fournit des conseils pour vous aider à résoudre les problèmes identifiés.

#### Important

Pour exécuter correctement cette automatisation, l'état de votre nœud de travail Amazon EC2 doit être égal `running` à celui du cluster Amazon EKS. `ACTIVE`

### [Exécuter cette automatisation \(console\)](#)

#### Type de document

Automatisation

#### Propriétaire

Amazon

#### Plateformes

Linux

#### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterName

Type : chaîne

Description : (Obligatoire) Nom du cluster Amazon EKS.

- Identifiant du travailleur

Type : chaîne

Description : (Obligatoire) L'ID du nœud de travail Amazon EC2 qui n'a pas réussi à rejoindre le cluster.

#### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

- `aws:assertAwsResourceProperty`- Confirme que le cluster Amazon EKS que vous spécifiez dans le `ClusterName` paramètre existe et est dans un `ACTIVE` état.
- `aws:assertAwsResourceProperty`- Confirme que le nœud de travail Amazon EC2 que vous spécifiez dans le `WorkerID` paramètre existe et est dans un `running` état.
- `aws:executeScript`- Exécute un script Python qui permet d'identifier les causes possibles de l'échec du nœud de travail à rejoindre le cluster.

## AWS-UpdateEKSCluster

### Description

Le `AWS-UpdateEKSCluster` runbook vous aide à mettre à jour votre cluster Amazon Elastic Kubernetes Service (Amazon EKS) vers la version de Kubernetes que vous souhaitez utiliser.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterName

Type : chaîne

Description : (Obligatoire) Le nom de votre cluster Amazon EKS.

- Version

Type : chaîne

Description : (Obligatoire) Version de Kubernetes vers laquelle vous souhaitez mettre à jour votre cluster.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- eks:DescribeUpdate
- eks:UpdateClusterVersion

## Étapes de document

- aws:executeAwsApi- Met à jour la version de Kubernetes utilisée par votre cluster Amazon EKS.
- aws:waitForAwsResourceProperty- Attend que l'état de la mise à jour soit atteint.

Successful

# AWS-UpdateEKSMangedNodeGroup

## Description

Le AWS-UpdateEKSMangedNodeGroup runbook vous aide à mettre à jour un groupe de nœuds géré par Amazon Elastic Kubernetes Service (Amazon EKS). Vous pouvez choisir un `Version` ou `Configuration` mettre à jour.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterName

Type : chaîne

Description : (Obligatoire) Le nom du cluster dont vous souhaitez mettre à jour le groupe de nœuds.

- NodeGroupName

Type : chaîne



Description : (Obligatoire) Nom du groupe de nœuds à mettre à jour.

- UpdateType

Type : chaîne

Valeurs valides : Mettre à jour la version du groupe de nœuds | Mettre à jour les configurations du groupe de nœuds

Par défaut : Mettre à jour la version du groupe de nœuds

Description : (Obligatoire) Type de mise à jour que vous souhaitez effectuer sur le groupe de nœuds.

Les paramètres suivants s'appliquent uniquement au type de Version mise à jour :

- AMI ReleaseVersion

Type : chaîne

Description : (Facultatif) Version optimisée d'Amazon EKS AMI que vous souhaitez utiliser. Par défaut, c'est la dernière version qui est utilisée.

- ForceUpgrade

Type : booléen

Description : (Facultatif) Si c'est vrai, la mise à jour n'échouera pas en cas de violation du budget lié à l'interruption du module.

- KubernetesVersion

Type : chaîne

Description : (Facultatif) Version de Kubernetes vers laquelle mettre à jour le groupe de nœuds.

- LaunchTemplateId

Type : chaîne

Description : (Facultatif) L'ID du modèle de lancement.

- LaunchTemplateName

Type : chaîne

Description : (Facultatif) Le nom du modèle de lancement.

- LaunchTemplateVersion

Type : chaîne

Description : (Facultatif) Version du modèle de lancement d'Amazon Elastic Compute Cloud (Amazon EC2). Ce paramètre n'est valide que si un groupe de nœuds a été créé à partir d'un modèle de lancement.

Les paramètres suivants s'appliquent uniquement au type de Configuration mise à jour :

- AddOrUpdateNodeGroupLabels

Type : StringMap

Description : (Facultatif) Étiquettes Kubernetes que vous souhaitez ajouter ou mettre à jour.

- AddOrUpdateKubernetesTaintsEffect

Type : StringList

Description : (Facultatif) Les tâches Kubernetes que vous souhaitez ajouter ou mettre à jour.

- MaxUnavailableNodeGroups

Type : entier

Par défaut : 0

Description : (Facultatif) Nombre maximal de nœuds indisponibles simultanément lors d'une mise à jour de version.

- MaxUnavailablePercentageNodeGroup

Type : entier

Par défaut : 0

Description : (Facultatif) Pourcentage de nœuds non disponibles lors d'une mise à jour de version.

- NodeGroupDesiredSize

Type : entier

Par défaut : 0

Description : (Facultatif) Nombre de nœuds que le groupe de nœuds gérés doit gérer.

- `NodeGroupMaxSize`

Type : entier

Par défaut : 0

Description : (Facultatif) Nombre maximal de nœuds que le groupe de nœuds gérés peut atteindre.

- `NodeGroupMinSize`

Type : entier

Par défaut : 0

Description : (Facultatif) Le nombre minimum de nœuds que le groupe de nœuds gérés peut atteindre.

- `RemoveKubernetesTaintsEffect`

Type : `StringList`

Description : (Facultatif) Les tâches de Kubernetes que vous souhaitez supprimer.

- `RemoveNodeGroupLabels`

Type : `StringList`

Description : (Facultatif) Liste séparée par des virgules des libellés que vous souhaitez supprimer.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

## Étapes de document

- `aws:executeScript`- Met à jour un groupe de nœuds de cluster Amazon EKS en fonction des valeurs que vous spécifiez pour les paramètres d'entrée du runbook.
- `aws:waitForAwsResourceProperty`- Attend que l'état de mise à jour du cluster soit atteint. `Successful`

## AWS-UpdateEKSSelfManagedLinuxNodeGroups

### Description

Le `AWS-UpdateEKSSelfManagedLinuxNodeGroups` runbook met à jour les groupes de nœuds autogérés dans votre cluster Amazon Elastic Kubernetes Service (Amazon EKS) à l'aide d'une pile. `AWS CloudFormation`

Si votre cluster utilise le dimensionnement automatique, nous vous recommandons de réduire le déploiement à deux répliques avant d'utiliser ce runbook.

Pour étendre un déploiement à deux répliques

1. Installez l'utilitaire de ligne de commande Kubernetes, `kubectl`. Pour plus d'informations, consultez [Installation de kubectl](#) dans le Guide de l'utilisateur Amazon EKS.
2. Exécutez la commande suivante.

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. Lancez le `AWS-UpdateEKSSelfManagedLinuxNodeGroups` runbook.
4. Réduisez le déploiement au nombre de répliques souhaité en exécutant la commande suivante.

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

### [Exécuter cette automatisation \(console\)](#)

### Type de document

### Automatisation

### Propriétaire

## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterName

Type : chaîne

Description : (Obligatoire) Nom du cluster Amazon EKS.

- NodeGroupName

Type : chaîne

Description : (Obligatoire) Nom du groupe de nœuds géré.

- ClusterControlPlaneSecurityGroup

Type : chaîne

Description : (Obligatoire) L'ID du groupe de sécurité du plan de contrôle.

- Désactiver IMDS V1

Type : booléen

Description : (Facultatif) Détermine si vous souhaitez autoriser le service de métadonnées d'instance version 1 (IMDSv1) et IMDSv2.

- KeyName

Type : chaîne

Description : (Facultatif) Le nom de clé des instances.

- NodeAutoScalingGroupDesiredCapacity

Type : chaîne

Description : (Facultatif) Nombre de nœuds que le groupe de nœuds doit gérer.

- NodeAutoScalingGroupMaxSize

Type : chaîne

Description : (Facultatif) Nombre maximal de nœuds que le groupe de nœuds peut atteindre.

- NodeAutoScalingGroupMinSize

Type : chaîne

Description : (Facultatif) Le nombre minimum de nœuds que le groupe de nœuds peut atteindre.

- NodeInstanceType

Type : chaîne

Par défaut : t3.large

Description : (Facultatif) Type d'instance que vous souhaitez utiliser pour le groupe de nœuds.

- NodeImageId

Type : chaîne

Description : (Facultatif) L'ID du Amazon Machine Image (AMI) que vous souhaitez que le groupe de nœuds utilise.

- NodeImageIdParamètre SSM

Type : chaîne

Par défaut : /aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image\_id

Description : (Facultatif) Le paramètre public de Systems Manager AMI que vous souhaitez que le groupe de nœuds utilise.

- StackName

Type : chaîne

Description : (Obligatoire) Nom de la AWS CloudFormation pile utilisée pour mettre à jour le groupe de nœuds.

- Sous-réseaux

Type : chaîne

Description : (Obligatoire) Liste séparée par des virgules des identifiants des sous-réseaux que vous souhaitez que votre cluster utilise.

- VpcId

Type : chaîne

Par défaut : Default

Description : (Obligatoire) Le cloud privé virtuel (VPC) sur lequel votre cluster est déployé.

#### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks>DeleteNodegroup`
- `eks>DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

#### Étapes de document

- `aws:executeScript`- Met à jour un groupe de nœuds de cluster Amazon EKS en fonction des valeurs que vous spécifiez pour les paramètres d'entrée du runbook.
- `aws:waitForAwsResourceProperty`- Attend que l'état de mise à jour de la AWS CloudFormation pile soit renvoyé.

## Elastic Beanstalk

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Elastic Beanstalk. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSSupport-CollectElasticBeanstalkLogs](#)
- [AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming](#)
- [AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications](#)
- [AWSSupport-TroubleshootElasticBeanstalk](#)

## AWSSupport-CollectElasticBeanstalkLogs

### Description

Le `AWSSupport-CollectElasticBeanstalkLogs` runbook rassemble les fichiers journaux AWS Elastic Beanstalk associés à partir d'une instance Amazon Elastic Compute Cloud (Amazon Windows Server EC2) lancée par Elastic Beanstalk pour vous aider à résoudre les problèmes courants. Pendant que l'automatisation collecte les fichiers journaux associés, des modifications sont apportées à la structure du système de fichiers, notamment la création de répertoires temporaires, la copie des fichiers journaux dans les répertoires temporaires et la compression des fichiers journaux dans une archive. Cette activité peut entraîner une augmentation de `CPUUtilization` l'instance Amazon EC2. Pour plus d'informations `CPUUtilization`, consultez la section [Mesures relatives aux instances](#) dans le guide de CloudWatch l'utilisateur Amazon.

Si vous spécifiez une valeur pour le `S3BucketName` paramètre, l'automatisation évalue l'état de la politique du bucket Amazon Simple Storage Service (Amazon S3) que vous spécifiez. Pour renforcer la sécurité des journaux collectés depuis votre instance Amazon EC2, si le statut de la politique `isPublic` est défini sur `true`, ou si la liste de contrôle d'accès (ACL) accorde des `READ|WRITE`



autorisations au groupe prédéfini `All Users Amazon S3`, les journaux ne sont pas chargés. Pour plus d'informations sur les groupes prédéfinis Amazon S3, consultez les [groupes prédéfinis Amazon S3](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Si vous ne spécifiez aucune valeur pour le `S3BucketName` paramètre, l'automatisation télécharge le bundle de journaux dans le Région AWS bucket Amazon S3 Elastic Beanstalk par défaut dans lequel vous exécutez l'automatisation. Le répertoire est nommé selon la structure suivante, `elasticbeanstalk-region - accountID`. Les valeurs de *région* et d'*AccountID* varient en fonction de la région dans Compte AWS laquelle vous exécutez l'automatisation. Le paquet de journaux sera enregistré `resources/environments/logs/bundle/environmentID / instanceID` dans le répertoire. Les valeurs *EnvironmentID* et *InstanceID* varient en fonction de votre environnement Elastic Beanstalk et de l'instance Amazon EC2 à partir de laquelle vous collectez les logs.

Par défaut, le profil d'instance AWS Identity and Access Management (IAM) attaché aux instances Amazon EC2 de l'environnement Elastic Beanstalk dispose des autorisations requises pour télécharger le bundle dans le compartiment Elastic Beanstalk Amazon S3 par défaut de votre environnement. Si vous spécifiez une valeur pour le `S3BucketName` paramètre, le profil d'instance attaché à l'instance Amazon EC2 doit autoriser les `s3:PutObject` actions `s3:GetBucketAcl`, `s3:GetBucketPolicies` et `s3:GetBucketPolicyStatus`, et pour le compartiment et le chemin Amazon S3 spécifiés.

#### Note

Cette automatisation nécessite au moins 500 Mo d'espace disque disponible sur le volume racine Amazon Elastic Block Store (Amazon EBS) attaché à votre instance Amazon EC2. Si l'espace disque disponible sur le volume racine est insuffisant, l'automatisation s'arrête.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

## Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- EnvironmentId

Type : chaîne

Description : (Obligatoire) L'ID de votre environnement Elastic Beanstalk à partir duquel vous souhaitez collecter le bundle de logs.

- InstanceId

Type : chaîne

(Obligatoire) L'ID de l'instance Amazon EC2 de votre environnement Elastic Beanstalk à partir de laquelle vous souhaitez collecter le bundle de logs.

- S3 BucketName

Type : chaîne

(Facultatif) Le compartiment Amazon S3 dans lequel vous souhaitez télécharger les journaux archivés.

- S3 BucketPath

Type : chaîne

(Facultatif) Le chemin du compartiment Amazon S3 vers lequel vous souhaitez télécharger le bundle de journaux. Ce paramètre est ignoré si vous ne spécifiez aucune valeur pour le S3BucketName paramètre.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`

### Étapes de document

- `aws:assertAwsResourceProperty`- Confirme que l'instance Amazon EC2 que vous spécifiez dans le `InstanceId` paramètre est gérée par. AWS Systems Manager
- `aws:assertAwsResourceProperty`- Confirme que l'instance Amazon EC2 que vous spécifiez dans le `InstanceId` paramètre est une Windows Server instance.
- `aws:runCommand`- Vérifie si l'instance fait partie d'un environnement Elastic Beanstalk, si l'espace disque est suffisant pour regrouper les journaux et si le compartiment Amazon S3 dans lequel les journaux seront téléchargés est public.
- `aws:runCommand`- Collecte les fichiers journaux et télécharge l'archive dans le compartiment Amazon S3 spécifié dans le `S3BucketName` paramètre ou dans le compartiment par défaut de votre environnement Elastic Beanstalk si aucune valeur n'est spécifiée.

## **AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming**

### Description

Le `AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming` runbook permet de se connecter à l'environnement AWS Elastic Beanstalk (Elastic Beanstalk) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- EnvironmentId

Type : chaîne

Description : (Obligatoire) L'ID de l'environnement Elastic Beanstalk auquel vous souhaitez activer la connexion.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

## Étapes de document

- aws:executeAwsApi- Active la journalisation sur l'environnement Elastic Beanstalk que vous spécifiez dans le paramètre. EnvironmentId

- `aws:waitForAwsResourceProperty`- Attend que l'état de l'environnement passe àReady.
- `aws:executeScript`- Vérifie que la journalisation a été activée dans l'environnement Elastic Beanstalk.

## **AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications**

### Description

Le `AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications` runbook active les notifications pour l'environnement AWS Elastic Beanstalk (Elastic Beanstalk) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `EnvironmentId`

Type : chaîne

Description : (Obligatoire) L'ID de l'environnement Elastic Beanstalk pour lequel vous souhaitez activer les notifications.

- TopicArn

Type : chaîne

Description : (Obligatoire) L'ARN de la rubrique Amazon Simple Notification Service (Amazon SNS) à laquelle vous souhaitez envoyer des notifications.

#### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

#### Étapes de document

- aws:executeAwsApi- Active les notifications pour l'environnement Elastic Beanstalk que vous spécifiez dans le paramètre. EnvironmentId
- aws:waitForAwsResourceProperty- Attend que l'état de l'environnement passe àReady.
- aws:executeScript- Vérifie que les notifications ont été activées pour l'environnement Elastic Beanstalk.

## **AWSSupport-TroubleshootElasticBeanstalk**

### Description

Le AWSSupport-TroubleshootElasticBeanstalk runbook vous aide à résoudre les causes potentielles pour lesquelles votre AWS Elastic Beanstalk environnement est dans un état Degraded ou Severe. Cette automatisation vérifie les AWS ressources suivantes associées à votre environnement Elastic Beanstalk :

- Détails de configuration pour un équilibreur de charge, une AWS CloudFormation pile, un groupe Amazon EC2 Auto Scaling, des instances Amazon Elastic Compute Cloud (Amazon EC2) et un cloud privé virtuel (VPC).
- Problèmes de configuration réseau liés aux règles de groupe de sécurité, aux tables de routage et aux listes de contrôle d'accès réseau (ACL) associées à vos sous-réseaux.
- Vérifie la connectivité aux points de terminaison Elastic Beanstalk et à l'accès public à Internet.
- Vérifie l'état de l'équilibreur de charge.
- Vérifie le statut des instances Amazon EC2.
- Récupère un ensemble de journaux depuis votre environnement Elastic Beanstalk et télécharge éventuellement les fichiers vers. AWS Support

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ApplicationName

Type : chaîne

Description : (Obligatoire) Le nom de votre application Elastic Beanstalk.

- EnvironmentName

Type : chaîne

Description : (Obligatoire) Le nom de votre environnement Elastic Beanstalk.

- AWSS3UploaderLink

Type : chaîne

Description : (Facultatif) URL qui vous a été fournie AWS Support pour télécharger le bundle de logs depuis votre environnement Elastic Beanstalk vers. Cette option n'est disponible que pour les clients qui ont acheté un AWS Support plan et qui ont ouvert un dossier de Support.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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*`

## Étapes de document

- `aws:executeScript`- Vérifie que le principal AWS Identity and Access Management (IAM) qui a lancé l'automatisation dispose des autorisations requises pour effectuer toutes les actions définies dans le runbook.
- `aws:branch`- Divise le flux de travail en fonction des résultats de l'étape précédente.
- `aws:executeScript`- Collecte des informations sur l'environnement Elastic Beanstalk, notamment l'équilibreur de charge AWS CloudFormation , la pile, le groupe Auto Scaling, les instances Amazon EC2 et la configuration VPC.
- `aws:executeScript`- Vérifie les problèmes de connectivité réseau liés aux tables de routage et aux ACL associées aux sous-réseaux de votre VPC.
- `aws:executeScript`- Vérifie les problèmes de connectivité réseau liés aux règles de groupe de sécurité associées à vos instances Amazon EC2.
- `aws:executeScript`- Vérifie les vérifications de statut pour les instances Amazon EC2.
- `aws:executeScript`- Génère un lien vers un ensemble de logs de votre environnement Elastic Beanstalk.
- `aws:executeScript`- Télécharge le bundle de logs vers AWS Support
- `aws:executeScript`- Produit un rapport contenant les mesures à prendre pour vous aider à résoudre les problèmes susceptibles d'affecter l'état de votre environnement Elastic Beanstalk.

## Elastic Load Balancing

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Elastic Load Balancing. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSConfigRemediation-DropInvalidHeadersForALB](#)
- [AWS-EnableCLBAccessLogs](#)
- [AWS-EnableCLBConnectionDraining](#)
- [AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing](#)
- [AWSConfigRemediation-EnableELBDeletionProtection](#)
- [AWSConfigRemediation-EnableLoggingForALBAndCLB](#)
- [AWSSupport-TroubleshootCLBConnectivity](#)
- [AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing](#)
- [AWS UpdateALB DesyncMitigationMode](#)
- [AWS UpdateCLB DesyncMitigationMode](#)

## AWSConfigRemediation-DropInvalidHeadersForALB

### Description

Le AWSConfigRemediation-DropInvalidHeadersForALB runbook permet à l'équilibreur de charge d'application que vous spécifiez de supprimer les en-têtes HTTP dont les en-têtes ne sont pas valides.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- LoadBalancerArn

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) de l'équilibreur de charge dont vous souhaitez supprimer les en-têtes non valides.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

### Étapes de document

- aws:executeAwsApi- Active le paramètre de suppression des en-têtes non valides pour l'équilibreur de charge que vous spécifiez dans le LoadBalancerArn paramètre.
- aws:executeScript- Vérifie que le paramètre Supprimer les en-têtes non valides a été activé sur l'équilibreur de charge que vous spécifiez dans le paramètre. LoadBalancerArn

## AWS-EnableCLBAccessLogs

### Description

Le AWS-EnableCLBAccessLogs runbook active les journaux d'accès pour un Classic Load Balancer.

[Exécuter cette automatisation \(console\)](#)

### Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- EmitInterval

Type : entier

Valeurs valides : 5 | 60

Par défaut : 60

Description : (Facultatif) Intervalle de publication des journaux d'accès en minutes.

- LoadBalancerNames

Type : chaîne

Description : (Obligatoire) Liste séparée par des virgules des équilibreurs de charge classiques pour lesquels vous souhaitez activer les journaux d'accès.

- S3 BucketName

Type : chaîne

Description : (Obligatoire) Nom du compartiment Amazon Simple Storage Service (Amazon S3) dans lequel les journaux d'accès sont stockés.

- S3 BucketPrefix

Type : chaîne

Description : (Facultatif) La hiérarchie logique que vous avez créée pour votre compartiment Amazon S3, par exemple `my-bucket-prefix/prod`. Si le préfixe n'est pas fourni, le journal est placé à la racine du compartiment.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

#### Étapes de document

- `aws:executeAwsApi`- Active les journaux d'accès pour les équilibreurs de charge classiques que vous spécifiez dans le `LoadBalancerNames` paramètre.

#### Sorties

`ActiveCLB.AccessLogs.SuccessesLoadBalancers` - Liste des noms des équilibreurs de charge pour lesquels les journaux d'accès ont été activés avec succès.

`ActiveCLB.AccessLogs.FailedLoadBalancers` - `MapList` des noms des équilibreurs de charge pour lesquels l'activation des journaux d'accès a échoué et de la raison de l'échec.

## AWS-EnableCLBConnectionDraining

### Description

Le `AWS-EnableCLBConnectionDraining` runbook permet de drainer la connexion sur un Classic Load Balancer (CLB) jusqu'à la valeur de délai spécifiée. Le drainage des connexions permet au CLB de traiter les demandes en cours adressées aux instances dont l'enregistrement est en cours ou qui ne fonctionnent pas correctement, le délai spécifié étant le temps pendant lequel les connexions restent actives avant de signaler que l'instance est désenregistrée. Pour plus d'informations sur le drainage des connexions sur les CLB, voir [Configurer le drainage des connexions pour votre Classic Load Balancer dans le Guide de l'utilisateur des Classic Load Balancers](#).

## [Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- LoadBalancerName

Type : chaîne

Description : (Obligatoire) Nom de l'équilibreur de charge sur lequel vous souhaitez activer l'épuisement des connexions.

- ConnectionTimeout

Type : entier

Valeurs valides : 1 à 3600

Valeur par défaut : 300

Description : (Obligatoire) La valeur du délai d'expiration de connexion pour l'équilibreur de charge. La valeur du délai d'attente peut être définie entre 1 et 3 600 secondes.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

#### Étapes de document

- `ModifyLoadBalancerConnectionDraining` (aws :`executeAwsApi`) : Active le drainage de la connexion et définit la valeur de délai d'expiration spécifiée pour l'équilibreur de charge que vous spécifiez.
- `VerifyLoadBalancerConnectionDrainingEnabled`(aws : `assertAwsResource Propriété`) : Vérifie que le drainage des connexions est activé pour l'équilibreur de charge.
- `VerifyLoadBalancerConnectionDrainingTimeout`(aws : `assertAwsResource Propriété`) : Vérifie que la valeur du délai d'expiration de connexion pour l'équilibreur de charge correspond à la valeur que vous avez spécifiée.

## **AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing**

### Description

Le `AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` runbook permet l'équilibrage de charge entre zones pour le Classic Load Balancer (CLB) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

## LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `LoadBalancerName`

Type : chaîne

Description : (Obligatoire) Nom du CLB sur lequel vous souhaitez activer l'équilibrage de charge entre zones.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

### Étapes de document

- `aws:executeAwsApi`- Active l'équilibrage de charge entre zones pour le CLB que vous spécifiez dans le `LoadBalancerName` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que l'équilibrage de charge entre zones a été activé sur le CLB.

## **AWSConfigRemediation-EnableELBDeletionProtection**

### Description



Le `AWSConfigRemediation-EnableELBDeletionProtection` runbook active la protection contre la suppression pour l'équilibreur de charge élastique (ELB) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `LoadBalancerArn`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) de l'ELB sur lequel vous souhaitez activer la protection contre la suppression.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`

- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

### Étapes de document

- `aws:executeScript`- Active la protection contre la suppression sur l'ELB que vous spécifiez dans le `LoadBalancerArn` paramètre.

## AWSConfigRemediation-EnableLoggingForALBAndCLB

### Description

Le `AWSConfigRemediation-EnableLoggingForALBAndCLB` runbook active la journalisation pour l' AWS Application Load Balancer ou un Classic Load Balancer (CLB) spécifié.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `LoadBalancerId`

Type : chaîne

Description : (Obligatoire) Le nom du Classic Load Balancer ou l'ARN de l'Application Load Balancer.

- S3 BucketName

Type : chaîne

Description : (Obligatoire) Le nom du compartiment Amazon S3.

- S3 BucketPrefix

Type : chaîne

Description : (Facultatif) Hiérarchie logique que vous avez créée pour votre bucket Amazon Simple Storage Service (Amazon S3), par exemple. `my-bucket-prefix/prod` Si le préfixe n'est pas fourni, le journal est placé à la racine du compartiment.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

### Étapes de document


- `aws:executeScript`- Active et vérifie la journalisation pour le Classic Load Balancer ou l'Application Load Balancer.

## **AWSSupport-TroubleshootCLBConnectivity**

### Description

Le `AWSSupport-TroubleshootCLBConnectivity` runbook vous aide à résoudre les problèmes de connectivité entre un Classic Load Balancer (CLB) et des instances Amazon Elastic Compute Cloud (Amazon EC2). Les problèmes de connectivité entre un client et le CLB sont également

examinés. Ce manuel passe également en revue les bilans de santé du CLB, vérifie que les meilleures pratiques sont suivies et crée un tableau de bord de dépannage pour vous. Vous pouvez éventuellement télécharger le résultat d'automatisation dans un compartiment Amazon Simple Storage Service (Amazon S3). Toutefois, ce runbook ne prend pas en charge le téléchargement de résultats vers des compartiments S3 accessibles au public. Nous vous recommandons de créer un compartiment S3 temporaire pour cette automatisation.

 Important

L'utilisation de ce runbook peut entraîner des frais pour le tableau de bord créé. Pour plus d'informations, consultez [Amazon CloudWatch Pricing](#)

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- InvestigationType

Type : chaîne

Valeurs valides : meilleures pratiques | Problèmes de connectivité | Tableau de bord de résolution des problèmes

Description : (Obligatoire) Les opérations que vous souhaitez que le runbook effectue.

- LoadBalancerName

Type : chaîne

Description : (Obligatoire) Le nom du CLB.

- Emplacement S3

Type : chaîne

Description : (Facultatif) Nom du compartiment S3 auquel vous souhaitez envoyer les résultats de l'automatisation. Les buckets accessibles au public ne sont pas pris en charge. Si votre compartiment S3 utilise le chiffrement côté serveur, l'utilisateur ou le rôle exécutant cette automatisation doit disposer d'`kms:GenerateDataKey` autorisations pour la AWS KMS clé.

- S3 LocationPrefix

Type : chaîne

Description : (Facultatif) Le préfixe de clé Amazon S3 (sous-dossier) vers lequel vous souhaitez télécharger la sortie d'automatisation. *Le format de sortie est stocké au format suivant : `DOC-EXAMPLE-BUCKET/S3 LocationPrefix/{} _ {{automation : EXECUTION_ID InvestigationType}} .txt`.*

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

- `aws:executeScript`- Vérifie que le CLB que vous spécifiez dans le `LoadBalancerName` paramètre existe.
- `aws:branch`- Branches basées sur la valeur spécifiée pour le `InvestigationType` paramètre.
- `aws:executeScript`- Vérifie la connectivité du CLB.

- `aws:executeScript`- Vérifie que la configuration CLB est conforme aux meilleures pratiques d'Elastic Load Balancing.
- `aws:executeScript`- Crée un CloudWatch tableau de bord Amazon pour votre CLB.
- `aws:executeScript`- Crée un fichier texte avec les résultats de l'automatisation et le télécharge dans le compartiment Amazon S3 que vous spécifiez dans le `S3Location` paramètre.

## Sorties

`RunBestPractices.Résumé`

`RunConnectivityChecks.Résumé`

`CreateTroubleshootingDashboard.Sortie`

`UploadOutputToSortie S3`.

# **AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing**

## Description

Le `AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` runbook permet l'équilibrage de charge entre zones pour l'équilibreur de charge réseau (NLB) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- LoadBalancerArn

Type : chaîne

Description : (Obligatoire) Nom de ressource Amazon (ARN) du NLB sur lequel vous souhaitez activer l'équilibrage de charge entre zones.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

### Étapes de document

- aws:executeAwsApi- Active l'équilibrage de charge entre zones pour le NLB que vous spécifiez dans le LoadBalancerArn paramètre.
- aws:executeScript- Vérifie que l'équilibrage de charge entre zones a été activé sur le NLB.

## AWS UpdateALB DesyncMitigationMode

### Description

Le AWS-UpdateALBDesyncMitigationMode runbook mettra à jour le mode d'atténuation de la désynchronisation sur un Application Load Balancer (ALB) selon le mode d'atténuation spécifié. Le mode d'atténuation de la désynchronisation détermine la manière dont l'équilibreur de charge gère les demandes susceptibles de présenter un risque de sécurité pour votre application.

[Exécuter cette automatisation \(console\)](#)



## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- LoadBalancerArn

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) de l'ALB dont vous souhaitez modifier le mode d'atténuation de la désynchronisation.

- DesyncMitigationMode

Type : chaîne

Valeurs valides : moniteur | défensif | le plus strict

Description : (Obligatoire) Mode d'atténuation que vous souhaitez que l'ALB utilise. Pour plus d'informations sur les modes d'atténuation de la désynchronisation, voir [Mode d'atténuation de la désynchronisation dans le Guide de l'utilisateur des équilibreurs de charge d'application](#).

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

### Étapes de document

- `VerifyLoadBalancerType` (aws : `assertAwsResource Property`) - Vérifie que la valeur spécifiée pour le paramètre `LoadBalancerArn` d'entrée est celle d'un équilibreur de charge d'application avant de passer à l'étape suivante.
- `ModifyLoadBalancerDesyncMode` (aws : `executeAwsApi`) - Met à jour l'ALB pour utiliser le paramètre spécifié `DesyncMitigationMode`.
- `VerifyLoadBalancerDesyncMitigationMode` (AWS: `ExecuteScript`) - Vérifie que le mode d'atténuation de la désynchronisation a été mis à jour pour l'ALB cible.

### Sorties

`VerifyLoadBalancerDesyncMitigationMode`. `ModificationResult` - Charge utile du message du script vérifiant la modification de votre ALB.

## AWS UpdateCLB DesyncMitigationMode

### Description

Le `AWS-UpdateCLBDesyncMitigationMode` runbook mettra à jour le mode d'atténuation de la désynchronisation sur un Classic Load Balancer (CLB) vers le mode d'atténuation spécifié. Le mode d'atténuation de la désynchronisation détermine la manière dont l'équilibreur de charge gère les demandes susceptibles de présenter un risque de sécurité pour votre application.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

## Amazon

### Plateformes

Linux macOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `LoadBalancerName`

Type : chaîne

Description : (Obligatoire) Nom du CLB dont vous souhaitez modifier le mode d'atténuation de la désynchronisation.

- `DesyncMitigationMode`

Type : chaîne

Valeurs valides : `moniteur` | `défensif` | `le plus strict`

Description : (Obligatoire) Mode d'atténuation que vous souhaitez que le CLB utilise. Pour plus d'informations sur les modes d'atténuation de la désynchronisation, voir [Mode d'atténuation de la désynchronisation dans le Guide de l'utilisateur des](#) équilibreurs de charge d'application.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

## Étapes de document

- `ModifyLoadBalancerDesyncMode` (aws :executeAwsApi) - Met à jour le CLB pour utiliser le paramètre spécifié `DesyncMitigationMode`.
- `VerifyLoadBalancerDesyncMitigationMode` (AWS:ExecuteScript) - Vérifie que le mode d'atténuation de la désynchronisation a été mis à jour pour le CLB cible.

## Sorties

`VerifyLoadBalancerDesyncMitigationMode`. `ModificationResult` - Charge utile du message du script vérifiant la modification de votre CLB.

# Amazon EMR

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon EMR. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWSSupport-AnalyzeEMRLogs](#)

## AWSSupport - AnalyzeEMRLogs

### Description

Ce runbook permet d'identifier les erreurs lors de l'exécution d'une tâche sur un cluster Amazon EMR. Le runbook analyse une liste de journaux définis sur le système de fichiers et recherche une liste de mots clés prédéfinis. Ces entrées de journal sont utilisées pour créer des CloudWatch événements Amazon Events afin que vous puissiez prendre les mesures nécessaires en fonction de ces événements. Le runbook publie éventuellement des entrées de journal dans le groupe de CloudWatch journaux Amazon Logs de votre choix. Ce runbook recherche actuellement les erreurs et modèles suivants dans les fichiers journaux :

- `container_out_of_memory` — Le conteneur YARN n'a plus de mémoire, la tâche en cours d'exécution peut échouer.

- `yarn_nodemanager_health` : le nœud CORE ou TASK manque d'espace disque et ne pourra pas exécuter de tâches.
- `node_state_change` : le nœud CORE ou TASK n'est pas accessible par le nœud MASTER.
- `step_failure` : une étape EMR a échoué.
- `no_core_nodes_running` : aucun nœud CORE n'est actuellement en cours d'exécution, le cluster est défectueux.
- `hdfs_missing_blocks` : Des blocs HDFS sont manquants, ce qui pourrait entraîner une perte de données.
- `hdfs_high_util` : L'utilisation de HDFS est élevée, ce qui peut affecter les tâches et l'état du cluster.
- `instance_controller_restart` : le processus Instance-Controller a redémarré. Ce processus est essentiel pour la santé du cluster.
- `instance_controller_restart_legacy` : le processus Instance-Controller a redémarré. Ce processus est essentiel pour la santé du cluster.
- `high_load` : charge moyenne élevée détectée, susceptible d'affecter les rapports sur l'état des nœuds ou d'entraîner des délais ou des ralentissements.
- `yarn_node_blacklisted` : Le nœud CORE ou TASK a été mis sur liste noire par YARN pour l'empêcher d'exécuter des tâches.
- `yarn_node_lost` : Le nœud CORE ou TASK a été marqué comme PERDU par YARN, problèmes de connectivité possibles.

Les instances associées à celles `ClusterID` que vous spécifiez doivent être gérées par AWS Systems Manager. Vous pouvez exécuter cette automatisation une seule fois, planifier l'automatisation pour qu'elle s'exécute à un intervalle de temps spécifique ou supprimer une planification créée précédemment par une automatisation. Ce runbook prend en charge les versions 5.20 à 6.30 d'Amazon EMR.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

## LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterID

Type : chaîne

Description : (Obligatoire) L'ID du cluster dont vous souhaitez analyser les logs des nœuds.

- Opération

Type : chaîne

Valeurs valides : Exécuter une fois | Planifier | Supprimer le calendrier

Description : (Obligatoire) Opération à effectuer sur le cluster.

- IntervalTime

Type : chaîne

Valeurs valides : 5 minutes | 10 minutes | 15 minutes

Description : (Facultatif) Durée entre deux exécutions de l'automatisation. Ce paramètre n'est applicable que si vous `Schedule` le `Operation` spécifiez.

- LogToCloudWatchLogs

Type : chaîne

Valeurs valides : oui | non

Description : (Facultatif) Si vous spécifiez `yes` la valeur de ce paramètre, l'automatisation crée un groupe de CloudWatch journaux avec le nom spécifié dans le `CloudWatchLogGroup` paramètre pour stocker toutes les entrées de journal correspondantes.

- **CloudWatchLogGroup**

Type : chaîne

Description : (Facultatif) Nom du groupe de CloudWatch journaux dans lequel vous souhaitez stocker les entrées de journal correspondantes. Ce paramètre n'est applicable que si vous yes le `LogToCloudWatchLogs` spécifiez.

- **CreateLogInsightsDashboard**

Type : chaîne

Valeurs valides : oui | non

Description : (Facultatif) Si vous le spécifiez `yes`, le tableau de CloudWatch bord est créé s'il n'existe pas déjà. Ce paramètre n'est applicable que si vous yes le `LogToCloudWatchLogs` spécifiez.

- **CreateMetricFilters**

Type : chaîne

Valeurs valides : oui | non

Description : (Facultatif) Spécifiez `yes` si vous souhaitez créer des filtres métriques pour le groupe de CloudWatch journaux Logs. Ce paramètre n'est applicable que si vous yes le `LogToCloudWatchLogs` spécifiez.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

- `aws:executeAwsApi`- Recueille des informations sur le cluster Amazon EMR spécifié dans `ClusterID` le paramètre.
- `aws:branch`- Branches basées sur les entrées.
  - Si l'opération proposée est `Run Once` ou `Schedule` :
    - `aws:assertAwsResourceProperty`- Vérifie que le cluster est disponible.



- `aws:executeAwsApi`- Rassemble les identifiants de toutes les instances exécutées dans le cluster.
- `aws:assertAwsResourceProperty`- Vérifie que l'agent SSM est en cours d'exécution sur toutes les instances du cluster.
- `aws:branch`- Branches selon que vous avez spécifié d'exécuter l'automatisation une fois ou selon un calendrier.
- Si l'opération proposée est `Run Once` :
  - `aws:branch`- Branches basées sur la valeur spécifiée dans le `LogToCloudWatchLogs` paramètre.
    - Si `LogToCloudWatchLogs` la valeur est `yes` :
      - `aws:executeScript`- Vérifie si un groupe de CloudWatch journaux avec le nom spécifié en paramètre existe `CloudWatchLogGroup` déjà. Dans le cas contraire, le groupe est créé avec le nom spécifié.
      - `aws:branch`- Branches basées sur la valeur spécifiée dans le `CreateMetricFilters` paramètre.
        - Si `CreateMetricFilters` la valeur est `yes` :
          - `aws:executeAwsApi`- 12 étapes sont exécutées pour chaque filtre métrique
          - `aws:branch`- Branches basées sur la valeur spécifiée dans le `CreateLogInsightsDashboard` paramètre.
            - Si `CreateLogInsightsDashboard` la valeur est `yes` :
              - `aws:executeAwsApi`- Crée un CloudWatch tableau de bord portant le même nom que celui indiqué dans le `CloudWatchLogGroup` paramètre, s'il n'existe pas déjà.
            - Si `CreateLogInsightsDashboard` la valeur est `no` :
              - `aws:runCommand`- Exécute un script shell pour rechercher des modèles de journalisation sur chaque instance du cluster.
        - Si `CreateMetricFilters` la valeur est `no` :
          - `aws:branch`- Branches basées sur la valeur spécifiée dans le `CreateLogInsightsDashboard` paramètre.
            - Si `CreateLogInsightsDashboard` la valeur est `yes` :

- `aws:executeAwsApi`- Crée un CloudWatch tableau de bord portant le même nom que celui indiqué dans le `CloudWatchLogGroup` paramètre, s'il n'existe pas déjà.
- Si `CreateLogInsightsDashboard` la valeur est `no` :
  - `aws:runCommand`- Exécute un script shell pour rechercher des modèles de journalisation sur chaque instance du cluster.
- Si `LogToCloudWatchLogs` la valeur est `no` :
  - `aws:executeAwsApi`- Exécute un script shell pour rechercher des modèles de journalisation sur chaque instance du cluster.
- Si l'opération proposée est `Schedule` :
  - `aws:createStack`- Crée un EventBridge événement Amazon qui cible ce runbook.
- Si l'opération proposée est `Remove Schedule` :
  - `aws:executeAwsApi`- Vérifie qu'un planning existe pour le cluster.
  - `aws:deleteStack`- Supprime le planning.

## Sorties

`GetClusterInformation.ClusterName`

`GetClusterInformation.ClusterState`

`ListingClusterInstances.Identifiants d'instance`

`CreatingScheduleCloudFormationStack.StackStatus`

`RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus`

`CheckIfLogGroupExists.sortie`

`FindLogPatternOnMernode.CommandId`

## Amazon OpenSearch Service

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon OpenSearch Service. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWSConfigRemediation-DeleteOpenSearchDomain](#)
- [AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain](#)
- [AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups](#)
- [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#)
- [AWSSupport-TroubleshootOpenSearchHighCPU](#)

## AWSConfigRemediation-DeleteOpenSearchDomain

### Description

Le `AWSConfigRemediation-DeleteOpenSearchDomain` runbook supprime le domaine Amazon OpenSearch Service donné à l'aide de l'[DeleteDomainAPI](#).

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `DomainName`

Type : chaîne

Valeurs autorisées : `(\ d {12}/) ? [a-z] {1} [a-z0-9-] {2,28}`

Description : (Obligatoire) Le nom du domaine Amazon OpenSearch Service que vous souhaitez supprimer.

- **AutomationAssumeRole**

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

#### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es>DeleteDomain`
- `es:DescribeDomain`

#### Étapes de document

- `aws:executeScript`- Accepte le nom de domaine Amazon OpenSearch Service comme entrée, le supprime et vérifie la suppression.

## **AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain**

### Description

Le AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain runbook est activé EnforceHTTPS sur un domaine Amazon OpenSearch Service donné à l'aide de l'[UpdateDomainConfigAPI](#).

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `DomainName`

Type : chaîne

Valeurs autorisées : `(\ d {12}/) ? [a-z] {1} [a-z0-9-] {2,28}`

Description : (Obligatoire) Le nom du domaine Amazon OpenSearch Service que vous souhaitez utiliser pour appliquer le protocole HTTPS.

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

### Étapes de document

- `aws:executeScript`- Active l'option de point de `EnforceHTTPS` terminaison sur le domaine Amazon OpenSearch Service que vous spécifiez dans le `DomainName` paramètre.

# AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

## Description

Le AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups runbook met à jour la configuration du groupe de sécurité sur un domaine Amazon OpenSearch Service donné à l'aide de l'[UpdateDomainConfigAPI](#).

### Note

AWS Les groupes de sécurité ne peuvent être appliqués qu'aux domaines Amazon OpenSearch Service configurés pour Amazon Virtual Private Cloud (VPC) Access, et non aux domaines Amazon OpenSearch Service configurés pour l'accès public.

## [Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- DomainName

Type : chaîne

Description : (Obligatoire) Le nom du domaine Amazon OpenSearch Service que vous souhaitez utiliser pour mettre à jour les groupes de sécurité.

- SecurityGroupList

Type : StringList

Description : (Obligatoire) Les identifiants de groupe de sécurité que vous souhaitez attribuer au domaine Amazon OpenSearch Service.

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

### Étapes de document

- aws:executeScript- Met à jour la configuration du groupe de sécurité sur le domaine Amazon OpenSearch Service que vous spécifiez dans le DomainName paramètre.

## AWSSupport-TroubleshootOpenSearchRedYellowCluster

### Description

AWSSupport-TroubleshootOpenSearchRedYellowClusterLe runbook d'automatisation est utilisé pour identifier la cause de l'état de santé du cluster [rouge](#) ou [jaune](#) et vous guider dans le retour du cluster au vert.

### Comment fonctionne-t-il ?

Le runbook vous `AWSsupport-TroubleshootOpenSearchRedYellowCluster` aide à résoudre la cause du cluster rouge ou jaune et fournit les étapes suivantes pour résoudre ce problème en analysant la configuration du cluster et l'utilisation des ressources.

Le runbook exécute les étapes suivantes :

- Appelle l'[DescribeDomain](#) API sur le domaine cible pour obtenir la configuration du cluster.
- Vérifie si le domaine du OpenSearch service est basé sur Internet (public) ou [Amazon Virtual Private Cloud \(VPC\)](#).
- Crée une fonction publique ou basée sur [Amazon VPC en AWS Lambda fonction](#) de la configuration du cluster. Remarque : La fonction Lambda contient le code de dépannage qui exécute les API de OpenSearch service sur le cluster afin de déterminer pourquoi le cluster est en rouge ou en jaune.
- Supprime la fonction Lambda.
- Affiche les vérifications effectuées et les prochaines étapes recommandées pour résoudre le problème du cluster rouge ou jaune.

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

Le `LambdaExecutionRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook :

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`

Vue d'ensemble de `LambdaExecutionRole` la politique :

Voici un exemple du rôle d'exécution (rôle AWS Identity and Access Management (IAM) d'une fonction Lambda) qui accorde à la fonction l'autorisation d'accéder aux AWS services et aux ressources requis par ce runbook. Pour plus d'informations, consultez [Rôle d'exécution Lambda](#).

**Note**

Les `ec2:DescribeNetworkInterfaces` et `ec2:CreateNetworkInterface`, et ne `ec2>DeleteNetworkInterface` sont obligatoires que si votre cluster de OpenSearch services est [basé sur Amazon VPC](#) pour permettre à la fonction Lambda de créer et de gérer les interfaces réseau Amazon VPC. Pour plus d'informations, consultez [Connecter le réseau sortant aux ressources dans un rôle d'exécution Amazon VPC](#) et [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"
    }
]
}
```

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez au [AWSSupport- TroubleshootOpenSearchRedYellowCluster](#) dans la AWS Systems Manager console.
2. Sélectionnez Exécute automation (Exécuter l'automatisation).
3. Pour les paramètres d'entrée, entrez ce qui suit :

- AutomationAssumeRole (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- LambdaExecutionRole (Obligatoire) :

L'ARN du rôle IAM que Lambda utilisera pour signer les demandes adressées à votre cluster OpenSearch Amazon Service.

- DomainName (Obligatoire) :

Nom du domaine de OpenSearch service dont l'état de santé du cluster est rouge ou jaune.

- UtilizationThreshold (Facultatif) :

Le pourcentage du seuil d'utilisation utilisé pour comparer les métriques CPUUtilization et MemoryPressure JVM. La valeur par défaut est 80.

**Input parameters**

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

Select an existing IAM Role

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

**DomainName**  
(Required) The name of the Amazon OpenSearch Service domain in red or yellow status.

opensearch-red-yellow-sample

**LambdaExecutionRole**  
(Required) The ARN of the IAM role that the AWS Lambda will use to sign requests to your Amazon OpenSearch Service cluster.

Select an existing IAM Role

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

**UtilizationThreshold**  
(Optional) The utilization threshold in percentage used to compare the 'CPUUtilization' and 'JVMMemoryPressure' metrics. Default value is '80'.

80

4. Si vous avez activé le [contrôle d'accès détaillé](#) sur un cluster de OpenSearch services, assurez-vous que l'ARN du LambdaExecutionRole rôle est mappé à un rôle disposant d'au moins une autorisation. `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::123456789012:role/LambdaExecutionRole Remove

Add another backend role

Cancel Map

5. Sélectionnez Exécuter.

6. L'automatisation démarre.

7. Le runbook d'automatisation exécute les étapes suivantes :

- GetClusterConfiguration:

Récupère la configuration du cluster OpenSearch de services.

- Créez AWSLambdaFunctionStack :

Crée une fonction Lambda temporaire dans votre compte à l'aide de. AWS CloudFormation La fonction Lambda est utilisée pour exécuter les API de OpenSearch service.

- WaitForAWSLambdaFunctionStack:

Attend que la CloudFormation pile soit terminée.

- **GetClusterMetricsFromCloudWatch:**

Obtient les métriques relatives aux clusters Amazon CloudWatch ClusterStatus, CPUUtilization et JVM MemoryPressure OpenSearch Service ainsi que leur date de création.

- **RunOpenSearchAPI :**

Utilise la fonction Lambda pour appeler les API de OpenSearch service et analyser les données des métriques du cluster afin de diagnostiquer la cause de l'état rouge ou jaune du cluster.

- **Supprimer AWSLambdaFunctionStack :**

Supprime la fonction Lambda créée par cette automatisation dans votre compte.

8. Une fois terminé, consultez la section Sorties pour connaître les résultats détaillés de l'exécution.

- **RootCause:**

Fournit une vue d'ensemble de la cause identifiée pour laquelle l'état de santé du cluster est passé en rouge ou en jaune.

- **IssueDescription:**

Fournit des informations sur les raisons pour lesquelles le cluster est en rouge ou en jaune et explique les étapes possibles pour le ramener à l'état vert.

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

### AWS documentation de service

- Reportez-vous à la section [Dépannage OpenSearch d'Amazon Service](#) pour plus d'informations

## **AWSSupport - TroubleshootOpenSearchHighCPU**

### Description

Le `AWSsupport-TroubleshootOpenSearchHighCPU` runbook fournit une solution automatisée pour collecter des données de diagnostic à partir d'un domaine Amazon OpenSearch Service afin de résoudre les problèmes de [processeur élevés](#).

Comment fonctionne-t-il ?

Le `AWSsupport-TroubleshootOpenSearchHighCPU` runbook permet de résoudre les problèmes d'utilisation élevée du processeur dans le domaine Amazon OpenSearch Service.

Le runbook exécute les étapes suivantes :

- Exécute l'[DescribeDomain](#) API sur le domaine Amazon OpenSearch Service fourni pour obtenir les métadonnées du cluster.
- Vérifie si le domaine Amazon OpenSearch Service est public ou basé sur Amazon VPC et, à l'aide de AWS CloudFormation, crée une fonction publique ou basée sur [Amazon AWS Lambda VPC](#).
- La fonction Lambda récupère les données de diagnostic depuis les domaines Amazon OpenSearch Service.
- Utilise une machine à AWS Step Functions états pour orchestrer plusieurs exécutions de fonctions Lambda afin de recueillir des données plus complètes.
- Stocke les données collectées dans un groupe de CloudWatch journaux Amazon pendant 24 heures par défaut.
- Supprime les ressources créées, à l'exception du groupe de CloudWatch journaux.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

Le `LambdaExecutionRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook :

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Le rôle d'exécution Lambda accorde à la fonction l'autorisation d'accéder aux AWS services et aux ressources requis par ce runbook. Pour plus d'informations, consultez [Rôle d'exécution Lambda](#).

#### Note

Les `ec2:DescribeNetworkInterfaces``ec2:CreateNetworkInterface`, et ne `ec2>DeleteNetworkInterface` sont obligatoires que si votre cluster de OpenSearch services est [basé sur Amazon VPC](#) pour permettre à la fonction Lambda de créer et de gérer les interfaces réseau Amazon VPC. Pour plus d'informations, consultez [Connecter le réseau sortant aux ressources dans un rôle d'exécution Amazon VPC](#) et [Lambda](#).

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez au [TroubleshootOpenSearchHighprocesseur AWSSupport -](#) dans la AWS Systems Manager console.
2. Sélectionnez Exécute automation (Exécuter l'automatisation).
3. Pour les paramètres d'entrée, entrez ce qui suit :
  - AutomationAssumeRole (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.



- **DomainName (Obligatoire) :**

Le nom du domaine Amazon OpenSearch Service que vous souhaitez résoudre en cas de problèmes de processeur élevés.

- **LambdaExecutionRoleForOpenSearch (Obligatoire) :**

L'ARN du rôle IAM à associer à la fonction Lambda. La fonction Lambda utilise les informations d'identification de ce rôle pour signer les demandes adressées au domaine Amazon OpenSearch Service. Si le contrôle d'accès détaillé est activé sur le domaine Amazon OpenSearch Service, vous devez associer ce rôle à un rôle principal de OpenSearch Service Dashboards avec une autorisation minimale de « cluster\_monitor ».

- **DataRetentionDays (Facultatif) :**

Le nombre de jours pendant lesquels les données de diagnostic collectées à partir du domaine Amazon OpenSearch Service sont conservées. Par défaut, les données sont conservées pendant 24 heures (un jour). Vous pouvez choisir de conserver les données pendant une durée maximale de 30 jours.

- **NumberOfDataSamples (Facultatif) :**

Le nombre d'échantillons de données à collecter à partir du domaine Amazon OpenSearch Service. Par défaut, 5 échantillons de données sont collectés. Vous pouvez collecter jusqu'à 10 échantillons et la fonction Lambda sera invoquée pour chaque collecte d'échantillons.

Input parameters	
<p><b>AutomationAssumeRole</b> (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</p> <input type="text"/>	<p><b>DomainName</b> (Required) The name of the Amazon OpenSearch domain that you want to troubleshoot for high CPU issues.</p> <input type="text" value="String"/>
<p><b>LambdaExecutionRoleForOpenSearch</b> (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.</p> <input type="text"/>	<p><b>DataRetentionDays</b> (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.</p> <input type="text" value="1"/>
<p><b>NumberOfDataSamples</b> (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.</p> <input type="text" value="5"/>	

4. Si vous avez activé le [contrôle d'accès détaillé](#) sur un cluster de OpenSearch services, assurez-vous que l'ARN du LambdaExecutionRole rôle est mappé à un rôle disposant d'au moins une autorisation. cluster\_monitor

The screenshot shows the 'Mapped users' configuration page in the AWS IAM console. The 'Permissions' tab is active. The 'Cluster permissions (1)' section shows a single permission named 'cluster\_monitor'. The 'Backend roles' section shows a role with the ARN 'arn:aws:iam::[redacted]:role/LambdaExecutionRole' and a 'Remove' button. At the bottom right, there are 'Cancel' and 'Map' buttons.

5. Sélectionnez Exécuter.

6. L'automatisation démarre.

7. Le runbook d'automatisation exécute les étapes suivantes :

- Vérifiez la simultanéité :

Garantit qu'il n'y a qu'une seule exécution de ce runbook ciblant le domaine Amazon OpenSearch Service spécifié. Si le runbook trouve une autre exécution ciblant le même nom de domaine, il renvoie une erreur et se termine.

- `getDomainConfig`:

Obtient les détails de configuration pour le domaine OpenSearch de service cible.

- Ressources d'approvisionnement :

Fournit les ressources nécessaires à la collecte de données à l'aide de AWS CloudFormation.

- `waitForStackCréation` :

Attend que la AWS CloudFormation pile soit terminée.

- `describeStackResources`:

Décrit la AWS CloudFormation pile et obtient l'ARN de la machine à états.

- `runStateMachine`:

Invoke la fonction Lambda du collecteur de données une ou plusieurs fois en exécutant une machine d'état Step Functions.

- `describeErrorsFromStackEvents`:

Décrit les erreurs provenant de la AWS CloudFormation pile pour détecter les erreurs.

- `unstageOpenSearchAutomatisation` élevée du processeur :

Supprime la `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation pile.

- `describeErrorsFromStackDeletion`:

Décrit les erreurs rencontrées lors de la suppression de la AWS CloudFormation pile.

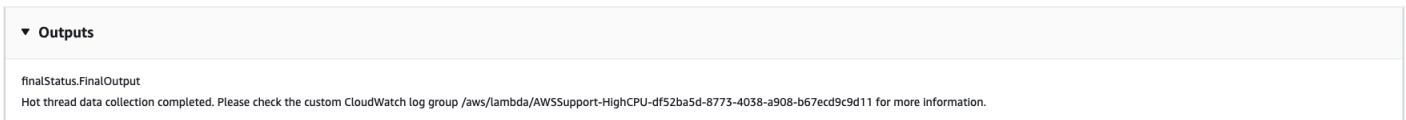
- État final :

Renvoie le résultat final du `AWSSupport-TroubleshootOpenSearchHighCPU` runbook.

8. Une fois terminé, consultez la section Sorties pour connaître les résultats détaillés de l'exécution.

- État final. `FinalOutput`:

Fournit le groupe de CloudWatch journaux dans lequel les données de diagnostic sont stockées.



## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

### AWS documentation de service

- Reportez-vous à la section [Dépannage OpenSearch d'Amazon Service](#) pour plus d'informations

# EventBridge

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon EventBridge. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-AddOpsItemDedupStringToEventBridgeRule](#)
- [AWS-DisableEventBridgeRule](#)

## AWS-AddOpsItemDedupStringToEventBridgeRule

### Description

Le `AWS-AddOpsItemDedupStringToEventBridgeRule` runbook ajoute une chaîne de déduplication pour tout ce qui est AWS Systems Manager OpsItems associé à une règle Amazon EventBridge. Le runbook n'ajoute pas de chaîne de déduplication à la règle si une chaîne a déjà été appliquée. Pour en savoir plus sur les chaînes de déduplication et OpsItems consultez la section [Réduction des doublons OpsItems](#) dans le Guide de AWS Systems Manager l'utilisateur.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `DedupString`

Type : chaîne

Description : (Obligatoire) Chaîne de déduplication que vous souhaitez ajouter à la règle.

- `RuleName`

Type : chaîne

Description : (Obligatoire) Nom de la règle à laquelle vous souhaitez ajouter la chaîne de déduplication.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

#### Étapes de document

- `aws:executeScript`- Ajoute une chaîne de déduplication à la EventBridge règle que vous spécifiez dans le `RuleName` paramètre.

## **AWS-DisableEventBridgeRule**

### Description

Le *AWS-DisableEventBridgeRule* runbook désactive la EventBridge règle Amazon que vous spécifiez. Pour en savoir plus sur les règles EventBridge , consultez les [règles Amazon EventBridge dans le guide de l'utilisateur](#) Amazon. EventBridge

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- EventBusName

Type : chaîne

Par défaut : par défaut

Description : (Facultatif) Bus d'événements associé à la règle que vous souhaitez désactiver.

- RuleName

Type : chaîne

Description : (Obligatoire) Nom de la règle que vous souhaitez désactiver.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

#### Étapes de document

- `aws:executeAwsApi`- Désactive la `EventBridge` règle que vous spécifiez dans le `RuleName` paramètre.

## GuardDuty

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon GuardDuty. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

#### Rubriques

- [AWSConfigRemediation-CreateGuardDutyDetector](#)

## AWSConfigRemediation-CreateGuardDutyDetector

#### Description

Le `AWSConfigRemediation-CreateGuardDutyDetector` runbook crée un détecteur Amazon GuardDuty (`GuardDuty`) dans l' Région AWS endroit où vous exécutez l'automatisation.

[Exécuter cette automatisation \(console\)](#)

#### Type de document

Automatisation

#### Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- guardduty:CreateDetector
- guardduty:GetDetector

## Étapes de document

- aws:executeAwsApi- Crée un GuardDuty détecteur.
- aws:assertAwsResourceProperty- Vérifie que Status le détecteur estENABLED.

## IAM

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Identity and Access Management. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-AttachIAMToInstance](#)



- [AWS-DeleteIAMInlinePolicy](#)
- [AWSConfigRemediation-DeleteIAMRole](#)
- [AWSConfigRemediation-DeleteIAMUser](#)
- [AWSConfigRemediation-DeleteUnusedIAMGroup](#)
- [AWSConfigRemediation-DeleteUnusedIAMPolicy](#)
- [AWSConfigRemediation-DetachIAMPolicy](#)
- [AWSConfigRemediation-EnableAccountAccessAnalyzer](#)
- [AWSSupport-GrantPermissionsToIAMUser](#)
- [AWSConfigRemediation-RemoveUserPolicies](#)
- [AWSConfigRemediation-ReplaceIAMInlinePolicy](#)
- [AWSConfigRemediation-RevokeUnusedIAMUserCredentials](#)
- [AWSConfigRemediation-SetIAMPasswordPolicy](#)

## AWS-AttachIAMToInstance

### Description

Attachez un rôle AWS Identity and Access Management (IAM) à une instance gérée.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ForceReplace

Type : booléen

Description : (Facultatif) Indicateur pour indiquer si le profil IAM existant doit être remplacé ou non.

Valeur par défaut : true

- InstanceId

Type : chaîne

Description : (Obligatoire) L'ID de l'instance à laquelle vous souhaitez attribuer un rôle IAM.

- RoleName

Type : chaîne

Description : (Obligatoire) Le nom du rôle IAM à ajouter à l'instance gérée.

## Étapes de document

1. `aws:executeAwsApi- DescribeInstanceProfile` - Trouvez le profil d'instance IAM attaché à l'instance EC2.
2. `aws:branch- CheckInstanceProfileAssociations` - Vérifiez le profil d'instance IAM attaché à l'instance EC2.
  - a. Si un profil d'instance IAM est attaché et `ForceReplace` est défini sur : `true`
    - i. `aws:executeAwsApi- DisassociateIAMInstanceProfile` - Dissociez le profil d'instance IAM de l'instance EC2.
  - b. `aws:executeAwsApi- ListInstanceProfilesForRole` - Répertoriez les profils d'instance pour le rôle IAM fourni.
  - c. `aws:branch- CheckInstanceProfileCreated` - Vérifiez si un profil d'instance est associé au rôle IAM fourni.

- i. Si un profil d'instance est associé au rôle IAM :
  - A. `aws:executeAwsApi- AttachIam ProfileToInstance` - Attachez le rôle de profil d'instance IAM à l'instance EC2.
- i. Si aucun profil d'instance n'est associé au rôle IAM :
  - A. `aws:executeAwsApi- CreateInstanceProfileForRole` - Créez un rôle de profil d'instance pour le rôle IAM spécifié.
  - B. `aws:executeAwsApi- AddRoleToInstanceProfile` - Attachez le rôle de profil d'instance au rôle IAM spécifié.
  - C. `aws:executeAwsApi- GetInstanceProfile` - Obtenez les données du profil d'instance pour le rôle IAM spécifié.
  - D. `aws:executeAwsApi- AttachIam ProfileToInstanceWithRetry` - Attachez le rôle de profil d'instance IAM à l'instance EC2.

## Sorties

`AttachIamProfileToInstanceWithRetry. AssociationId`

`GetInstanceProfile.InstanceProfileName`

`GetInstanceProfile.InstanceProfileArn`

`AttachIamProfileToInstance. AssociationId`

`ListInstanceProfilesForRole.InstanceProfileName`

`ListInstanceProfilesForRole.InstanceProfileArn`

## **AWS-DeleteIAMInlinePolicy**

### Description

Le `AWS-DeleteIAMInlinePolicy` runbook supprime toutes les politiques en ligne AWS Identity and Access Management (IAM) associées aux identités IAM que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

#### Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- iamArns

Type : chaîne

Description : (Obligatoire) Une liste d'ARN séparés par des virgules pour les identités IAM dont vous souhaitez supprimer les politiques intégrées. Cette liste peut inclure des utilisateurs, des groupes ou des rôles IAM.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- iam:DeleteGroupPolicy
- iam:DeleteRolePolicy
- iam:DeleteUserPolicy
- iam:ListGroupPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies

## Étapes de document

- `aws:executeScript`- Supprime les politiques en ligne IAM associées aux identités IAM ciblées.

## AWSConfigRemediation-DeleteIAMRole

### Description

Le `AWSConfigRemediation-DeleteIAMRole` runbook supprime le rôle AWS Identity and Access Management (IAM) que vous spécifiez. Cette automatisation ne supprime pas les profils d'instance associés au rôle IAM, ni les rôles liés à un service.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `Je suis Roleid`

Type : chaîne

Description : (Obligatoire) L'ID du rôle IAM que vous souhaitez supprimer.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:GetRole`
- `iam>ListAttachedRolePolicies`
- `iam>ListInstanceProfilesForRole`
- `iam>ListRolePolicies`
- `iam>ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

#### Étapes de document

- `aws:executeScript`- Rassemble le nom du rôle IAM que vous spécifiez dans le `IAMRoleID` paramètre.
- `aws:executeScript`- Rassemble les politiques et les profils d'instance associés au rôle IAM.
- `aws:executeScript`- Supprime les politiques jointes.
- `aws:executeScript`- Supprime le rôle IAM et vérifie qu'il a été supprimé.

## **AWSConfigRemediation-DeleteIAMUser**

### Description

Le `AWSConfigRemediation-DeleteIAMUser` runbook supprime l'utilisateur AWS Identity and Access Management (IAM) que vous spécifiez. Cette automatisation supprime ou détache les ressources suivantes associées à l'utilisateur IAM :

- Clés d'accès
- Politiques gérées associées
- Informations d'identification Git
- Adhésions au groupe IAM

- Mot de passe utilisateur IAM
- Politiques en ligne
- Dispositifs d'authentification multifactorielle (MFA)
- Certificats de signature
- Clés publiques SSH

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- IAM UserId

Type : chaîne

Description : (Obligatoire) L'ID de l'utilisateur IAM que vous souhaitez supprimer.

Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

- `aws:executeScript`- Rassemble le nom d'utilisateur de l'utilisateur IAM que vous spécifiez dans le `IAMUserId` paramètre.
- `aws:executeScript`- Rassemble les clés d'accès, les certificats, les informations d'identification, les périphériques MFA et les clés SSH associés à l'utilisateur IAM.



- `aws:executeScript`- Rassemble les appartenances aux groupes et les politiques de l'utilisateur IAM.
- `aws:executeScript`- Supprime les clés d'accès, les certificats, les informations d'identification, les périphériques MFA et les clés SSH associés à l'utilisateur IAM.
- `aws:executeScript`- Supprime les appartenances aux groupes et les politiques de l'utilisateur IAM.
- `aws:executeScript`- Supprime l'utilisateur IAM et vérifie qu'il a été supprimé.

## **AWSConfigRemediation-DeleteUnusedIAMGroup**

### Description

Le `AWSConfigRemediation-DeleteUnusedIAMGroup` runbook supprime un groupe IAM qui ne contient aucun utilisateur.

Le `AWSConfigRemediation-DeleteUnusedIAMGroup` runbook supprime un groupe IAM qui ne contient aucun utilisateur.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- **GroupName**

Type : chaîne

Description : (Obligatoire) Nom du groupe IAM que vous souhaitez supprimer.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam>DeleteGroup`
- `iam>DeleteGroupPolicy`
- `iam:DetachGroupPolicy`

#### Étapes de document

- `aws:executeScript`- Supprime les politiques IAM gérées et intégrées associées au groupe IAM cible, puis supprime le groupe IAM.

## **AWSConfigRemediation-DeleteUnusedIAMPolicy**

### Description

Le `AWSConfigRemediation-DeleteUnusedIAMPolicy` runbook supprime une politique AWS Identity and Access Management (IAM) qui n'est attachée à aucun utilisateur, groupe ou rôle.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

## LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- IAM ResourceId

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de la politique IAM que vous souhaitez supprimer.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config>ListDiscoveredResources
- iam>DeletePolicy
- iam>DeletePolicyVersion
- iam:GetPolicy
- iam>ListEntitiesForPolicy
- iam>ListPolicyVersions

### Étapes de document

- aws:executeScript- Supprime la politique que vous spécifiez dans le IAMResourceId paramètre et vérifie qu'elle a été supprimée.

# AWSConfigRemediation-DetachIAMPolicy

## Description

Le AWSConfigRemediation-DetachIAMPolicy runbook détache la politique AWS Identity and Access Management (IAM) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- IAM ResourceId

Type : chaîne

Description : (Obligatoire) L'ID de la politique IAM que vous souhaitez détacher.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config>ListDiscoveredResources`
- `iam:DetachGroupPolicy`
- `iam:DetachRolePolicy`
- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam>ListEntitiesForPolicy`

### Étapes de document

- `aws:executeScript`- Détache la politique IAM de toutes les ressources.

## AWSConfigRemediation-EnableAccountAccessAnalyzer

### Description

Le `AWSConfigRemediation-EnableAccountAccessAnalyzer` runbook crée un analyseur d'accès AWS Identity and Access Management (IAM) dans votre. Compte AWS Pour plus d'informations sur Access Analyzer, consultez la section [Utilisation d' AWS IAM Access Analyzer](#) dans le guide de l'utilisateur d'IAM.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AnalyzerName`

Type : chaîne

Description : (Obligatoire) Nom de l'analyseur à créer.

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- access-analyzer:CreateAnalyzer
- access-analyzer:GetAnalyzer

### Étapes de document

- aws:executeAwsApi- Crée un analyseur d'accès pour votre compte.
- aws:waitForAwsResourceProperty- Attend que l'état de l'analyseur d'accès soit atteint. ACTIVE
- aws:assertAwsResourceProperty- Confirme que l'état de l'analyseur d'accès estACTIVE.

## AWSSupport-GrantPermissionsToIAMUser

### Description

Ce runbook accorde les autorisations spécifiées à un groupe IAM (nouveau ou existant) et y ajoute l'utilisateur IAM existant. Stratégies que vous pouvez choisir : [Billing](#) ou [Support](#). Pour activer l'accès à la facturation pour IAM, n'oubliez pas d'activer également l'[accès des utilisateurs IAM et fédérés aux pages Billing and Cost Management](#).

**⚠ Important**

Si vous fournissez un groupe IAM, tous les utilisateurs IAM du groupe reçoivent les nouvelles autorisations.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- IAM GroupName

Type : chaîne

Par défaut : ExampleSupportAndBillingGroup

Description : (Obligatoire) il peut d'agir d'un groupe nouveau ou existant. Doit se conformer aux [Limites des noms d'entité IAM](#).

- IAM UserName

Type : chaîne

Par défaut : ExampleUser

Description : (Obligatoire) il doit s'agir d'un utilisateur existant.

- LambdaAssumeRole

Type : chaîne

Description : (Facultatif) ARN du rôle assumé par la fonction Lambda.

- Autorisations

Type : chaîne

Valeurs valides : SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

Par défaut : SupportAndBillingFullAccess

Description : (Obligatoire) Choisissez l'une des options suivantes : `SupportFullAccess` accorde un accès complet au centre de support. `BillingFullAccess` accorde un accès complet au tableau de bord de facturation. `SupportAndBillingFullAccess` accorde un accès complet au centre de Support et au tableau de bord de facturation. Plus d'informations sur les stratégies sous Détails du document.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Les autorisations requises dépendent du mode `AWSSupport-GrantPermissionsToIAMUser` d'exécution.

Exécuter en tant qu'utilisateur ou rôle actuellement connecté

Il est recommandé de joindre la politique gérée par `AmazonSSMAutomationRole` Amazon et les autorisations supplémentaires suivantes pour pouvoir créer la fonction Lambda et le rôle IAM à transmettre à 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" : "*"
    }
]
}

```

## Utilisation AutomationAssumeRole et LambdaAssumeRole

L'utilisateur doit disposer des StartAutomationExecution autorisations ssm : sur le runbook et iam : PassRole sur les rôles IAM transmis sous forme et. AutomationAssumeRoleLambdaAssumeRole Voici les autorisations dont chaque rôle IAM a besoin :

### 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" : "*"
}
]
}

```

## Étapes de document

1. `aws:createStack`- Exécutez AWS CloudFormation Template pour créer une fonction Lambda.
2. `aws:invokeLambdaFunction`- Exécutez Lambda pour définir les autorisations IAM.
3. `aws:deleteStack`- Supprimer le CloudFormation modèle.

## Sorties

configureIAM.Payload

## AWSConfigRemediation-RemoveUserPolicies

### Description

Le AWSConfigRemediation-RemoveUserPolicies runbook supprime les politiques intégrées AWS Identity and Access Management (IAM) et détache toutes les politiques gérées associées à l'utilisateur que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- ID utilisateur IAM

Type : chaîne

Description : (Obligatoire) L'ID de l'utilisateur dont vous souhaitez supprimer les politiques.

- PolicyType

Type : chaîne

Valeurs valides : Toutes | Inline | Géré

Par défaut : Tous

Description : (Obligatoire) Type de politiques IAM que vous souhaitez supprimer pour l'utilisateur.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam>DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam>ListAttachedUserPolicies`
- `iam>ListUserPolicies`
- `iam>ListUsers`

### Étapes de document

- `aws:executeScript`- Supprime et détache les politiques IAM de l'utilisateur que vous spécifiez dans le paramètre. IAMUserID

## **AWSConfigRemediation-ReplaceIAMInlinePolicy**

### Description

Le AWSConfigRemediation-ReplaceIAMInlinePolicy runbook remplace une politique en ligne AWS Identity and Access Management (IAM) par une stratégie IAM gérée répliquée. Pour une politique intégrée attachée à un utilisateur, un groupe ou un rôle, les autorisations de politique en ligne sont clonées dans une stratégie IAM gérée. La stratégie IAM gérée est ajoutée à la ressource et la stratégie intégrée est supprimée. AWS Config doit être activé dans l' Région AWS endroit où vous exécutez cette automatisation.

[Exécuter cette automatisation \(console\)](#)

### Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- InlinePolicyName

Type : StringList

Description : (Obligatoire) La politique IAM intégrée que vous souhaitez remplacer.

- ResourceId

Type : chaîne

Description : (Obligatoire) L'ID de l'utilisateur, du groupe ou du rôle IAM dont vous souhaitez remplacer la politique en ligne.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

#### Étapes de document

- `aws:executeScript`- Remplacez la stratégie IAM intégrée par une stratégie AWS répliquée sur la ressource que vous spécifiez.

## **AWSConfigRemediation-RevokeUnusedIAMUserCredentials**

### Description

Le `AWSConfigRemediation-RevokeUnusedIAMUserCredentials` runbook révoque les mots de passe AWS Identity and Access Management (IAM) non utilisés et les clés d'accès actives. Ce runbook désactive également les clés d'accès expirées et supprime les profils de connexion expirés. AWS Config doit être activé dans l' Région AWS endroit où vous exécutez cette automatisation.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- IAM ResourceId

Type : chaîne

Description : (Obligatoire) L'ID de la ressource IAM dont vous souhaitez révoquer les informations d'identification non utilisées.

- MaxCredentialUsageAge

Type : chaîne

Valeur par défaut : 90

Description : (Obligatoire) Le nombre de jours pendant lesquels l'identifiant doit avoir été utilisé.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:ListDiscoveredResources
- iam>DeleteAccessKey
- iam>DeleteLoginProfile
- iam:GetAccessKeyLastUsed
- iam:GetLoginProfile



- `iam:GetUser`
- `iam:ListAccessKeys`
- `iam:UpdateAccessKey`

### Étapes de document

- `aws:executeScript`- Révoque les informations d'identification IAM de l'utilisateur spécifié dans le `IAMResourceId` paramètre. Les clés d'accès expirées sont désactivées et les profils de connexion expirés sont supprimés.

#### Note

Assurez-vous de configurer le `MaxCredentialUsageAge` paramètre de cette action de correction pour qu'il corresponde au `maxAccessKeyAge` paramètre de la AWS Config règle que vous utilisez pour déclencher cette action : [access-keys-rotated](#).

## AWSConfigRemediation-SetIAMPASSWORDPolicy

### Description

Le `AWSConfigRemediation-SetIAMPASSWORDPolicy` runbook définit la politique de mot de passe utilisateur AWS Identity and Access Management (IAM) pour votre. Compte AWS

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- AllowUsersToChangePassword

Type : booléen

Valeur par défaut : false

Description : (Facultatif) Si ce paramètre est défini sur `true`, tous les utilisateurs IAM de votre site Compte AWS peuvent l'utiliser AWS Management Console pour modifier leur mot de passe.

- HardExpiry

Type : booléen

Valeur par défaut : false

Description : (Facultatif) Si ce paramètre est défini sur `true`, les utilisateurs IAM ne peuvent pas réinitialiser leur mot de passe une fois celui-ci expiré.

- MaxPasswordAge

Type : entier

Par défaut : 0

Description : (Facultatif) Le nombre de jours pendant lesquels le mot de passe d'un utilisateur IAM est valide.

- MinimumPasswordLength

Type : entier

Par défaut : 6

Description : (Facultatif) Le nombre minimal de caractères que peut contenir le mot de passe d'un utilisateur IAM.

Type : entier

Par défaut : 0

Description : (Facultatif) Nombre de mots de passe précédents qu'un utilisateur IAM n'a pas pu réutiliser.

- RequireLowercaseCharacters

Type : booléen

Valeur par défaut : false

Description : (Facultatif) S'il est défini sur `true`, le mot de passe d'un utilisateur IAM doit contenir un caractère minuscule issu de l'alphabet latin de base ISO (a à z).

- RequireNumbers

Type : booléen

Valeur par défaut : false

Description : (Facultatif) S'il est défini sur `true`, le mot de passe d'un utilisateur IAM doit contenir un caractère numérique (0-9).

- RequireSymbols

Type : booléen

Valeur par défaut : false

Description : (Facultatif) S'il est défini sur `true`, le mot de passe d'un utilisateur IAM doit contenir un caractère non alphanumérique (! @ # \$ % ^ \* ( ) \_ + - = [ ] { } | ').

- RequireUppercaseCharacters

Type : booléen

Valeur par défaut : false

Description : (Facultatif) S'il est défini sur `true`, le mot de passe d'un utilisateur IAM doit contenir un caractère majuscule issu de l'alphabet latin de base ISO (A à Z).

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

## Étapes de document

- `aws:executeScript`- Définit la politique de mot de passe utilisateur IAM en fonction des valeurs que vous spécifiez pour les paramètres du runbook de votre. Compte AWS

## Amazon Kinesis Data Streams

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Kinesis Data Streams. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-EnableKinesisStreamEncryption](#)

## AWS-EnableKinesisStreamEncryption

### Description

Le `AWS-EnableKinesisStreamEncryption` runbook permet le chiffrement sur un Amazon Kinesis Data Streams (Kinesis Data Streams). Les applications productrices écrivant dans un flux crypté rencontreront des erreurs si elles n'ont pas accès à la clé AWS Key Management Service (AWS KMS).

[Exécuter cette automatisation \(console\)](#)

### Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- KinesisStreamName

Type : chaîne

Description : (Obligatoire) Nom du flux sur lequel vous souhaitez activer le chiffrement.

- KeyId

Type : chaîne

Par défaut : alias/aws/kinesis

Description : (Obligatoire) La AWS KMS clé gérée par le client que vous souhaitez utiliser pour le chiffrement. Cette valeur peut être un identifiant unique global, un ARN associé à un alias ou à une clé, ou un nom d'alias préfixé par « alias/ ». Vous pouvez également utiliser la clé AWS gérée en utilisant la valeur par défaut du paramètre.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

### Étapes de document

- `VerifyKinesisStreamStatus` (aws : `waitforAwsResource Property`) - Vérifie l'état des Kinesis Data Streams.
- `EnableKinesisStreamEncryption` (aws : `executeAwsApi`) - Active le chiffrement pour les Kinesis Data Streams.
- `VerifyKinesisStreamUpdateComplete` (aws : `waitForAwsResourceProperty`) - Attend que le statut de Kinesis Data Streams revienne à `ACTIVE`
- `VerifyKinesisStreamEncryption` (aws : `assertAwsResource Propriété`) - Vérifie que le chiffrement est activé pour les Kinesis Data Streams.

## AWS KMS

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Key Management Service. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSConfigRemediation-CancelKeyDeletion](#)
- [AWSConfigRemediation-EnableKeyRotation](#)

## AWSConfigRemediation-CancelKeyDeletion

### Description

Le `AWSConfigRemediation-CancelKeyDeletion` runbook annule la suppression de la clé gérée par le client AWS Key Management Service (AWS KMS) que vous spécifiez.

## [Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- KeyId

Type : chaîne

Description : (Obligatoire) L'ID de la clé gérée par le client dont vous souhaitez annuler la suppression.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CancelKeyDeletion`
- `kms:DescribeKey`

### Étapes de document

- `aws:executeAwsApi`- Annule la suppression de la clé gérée par le client que vous avez spécifiée dans le `KeyId` paramètre.
- `aws:assertAwsResourceProperty`- Confirme que la suppression des clés est désactivée sur votre clé gérée par le client.

## AWSConfigRemediation-EnableKeyRotation

### Description

Le `AWSConfigRemediation-EnableKeyRotation` runbook permet la rotation automatique des clés pour la clé symétrique AWS Key Management Service (AWS KMS) gérée par le client.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `KeyId`

Type : chaîne

Description : (Obligatoire) L'ID de la clé gérée par le client sur laquelle vous souhaitez activer la rotation automatique des clés.



## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

## Étapes de document

- `aws:executeAwsApi`- Active la rotation automatique des clés sur la clé gérée par le client que vous spécifiez dans le `KeyId` paramètre.
- `aws:assertAwsResourceProperty`- Confirme que la rotation automatique des clés est activée sur votre clé gérée par le client.

## Lambda

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Lambda.

Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing](#)
- [AWSConfigRemediation-DeleteLambdaFunction](#)
- [AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK](#)
- [AWSConfigRemediation-MoveLambdaToVPC](#)
- [AWSSupport-RemediateLambdaS3Event](#)
- [AWSSupport-TroubleshootLambdaInternetAccess](#)
- [AWSSupport-TroubleshootLambdaS3Event](#)

## **AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing**

### Description

Le `AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing` runbook permet le suivi AWS X-Ray en direct de la AWS Lambda fonction que vous spécifiez dans le `FunctionName` paramètre.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `FunctionName`

Type : chaîne

Description : (Obligatoire) Le nom ou l'ARN de la fonction Lambda sur laquelle activer le suivi.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `lambda:UpdateFunctionConfiguration`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

## Étapes de document

- `aws:executeAwsApi`- Active le traçage X-Ray sur la fonction Lambda que vous spécifiez dans le `FunctionName` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que le traçage X-Ray a été activé sur la fonction Lambda.

## Sorties

`UpdateLambdaConfig.UpdateFunctionConfigurationResponse` - Réponse de l'appel `UpdateFunctionConfiguration` d'API.

# AWSConfigRemediation-DeleteLambdaFunction

## Description

Le `AWSConfigRemediation-DeleteLambdaFunction` runbook supprime la AWS Lambda fonction que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- **LambdaFunctionName**

Type : chaîne

Description : (Obligatoire) Nom de la fonction Lambda que vous souhaitez supprimer.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

#### Étapes de document

- `aws:executeAwsApi`- Supprime la fonction Lambda spécifiée dans `LambdaFunctionName` le paramètre.
- `aws:executeScript`- Vérifie que la fonction Lambda a été supprimée.

## **AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK**

### Description

Le `AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` runbook chiffre, au repos, les variables d'environnement de la fonction (AWS Lambda Lambda) que vous spécifiez à l'aide d'une clé gérée par le client AWS Key Management Service (AWS KMS). Ce manuel d'exécution ne doit être utilisé que comme référence pour garantir que les variables d'environnement de votre fonction Lambda sont chiffrées conformément aux meilleures pratiques de sécurité minimales recommandées. Nous recommandons de chiffrer plusieurs fonctions à l'aide de différentes clés gérées par le client.

[Exécuter cette automatisation \(console\)](#)

### Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- FunctionName

Type : chaîne

Description : (Obligatoire) Le nom ou l'ARN de la fonction Lambda dont vous souhaitez chiffrer les variables d'environnement.

- KMS KeyArn

Type : chaîne

Description : (Obligatoire) L'ARN de la clé gérée par le AWS KMS client que vous souhaitez utiliser pour chiffrer les variables d'environnement de votre fonction Lambda.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

## Étapes de document

- `aws:waitForAwsResourceProperty`- Il attend que la `LastUpdateStatus` propriété soit prête. `Successful`
- `aws:executeAwsApi`- Chiffre les variables d'environnement pour la fonction Lambda que vous spécifiez dans `FunctionName` le paramètre à l'aide de la clé gérée par AWS KMS le client que vous spécifiez dans `KMSKeyArn` le paramètre.
- `aws:assertAwsResourceProperty`- Confirme que le chiffrement est activé sur les variables d'environnement de votre fonction Lambda.

## AWSConfigRemediation-MoveLambdaToVPC

### Description

Le `AWSConfigRemediation-MoveLambdaToVPC` runbook déplace une fonction AWS Lambda (Lambda) vers un Amazon Virtual Private Cloud (Amazon VPC).

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- **FunctionName**

Type : chaîne

Description : (Obligatoire) Nom de la fonction Lambda à déplacer vers un Amazon VPC.

- **SecurityGroupIds**

Type : chaîne

Description : (Obligatoire) Les identifiants de groupe de sécurité que vous souhaitez attribuer aux interfaces réseau élastiques (ENI) associées à votre fonction Lambda.

- **SubnetIds**

Type : chaîne

Description : (Obligatoire) Les identifiants de sous-réseau auxquels vous souhaitez créer les interfaces réseau élastiques (ENI) associées à votre fonction Lambda.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

### Étapes de document

- `aws:executeAwsApi`- Met à jour la configuration Amazon VPC pour la fonction Lambda que vous spécifiez dans le paramètre. `FunctionName`
- `aws:waitForAwsResourceProperty`- Attend que la `LastUpdateStatus` fonction Lambda soit activée. `successful`
- `aws:executeScript`- Vérifie que la configuration Amazon VPC de la fonction Lambda a été correctement mise à jour.

# AWSSupport-RemediateLambdaS3Event

## Description

Le `AWSSupport-TroubleshootLambdaS3Event` runbook fournit une solution automatisée pour les procédures décrites dans les articles du centre de AWS connaissances. [Pourquoi ma notification d'événement Amazon S3 ne déclenche-t-elle pas ma fonction Lambda ?](#) et [pourquoi le message d'erreur « Impossible de valider les configurations de destination suivantes » s'affiche-t-il lorsque je crée une notification d'événement Amazon S3 pour déclencher ma fonction Lambda ?](#) Ce runbook vous aide à identifier et à corriger pourquoi une notification d'événement Amazon Simple Storage Service (Amazon S3) n'a pas réussi à déclencher la fonction que vous avez spécifiée. AWS Lambda [Si la sortie du runbook suggère de valider et de configurer la simultanéité de votre fonction Lambda, consultez les sections Invocation asynchrone et Dimensionnement des fonctions.](#)[AWS Lambda](#)

### Note

Des erreurs « Impossible de valider les configurations de destination suivantes » peuvent également se produire en raison de configurations d'événements Amazon Simple Notification Service (Amazon SNS) et Amazon Simple Queue Service (Amazon SQS) Amazon S3 incorrectes. Ce runbook vérifie uniquement les configurations des fonctions Lambda. Si, après avoir utilisé le runbook, vous recevez toujours le message d'erreur « Impossible de valider les configurations de destination suivantes », veuillez consulter toutes les configurations d'événements Amazon SNS et Amazon SQS Amazon S3 existantes.

## [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres



- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- LambdaFunctionArn

Type : chaîne

Description : (Obligatoire) L'ARN de la fonction Lambda.

- S3 BucketName

Type : chaîne

Description : (Obligatoire) Le nom du compartiment Amazon S3 dont les notifications d'événements déclenchent la fonction Lambda.

- Action

Type : chaîne

Valeurs valides : Résoudre les problèmes | Corriger

Description : (Obligatoire) L'action que vous souhaitez que le runbook exécute.

L'option `Troubleshoot` permet d'identifier les problèmes, mais n'effectue aucune action de mutation pour résoudre le problème. L'option `Remediate` permet d'identifier les problèmes et de tenter de les résoudre pour vous.

## Autorisations IAM requises

Le paramètre `AutomationAssumeRole` nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`

- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

## Étapes de document

- `aws:branch`- Branches basées sur l'entrée spécifiée pour le Action paramètre.

Si la valeur spécifiée est `Troubleshoot` :

- `aws:executeAutomation`- Exécute le `AWSSupport-TroubleshootLambdaS3Event` runbook.
- `aws:executeAwsApi`- Vérifie le résultat du `AWSSupport-TroubleshootLambdaS3Event` runbook exécuté à l'étape précédente.

Si la valeur spécifiée est `Remediate` :

- `aws:executeScript`- Exécute un script pour résoudre les problèmes décrits dans la section [Pourquoi ma notification d'événement Amazon S3 ne déclenche-t-elle pas ma fonction Lambda ? et pourquoi le message d'erreur « Impossible de valider les configurations de destination suivantes » s'affiche-t-il lorsque je crée une notification d'événement Amazon S3 pour déclencher ma fonction Lambda ?](#) Articles du centre de connaissances.

## Sorties

`Checkout.Output`

Corriger l'événement `Lambdas3output`

## **AWSSupport-TroubleshootLambdaInternetAccess**

### Description

Le `AWSSupport-TroubleshootLambdaInternetAccess` runbook vous aide à résoudre les problèmes d'accès à Internet liés à une AWS Lambda fonction lancée dans Amazon Virtual Private Cloud (Amazon VPC). Les ressources telles que les itinéraires de sous-réseau, les règles des

groupes de sécurité et les règles de liste de contrôle d'accès réseau (ACL) sont examinées pour confirmer que l'accès Internet sortant est autorisé.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- FunctionName

Type : chaîne

Description : (Obligatoire) Nom de la fonction Lambda pour laquelle vous souhaitez résoudre les problèmes d'accès à Internet.

- destinationIp

Type : chaîne

Description : (Obligatoire) Adresse IP de destination à laquelle vous souhaitez établir une connexion sortante.

- destinationPort

Type : chaîne

Par défaut: 443

Description : (Facultatif) Le port de destination sur lequel vous souhaitez établir une connexion sortante.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

### Étapes de document

- `aws:executeScript`- Vérifie la configuration des différentes ressources de votre VPC où la fonction Lambda a été lancée.
- `aws:branch`- Branches basées sur le fait que la fonction Lambda spécifiée se trouve dans un VPC ou non.
- `aws:executeScript`- Examine les routes de la table de routage pour le sous-réseau sur lequel la fonction Lambda a été lancée et vérifie que les routes menant à une passerelle de traduction d'adresses réseau (NAT) et à une passerelle Internet sont présentes. Confirme que la fonction Lambda ne se trouve pas dans un sous-réseau public.
- `aws:executeScript`- Vérifie que le groupe de sécurité associé à la fonction Lambda autorise l'accès Internet sortant en fonction des valeurs spécifiées pour `destinationIp` les paramètres et `destinationPort`
- `aws:executeScript`- Vérifie les règles ACL associées aux sous-réseaux de la fonction Lambda et la passerelle NAT autorise l'accès Internet sortant en fonction des valeurs spécifiées pour les paramètres et `destinationIp destinationPort`

### Sorties

CheckVPC.vpc : ID du VPC sur lequel votre fonction Lambda a été lancée.

CheckVPC.subnet - Les identifiants des sous-réseaux sur lesquels votre fonction Lambda a été lancée.

CheckVPC.SecurityGroups - Groupes de sécurité associés à la fonction Lambda.

Checknacl.nacl - Message d'analyse avec les noms des ressources. LambdaIp fait référence à l'adresse IP privée de l'interface elastic network de votre fonction Lambda. L'objet LambdaIpRules n'est généré que pour les sous-réseaux dotés d'une route vers une passerelle NAT. Le contenu suivant est un exemple de sortie.

```
{
  "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 : analyse du groupe de sécurité associé à votre fonction Lambda. Le contenu suivant est un exemple de sortie.

```
{
```

```
"sg-123456789":{
  "Status":"Allowed",
  "Analysis":"This security group has allowed destintion IP and port in its
outbuond rule."
}
```

Checksubnet.subnets - Analyse des sous-réseaux de votre VPC associés à votre fonction Lambda. Le contenu suivant est un exemple de sortie.

```
{
  "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

### Description

Le AWSSupport-TroubleshootLambdaS3Event runbook fournit une solution automatisée pour les procédures décrites dans les articles du centre de AWS connaissances. [Pourquoi ma notification d'événement Amazon S3 ne déclenche-t-elle pas ma fonction Lambda ?](#) et [pourquoi le message d'erreur « Impossible de valider les configurations de destination suivantes » s'affiche-t-il lorsque je crée une notification d'événement Amazon S3 pour déclencher ma fonction Lambda ?](#) Ce runbook vous aide à identifier pourquoi une notification d'événement Amazon Simple Storage Service (Amazon S3) n'a pas réussi à déclencher AWS Lambda la fonction que vous avez spécifiée. [Si la sortie du runbook suggère de valider et de configurer la simultanéité de votre fonction Lambda, consultez les sections Invocation asynchrone et Dimensionnement des fonctions.AWS Lambda](#)

[Exécuter cette automatisation \(console\)](#)

### Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- LambdaFunctionArn

Type : chaîne

Description : (Obligatoire) L'ARN de la fonction Lambda déclenchée par la notification d'événement Amazon S3.

- S3 BucketName

Type : chaîne

Description : (Obligatoire) Le nom du compartiment Amazon S3 dont les notifications d'événements déclenchent la fonction Lambda.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

## Étapes de document

- `aws:executeScript`- Exécute le script pour valider les paramètres de configuration pour la notification d'événement Amazon S3. Valide la politique IAM basée sur les ressources pour votre fonction Lambda et génère une commande AWS Command Line Interface (AWS CLI) pour ajouter les autorisations nécessaires si les autorisations requises ne figurent pas dans la politique. Valide les politiques de ressources des autres fonctions Lambda qui font partie des notifications d'événements pour le même compartiment S3 et génère AWS CLI une commande en sortie si les autorisations requises sont manquantes.

## Sorties

Lambda S3 Event.output

# Amazon Managed Workflows for Apache Airflow

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Managed Workflows pour Apache Airflow. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWSSupport-TroubleshootMWAAEnvironmentCreation](#)

## **AWSSupport-TroubleshootMWAAEnvironmentCreation**

### Description

Le `AWSSupport-TroubleshootMWAAEnvironmentCreation` runbook fournit des informations pour résoudre les problèmes liés à la création de l'environnement Amazon Managed Workflows for Apache Airflow (Amazon MWAA), et pour effectuer des vérifications, accompagnées des raisons documentées, dans la mesure du possible pour identifier la panne.

### Comment fonctionne-t-il ?

Le runbook exécute les étapes suivantes :

- Récupère les détails de l'environnement Amazon MWAA.



- Vérifie les autorisations du rôle d'exécution.
- Vérifie si l'environnement est autorisé à utiliser la AWS KMS clé fournie pour la journalisation et si le groupe de CloudWatch journaux requis existe.
- Analyse les journaux du groupe de journaux fourni pour détecter les erreurs éventuelles.
- Vérifie la configuration réseau pour vérifier si l'environnement Amazon MWAA a accès aux points de terminaison requis.
- Génère un rapport contenant les résultats.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

/

Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetPublicAccessBlock
- s3control:GetPublicAccessBlock
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez [AWS Support - Troubleshoot MWAA Environment Creation](#) à Systems Manager sous Documents.
2. Sélectionnez Exécute automation (Exécuter l'automatisation).
3. Pour les paramètres d'entrée, entrez ce qui suit :
  - AutomationAssumeRole (Facultatif) :  
  
Amazon Resource Name (ARN) du rôle AWS AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.
  - EnvironmentName (Obligatoire) :  
  
Nom de l'environnement Amazon MWAA que vous souhaitez évaluer.

**Input parameters**

<b>AutomationAssumeRole</b> <small>(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</small>	<b>EnvironmentName</b> <small>(Required) Name of the MWAAs environment you wish to evaluate.</small>
<input type="text"/>	<input type="text" value="String"/>

- Sélectionnez Exécuter.
- L'automatisation démarre.
- Le document exécute les étapes suivantes :

- **GetMWAASystemDetails :**

Récupère les détails de l'environnement Amazon MWAAS. Si cette étape échoue, le processus d'automatisation s'arrête et s'affiche comme Failed.

- **CheckIAMPermissionsOnExecutionRole :**

Vérifie que le rôle d'exécution dispose des autorisations requises pour les ressources Amazon MWAAS, Amazon S3 CloudWatch, CloudWatch Logs et Amazon SQS. S'il détecte une clé gérée par le client AWS Key Management Service (AWS KMS), l'automatisation valide les autorisations requises pour la clé. Cette étape utilise l'iam:SimulateCustomPolicyAPI pour déterminer si le rôle d'exécution de l'automatisation répond à toutes les autorisations requises.

- **CheckKMSPolicyOnKMSKey :**

Vérifie si la politique de AWS KMS clé autorise l'environnement Amazon MWAAS à utiliser la clé pour chiffrer les journaux. CloudWatch Si la AWS KMS clé est AWS gérée, l'automatisation ignore cette vérification.

- **CheckIfRequiredLogGroupsExists :**

Vérifie si les groupes de CloudWatch journaux requis pour l'environnement Amazon MWAAS existent. Dans le cas contraire, l'automatisation vérifie CloudTrail CreateLogGroup les DeleteLogGroup événements. Cette étape vérifie également les CreateLogGroup événements.

- **BranchOnLogGroupsFindings :**

Branches basées sur l'existence de groupes de CloudWatch journaux liés à l'environnement Amazon MWAAS. S'il existe au moins un groupe de journaux, l'automatisation l'analyse pour localiser les erreurs. Si aucun groupe de journaux n'est présent, l'automatisation ignore l'étape suivante.

- **CheckForErrorsInLogGroups :**

Analyse les groupes de CloudWatch journaux pour localiser les erreurs.

- **GetRequiredEndpointsDetails:**

Récupère les points de terminaison de service utilisés par l'environnement Amazon MWAA.

- **CheckNetworkConfiguration:**

Vérifie que la configuration réseau de l'environnement Amazon MWAA répond aux exigences, notamment en vérifiant les groupes de sécurité, les ACL réseau, les sous-réseaux et les configurations des tables de routage.

- **CheckEndpointsConnectivity:**

Invoke l'automatisation `AWSSupport-ConnectivityTroubleshooter` secondaire pour valider la connectivité de l'Amazon MWAA aux points de terminaison requis.

- **CheckS3BlockPublicAccess:**

Vérifie si le compartiment Amazon S3 de l'environnement Amazon MWAA est `Block Public Access` activé et passe également en revue les paramètres généraux de blocage de l'accès public à Amazon S3 du compte.

- **GenerateReport:**

Collecte les informations issues de l'automatisation et imprime le résultat ou la sortie de chaque étape.

7. Une fois terminé, consultez la section Sorties pour obtenir les résultats détaillés de l'exécution :

- Vérification des autorisations du rôle d'exécution de l'environnement Amazon MWAA :

Vérifie si le rôle d'exécution dispose des autorisations requises pour les ressources Amazon MWAA, Amazon S3 CloudWatch, CloudWatch Logs et Amazon SQS. Si une AWS KMS clé gérée par le client est détectée, l'automatisation valide les autorisations requises pour la clé.

- Vérification de la politique AWS KMS clé de l'environnement Amazon MWAA :

Vérifie si le rôle d'exécution possède les autorisations nécessaires pour les ressources Amazon MWAA, Amazon S3 CloudWatch, CloudWatch Logs et Amazon SQS. De plus, si une AWS KMS clé gérée par le client est détectée, l'automatisation vérifie les autorisations requises pour la clé.

- Vérification des groupes de CloudWatch journaux de l'environnement Amazon MWAA :

Vérifie si les groupes de CloudWatch journaux requis pour l'environnement Amazon MWAA existent. Si ce n'est pas le cas, l'automatisation vérifie ensuite CloudTrail la localisation `CreateLogGroup` et les `DeleteLogGroup` événements.

- Vérification des tables de routage de l'environnement Amazon MWAA :

Vérifie si les tables de routage Amazon VPC dans l'environnement Amazon MWAA sont correctement configurées.

- Vérification des groupes de sécurité de l'environnement Amazon MWAA :

Vérifie si les groupes de sécurité Amazon VPC de l'environnement Amazon MWAA sont correctement configurés.

- Vérification des ACL du réseau de l'environnement Amazon MWAA :

Vérifie si les groupes de sécurité Amazon VPC dans l'environnement Amazon MWAA sont correctement configurés.

- Vérification des sous-réseaux de l'environnement Amazon MWAA :

Vérifie si les sous-réseaux de l'environnement Amazon MWAA sont privés.

- La vérification de l'environnement Amazon MWAA nécessitait la connectivité des points de terminaison :

Vérifie si l'environnement Amazon MWAA peut accéder aux points de terminaison requis. À cette fin, l'automatisation invoque `AWSSupport-ConnectivityTroubleshooter`automatisation.

- Vérification du compartiment Amazon S3 de l'environnement Amazon MWAA :

Vérifie si le compartiment Amazon S3 de l'environnement Amazon MWAA est `Block Public Access` activé et passe également en revue les paramètres de blocage de l'accès public à Amazon S3 du compte.

- La vérification de l'environnement Amazon MWAA CloudWatch enregistre les erreurs des groupes :

Analyse les groupes de CloudWatch journaux existants de l'environnement Amazon MWAA pour localiser les erreurs.

## ▼ Outputs

## GenerateReportAutomationReport

Troubleshooting report for MIAA environment

👉 The automation found no issues with the MIAA environment configuration ✓

🔍 Checking the MIAA environment execution role permissions

All the required permissions for the MIAA environment execution role are in place ✓

🔍 Checking the MIAA environment KMS key policy

KMS key is an AWS managed key ✓

🔍 Checking the MIAA environment CloudWatch logs groups

The number of CloudWatch log groups found is 5 and the number of enabled log groups for the MIAA environment [redacted] is 5. This suggests that all log groups were created successfully ✓

🔍 Checking the MIAA environment Route Tables

NAT GW [redacted] has Internet route: subnet: [redacted] -> nat: [redacted] -> igw: [redacted] ✓

NAT GW [redacted] has Internet route: subnet: [redacted] -> nat: [redacted] -> igw: [redacted] ✓

🔍 Checking the MIAA environment Security Groups

Security group [redacted] has self-referencing rules for all traffic. ✓

🔍 Checking the MIAA environment Network ACLs

NACL: [redacted] allows port 5432 on egress ✓ and allows port 5432 on ingress ✓

🔍 Checking the MIAA environment Subnets

Subnet: subnet: [redacted] is private ✓

Subnet: subnet: [redacted] is private ✓

🔍 Checking the MIAA environment required endpoints connectivity

✓ Testing connectivity with sqs.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and sqs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MIAA environment has access to the sqs.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

✓ Testing connectivity with api.ecr.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and api.ecr.eu-west-1.amazonaws.com on port 443 was successful, this means that the MIAA environment has access to the api.ecr.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

✓ Testing connectivity with monitoring.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and monitoring.eu-west-1.amazonaws.com on port 443 was successful, this means that the MIAA environment has access to the monitoring.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

✓ Testing connectivity with kms.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and kms.eu-west-1.amazonaws.com on port 443 was successful, this means that the MIAA environment has access to the kms.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

✓ Testing connectivity with s3.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and s3.eu-west-1.amazonaws.com on port 443 was successful, this means that the MIAA environment has access to the s3.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and env.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MIAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and env.airflow.eu-west-1.amazonaws.com on port 5432 was successful, this means that the MIAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

✓ Testing connectivity with api.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and api.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MIAA environment has access to the api.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

✓ Testing connectivity with logs.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and logs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MIAA environment has access to the logs.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

✓ Testing connectivity with ops.airflow.eu-west-1.amazonaws.com:

Connectivity test between ENI [redacted] and ops.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MIAA environment has access to the ops.airflow.eu-west-1.amazonaws.com service ✓

To check the SSM automation execution click here: [https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/\[redacted\]?region=eu-west-1](https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1)

🔍 Checking the MIAA environment S3 bucket

Environment's S3 bucket and/or account block public access ✓

🔍 Checking the MIAA environment CloudWatch logs groups errors

Parsed log group [redacted] DAGProcessing - no errors found ✓

Parsed log group [redacted] Scheduler - no errors found ✓

Parsed log group [redacted] Task - no errors found ✓

Parsed log group [redacted] WebServer - no errors found ✓

Parsed log group [redacted] Worker - no errors found ✓

## Références

## Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

# Neptune

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Neptune. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-EnableNeptuneDbAuditLogsToCloudWatch](#)
- [AWS-EnableNeptuneDbBackupRetentionPeriod](#)
- [AWS-EnableNeptuneClusterDeletionProtection](#)

## AWS-EnableNeptuneDbAuditLogsToCloudWatch

### Description

Le `AWS-EnableNeptuneDbAuditLogsToCloudWatch` runbook vous permet d'envoyer les journaux d'audit d'un cluster de base de données Amazon Neptune à Amazon CloudWatch Logs.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre

nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `DbClusterResourceId`

Type : chaîne

Description : (Obligatoire) L'ID de ressource du cluster de base de données Neptune pour lequel vous souhaitez activer les journaux d'audit.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

### Étapes de document

- `GetNeptuneDbClusterIdentifier` (`aws :executeAwsApi`) - Renvoie l'ID du cluster de base de données Neptune.
- `VerifyNeptuneDbEngine` (`aws : assertAwsResource Property`) - Vérifie que le type de moteur de base de données Neptune est. `neptune`
- `EnableNeptuneDbAuditLogs` (`aws :executeAwsApi`) - Permet d'envoyer CloudWatch des journaux d'audit pour le cluster de base de données Neptune.
- `VerifyNeptuneDbStatus` (`aws : waitAwsResource Propriété`) - Vérifie que l'état du cluster de base de données Neptune est. `available`
- `VerifyNeptuneDbAuditLogs` (`AWS:ExecuteScript`) - Vérifie que les journaux d'audit ont été correctement configurés pour être envoyés à Logs. CloudWatch



# AWS-EnableNeptuneDbBackupRetentionPeriod

## Description

Le AWS-EnableNeptuneDbBackupRetentionPeriod runbook vous aide à activer les sauvegardes automatisées avec une période de conservation des sauvegardes comprise entre 7 et 35 jours pour un cluster de base de données Amazon Neptune.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- DbClusterResourceid

Type : chaîne

Description : (Obligatoire) L'ID de ressource du cluster de base de données Neptune pour lequel vous souhaitez activer les sauvegardes.

- BackupRetentionPeriod

Type : entier

Valeurs valides : 7-35

Description : (Obligatoire) Nombre de jours pendant lesquels les sauvegardes sont conservées.

- PreferredBackupWindow

Type : chaîne

Description : (Facultatif) Période quotidienne d'au moins 30 minutes pendant laquelle les sauvegardes sont effectuées. La valeur doit être en temps universel coordonné (UTC) et utiliser le format :hh24:mm-hh24:mm. La période de conservation des sauvegardes ne doit pas entrer en conflit avec la fenêtre de maintenance préférée.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

### Étapes de document

- `GetNeptuneDbClusterIdentifier` (aws :executeAwsApi) - Renvoie l'ID du cluster de base de données Neptune.
- `VerifyNeptuneDbEngine` (aws : assertAwsResource Property) - Vérifie que le type de moteur de base de données Neptune est. `neptune`
- `VerifyNeptuneDbStatus` (aws : waitAwsResource Propriété) - Vérifie que l'état du cluster de base de données Neptune est. `available`
- `ModifyNeptuneDbRetentionPeriod` (aws :executeAwsApi) - Définit la période de rétention pour le cluster de base de données Neptune.
- `VerifyNeptuneDbBackupsEnabled` (AWS:ExecuteScript) - Vérifie que la période de rétention et la fenêtre de sauvegarde ont été correctement définies.

# AWS-EnableNeptuneClusterDeletionProtection

## Description

Le `AWS-EnableNeptuneClusterDeletionProtection` runbook active la protection contre la suppression pour le cluster Amazon Neptune que vous spécifiez.

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux, macOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `DbClusterResourceId`

Type : chaîne

Description : (Obligatoire) L'ID du cluster Neptune sur lequel vous souhaitez activer la protection contre les suppressions.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:GetAutomationExecution`

- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

## Étapes de document

- `GetNeptuneDbClusterIdentifier` (`aws :executeAwsApi`) - Renvoie l'ID du cluster de base de données Neptune.
- `VerifyNeptuneDbEngine` (`aws :assertAwsResource Property`) - Vérifie que le type de moteur du cluster de base de données spécifié est `neptune`.
- `VerifyNeptuneStatus` (`aws :waitForAwsResourceProperty`) - Vérifie que l'état du cluster est `available`.
- `EnableNeptuneDbDeletionProtection` (`aws :executeAwsApi`) - Active la protection contre les suppressions sur le cluster de base de données Neptune.
- `VerifyNeptuneDbDeletionProtection` (`aws :assertAwsResource Property`) - Vérifie que la protection contre la suppression est activée sur le cluster de base de données.

## Sorties

- `EnableNeptuneDbDeletionProtection`. `EnableNeptuneDbDeletionProtectionResponse` - Le résultat de l'opération API.

## Amazon RDS

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Relational Database Service. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [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**

### Description

Le `AWS-CreateEncryptedRdsSnapshot` runbook crée un instantané chiffré à partir d'une instance non chiffrée d'Amazon Relational Database Service (Amazon RDS).

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- DB InstanceIdentifier

Type : chaîne

Description : (Obligatoire) L'ID de l'instance Amazon RDS dont vous souhaitez créer un instantané.

- DB SnapshotIdentifier

Type : chaîne

Description : (Facultatif) Modèle de nom pour l'instantané Amazon RDS. Le modèle de nom par défaut est *DB InstanceIdentifier -yyyymmddhhmmss*.

- DB cryptée SnapshotIdentifier

Type : chaîne

Description : (Facultatif) Nom du cliché chiffré. Le nom par défaut est la valeur que vous spécifiez pour le DBSnapshotIdentifier paramètre ajouté. -encrypted

- InstanceTags

Type : chaîne

Description : (Facultatif) Tags à ajouter à l'instance de base de données. (Exemple : key=tagkey1, value=tagvalue1 ; key=tagkey2, value=tagValue2) '

- KmsKeyId

Type : chaîne

Par défaut : alias/aws/rds

Description : (Facultatif) L'ARN, l'ID de clé ou l'alias de clé de la clé gérée par le client que vous souhaitez utiliser pour chiffrer l'instantané.

- SnapshotTags

Type : chaîne

Description : (Facultatif) Balises à ajouter à l'instantané. (Exemple : key=tagkey1, value=tagvalue1 ; key=tagkey2, value=tagValue2) '

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- rds:AddTagsToResource
- rds:CopyDBSnapshot
- rds:CreateDBSnapshot
- rds>DeleteDBSnapshot
- rds:DescribeDBSnapshots

### Étapes de document

- aws:executeScript- Crée un instantané de l'instance de base de données que vous spécifiez dans le DBInstanceIdentifier paramètre.
- aws:executeScript- Vérifie que l'instantané créé à l'étape précédente existe et existeavailable.

- `aws:executeScript`- Copie le cliché créé précédemment dans un instantané chiffré.
- `aws:executeScript`- Vérifie que l'instantané chiffré créé à l'étape précédente existe.

## Sorties

`CopyRdsSnapshotToEncryptedRdsSnapshot`. `EncryptedSnapshotId` - L'ID de l'instantané Amazon RDS chiffré.

# AWS-CreateRdsSnapshot

## Description

Créez un instantané Amazon Relational Database Service (Amazon RDS) pour une instance Amazon RDS.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

## Bases de données

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `DB InstanceIdentifier`



Type : chaîne

Description : (Obligatoire) L'InstanceID ID de base de données de l'instance RDS à partir de laquelle créer un instantané.

- DB SnapshotIdentifier

Type : chaîne

Description : (Facultatif) SnapshotIdentifier ID de base de données du snapshot RDS à créer.

- InstanceTags

Type : chaîne

Description : (Facultatif) Balises à créer pour l'instance.

- SnapshotTags

Type : chaîne

Description : (Facultatif) Balises à créer pour l'instantané.

Étapes de document

CreatorDSSnapshot — Crée l'instantané RDS et renvoie l'ID de l'instantané.

VerifyRDSnapshot — Vérifie que l'instantané créé à l'étape précédente existe.

Sorties

CreatorDSSnapshot. SnapshotId — L'ID de l'instantané créé.

## **AWSConfigRemediation-DeleteRDSCluster**

Description

Le `AWSConfigRemediation-DeleteRDSCluster` runbook supprime le cluster Amazon Relational Database Service (Amazon RDS) que vous spécifiez. AWS Config doit être activé dans l' Région AWS endroit où vous exécutez cette automatisation.

[Exécuter cette automatisation \(console\)](#)

Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- DB ClusterId

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource du cluster de base de données sur lequel vous souhaitez activer la protection contre les suppressions.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds>DeleteDBCluster
- rds>DeleteDBInstance
- rds:DescribeDBClusters

### Étapes de document

- `aws:executeScript`- Supprime le cluster de base de données que vous spécifiez dans le `DBClusterId` paramètre.

## AWSConfigRemediation-DeleteRDSClusterSnapshot

### Description

Le `AWSConfigRemediation-DeleteRDSClusterSnapshot` runbook supprime l'instantané du cluster Amazon Relational Database Service (Amazon RDS) donné.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `DB ClusterSnapshotId`

Type : chaîne

Description : (Obligatoire) L'identifiant de capture d'écran du cluster Amazon RDS à supprimer.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

### Étapes de document

- `aws:branch`- Vérifie si le snapshot du cluster est en bon available état. S'il n'est pas disponible, le flux se termine.
- `aws:executeAwsApi`- Supprime l'instantané de cluster Amazon RDS donné à l'aide de l'identifiant d'instantané de cluster de base de données (DB).
- `aws:executeScript`- Vérifie que l'instantané du cluster Amazon RDS donné a été supprimé.

## AWSConfigRemediation-DeleteRDSInstance

### Description

Le `AWSConfigRemediation-DeleteRDSInstance` runbook supprime l'instance Amazon Relational Database Service (Amazon RDS) que vous spécifiez. Lorsque vous supprimez une instance de base de données (DB), toutes les sauvegardes automatiques de cette instance sont supprimées et ne peuvent pas être restaurées. Les instantanés de base de données manuels ne sont pas supprimés. Si l'instance de base de données que vous souhaitez supprimer est dans l'`incompatible-restoreétat failedincompatible-network`, ou, vous devez définir le `SkipFinalSnapshot` paramètre sur `true`.

#### Note

Si l'instance de base de données que vous souhaitez supprimer se trouve dans un cluster de base de données Amazon Aurora, le runbook ne supprimera pas l'instance de base de données s'il s'agit d'une réplique en lecture et de la seule instance du cluster de base de données.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- DbResourceId

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de l'instance de base de données que vous souhaitez supprimer.

- SkipFinalSnapshot

Type : booléen

Valeur par défaut : false

Description : (Facultatif) Si ce paramètre est défini sur `true`, aucun instantané final n'est créé avant la suppression de l'instance de base de données.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `rds>DeleteDBInstance`
- `rds:DescribeDBInstances`

### Étapes de document

- `aws:executeAwsApi`- Recueille le nom de l'instance de base de données à partir de la valeur que vous spécifiez dans le `DbiResourceId` paramètre.
- `aws:branch`- Branches basées sur la valeur que vous spécifiez dans le `SkipFinalSnapshot` paramètre.
- `aws:executeAwsApi`- Supprime l'instance de base de données que vous spécifiez dans le `DbiResourceId` paramètre.
- `aws:executeAwsApi`- Supprime l'instance de base de données que vous spécifiez dans le `DbiResourceId` paramètre après la création de l'instantané final.
- `aws:assertAwsResourceProperty`- Vérifie que l'instance de base de données a été supprimée.

## **AWSConfigRemediation-DeleteRDSInstanceSnapshot**

### Description

Le `AWSConfigRemediation-DeleteRDSInstanceSnapshot` runbook supprime l'instantané d'instance Amazon Relational Database Service (Amazon RDS) que vous spécifiez. Seuls les instantanés dans `available` cet état sont supprimés. Ce runbook ne permet pas de supprimer des instantanés des instances de base de données Amazon Aurora.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- DbSnapshotId

Type : chaîne

Description : (Obligatoire) L'ID de l'instantané que vous souhaitez supprimer.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds>DeleteDBSnapshot
- rds:DescribeDBSnapshots

### Étapes de document

- aws:executeAwsApi- Rassemble l'état de l'instantané spécifié dans le DbSnapshotId paramètre.
- aws:assertAwsResourceProperty- Confirme que l'état de l'instantané est disponible.
- aws:executeAwsApi- Supprime le cliché spécifié dans le DbSnapshotId paramètre.
- aws:executeScript- Vérifie que l'instantané a été supprimé.

## **AWSConfigRemediation-DisablePublicAccessToRDSInstance**

### Description

Le `AWSConfigRemediation-DisablePublicAccessToRDSInstance` runbook désactive l'accessibilité publique pour l'instance de base de données (DB) Amazon Relational Database Service (Amazon RDS) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `DbiResourceId`

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de l'instance de base de données pour laquelle vous souhaitez désactiver l'accessibilité publique.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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



- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

### Étapes de document

- `aws:executeAwsApi`- Recueille l'identifiant de l'instance de base de données à partir de l'identifiant de ressource de l'instance de base de données.
- `aws:assertAwsResourceProperty`- Vérifie que les instances de base de données sont dans un AVAILABLE état.
- `aws:executeAwsApi`- Désactive l'accessibilité publique sur votre instance de base de données.
- `aws:waitForAwsResourceProperty`- Attend que l'instance de base de données passe à un MODIFYING état.
- `aws:waitForAwsResourceProperty`- Attend que l'instance de base de données passe à un AVAILABLE état.
- `aws:assertAwsResourceProperty`- Confirme que l'accessibilité publique est désactivée sur l'instance de base de données.

## **AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster**

### Description

Le `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` runbook active le `CopyTagsToSnapshot` paramètre sur le cluster Amazon Relational Database Service (Amazon RDS) que vous spécifiez. L'activation de ce paramètre copie toutes les balises du cluster de base de données vers des instantanés du cluster de base de données. Par défaut, ils ne sont pas copiés. AWS Config doit être activé dans l' Région AWS endroit où vous exécutez cette automatisation.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

## Plateformes

### Bases de données

#### Paramètres

- `ApplyImmediately`

Type : booléen

Valeur par défaut : `false`

Description : (Facultatif) Si vous spécifiez `true` ce paramètre, les modifications de cette demande et les modifications en attente sont appliquées de manière asynchrone dès que possible, quel que soit le `PreferredMaintenanceWindow` paramètre du cluster de base de données.

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `DbClusterResourceid`

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource du cluster de base de données sur lequel vous souhaitez activer le `CopyTagsToSnapshot` paramètre.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

## Étapes de document

- `aws:executeAwsApi`- Recueille l'identifiant du cluster de base de données à partir de l'identifiant de ressource du cluster de base de données.
- `aws:assertAwsResourceProperty`- Confirme que le cluster de base de données est dans un AVAILABLE état.
- `aws:executeAwsApi`- Active le `CopyTagsToSnapshot` paramètre sur votre cluster de base de données.
- `aws:assertAwsResourceProperty`- Confirme que le `CopyTagsToSnapshot` paramètre est activé sur votre cluster de base de données.

## **AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance**

### Description

Le `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance` runbook active le `CopyTagsToSnapshot` paramètre sur l'instance Amazon Relational Database Service (Amazon RDS) que vous spécifiez. L'activation de ce paramètre copie toutes les balises de l'instance de base de données vers des instantanés de l'instance de base de données. Par défaut, ils ne sont pas copiés. AWS Config doit être activé dans l' Région AWS endroit où vous exécutez cette automatisation.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `ApplyImmediately`

Type : booléen

Valeur par défaut : `false`

Description : (Facultatif) Si vous spécifiez `true` ce paramètre, les modifications de cette demande et les modifications en attente sont appliquées de manière asynchrone dès que possible, quel que soit le `PreferredMaintenanceWindow` paramètre de l'instance de base de données.

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `DbiResourceId`

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de l'instance de base de données sur laquelle vous souhaitez activer le `CopyTagsToSnapshot` paramètre.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

### Étapes de document

- `aws:executeAwsApi`- Recueille l'identifiant de l'instance de base de données à partir de l'identifiant de ressource de l'instance de base de données.

- `aws:assertAwsResourceProperty`- Confirme que l'instance de base de données est dans un `AVAILABLE` état.
- `aws:executeAwsApi`- Active le `CopyTagsToSnapshot` paramètre sur votre instance de base de données.
- `aws:assertAwsResourceProperty`- Confirme que le `CopyTagsToSnapshot` paramètre est activé sur votre instance de base de données.

## **AWSConfigRemediation- EnableEnhancedMonitoringOnRDSInstance**

### Description

Le `AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance` runbook permet une surveillance améliorée sur l'instance de base de données Amazon RDS que vous spécifiez. Pour plus d'informations sur la surveillance améliorée, consultez la section [Surveillance améliorée](#) dans le guide de l'utilisateur Amazon RDS.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- **MonitoringInterval**

Type : entier

Valeurs valides : 1 | 5 | 10 | 15 | 30 | 60

Description : (Obligatoire) Intervalle en secondes pendant lequel les métriques de surveillance améliorée sont collectées à partir de l'instance de base de données.

- **MonitoringRoleArn**

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle IAM qui permet à Amazon RDS d'envoyer des métriques de surveillance améliorées à Amazon CloudWatch Logs.

- **ResourceId**

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de l'instance de base de données sur laquelle vous souhaitez activer la surveillance améliorée.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

### Étapes de document

- `aws:executeAwsApi`- Recueille l'identifiant de l'instance de base de données à partir de l'identifiant de ressource de l'instance de base de données.
- `aws:assertAwsResourceProperty`- Confirme que l'instance de base de données est dans un `AVAILABLE` état.
- `aws:executeAwsApi`- Active la surveillance améliorée sur votre instance de base de données.

- `aws:executeScript`- Confirmez que la surveillance améliorée est activée sur votre instance de base de données.

## AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

### Description

Le `AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS` runbook active le `AutoMinorVersionUpgrade` paramètre sur l'instance de base de données Amazon RDS que vous spécifiez. L'activation de ce paramètre signifie que les mises à niveau des versions mineures sont appliquées automatiquement à l'instance de base de données pendant la fenêtre de maintenance.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `DbiResourceId`

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de l'instance de base de données sur laquelle vous souhaitez `AutoMinorVersionUpgrade` définir le paramètre.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

## Étapes de document

- `aws:executeAwsApi`- Recueille l'identifiant de l'instance de base de données à partir de l'identifiant de ressource de l'instance de base de données.
- `aws:assertAwsResourceProperty`- Confirme que l'instance de base de données est dans un `AVAILABLE` état.
- `aws:executeAwsApi`- Active le `AutoMinorVersionUpgrade` paramètre sur votre instance de base de données.
- `aws:executeScript`- Confirme que le `AutoMinorVersionUpgrade` paramètre est activé sur votre instance de base de données.

## **AWSConfigRemediation-EnableMultiAZOnRDSInstance**

### Description

Le `AWSConfigRemediation-EnableMultiAZOnRDSInstance` runbook remplace votre instance de base de données (DB) Amazon Relational Database Service (Amazon RDS) par un déploiement multi-AZ. La modification de ce paramètre n'entraîne pas d'interruption. La modification est appliquée lors de la fenêtre de maintenance suivante, sauf si vous définissez le `ApplyImmediately` paramètre sur `true`.

[Exécuter cette automatisation \(console\)](#)

### Type de document

#### Automatisation



## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- `ApplyImmediately`

Type : booléen

Valeur par défaut : `false`

Description : (Facultatif) Si vous spécifiez `true` ce paramètre, les modifications de cette demande et les modifications en attente sont appliquées de manière asynchrone dès que possible, quel que soit le `PreferredMaintenanceWindow` paramètre de l'instance de base de données.

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `DbiResourceId`

Type : chaîne

Description : (Obligatoire) L'identifiant Région AWS unique et immuable de l'instance de base de données pour activer le `MultiAZ` paramètre.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`
- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`

## Étapes de document

- `aws:executeAwsApi`- Récupère le nom de l'instance de base de données à l'aide de la valeur fournie dans le `DBInstanceId` paramètre.
- `aws:executeAwsApi`- Vérifie que `DBInstanceStatus` c'est `available` le cas.
- `aws:branch`- Vérifie si le `MultiAZ` est déjà défini `true` sur l'instance de base de données que vous spécifiez dans le `DbiResourceId` paramètre.
- `aws:executeAwsApi`- Modifie le `MultiAZ` paramètre `true` sur l'instance de base de données que vous spécifiez dans le `DbiResourceId` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que le paramètre `MultiAZ` est défini `true` sur l'instance de base de données que vous spécifiez dans le `DbiResourceId` paramètre.

## **AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance**

### Description

Le `AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance` runbook active Performance Insights sur l'instance de base de données Amazon RDS que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `DbiResourceId`

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de l'instance de base de données sur laquelle vous souhaitez activer Performance Insights.

- `PerformanceInsightsKMSKeyId`

Type : chaîne

Par défaut : `alias/aws/rd`

Description : (Facultatif) Le nom de ressource Amazon (ARN), l'identifiant de clé ou l'alias de clé AWS Key Management Service (AWS KMS) gérée par le client que vous souhaitez que Performance Insights utilise pour chiffrer toutes les données potentiellement sensibles. Si vous entrez l'alias de clé pour ce paramètre, préfixez la valeur par **alias/**. Si vous ne spécifiez aucune valeur pour ce paramètre, le Clé gérée par AWS est utilisé.

- `PerformanceInsightsRetentionPeriod`

Type : entier

Valeurs valides : 7 731

Valeur par défaut : 7

Description : (Facultatif) Le nombre de jours pendant lesquels vous souhaitez conserver les données Performance Insights.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

### Étapes de document

- `aws:executeAwsApi`- Recueille l'identifiant de l'instance de base de données à partir de l'identifiant de ressource de l'instance de base de données.
- `aws:assertAwsResourceProperty`- Confirme que le statut de l'instance de base de données est disponible.
- `aws:executeAwsApi`- Rassemble l'ARN de la clé gérée par le AWS KMS client spécifiée dans le `PerformanceInsightsKMSKeyId` paramètre.
- `aws:branch`- Vérifie si une valeur est déjà attribuée à la `PerformanceInsightsKMSKeyId` propriété de l'instance de base de données.
- `aws:executeAwsApi`- Active Performance Insights sur l'instance de base de données que vous spécifiez dans le `DbiResourceId` paramètre.
- `aws:assertAwsResourceProperty`- Confirme que la valeur spécifiée pour le `PerformanceInsightsKMSKeyId` paramètre a été utilisée pour activer le chiffrement pour Performance Insights sur l'instance de base de données.
- `aws:assertAwsResourceProperty`- Confirme que Performance Insights est activé sur l'instance de base de données.

## **AWSConfigRemediation-EnableRDSClusterDeletionProtection**

### Description

Le `AWSConfigRemediation-EnableRDSClusterDeletionProtection` runbook active la protection contre la suppression sur le cluster Amazon Relational Database Service (Amazon RDS) que vous spécifiez. AWS Config doit être activé dans l' Région AWS endroit où vous exécutez cette automatisation.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- ClusterId

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource du cluster de base de données sur lequel vous souhaitez activer la protection contre les suppressions.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds:DescribeDBClusters
- rds:ModifyDBCluster

## Étapes de document

- `aws:executeAwsApi`- Recueille le nom du cluster de base de données à partir de l'identifiant de ressource du cluster de base de données.
- `aws:assertAwsResourceProperty`- Vérifie que l'état du cluster de base de données est `available`.
- `aws:executeAwsApi`- Active la protection contre la suppression sur le cluster de base de données que vous spécifiez dans le `ClusterId` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que la protection contre les suppressions a été activée sur le cluster de base de données.

## AWSConfigRemediation-EnableRDSInstanceBackup

### Description

Le `AWSConfigRemediation-EnableRDSInstanceBackup` runbook permet de sauvegarder l'instance de base de données Amazon Relational Database Service (Amazon RDS) que vous spécifiez. Ce runbook ne prend pas en charge l'activation des sauvegardes pour les instances de base de données Amazon Aurora.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Bases de données

### Paramètres

- `ApplyImmediately`

Type : booléen

Valeur par défaut : `false`

Description : (Facultatif) Si vous spécifiez `true` ce paramètre, les modifications de cette demande et les modifications en attente sont appliquées de manière asynchrone dès que possible, quel que soit le `PreferredMaintenanceWindow` paramètre de l'instance de base de données.

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `BackupRetentionPeriod`

Type : entier

Valeurs valides : 1 à 35

Description : (Obligatoire) Nombre de jours pendant lesquels les sauvegardes sont conservées.

- `DbiResourceId`

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de l'instance de base de données pour laquelle vous souhaitez activer les sauvegardes.

- `PreferredBackupWindow`

Type : chaîne

Description : (Facultatif) La plage horaire quotidienne (en UTC) pendant laquelle les sauvegardes sont créées.

Contraintes :

- Doit être au format `hh24:mi-hh24:mi`
- Doit être en temps universel coordonné (UTC)
- Ne doit pas être en conflit avec la fenêtre de maintenance préférée
- Doit être de 30 minutes minimum.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

### Étapes de document

- `aws:executeScript`- Recueille l'identifiant de l'instance de base de données à partir de l'identifiant de ressource de l'instance de base de données. Active les sauvegardes pour votre instance de base de données. Confirme que les sauvegardes sont activées sur l'instance de base de données.

## **AWSConfigRemediation-EnableRDSInstanceDeletionProtection**

### Description

Le `AWSConfigRemediation-EnableRDSInstanceDeletionProtection` runbook active la protection contre la suppression sur l'instance de base de données Amazon RDS que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `ApplyImmediately`



Type : booléen

Valeur par défaut : false

Description : (Facultatif) Si vous spécifiez `true` ce paramètre, les modifications de cette demande et les modifications en attente sont appliquées de manière asynchrone dès que possible, quel que soit le `PreferredMaintenanceWindow` paramètre de l'instance de base de données.

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `DbInstanceResourceid`

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de l'instance de base de données sur laquelle vous souhaitez activer la protection contre les suppressions.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

### Étapes de document

- `aws:executeAwsApi`- Recueille l'identifiant de l'instance de base de données à partir de l'identifiant de ressource de l'instance de base de données.
- `aws:executeAwsApi`- Active la protection contre les suppressions sur votre instance de base de données.

- `aws:assertAwsResourceProperty`- Confirme que la protection contre la suppression est activée sur l'instance de base de données.

## AWSConfigRemediation-ModifyRDSInstancePortNumber

### Description

Le `AWSConfigRemediation-ModifyRDSInstancePortNumber` runbook modifie le numéro de port sur lequel l'instance Amazon Relational Database Service (Amazon RDS) accepte les connexions. L'exécution de cette automatisation redémarrera la base de données.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `PortNumber`

Type : chaîne

Description : (Facultatif) Le numéro de port sur lequel vous souhaitez que l'instance de base de données accepte les connexions.

- **RDSDB InstanceResourceId**

Type : chaîne

Description : (Obligatoire) L'identifiant de ressource de l'instance de base de données dont vous souhaitez modifier le numéro de port entrant.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

#### Étapes de document

- `aws:executeAwsApi`- Recueille l'identifiant de l'instance de base de données à partir de l'identifiant de ressource de l'instance de base de données.
- `aws:assertAwsResourceProperty`- Confirme que l'instance de base de données est dans un `AVAILABLE` état.
- `aws:executeAwsApi`- Modifie le numéro de port entrant sur lequel votre instance de base de données accepte les connexions.
- `aws:waitForAwsResourceProperty`- Attend que l'instance de base de données soit dans un `MODIFYING` état.
- `aws:waitForAwsResourceProperty`- Attend que l'instance de base de données soit dans un `AVAILABLE` état.

## **AWSSupport-ModifyRDSSnapshotPermission**

### Description

Le `AWSSupport-ModifyRDSSnapshotPermission` runbook vous permet de modifier les autorisations pour plusieurs instantanés Amazon Relational Database Service (Amazon RDS). À

l'aide de ce runbook, vous pouvez créer des instantanés `Public` ou `Private` les partager avec d'autres. Comptes AWS Les instantanés chiffrés avec une clé KMS par défaut ne peuvent pas être partagés avec d'autres comptes utilisant ce runbook.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `AccountIds`

Type : `StringList`

Par défaut: Aucun

Description : (Facultatif) Les identifiants des comptes avec lesquels vous souhaitez partager des instantanés. Ce paramètre est obligatoire si vous entrez `No` la valeur du `Private` paramètre.

- `AccountPermissionOperation`

Type : chaîne

Valeurs valides : `ajouter` | `supprimer`

Par défaut: Aucun

Description : (Facultatif) Type d'opération à effectuer.

- Privé

Type : chaîne

Valeurs valides : Oui | Non

Description : (Obligatoire) Entrez No la valeur si vous souhaitez partager des instantanés avec des comptes spécifiques.

- SnapshotIdentifiers

Type : StringList

Description : (Obligatoire) Les noms des instantanés Amazon RDS dont vous souhaitez modifier l'autorisation.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`
- `rds:ModifyDBSnapshotAttribute`

### Étapes de document

1. `aws:executeScript`- Vérifie les identifiants des instantanés fournis dans le `SnapshotIdentifiers` paramètre. Après avoir vérifié les identifiants, le script recherche les instantanés chiffrés et affiche une liste s'ils sont trouvés.
2. `aws:branch`- Branche l'automatisation en fonction de la valeur que vous entrez pour le `Private` paramètre.
3. `aws:executeScript`- Modifie les autorisations des instantanés spécifiés pour les partager avec les comptes spécifiés.

#### 4. `aws:executeScript`- Modifie les autorisations des instantanés pour les faire passer de `Public` à `Private`

Sorties

`ValidateSnapshots.EncryptedSnapshots`

`SharewithOtherAccounts.Résultat`

`MakePrivate.Résultat`

`MakePrivate.Commandes`

## **AWSPremiumSupport-PostgreSQLWorkloadReview**

Description

Le `AWSPremiumSupport-PostgreSQLWorkloadReview` runbook capture plusieurs instantanés des statistiques d'utilisation de votre base de données PostgreSQL Amazon Relational Database Service (Amazon RDS). Les statistiques capturées sont nécessaires pour qu'un expert [des services AWS Support proactifs](#) puisse effectuer un examen opérationnel. Les statistiques sont collectées à l'aide d'un ensemble de scripts SQL et shell personnalisés. Ces scripts sont téléchargés sur une instance Amazon Elastic Compute Cloud (Amazon EC2) temporaire dans Compte AWS votre instance créée par ce runbook. Le runbook vous demande de fournir des informations d'identification à l'aide d'un AWS Secrets Manager secret contenant une paire clé-valeur du nom d'utilisateur et du mot de passe. Le nom d'utilisateur doit être autorisé à interroger les vues et fonctions statistiques standard de PostgreSQL.

Ce runbook crée automatiquement les AWS ressources suivantes dans votre fichier à Compte AWS l'aide d'une AWS CloudFormation pile. Vous pouvez surveiller la création de la pile à l'aide de la AWS CloudFormation console.

- Un cloud privé virtuel (VPC) et une instance Amazon EC2 lancés dans un sous-réseau privé du VPC avec une connectivité optionnelle à Internet via une passerelle NAT.
- Rôle AWS Identity and Access Management (IAM) attaché à l'instance temporaire Amazon EC2 avec les autorisations nécessaires pour récupérer la valeur secrète de Secrets Manager. Le rôle fournit également des autorisations pour télécharger des fichiers dans un bucket Amazon Simple Storage Service (Amazon S3) de votre choix, et éventuellement dans un boîtier. AWS Support

- Une connexion d'appairage VPC pour permettre la connectivité entre votre instance de base de données et l'instance temporaire Amazon EC2.
- Points de terminaison Systems Manager, Secrets Manager et Amazon S3 VPC attachés au VPC temporaire.
- Une fenêtre de maintenance avec des tâches enregistrées qui démarrent et arrêtent périodiquement l'instance temporaire Amazon EC2, exécutent des scripts de collecte de données et chargent des fichiers dans un compartiment Amazon S3. Un rôle IAM est également créé pour la fenêtre de maintenance qui fournit les autorisations nécessaires pour effectuer les tâches enregistrées.

Lorsque le runbook est terminé, la AWS CloudFormation pile utilisée pour créer les AWS ressources nécessaires est supprimée et le rapport est chargé dans le compartiment Amazon S3 de votre choix, et éventuellement dans un AWS Support dossier.

#### Note

Par défaut, le volume Amazon EBS racine de l'instance Amazon EC2 temporaire est préservé. Vous pouvez annuler cette option en définissant le `EbsVolumeDeleteOnTermination` paramètre sur `true`

## Prérequis

- Abonnement au support d'entreprise Ce manuel et les diagnostics et révisions de la charge de travail de Proactive Services nécessitent un abonnement au support d'entreprise. Avant d'utiliser ce manuel, contactez votre responsable de compte technique (TAM) ou votre spécialiste TAM (STAM) pour obtenir des instructions. Pour plus d'informations, consultez [AWS Support Proactive Services](#).
- Compte et Région AWS quotas Vérifiez que vous n'avez pas atteint le nombre maximum d'instances ou de VPC Amazon EC2 que vous pouvez créer dans votre compte et dans la région dans laquelle vous utilisez ce runbook. Si vous devez demander une augmentation de limite, consultez le [formulaire d'augmentation de limite de service](#).
- Configuration de base de données
  1. L'`pg_stat_statements` extension doit être configurée pour la base de données que vous spécifiez dans le `DatabaseName` paramètre. Si vous n'avez pas configuré `pg_stat_statements` dans `shared_preload_libraries`, vous devez modifier la valeur dans le groupe de paramètres de base de données et appliquer les modifications.

Les modifications apportées au paramètre `shared_preload_libraries` nécessitent le redémarrage de votre instance de base de données. Pour plus d'informations, veuillez consulter [Utilisation des groupes de paramètres](#). L'ajout `pg_stat_statements` à `shared_preload_libraries` ajoutera une certaine surcharge en termes de performances. Cependant, cela est utile pour suivre les performances des relevés individuels. Pour plus d'informations sur l'`pg_stat_statements` extension, consultez la documentation de [PostgreSQL](#). Si vous ne configurez pas l'`pg_stat_statements` extension ou si l'extension n'est pas présente dans la base de données utilisée pour la collecte des statistiques, l'analyse au niveau des instructions ne sera pas présentée dans la revue opérationnelle.

2. Assurez-vous que les `track_activities` paramètres `track_counts` et ne sont pas désactivés. Si ces paramètres sont désactivés dans le groupe de paramètres de base de données, aucune statistique significative ne sera disponible. La modification de ces paramètres vous obligera à redémarrer votre instance de base de données. Pour plus d'informations, consultez [Utilisation des paramètres sur votre instance de base de données Amazon RDS for PostgreSQL](#).
3. Si le `track_io_timing` paramètre est désactivé, les statistiques du niveau d'E/S ne seront pas incluses dans la revue opérationnelle. La modification vous `track_io_timing` obligera à redémarrer votre instance de base de données et entraînera une surcharge de performance supplémentaire en fonction de la charge de travail de l'instance de base de données. Malgré la surcharge de performance associée aux charges de travail critiques, ce paramètre fournit des informations utiles relatives au temps d'E/S par requête.

**Facturation et frais** Les coûts associés à l'instance Amazon EC2 temporaire, au volume Amazon EBS associé, à la passerelle NAT et aux données transférées pendant l'exécution de cette automatisation Compte AWS vous seront facturés. Par défaut, ce runbook crée une instance `t3.micro` Amazon Linux 2 pour collecter les statistiques. Le runbook démarre et arrête l'instance entre les étapes afin de réduire les coûts.

**Sécurité et gouvernance des données** Ce runbook collecte des statistiques en interrogeant les vues et les fonctions statistiques de [PostgreSQL](#). Assurez-vous que les informations d'identification fournies dans le `SecretId` paramètre n'autorisent que les autorisations en lecture seule pour les vues et les fonctions des statistiques. Dans le cadre de l'automatisation, les scripts de collecte sont chargés dans votre compartiment Amazon S3 et peuvent y être localisés `s3://DOC-EXAMPLE-BUCKET/automation execution id/queries/`.

Ces scripts collectent des données qui sont utilisées par un AWS spécialiste pour examiner les indicateurs de performance clés au niveau de l'objet. Le script collecte des informations telles que



le nom de la table, le nom du schéma et le nom de l'index. Si l'une de ces informations contient des informations sensibles telles que des indicateurs de revenus, un nom d'utilisateur, une adresse e-mail ou toute autre information personnellement identifiable, nous vous recommandons de mettre fin à cet examen de la charge de travail. Contactez votre AWS TAM pour discuter d'une autre approche pour l'examen de la charge de travail.

Assurez-vous d'avoir l'approbation et l'autorisation nécessaires pour partager les statistiques et les métadonnées collectées par cette automatisation avec AWS.

**Considérations relatives à la sécurité** Si vous définissez le `UpdateRdsSecurityGroup` paramètre suryes, le runbook met à jour le groupe de sécurité associé à votre instance de base de données afin d'autoriser le trafic entrant depuis l'adresse IP privée de l'instance temporaire Amazon EC2.

Si vous définissez le `UpdateRdsRouteTable` paramètre suryes, le runbook met à jour la table de routage associée au sous-réseau dans lequel votre instance de base de données s'exécute afin d'autoriser le trafic vers l'instance temporaire Amazon EC2 via la connexion d'appairage VPC.

**Création d'un utilisateur** Pour permettre au script de collecte de se connecter à votre base de données Amazon RDS, vous devez configurer un utilisateur autorisé à lire les vues statistiques. Vous devez ensuite enregistrer les informations d'identification dans Secrets Manager. Nous vous recommandons de créer un nouvel utilisateur dédié pour cette automatisation. La création d'un utilisateur distinct vous permet d'auditer et de suivre les activités effectuées par cette automatisation.

1. Créez un nouvel utilisateur.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. Assurez-vous que cet utilisateur ne peut établir que des connexions en lecture seule.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. Définissez des limites de niveau utilisateur.

```
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. Accordez `pg_monitor` des autorisations au nouvel utilisateur afin qu'il puisse accéder aux statistiques de la base de données. (Le `pg_monitor` rôle est membre de `pg_read_all_settings`, `pg_read_all_stats`, `etpg_stat_scan_table`.)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

Autorisations ajoutées au profil d'instance temporaire Amazon EC2 par cette solution Systems Manager Automation Les autorisations suivantes sont ajoutées au rôle IAM associé à l'instance Amazon EC2 temporaire. La politique AmazonSSMManagedInstanceCore gérée est également associée au rôle IAM pour permettre à l'instance Amazon EC2 d'être gérée par Systems Manager.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/automation execution id/*",
      "Effect": "Allow"
    }
  ]
}
```

```

    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:region:account id:secret:secret id",
    "Effect": "Allow"
  },
  {
    "Action": [
      "support:AddAttachmentsToSet",
      "support:AddCommunicationToCase",
      "support:DescribeCases"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
]
}

```

Autorisations ajoutées à la fenêtre de maintenance temporaire par cette automatisation de Systems Manager Les autorisations suivantes sont automatiquement ajoutées au rôle IAM associé aux tâches de maintenance Windows. Les tâches Windows de maintenance démarrent, s'arrêtent et envoient des commandes à l'instance temporaire Amazon EC2.

```

{
  "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"
}
]
```

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- DB Instanceldentifier

Type : chaîne

Description : (Obligatoire) L'ID de votre instance de base de données.

- DatabaseName

Type : chaîne

Description : (Obligatoire) Le nom de la base de données hébergée sur votre instance de base de données.

- SecretId

Type : chaîne

Description : (Obligatoire) L'ARN de votre secret Secrets Manager contenant la paire clé/valeur du nom d'utilisateur et du mot de passe. La AWS CloudFormation pile crée une politique IAM avec des autorisations pour l'GetSecretValueopération sur cet ARN. Les informations d'identification sont utilisées pour permettre à l'instance temporaire de collecter les statistiques de la base de données. Contactez votre TAM ou votre STAM pour discuter des autorisations minimales requises.

- Reconnaître

Type : chaîne

Description : (Obligatoire) Entrez **yes** si vous reconnaissez que ce runbook créera des ressources temporaires dans votre compte pour collecter des statistiques à partir de votre instance de base de données. Nous vous recommandons de contacter votre TAM ou STAM avant d'exécuter cette automatisation.

- SupportCase

Type : chaîne

Description : (Facultatif) Le numéro de AWS Support dossier fourni par votre TAM ou STAM. S'il est fourni, le runbook met à jour le dossier et y joint les données collectées. Cette option

nécessite que l'instance Amazon EC2 temporaire dispose d'une connexion Internet pour accéder au point de terminaison de l' AWS Support API. Vous devez définir le `AllowVpcInternetAccess` paramètre sur `true`. L'objet du dossier doit contenir la phrase `AWSPremiumSupport-PostgreSQLWorkloadReview`.

- `S3 BucketName`

Type : chaîne

Description : (Obligatoire) Le nom du compartiment Amazon S3 de votre compte dans lequel vous souhaitez télécharger les données collectées par l'automatisation. Vérifiez que la politique du compartiment n'accorde aucune autorisation de lecture ou d'écriture inutile aux principaux qui n'ont pas besoin d'accéder au contenu du compartiment. Nous vous recommandons de créer un nouveau compartiment Amazon S3 temporaire aux fins de cette automatisation. Le runbook fournit des autorisations pour le fonctionnement de `s3:PutObjectAPI` au rôle IAM attaché à l'instance Amazon EC2 temporaire. Les fichiers téléchargés seront situés dans `s3://bucket name/automation execution id/`.

- `InstanceType`

Type : chaîne

Description : (Facultatif) Type d'instance Amazon EC2 temporaire qui exécutera les scripts SQL et shell personnalisés.

Valeurs valides : `t2.micro` | `t2.small` | `t2.medium` | `t2.large` | `t3.micro` | `t3.small` | `t3.medium` | `t3.large`

Par défaut : `t3.micro`

- `VpcCidr`

Type : chaîne

Description : (Facultatif) La plage d'adresses IP en notation CIDR pour le nouveau VPC (par exemple `172.31.0.0/16`). Assurez-vous de sélectionner un CIDR qui ne chevauche ni ne correspond à aucun VPC existant connecté à votre instance de base de données. Le plus petit VPC que vous pouvez créer utilise un masque de sous-réseau `/28`, tandis que le plus grand VPC utilise un masque de sous-réseau `/16`.

Par défaut : `172.31.0.0/16`

- `StackResourcesNamePrefix`

Type : chaîne

Description : (Facultatif) Le préfixe et la balise du nom des ressources de la AWS CloudFormation pile. Le runbook crée les ressources de la AWS CloudFormation pile en utilisant ce préfixe dans le nom et la balise appliqués aux ressources. La structure de la paire clé-valeur du tag est.

*StackResourcesNamePrefix*: {{automation:EXECUTION\_ID}}

Par défaut : AWSPostgreSQLWorkloadReview

- Planificateur

Type : chaîne

Description : (Facultatif) Le calendrier de la fenêtre de maintenance. Spécifie la fréquence à laquelle la fenêtre de maintenance exécute les tâches. La valeur par défaut est `every1 hour`.

Valeurs valides : 15 minutes | 30 minutes | 1 heure | 2 heures | 4 heures | 6 heures | 12 heures | 1 jour | 2 jours | 4 jours

Par défaut : 1 heure

- Durée

Type : entier

Description : (Facultatif) Durée maximale, en minutes, pendant laquelle vous souhaitez autoriser l'exécution de l'automatisation. La durée maximale prise en charge est de 8 640 minutes (6 jours). La valeur par défaut est de 4 320 minutes (3 jours).

Valeurs valides : 30-8640

Par défaut : 4320

- UpdateRdsRouteTable

Type : chaîne

Description : (Facultatif) Si ce paramètre est défini sur `true`, le runbook met à jour la table de routage associée au sous-réseau dans lequel s'exécute votre instance de base de données. Une route IPv4 est ajoutée pour acheminer le trafic vers l'adresse IPV4 privée de l'instance Amazon EC2 temporaire via la connexion d'appairage VPC nouvellement créée.

Valeurs valides : `true` | `false`

Valeur par défaut : `false`

- `AllowVpcInternetAccess`

Type : chaîne

Description : (Facultatif) S'il est défini sur `true`, le runbook crée une passerelle NAT pour fournir une connectivité Internet à l'instance temporaire Amazon EC2 afin de communiquer avec le point de terminaison de AWS Support l'API. Vous pouvez laisser ce paramètre comme `false` si vous voulez uniquement que le runbook télécharge la sortie dans votre compartiment Amazon S3.

Valeurs valides : `true` | `false`

Valeur par défaut : `false`

- `UpdateRdsSecurityGroup`

Type : chaîne

Description : (Facultatif) Si ce paramètre est défini sur `true`, le runbook met à jour le groupe de sécurité associé à votre instance de base de données afin d'autoriser le trafic provenant de l'adresse IP privée de l'instance temporaire.

Valeurs valides : `faux` | `vrai`

Valeur par défaut : `false`

- `EbsVolumeDeleteOnTermination`

Type : chaîne

Description : (Facultatif) Si ce paramètre est défini sur `true`, le volume racine de l'instance temporaire Amazon EC2 est supprimé une fois le runbook terminé et la pile supprimée. AWS CloudFormation

Valeurs valides : `faux` | `vrai`

Valeur par défaut : `false`

Autorisations IAM requises



Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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:RemoveTagsForResource`
- `ssm:SendCommand`
- `support:AddAttachmentsToSet`
- `support:AddCommunicationToCase`
- `support:DescribeCases`

## Étapes de document

1. `aws:assertAwsResourceProperty`- Confirme que l'instance de base de données est en available bon état.
2. `aws:executeAwsApi`- Rassemble des informations sur l'instance de base de données.
3. `aws:executeScript`- Vérifie si le compartiment Amazon S3 spécifié dans le `S3BucketName` permet des autorisations d'accès anonymes ou publiques en lecture ou en écriture.
4. `aws:executeScript`- Extrait le contenu du AWS CloudFormation modèle à partir de la pièce jointe du runbook Automation qui est utilisée pour créer les AWS ressources temporaires dans votre Compte AWS.
5. `aws:createStack`- Crée les ressources de la AWS CloudFormation pile.
6. `aws:waitForAwsResourceProperty`- Attend que l'instance Amazon EC2 créée par le modèle soit en cours d' AWS CloudFormation exécution.

7. `aws:executeAwsApi`- Obtient les identifiants de l'instance Amazon EC2 temporaire et de la connexion d'appairage VPC créée par. AWS CloudFormation
8. `aws:executeAwsApi`- Obtient l'adresse IP de l'instance Amazon EC2 temporaire pour configurer la connectivité avec votre instance de base de données.
9. `aws:executeAwsApi`- Marque le volume Amazon EBS attaché à l'instance Amazon EC2 temporaire.
- 10 `aws:waitForAwsResourceProperty`- Attend que l'instance temporaire Amazon EC2 passe les vérifications de statut.
- 11 `aws:waitForAwsResourceProperty`- Attend que l'instance temporaire Amazon EC2 soit gérée par Systems Manager. Si cette étape expire ou échoue, le runbook redémarre l'instance.
  - a. `aws:executeAwsApi`- Redémarre l'instance Amazon EC2 temporaire si l'étape précédente a échoué ou a expiré.
  - b. `aws:waitForAwsResourceProperty`- Attend que l'instance temporaire Amazon EC2 soit gérée par Systems Manager après le redémarrage.
- 12 `aws:runCommand`- Installe les exigences de l'application de collecte de métadonnées sur l'instance temporaire Amazon EC2.
- 13 `aws:runCommand`- Configure l'accès à votre instance de base de données en créant un fichier de configuration sur l'instance temporaire Amazon EC2.
- 14 `aws:executeAwsApi`- Crée une fenêtre de maintenance pour exécuter régulièrement l'application de collecte de métadonnées à l'aide de la commande Exécuter. La fenêtre de maintenance démarre et arrête l'instance entre les commandes.
- 15 `aws:waitForAwsResourceProperty`- Attend que la fenêtre de maintenance créée par le AWS CloudFormation modèle soit prête.
- 16 `aws:executeAwsApi`- Obtient les identifiants de la fenêtre de maintenance et du calendrier des modifications créés par AWS CloudFormation.
- 17 `aws:sleep`- Attend la date de fin de la fenêtre de maintenance.
- 18 `aws:executeAwsApi`- Désactive la fenêtre de maintenance.
- 19 `aws:executeScript`- Obtient les résultats des tâches exécutées pendant la fenêtre de maintenance.
- 20 `aws:waitForAwsResourceProperty`- Attend que la fenêtre de maintenance termine la dernière tâche avant de continuer.
- 21 `aws:branch`- Branche le flux de travail selon que vous avez fourni ou non une valeur pour le `SupportCase` paramètre.

- a. `aws:changeInstanceState`- Démarre l'instance Amazon EC2 temporaire et attend que les vérifications de statut soient passées avant de télécharger le rapport.
  - b. `aws:waitForAwsResourceProperty`- Attend que l'instance temporaire Amazon EC2 soit gérée par Systems Manager. Si cette étape expire ou échoue, le runbook redémarre l'instance.
    - i. `aws:executeAwsApi`- Redémarre l'instance Amazon EC2 temporaire si l'étape précédente a échoué ou a expiré.
    - ii. `aws:waitForAwsResourceProperty`- Attend que l'instance temporaire Amazon EC2 soit gérée par Systems Manager après le redémarrage.
  - c. `aws:runCommand`- Joint le rapport de métadonnées au AWS Support dossier si vous avez fourni une valeur pour le `SupportCase` paramètre. Le script compresse et divise le rapport en fichiers de 5 Mo. Le nombre maximum de fichiers que le script joint à un AWS Support dossier est de 12.
- 22.`aws:changeInstanceState`- Arrête l'instance Amazon EC2 temporaire au cas où la AWS CloudFormation pile ne serait pas supprimée.
- 23.`aws:executeAwsApi`- Décrit les événements de la AWS CloudFormation pile si les runbooks ne parviennent pas à créer ou à mettre à jour la AWS CloudFormation pile.
- 24.`aws:waitForAwsResourceProperty`- Attend que la AWS CloudFormation pile soit en état de terminal avant de la supprimer.
- 25.`aws:executeAwsApi`- Supprime la AWS CloudFormation pile à l'exception de la fenêtre de maintenance. Le volume Amazon EBS racine associé à l'instance Amazon EC2 temporaire est préservé si `EbsVolumeDeleteOnTermination` la valeur du paramètre a été définie sur `false`

## AWS-RebootRdsInstance

### Description

Le `AWS-RebootRdsInstance` runbook redémarre une instance de base de données Amazon Relational Database Service (Amazon RDS) si ce n'est déjà fait.

[Exécuter cette automatisation \(console\)](#)

### Type de document

### Automatisation

### Propriétaire

## Amazon

### Plateformes

### Bases de données

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- InstanceId

Type : chaîne

Description : (Obligatoire) L'ID de l'instance de base de données Amazon RDS que vous souhaitez redémarrer.

### Étapes de document

RebootInstance - Redémarre l'instance de base de données si ce n'est pas déjà fait.

WaitForAvailableState - Attend que l'instance de base de données termine le processus de redémarrage.

### Sorties

Cette automatisation n'a aucune sortie.

## **AWSsupport - ShareRDSSnapshot**

### Description

Le `AWSsupport - ShareRDSSnapshot` runbook fournit une solution automatisée pour la procédure décrite dans l'article du centre de connaissances [Comment partager un instantané de base de données Amazon RDS chiffré avec un autre compte ?](#) Si votre instantané Amazon Relational Database Service (Amazon RDS) a été chiffré à l'aide de la Clé gérée par AWS valeur par défaut,

vous ne pouvez pas partager l'instantané. Dans ce cas, vous devez copier l'instantané à l'aide d'une clé gérée par le client, puis partager l'instantané avec le compte cible. Cette automatisation exécute ces étapes en utilisant la valeur que vous spécifiez dans le SnapshotName paramètre ou le dernier instantané trouvé pour l'instance ou le cluster de base de données Amazon RDS sélectionné.

#### Note

Si vous ne spécifiez aucune valeur pour le KMSKey paramètre, l'automatisation crée une nouvelle clé gérée par le AWS KMS client dans votre compte qui est utilisée pour chiffrer l'instantané.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- AccountIds

Type : StringList

Description : (Obligatoire) Liste d'identifiants de compte séparés par des virgules avec lesquels partager l'instantané.

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.



- Base de données

Type : chaîne

Description : (Obligatoire) Le nom de l'instance ou du cluster de base de données Amazon RDS dont vous souhaitez partager l'instantané. Ce paramètre est facultatif si vous spécifiez une valeur pour le SnapshotName paramètre.

- Clé KMS

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon complet (ARN) de la clé gérée par le AWS KMS client utilisée pour chiffrer l'instantané.

- SnapshotName

Type : chaîne

Description : (Facultatif) L'ID du cluster de base de données ou du snapshot d'instance que vous souhaitez utiliser.

#### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:DescribeDBSnapshots`
- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

Les AutomationAssumeRole actions suivantes sont nécessaires pour démarrer correctement le runbook d'un cluster de base de données.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBClusters`
- `rds:DescribeDBClusterSnapshots`

- `rds:CopyDBClusterSnapshot`
- `rds:ModifyDBClusterSnapshotAttribute`

Le rôle IAM utilisé pour exécuter l'automatisation doit être ajouté en tant qu'utilisateur clé pour utiliser la clé KMS spécifiée dans le `ARNKmsKey` paramètre. Pour plus d'informations sur l'ajout d'utilisateurs clés à une clé KMS, consultez la section [Modification d'une politique clé](#) dans le guide du AWS Key Management Service développeur.

Les `AutomationAssumeRole` actions supplémentaires suivantes sont nécessaires pour démarrer correctement le runbook si vous ne spécifiez aucune valeur pour le `KMSKey` paramètre.

- `kms:CreateKey`
- `kms:ScheduleKeyDeletion`

### Étapes de document

1. `aws:executeScript`- Vérifie si une valeur a été fournie pour le `KMSKey` paramètre et crée une clé gérée par le AWS KMS client si aucune valeur n'est trouvée.
2. `aws:branch`- Vérifie si une valeur a été fournie pour le `SnapshotName` paramètre et branche en conséquence.
3. `aws:executeAwsApi`- Vérifie si le snapshot fourni provient d'une instance de base de données.
4. `aws:executeScript`- Formate le `SnapshotName` paramètre en remplaçant les deux points par un tiret.
5. `aws:executeAwsApi`- Copie le cliché en utilisant le paramètre spécifié `KMSKey`.
6. `aws:waitForAwsResourceProperty`- Attend la fin de l'opération de copie instantanée.
7. `aws:executeAwsApi`- Partage le nouvel instantané avec le cliché `AccountIds` spécifié.
8. `aws:executeAwsApi`- Vérifie si le snapshot fourni provient d'un cluster de base de données.
9. `aws:executeScript`- Formate le `SnapshotName` paramètre en remplaçant les deux points par un tiret.
10. `aws:executeAwsApi`- Copie le cliché en utilisant le paramètre spécifié `KMSKey`.
11. `aws:waitForAwsResourceProperty`- Attend la fin de l'opération de copie instantanée.
12. `aws:executeAwsApi`- Partage le nouvel instantané avec le cliché `AccountIds` spécifié.
13. `aws:executeAwsApi`- Vérifie si la valeur fournie pour le `Database` paramètre est une instance de base de données.

14. `aws:executeAwsApi`- Vérifie si la valeur fournie pour le Database paramètre est un cluster de base de données.
15. `aws:executeAwsApi`- Récupère une liste d'instantanés pour le fichier spécifié. Database
16. `aws:executeScript`- Détermine le dernier instantané disponible à partir de la liste compilée à l'étape précédente.
17. `aws:executeAwsApi`- Copie le snapshot de l'instance de base de données en utilisant le paramètre spécifié `KMSKey`.
18. `aws:waitForAwsResourceProperty`- Attend la fin de l'opération de copie instantanée.
19. `aws:executeAwsApi`- Partage le nouvel instantané avec le cliché `AccountIds` spécifié.
20. `aws:executeAwsApi`- Récupère une liste d'instantanés pour le fichier spécifié. Database
21. `aws:executeScript`- Détermine le dernier instantané disponible à partir de la liste compilée à l'étape précédente.
22. `aws:executeAwsApi`- Copie le snapshot de l'instance de base de données en utilisant le paramètre spécifié `KMSKey`.
23. `aws:waitForAwsResourceProperty`- Attend la fin de l'opération de copie instantanée.
24. `aws:executeAwsApi`- Partage le nouvel instantané avec le cliché `AccountIds` spécifié.
25. `aws:executeScript`- Supprime la clé gérée par le AWS KMS client créée par l'automatisation si vous n'avez pas spécifié de valeur pour le `KMSKey` paramètre et que l'automatisation échoue.

## AWS-StartRdsInstance

### Description

Démarrez une instance Amazon Relational Database Service (Amazon RDS).

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- InstanceId

Type : chaîne

Description : ID (obligatoire) de l'instance Amazon RDS à démarrer.

## AWS-StartStopAuroraCluster

### Description

Ce runbook démarre ou arrête un cluster Amazon Aurora.

#### Note

Pour démarrer un cluster, celui-ci doit avoir un `stopped` statut. Pour arrêter un cluster, il doit avoir un `available` statut. Ce runbook ne peut pas être utilisé pour démarrer ou arrêter un cluster Aurora Serverless, un cluster multi-maîtres Aurora, faisant partie d'une base de données globale Aurora ou un cluster utilisant une requête parallèle Aurora.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

## Bases de données

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- ClusterName

Type : chaîne

Description : (Obligatoire) Nom du cluster Aurora que vous souhaitez arrêter ou démarrer.

- Action

Type : chaîne

Valeurs valides : Start | Stop

Par défaut : Démarrer

Description : (Obligatoire) Nom du cluster Aurora que vous souhaitez arrêter ou démarrer.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- rds:DescribeDBClusters
- rds:StartDBCluster
- rds:StopDBCluster

### Étapes de document

- aws:executeScript- Démarre ou arrête le cluster en fonction des valeurs que vous spécifiez pour le.

## Sorties

StartStopAuroraCluster. ClusterName - Le nom du cluster Aurora

StartStopAuroraCluster. CurrentStatus - L'état actuel du cluster Aurora

StartStopAuroraCluster.Message - Détails de l'automatisation

## AWS-StopRdsInstance

### Description

Arrêtez une instance Amazon Relational Database Service (Amazon RDS).

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- InstanceId

Type : chaîne

Description : ID (obligatoire) de l'instance Amazon RDS à arrêter.

# AWSSupport-TroubleshootConnectivityToRDS

## Description

Le `AWSSupport-TroubleshootConnectivityToRDS` runbook diagnostique les problèmes de connectivité entre une instance EC2 et une instance Amazon Relational Database Service. L'automatisation garantit la disponibilité de l'instance DB, puis vérifie les règles de groupe de sécurité associées, les listes de contrôle d'accès réseau (liste ACL réseau) et les tables de routage pour détecter les problèmes de connectivité potentiels.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `DB InstanceIdentifier`

Type : chaîne

Description : (Obligatoire) L'ID de l'instance de DB pour tester la connectivité.

- `SourceInstance`

Type : chaîne

Modèle autorisé : `^i-[a-z0-9]{8,17}$`

Description : (obligatoire) ID de l'instance EC2 à partir de laquelle tester la connectivité.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

### Étapes de document

- `aws:assertAwsResourceProperty`- Confirme que le statut de l'instance de base de données est disponible.
- `aws:executeAwsApi`- Obtient des informations sur l'instance de base de données.
- `aws:executeAwsApi`- Obtient des informations sur les ACL du réseau des instances de base de données.
- `aws:executeAwsApi`- Obtient le CIDR du sous-réseau de l'instance de base de données.
- `aws:executeAwsApi`- Obtient des informations sur l'instance EC2.
- `aws:executeAwsApi`- Obtient des informations sur les ACL du réseau d'instances EC2.
- `aws:executeAwsApi`- Obtient des informations sur les groupes de sécurité associés à l'instance EC2.
- `aws:executeAwsApi`- Obtient des informations sur les groupes de sécurité associés à l'instance de base de données.
- `aws:executeAwsApi`- Obtient des informations sur les tables de routage associées à l'instance EC2.



- `aws:executeAwsApi`- Obtient des informations sur la table de routage principale associée au VPC Amazon pour l'instance EC2.
- `aws:executeAwsApi`- Obtient des informations sur les tables de routage associées à l'instance de base de données.
- `aws:executeAwsApi`- Obtient des informations sur la table de routage principale associée au VPC Amazon pour l'instance de base de données.
- `aws:executeScript`- Évalue les règles du groupe de sécurité.
- `aws:executeScript`- Évalue les ACL du réseau.
- `aws:executeScript`- Évalue les tables de routage.
- `aws:sleep`- Met fin à l'automatisation.

## Sorties

`GetRDS InstanceProperties .DB InstanceIdentifier` - L'instance de base de données utilisée dans l'automatisation.

`GetRDS InstanceProperties .DB InstanceStatus` - L'état actuel de la `DBInstance`.

`evalSecurityGroupRègles. SecurityGroupEvaluation` - Résultats de la comparaison des règles du groupe `SourceInstance` de sécurité avec les règles du groupe de sécurité de l'instance de base de données.

`evalNetworkAclRègles. NetworkAclEvaluation` - Résultats de la comparaison des ACL du `SourceInstance` réseau aux ACL du réseau de l'instance de base de données.

`evalRouteTableEntrées. RouteTableEvaluation` - Résultats de la comparaison de la table de `SourceInstance` routage avec les routes de l'instance de base de données.

## **AWSSupport-TroubleshootRDSIAMAuthentication**

### Description

Il `AWSSupport-TroubleshootRDSIAMAuthentication` permet de résoudre les problèmes d'authentification AWS Identity and Access Management (IAM) pour Amazon RDS pour PostgreSQL, Amazon RDS pour MySQL, Amazon RDS pour MariaDB, Amazon Aurora PostgreSQL et Amazon Aurora MySQL. Utilisez ce runbook pour vérifier la configuration requise pour l'authentification IAM avec une instance Amazon RDS ou un cluster Aurora. Il fournit également des étapes pour corriger les problèmes de connectivité liés à l'instance Amazon RDS ou au cluster Aurora.

**⚠ Important**

Ce runbook ne prend pas en charge Amazon RDS pour Oracle ou Amazon RDS pour Microsoft SQL Server.

**⚠ Important**

Si une instance Amazon EC2 source est fournie et que la base de données cible est Amazon RDS, une automatisation secondaire `AWSSupport-TroubleshootConnectivityToRDS` est invoquée pour résoudre les problèmes de connectivité TCP. La sortie fournit également des commandes que vous pouvez exécuter sur votre instance Amazon EC2 ou sur votre machine source pour vous connecter aux instances Amazon RDS à l'aide de l'authentification IAM.

Comment fonctionne-t-il ?

Ce runbook comprend six étapes :

- Étape 1 : Valider les entrées : valide les entrées de l'automatisation.
- Étape 2 : `branchOnSource` fourni par EC2 : vérifie si un ID d'instance Amazon EC2 source est fourni dans les paramètres d'entrée.
- Étape 3 : `ValidateDSConnectivity` : valide la connectivité Amazon RDS à partir de l'instance Amazon EC2 source, si elle est fournie.
- Étape 4 : `ValidateDSIAMAuthentication` : valide si la fonctionnalité d'authentification IAM est activée.
- Étape 5 : `ValidateIAMPolices` : vérifie si les autorisations IAM requises sont présentes dans l'utilisateur/le rôle IAM fourni.
- Étape 6 : Générer un rapport : génère un rapport des résultats des étapes précédemment exécutées.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Type RDS

Type : chaîne

Description : (Obligatoire) : Sélectionnez le type de base de données relationnelle à laquelle vous essayez de vous connecter et de vous authentifier.

Valeurs autorisées : Amazon RDS ou Amazon Aurora Cluster.

- DB InstanceIdentifier

Type : chaîne

Description : (Obligatoire) L'identifiant de l'instance de base de données Amazon RDS ou du cluster de base de données Aurora cible.

Modèle autorisé :  $^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$$

Nombre maximum de caractères : 63

- SourceEc2 InstanceIdentifier

Type : `AWS::EC2::Instance::Id`

Description : (Facultatif) L'ID de l'instance Amazon EC2 si vous vous connectez à l'instance de base de données Amazon RDS à partir d'une instance Amazon EC2 exécutée dans le même

compte et dans la même région. Ne spécifiez pas ce paramètre si la source n'est pas une instance Amazon EC2 ou si le type Amazon RDS cible est un cluster de base de données Aurora.

Par défaut : ""

- DBIAM RoleName

Type : chaîne

Description : (Facultatif) Le nom du rôle IAM utilisé pour l'authentification basée sur IAM.

Indiquez uniquement si le paramètre `DBIAMUserName` n'est pas fourni, sinon laissez-le vide. L'un `DBIAMRoleName` ou l'autre `DBIAMUserName` doit être fourni.

Modèle autorisé : `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

Nombre maximum de caractères : 64

Par défaut : ""

- DBIAM UserName

Type : chaîne

Description : (Facultatif) Le nom d'utilisateur IAM utilisé pour l'authentification basée sur IAM.

Indiquez uniquement si le `DBIAMRoleName` paramètre n'est pas fourni, sinon laissez-le vide. L'un `DBIAMRoleName` ou l'autre `DBIAMUserName` doit être fourni.

Modèle autorisé : `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

Nombre maximum de caractères : 64

Par défaut : ""

- DB UserName

Type : chaîne

Description : (Facultatif) Le nom d'utilisateur de base de données mappé à un rôle/utilisateur IAM pour l'authentification basée sur IAM au sein de la base de données. L'option par défaut `*` évalue si `rds-db:connect` autorisation est accordée à tous les utilisateurs de la base de données.

Modèle autorisé : `^[a-zA-Z0-9+=, .*_-]{1,64}$`

**Nombre maximum de caractères : 64**

Par défaut : \*

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Instructions

1. Accédez à [AWSSupport-TroubleshootRDSIAMAuthentication dans la console](#). AWS Systems Manager
2. Sélectionnez Exécuter l'automatisation
3. Pour les paramètres d'entrée, entrez ce qui suit :

- `AutomationAssumeRole` (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `RDSType` (obligatoire) :

Sélectionnez le type d'Amazon RDS auquel vous essayez de vous connecter et de vous authentifier. Choisissez l'une des deux valeurs autorisées : `Amazon RDS` ou `Amazon Aurora Cluster`.

- `Base de données InstanceIdentifier` (obligatoire) :

Entrez l'identifiant de l'instance de base de données Amazon RDS cible ou du cluster Aurora auquel vous essayez de vous connecter et utilisez les informations d'identification IAM pour l'authentification.

- `SourceEc2 InstanceIdentifier` (Facultatif) :

Fournissez l'ID d'instance Amazon EC2 si vous vous connectez à l'instance de base de données Amazon RDS à partir d'une instance Amazon EC2 présente dans le même compte et dans la même région. Laissez ce champ vide si la source n'est pas Amazon EC2 ou si le type Amazon RDS cible est un cluster Aurora.

- `DBIAM RoleName` (facultatif) :

Entrez le nom du rôle IAM utilisé pour l'authentification basée sur IAM. Indiquez uniquement si `DBIAMUserName` ce n'est pas le cas ; dans le cas contraire, laissez le champ vide. L'un `DBIAMRoleName` ou l'autre `DBIAMUserName` doit être fourni.

- `DBIAM UserName` (facultatif) :

Entrez l'utilisateur IAM utilisé pour l'authentification basée sur IAM. Indiquez uniquement si `DBIAMRoleName` ce n'est pas le cas, sinon, laissez le champ vide. L'un `DBIAMRoleName` ou l'autre `DBIAMUserName` doit être fourni.

- `Base de données UserName` (facultatif) :

Entrez l'utilisateur de base de données mappé à un rôle/utilisateur IAM pour l'authentification basée sur IAM au sein de la base de données. L'option par défaut `*` est utilisée pour évaluer ; rien n'est fourni dans ce champ.

**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

< 1 ... >

Name	Instance ID	State	Availability zone	Platform
<p>There are no managed Instances in this account.</p> <p>We recommend using <a href="#">Quick Setup</a> to configure your Instances for Systems Manager.</p> <p>After configuring your Instances for Systems Manager, the Instances will be displayed here in a few minutes.</p>				

**AutomationAssumeRole**  
 (Optional) The Amazon Resource Name (ARN) of the role that allows the Automation runbook to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your current IAM user permissions context to execute this runbook.

**RDSInstanceIdentifier**  
 (Required) The identifier of the target Amazon RDS DB instance or Amazon Aurora DB cluster.

**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. Sélectionnez Exécuter.

5. Notez que l'automatisation démarre.

6. Le document exécute les étapes suivantes :

- Étape 1 : valider les entrées :

Valide les entrées de l'automatisation - `SourceEC2InstanceIdentifier` (facultatif), `DBInstanceIdentifier` ou `ClusterID`, et `DBIAMRoleName` ou `DBIAMUserName`. Il vérifie si les paramètres de saisie sont présents dans votre compte et dans votre région. Il vérifie également si l'utilisateur a saisi l'un des paramètres IAM (par exemple, `DBIAMRoleName` ou `DBIAMUserName`). En outre, il effectue d'autres vérifications, par exemple si la base de données mentionnée est dans le statut Disponible.

- Étape 2 : `branchOnSource EC2` a fourni :

Vérifie si la source Amazon EC2 est fournie dans les paramètres d'entrée et si la base de données est Amazon RDS. Dans l'affirmative, il passe à l'étape 3. Dans le cas contraire, il ignore l'étape 3, qui est la validation de la connectivité Amazon EC2-Azure RDS, et passe à l'étape 4.

- Étape 3 : validation de la connectivité DSD :

Si la source Amazon EC2 est fournie dans les paramètres d'entrée et que la base de données est Amazon RDS, l'étape 2 lance l'étape 3. Au cours de cette étape, l'automatisation secondaire

`AWSsupport-TroubleshootConnectivityToRDS` est invoquée pour valider la connectivité Amazon RDS à partir de la source Amazon EC2. Le manuel d'automatisation des enfants `AWSsupport-TroubleshootConnectivityToRDS` vérifie si les configurations réseau requises (Amazon Virtual Private Cloud [Amazon VPC], groupes de sécurité, liste de contrôle d'accès réseau [NACL], disponibilité d'Amazon RDS) sont en place afin que vous puissiez vous connecter de l'instance Amazon EC2 à l'instance Amazon RDS.

- Étape 4 : validation de l'authentification DS IAM :

Valide si la fonctionnalité d'authentification IAM est activée sur l'instance Amazon RDS ou le cluster Aurora.

- Étape 5 : valider les politiques IAM :

Vérifie si les autorisations IAM requises sont présentes dans l'utilisateur/le rôle IAM transmis pour permettre aux informations d'identification IAM de s'authentifier dans l'instance Amazon RDS pour l'utilisateur de base de données spécifié (le cas échéant).

- Étape 6 : Générer un rapport :

Obtient toutes les informations des étapes précédentes et imprime le résultat ou le résultat de chaque étape. Il répertorie également les étapes à suivre et à effectuer pour se connecter à l'instance Amazon RDS à l'aide des informations d'identification IAM.

7. Lorsque l'automatisation est terminée, consultez la section Sorties pour obtenir les résultats détaillés :

- Vérification de l'autorisation utilisateur/rôle IAM pour se connecter à la base de données :

Vérifie si les autorisations IAM requises sont présentes dans l'utilisateur/le rôle IAM transmis pour permettre aux informations d'identification IAM de s'authentifier dans l'instance Amazon RDS pour l'utilisateur de base de données spécifié (le cas échéant).

- Vérification de l'attribut d'authentification basé sur IAM pour la base de données :

Vérifie si la fonctionnalité d'authentification IAM est activée pour la base de données Amazon RDS ou le cluster Aurora spécifiés.

- Vérification de la connectivité entre une instance Amazon EC2 et une instance Amazon RDS :

Vérifie si les configurations réseau requises (Amazon VPC, groupes de sécurité, NACL, disponibilité d'Amazon RDS) sont en place afin que vous puissiez vous connecter de l'instance Amazon EC2 à l'instance Amazon RDS.

- Étapes suivantes:



## Répertorie les commandes et les étapes à suivre et à exécuter pour se connecter à l'instance Amazon RDS à l'aide des informations d'identification 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=$(aws rds generate-db-auth-token --hostname a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com --port 3306 --region us-[REDACTED]-2 --username <name of the DB user>)'
mysql --host=a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com --port=3306 --ssl-ca=global-bundle.pem --enable-clear-text-plugin --user=<name of the DB user> --password=$DBPASS

Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html
```

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

## AWSSupport-ValidateRdsNetworkConfiguration

### Description

AWSSupport-ValidateRdsNetworkConfiguration l'automatisation permet d'éviter un état de réseau incompatible pour votre instance Amazon Relational Database Service (Amazon RDS) /Amazon Aurora/Amazon DocumentDB existante avant l'exécution ou l'opération.

ModifyDBInstance StartDBInstance Si l'instance est déjà dans un état de réseau incompatible, le runbook en fournira la raison.

### Comment fonctionne-t-il ?

Ce runbook détermine si votre instance de base de données Amazon RDS va passer dans un état de réseau incompatible, ou si c'est le cas, détermine la raison pour laquelle elle se trouve dans un état de réseau incompatible.

Le runbook effectue les vérifications suivantes par rapport à votre instance de base de données Amazon RDS :

- Quota Amazon Elastic Network Interface (ENI) par région.
- Tous les sous-réseaux du groupe de sous-réseaux de base de données existent.
- Il existe suffisamment d'adresses IP gratuites disponibles pour le ou les sous-réseaux.
- (Pour les instances Amazon RDS accessibles au public) Paramètres des attributs VPC `enableDnsSupport` (`enableDnsHostnameset`).

#### Important

Lorsque vous utilisez ce document sur des clusters Amazon Aurora/Amazon DocumentDB, assurez-vous de l'utiliser à la `DBInstanceIdentifier` place de `ClusterIdentifier`. Dans le cas contraire, le document échouera lors de la première étape.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `rds:DescribeDBInstances`

- `servicequotas:GetServiceQuota`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeSubnets`

Exemple de politique :

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

## Instructions

1. Accédez au [AWSSupport- ValidateRdsNetworkConfiguration](#) dans la AWS Systems Manager console.
2. Sélectionnez Exécuter l'automatisation
3. Pour les paramètres d'entrée, entrez ce qui suit :
  - AutomationAssumeRole (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle

n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Base de données InstanceIdentifier (obligatoire) :

Entrez l'identifiant de l'instance Amazon Relational Database Service.

The screenshot shows the 'Input parameters' section of a Systems Manager Automation runbook configuration. It contains two input fields:

- AutomationAssumeRole**: An optional field for the IAM role. A dropdown menu is open, showing 'AutomationAssumeRoleSSM' as the selected option. Below the dropdown, the ARN 'arn:aws:iam::<account-id>/role/AutomationAssumeRoleSSM' is visible.
- DBInstanceIdentifier**: A required field for the RDS instance ID. The text 'my-rds-instance-01' is entered in the input box.

4. Sélectionnez Exécuter.

5. Notez que l'automatisation démarre.

6. Le document exécute les étapes suivantes :

- Étape 1 assertRdsState :

Vérifie si l'identifiant d'instance fourni existe et possède l'un des états suivants : `available`, `stopped`, ou `incompatible-network`.

- Étape 2 gatherRdsInformation :

Recueille les informations requises sur l'instance Amazon RDS à utiliser ultérieurement dans le cadre de l'automatisation.

- Étape 3 checkEniQuota :

Vérifie le quota actuellement disponible d'Amazon ENI pour la région.

- Étape 4 validateVpcAttributes :

Valide que les paramètres DNS (`enableDnsSupport` et `enableDnsHostnames`) de l'Amazon VPC sont définis sur `true` (ou non si l'instance Amazon RDS l'est). `PubliclyAccessible`

- Étape 5 validateSubnetAttributes :

Valide l'existence de sous-réseaux dans le `DBSubnetGroup` et vérifie les adresses IP disponibles pour chaque sous-réseau.

- Étape 6 : Générer un rapport :

Obtient toutes les informations des étapes précédentes et imprime le résultat ou le résultat de chaque étape. Il répertorie également les étapes à suivre et à effectuer pour se connecter à l'instance Amazon RDS à l'aide des informations d'identification IAM.

## 7. Lorsque l'automatisation est terminée, consultez la section Sorties pour obtenir les résultats détaillés :

### Instance Amazon RDS avec configuration réseau valide :

#### ▼ 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.
```

### Instance Amazon RDS avec une configuration réseau incorrecte (l'enableDnsHostnames attribut VPC est défini sur false) :

## ▼ Outputs

```

generateReport.Report
# AWS RDS Network Configuration Checks: test-fail-sazrds-vcattr (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.

```

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

### AWSdocumentation de service

- [Comment résoudre les problèmes liés à une base de données Amazon RDS dont l'état de réseau est incompatible ?](#)
- [Comment résoudre les problèmes liés à une instance Amazon DocumentDB dont l'état de réseau est incompatible ?](#)

# Amazon Redshift

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Redshift. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWSConfigRemediation-DeleteRedshiftCluster](#)
- [AWSConfigRemediation-DisablePublicAccessToRedshiftCluster](#)
- [AWSConfigRemediation-EnableRedshiftClusterAuditLogging](#)
- [AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot](#)
- [AWSConfigRemediation-EnableRedshiftClusterEncryption](#)
- [AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting](#)
- [AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster](#)
- [AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings](#)
- [AWSConfigRemediation-ModifyRedshiftClusterNodeType](#)

## AWSConfigRemediation-DeleteRedshiftCluster

### Description

Le `AWSConfigRemediation-DeleteRedshiftCluster` runbook supprime le cluster Amazon Redshift que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

Bases de données

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `ClusterIdentifier`

Type : chaîne

Description : (Obligatoire) L'ID du cluster Amazon Redshift que vous souhaitez supprimer.

- `SkipFinalClusterSnapshot`

Type : booléen

Valeur par défaut : `false`

Description : (Facultatif) Si ce paramètre est défini sur `false`, l'automatisation crée un instantané avant de supprimer le cluster Amazon Redshift. Si ce paramètre est défini sur `true`, aucun instantané final du cluster n'est créé.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift>DeleteCluster`
- `redshift:DescribeClusters`

### Étapes de document

- `aws:branch`- Branches basées sur la valeur que vous spécifiez pour le `SkipFinalClusterSnapshot` paramètre.
- `aws:executeAwsApi`- Supprime le cluster Amazon Redshift spécifié dans `ClusterIdentifier` le paramètre.



- `aws:assertAwsResourceProperty`- Vérifie que le cluster Amazon Redshift a été supprimé.

## **AWSConfigRemediation-DisablePublicAccessToRedshiftCluster**

### Description

Le `AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` runbook désactive l'accessibilité publique pour le cluster Amazon Redshift que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `ClusterIdentifier`

Type : chaîne

Description : (Obligatoire) L'identifiant unique du cluster pour lequel vous souhaitez désactiver l'accessibilité publique.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

#### Étapes de document

- `aws:executeAwsApi`- Désactive l'accessibilité publique pour le cluster spécifié dans le `ClusterIdentifier` paramètre.
- `aws:waitForAwsResourceProperty`- Attend que l'état du cluster passe à `available`.
- `aws:assertAwsResourceProperty`- Confirme que le paramètre d'accessibilité publique est désactivé sur le cluster.

## **AWSConfigRemediation-EnableRedshiftClusterAuditLogging**

### Description

Le `AWSConfigRemediation-EnableRedshiftClusterAuditLogging` runbook active la journalisation des audits pour le cluster Amazon Redshift que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- BucketName

Type : chaîne

Description : (Obligatoire) Le nom du compartiment Amazon Simple Storage Service (Amazon S3) dans lequel vous souhaitez télécharger les journaux.

- ClusterIdentifier

Type : chaîne

Description : (Obligatoire) L'identifiant unique du cluster sur lequel vous souhaitez activer la connexion aux audits.

- S3 KeyPrefix

Type : chaîne

Description : (Facultatif) Le préfixe de clé Amazon S3 (sous-dossier) vers lequel vous souhaitez télécharger les journaux.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeLoggingStatus
- redshift:EnableLogging
- s3:GetBucketAcl
- s3:PutObject

## Étapes de document

- `aws:branch`- Branches selon qu'une valeur a été spécifiée ou non pour le `S3KeyPrefix` paramètre.
- `aws:executeAwsApi`- Active la journalisation des audits sur le cluster spécifié dans le `ClusterIdentifier` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que la journalisation des audits a été activée sur le cluster.

## **AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot**

### Description

Le `AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` runbook permet de créer des instantanés automatisés pour le cluster Amazon Redshift que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `AutomatedSnapshotRetentionPeriod`

Type : entier

Valeurs valides : 1 à 35

Description : (Obligatoire) Nombre de jours pendant lesquels les instantanés automatisés sont conservés.

- `ClusterIdentifier`

Type : chaîne

Description : (Obligatoire) L'identifiant unique du cluster sur lequel vous souhaitez activer les instantanés automatisés.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

#### Étapes de document

- `aws:executeAwsApi`- Active les instantanés d'automatisation sur le cluster spécifié dans le `ClusterIdentifier` paramètre.
- `aws:waitForAwsResourceProperty`- Attend que l'état du cluster passe à `available`.
- `aws:executeScript`- Confirme que les instantanés automatisés ont été activés sur le cluster.

## **AWSConfigRemediation-EnableRedshiftClusterEncryption**

### Description

Le `AWSConfigRemediation-EnableRedshiftClusterEncryption` runbook active le chiffrement sur le cluster Amazon Redshift que vous spécifiez à l'aide AWS Key Management Service

d'une clé gérée par le client AWS KMS(). Ce runbook ne doit être utilisé que comme référence pour garantir que vos clusters Amazon Redshift sont chiffrés conformément aux meilleures pratiques de sécurité minimales recommandées. Nous recommandons de chiffrer plusieurs clusters avec différentes clés gérées par le client. Ce runbook ne peut pas modifier la clé gérée par le AWS KMS client utilisée sur un cluster déjà chiffré. Pour modifier la clé gérée par le AWS KMS client utilisée pour chiffrer un cluster, vous devez d'abord désactiver le chiffrement sur le cluster.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- ClusterIdentifier

Type : chaîne

Description : (Obligatoire) L'identifiant unique du cluster sur lequel vous souhaitez activer le chiffrement.

- Fil à clés KMS

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) de la clé gérée par le AWS KMS client que vous souhaitez utiliser pour chiffrer les données du cluster.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

## Étapes de document

- `aws:executeAwsApi`- Active le chiffrement sur le cluster Amazon Redshift spécifié dans le `ClusterIdentifier` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que le chiffrement a été activé sur le cluster.

# **AWSConfigRemediation- EnableRedshiftClusterEnhancedVPCRouting**

## Description

Le `AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` runbook permet un routage amélioré du cloud privé virtuel (VPC) pour le cluster Amazon Redshift que vous spécifiez. Pour plus d'informations sur le routage VPC amélioré, consultez le routage [VPC amélioré Amazon Redshift dans le guide](#) de gestion Amazon Redshift.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

## Bases de données

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- ClusterIdentifier

Type : chaîne

Description : (Obligatoire) L'identifiant unique du cluster sur lequel vous souhaitez activer le routage VPC amélioré.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

## Étapes de document

- aws:executeAwsApi- Active le routage VPC amélioré sur le cluster spécifié dans le ClusterIdentifier paramètre.
- assertAwsResourceProperty- Confirme que le routage VPC amélioré a été activé sur le cluster.

## **AWSConfigRemediation- EnforceSSLOnlyConnectionsToRedshiftCluster**

### Description



Le `AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` runbook nécessite des connexions entrantes pour utiliser le protocole SSL pour le cluster Amazon Redshift que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `ClusterIdentifier`

Type : chaîne

Description : (Obligatoire) L'identifiant unique du cluster sur lequel vous souhaitez activer le routage VPC amélioré.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

#### Étapes de document

- `aws:executeAwsApi`- Recueille les détails des paramètres à partir du cluster spécifié dans le `ClusterIdentifier` paramètre.
- `aws:executeAwsApi`- Active le `require_ssl` réglage sur le cluster spécifié dans le `ClusterIdentifier` paramètre.
- `aws:assertAwsResourceProperty`- Confirme que le `require_ssl` paramètre a été activé sur le cluster.
- `aws:executeScript`- Vérifie le `require_ssl` réglage du cluster.

## **AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings**

### Description

Le `AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` runbook modifie les paramètres de maintenance du cluster Amazon Redshift que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

### Bases de données

### Paramètres

- `AllowVersionUpgrade`

Type : booléen

Description : (Obligatoire) Si ce paramètre est défini sur `true`, les mises à niveau des versions majeures sont appliquées automatiquement au cluster pendant la période de maintenance.

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `AutomatedSnapshotRetentionPeriod`

Type : entier

Valeurs valides : 1 à 35

Description : (Obligatoire) Nombre de jours pendant lesquels les instantanés automatisés sont conservés.

- `ClusterIdentifier`

Type : chaîne

Description : (Obligatoire) L'identifiant unique du cluster sur lequel vous souhaitez activer le routage VPC amélioré.

- `PreferredMaintenanceWindow`

Type : chaîne

Description : (Obligatoire) La plage horaire hebdomadaire (en UTC) pendant laquelle la maintenance du système peut avoir lieu.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

### Étapes de document

- `aws:executeAwsApi`- Modifie les paramètres de maintenance pour le cluster spécifié dans le `ClusterIdentifier` paramètre.
- `aws:assertAwsResourceProperty`- Confirme que les paramètres de maintenance modifiés ont été configurés pour le cluster.

## AWSConfigRemediation-ModifyRedshiftClusterNodeType

### Description

Le `AWSConfigRemediation-ModifyRedshiftClusterNodeType` runbook modifie le type de nœud et le nombre de nœuds pour le cluster Amazon Redshift que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Bases de données

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- **Classique**

Type : booléen

Description : (Facultatif) Si ce paramètre est défini sur `true`, l'opération de redimensionnement utilise le processus de redimensionnement classique.

- **ClusterIdentifier**

Type : chaîne

Description : (Obligatoire) L'identifiant unique du cluster dont vous souhaitez modifier le type de nœud.

- **ClusterType**

Type : chaîne

Valeurs valides : nœud unique | nœud multiple

Description : (Obligatoire) Type de cluster que vous souhaitez attribuer à votre cluster.

- **NodeType**

Type : chaîne

Valeurs valides : ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

Description : (Obligatoire) Type de nœud que vous souhaitez attribuer à votre cluster.

- **NumberOfNodes**

Type : entier

Valeurs valides : 2 à 100

Description : (Facultatif) Le nombre de nœuds que vous souhaitez attribuer à votre cluster. Si votre cluster est un `single-node` type, ne spécifiez pas de valeur pour ce paramètre.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le [runbook](#).

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

### Étapes de document

- `aws:executeScript`- Modifie le type de nœud et le nombre de nœuds pour le cluster spécifié dans le `ClusterIdentifier` paramètre.

## Amazon S3

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Simple Storage Service. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWS-ArchiveS3BucketToIntelligentTiering](#)
- [AWS-ConfigureS3BucketLogging](#)
- [AWS-ConfigureS3BucketVersioning](#)
- [AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock](#)
- [AWSConfigRemediation-ConfigureS3PublicAccessBlock](#)
- [AWS-CreateS3PolicyToExpireMultipartUploads](#)
- [AWS-DisableS3BucketPublicReadWrite](#)
- [AWS-EnableS3BucketEncryption](#)
- [AWS-EnableS3BucketKeys](#)
- [AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy](#)
- [AWSConfigRemediation-RestrictBucketSSLRequestsOnly](#)
- [AWSSupport-TroubleshootS3PublicRead](#)

# AWS-ArchiveS3BucketToIntelligentTiering

## Description

Le `AWS-ArchiveS3BucketToIntelligentTiering` runbook crée ou remplace une configuration de hiérarchisation intelligente pour le bucket Amazon Simple Storage Service (Amazon S3) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- BucketName

Type : chaîne

Description : (Obligatoire) Nom du compartiment S3 pour lequel vous souhaitez créer une configuration de hiérarchisation intelligente.

- ConfigurationId

Type : chaîne

Description : (Obligatoire) L'ID de la configuration de hiérarchisation intelligente. Il peut s'agir d'un nouvel ID de configuration ou de l'ID d'une configuration existante.

- NumberOfDaysToArchive

Type : chaîne

Valeurs valides : 90-730

Description : (Obligatoire) Nombre de jours consécutifs après qu'un objet de votre compartiment est éligible à la transition vers le niveau d'accès aux archives.

- NumberOfDaysToDeepArchive

Type : chaîne

Valeurs valides : 180-730

Description : (Obligatoire) Nombre de jours consécutifs après qu'un objet de votre bucket est éligible à la transition vers le niveau Deep Archive Access.

- S3Prefix

Type : chaîne

Description : (Facultatif) Le préfixe du nom clé des objets auxquels vous souhaitez appliquer la configuration.

- Balises

Type : MapList

Description : (Facultatif) Métadonnées attribuées aux objets auxquels vous souhaitez appliquer la configuration. Les balises se composent d'une clé et d'une valeur définies par l'utilisateur.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution



- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

### Étapes de document

- `PutBucketIntelligentTieringConfiguration` (AWS:ExecuteScript) - Crée ou met à jour une configuration Amazon S3 Intelligent-Tiering pour le compartiment spécifié.
- `VerifyBucketIntelligentTieringConfiguration`(aws : assertAwsResource Propriété) - Vérifie que la configuration intelligente du compartiment S3 a été appliquée au compartiment spécifié.

## AWS-ConfigureS3BucketLogging

### Description

Activez la journalisation sur un bucket Amazon Simple Storage Service (Amazon S3).

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `BucketName`

Type : chaîne

Description : (Obligatoire) Nom du compartiment Amazon S3 pour lequel vous souhaitez configurer la journalisation.

- GrantedPermission

Type : chaîne

Valeurs valides : FULL\_CONTROL | READ | WRITE

Description : (Obligatoire) autorisations de journalisation attribuées au bénéficiaire du compartiment.

- GranteeEmailAddress

Type : chaîne

(Facultatif) Adresse e-mail du bénéficiaire.

- GranteeId

Type : chaîne

Description : (Facultatif) ID d'utilisateur canonique du bénéficiaire.

- GranteeType

Type : chaîne

Valeurs valides : CanonicalUser | AmazonCustomerByEmail | Groupe

Description : (Obligatoire) type de bénéficiaire.

- GranteeUri

Type : chaîne

Description : (Facultatif) URI du groupe de bénéficiaires.

- TargetBucket

Type : chaîne

Description : (Obligatoire) Spécifie le compartiment dans lequel vous souhaitez qu'Amazon S3 stocke les journaux d'accès au serveur. Les journaux peuvent être fournis dans n'importe quel

compartiment que vous possédez. Vous pouvez également configurer plusieurs compartiments pour diffuser leurs journaux vers le même compartiment cible. Dans ce cas, vous devez en choisir un différent TargetPrefix pour chaque compartiment source afin que les fichiers journaux fournis puissent être distingués par clé.

- TargetPrefix

Type : chaîne

Par défaut : /

Description : (Facultatif) spécifie un préfixe pour les clés sous lesquelles les fichiers journaux sont stockés.

## AWS-ConfigureS3BucketVersioning

### Description

Configurez le versionnement pour un bucket Amazon Simple Storage Service (Amazon S3).

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre

nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- BucketName

Type : chaîne

Description : (Obligatoire) Le nom du compartiment Amazon S3 pour lequel vous souhaitez configurer le versionnement.

- VersioningState

Type : chaîne

Valeurs valides : Activé | Suspendu

Par défaut : Enabled

Description : (Facultatif) Appliqué au VersioningConfiguration .Status. Lorsque ce paramètre est défini sur « Enabled », ce processus permet la gestion des versions pour les objets du compartiment. Tous les objets ajoutés à ce compartiment reçoivent un ID de version unique. Lorsqu'il est défini surSuspended, ce processus désactive la gestion des versions pour les objets du compartiment. Tous les objets ajoutés au compartiment reçoivent l'ID de versionnull.

## **AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock**

### Description

Le AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock runbook configure les paramètres de blocage de l'accès public Amazon Simple Storage Service (Amazon S3) pour un compartiment Amazon S3 en fonction des valeurs que vous spécifiez dans les paramètres du runbook.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- BlockPublicAcls

Type : booléen

Valeur par défaut : true

Description : (Facultatif) Si ce paramètre est défini sur `true`, Amazon S3 bloque les listes de contrôle d'accès public (ACL) pour le compartiment S3 et les objets stockés dans le compartiment S3 que vous spécifiez dans le `BucketName` paramètre.

- BlockPublicPolicy

Type : booléen

Valeur par défaut : true

Description : (Facultatif) Si ce paramètre est défini sur `true`, Amazon S3 bloque les politiques de compartiment public pour le compartiment S3 que vous spécifiez dans le `BucketName` paramètre.

- BucketName

Type : chaîne

Description : (Obligatoire) Nom du compartiment S3 que vous souhaitez configurer.

- IgnorePublicAcls

Type : booléen

Valeur par défaut : true

Description : (Facultatif) Si ce paramètre est défini sur `true`, Amazon S3 ignore toutes les ACL publiques pour le compartiment S3 que vous spécifiez dans le `BucketName` paramètre.

- `RestrictPublicBuckets`

Type : booléen

Valeur par défaut : `true`

Description : (Facultatif) Si ce paramètre est défini sur `true`, Amazon S3 restreint les politiques de compartiment public pour le compartiment S3 que vous spécifiez dans le `BucketName` paramètre.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

### Étapes de document

- `aws:executeAwsApi`- Crée ou modifie la `PublicAccessBlock` configuration du compartiment S3 spécifié dans le `BucketName` paramètre.
- `aws:executeScript`- Renvoie la `PublicAccessBlock` configuration du compartiment S3 spécifié dans le `BucketName` paramètre et vérifie que les modifications ont été effectuées avec succès sur la base des valeurs spécifiées dans les paramètres du runbook.

## **AWSConfigRemediation-ConfigureS3PublicAccessBlock**

### Description

Le `AWSConfigRemediation-ConfigureS3PublicAccessBlock` runbook configure les paramètres de blocage d'accès public Compte AWS Amazon Simple Storage Service (Amazon S3) d'un utilisateur en fonction des valeurs que vous spécifiez dans les paramètres du runbook.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AccountId`

Type : chaîne

Description : (Obligatoire) L'ID du propriétaire du compartiment S3 Compte AWS que vous configurez.

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `BlockPublicAcls`

Type : booléen

Valeur par défaut : `true`

Description : (Facultatif) Si ce paramètre est défini sur `true`, Amazon S3 bloque les listes de contrôle d'accès public (ACL) pour les compartiments S3 appartenant à ceux Compte AWS que vous spécifiez dans le `AccountId` paramètre.

- **BlockPublicPolicy**

Type : booléen

Valeur par défaut : true

Description : (Facultatif) Si ce paramètre est défini sur `true`, Amazon S3 bloque les politiques de compartiment public pour les compartiments S3 appartenant à ceux Compte AWS que vous spécifiez dans le `AccountId` paramètre.

- **IgnorePublicAcls**

Type : booléen

Valeur par défaut : true

Description : (Facultatif) Si ce paramètre est défini sur `true`, Amazon S3 ignore toutes les ACL publiques pour les compartiments S3 appartenant à ceux Compte AWS que vous spécifiez dans le paramètre. `AccountId`

- **RestrictPublicBuckets**

Type : booléen

Valeur par défaut : true

Description : (Facultatif) Si ce paramètre est défini sur `true`, Amazon S3 restreint les politiques relatives aux compartiments publics pour les compartiments S3 appartenant à ceux Compte AWS que vous spécifiez dans le `AccountId` paramètre.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

## Étapes de document



- `aws:executeAwsApi`- Crée ou modifie la `PublicAccessBlock` configuration pour ce qui est Compte AWS spécifié dans le `AccountId` paramètre.
- `aws:executeScript`- Renvoie la `PublicAccessBlock` configuration Compte AWS spécifiée dans le `AccountId` paramètre et vérifie que les modifications ont été effectuées avec succès en fonction des valeurs spécifiées dans les paramètres du runbook.

## AWS-CreateS3PolicyToExpireMultipartUploads

### Description

Le `AWS-CreateS3PolicyToExpireMultipartUploads` runbook crée une politique de cycle de vie pour un compartiment spécifié qui expire après un certain nombre de jours pour les téléchargements partiels incomplets en cours. Ce runbook fusionne la nouvelle politique de cycle de vie avec toutes les politiques de compartiment de cycle de vie existantes qui existent déjà.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- **BucketName**

Type : chaîne

Description : (Obligatoire) Nom du compartiment S3 que vous souhaitez configurer.

- **DaysUntilExpire**

Type : entier

Description : (Obligatoire) Le nombre de jours pendant lesquels Amazon S3 attend avant de supprimer définitivement toutes les parties du téléchargement.

- **RuleId**

Type : chaîne

Description : (Obligatoire) L'ID utilisé pour identifier la règle du bucket de cycle de vie. Il doit s'agir d'une valeur unique.

- **S3Prefix**

Type : chaîne

Description : (Facultatif) Le préfixe du nom clé des objets auxquels vous souhaitez appliquer la configuration.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

## Étapes de document

- `ConfigureExpireMultipartUploads (AWS:ExecuteScript)` - Configure la politique de cycle de vie du bucket.

- `VerifyExpireMultipartUploads (AWS:ExecuteScript)` - Vérifie que la politique de cycle de vie a été configurée pour le bucket.

## Sorties

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

# AWS-DisableS3BucketPublicReadWrite

## Description

Utilisez Amazon Simple Storage Service (Amazon Block Public Access S3) pour désactiver l'accès en lecture et en écriture à un compartiment S3 public. Pour plus d'informations, consultez la section [Utilisation d'Amazon S3 Block Public Access](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- S3 BucketName

Type : chaîne

Description : (obligatoire) compartiment S3 au niveau duquel vous souhaitez restreindre l'accès.

## AWS-EnableS3BucketEncryption

### Description

Configure le chiffrement par défaut pour un bucket Amazon Simple Storage Service (Amazon S3).

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- BucketName

Type : chaîne

Description : (obligatoire) nom du compartiment S3 dans lequel vous souhaitez chiffrer le contenu.

- SSEAlgorithm

Type : chaîne

Valeur par défaut : AES256

Description : (Facultatif) algorithme de chiffrement côté serveur à utiliser pour le chiffrement par défaut.

## AWS-EnableS3BucketKeys

### Description

Le `AWS-EnableS3BucketKeys` runbook active les clés de compartiment sur le compartiment Amazon Simple Storage Service (Amazon S3) que vous spécifiez. Cette clé au niveau du compartiment crée des clés de données pour les nouveaux objets au cours de leur cycle de vie. Si vous ne spécifiez aucune valeur pour le `KmsKeyId` paramètre, le chiffrement côté serveur à l'aide de clés gérées Amazon S3 (SSE-S3) est utilisé pour la configuration de chiffrement par défaut.

#### Note

Les clés de compartiment Amazon S3 ne sont pas prises en charge pour le chiffrement double couche côté serveur avec des clés AWS Key Management Service (AWS KMS) (DSSE-KMS).

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- BucketName

Type : chaîne

Description : (Obligatoire) Nom du compartiment S3 pour lequel vous souhaitez activer les clés de compartiment.

- KMS KeyId

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN), l'ID de clé ou l'alias de clé AWS Key Management Service (AWS KMS) gérée par le client que vous souhaitez utiliser pour le chiffrement côté serveur.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetEncryptionConfiguration
- s3:PutEncryptionConfiguration

### Étapes de document

- ChooseEncryptionType (aws:branch) - Évalue la valeur fournie pour le KmsKeyId paramètre afin de déterminer si le SSE-S3 (AES256) ou le SSE-KMS seront utilisés.
- PutBucketKeysKMS (aws :executeAwsApi) - Définit la BucketKeyEnabled propriété sur true pour le compartiment S3 spécifié en utilisant le paramètre spécifiéKmsKeyId.

- PutBucketKeysAES256 (aws :executeAwsApi) - Définit la BucketKeyEnabled propriété sur true pour le compartiment S3 spécifié avec un chiffrement AES256.
- VerifyS3 BucketKeysEnabled (aws : assertAwsResource Property) : vérifie que les clés de compartiment sont activées sur le compartiment S3 cible.

## **AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy**

### Description

Le AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy runbook supprime les principales déclarations de politique contenant des caractères génériques (Principal: \*ouPrincipal: "AWS": \*) pour les Allow actions de votre politique de compartiment Amazon Simple Storage Service (Amazon S3). Les déclarations de politique assorties de conditions sont également supprimées.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- BucketName

Type : chaîne

Description : (Obligatoire) Le nom du compartiment Amazon S3 dont vous souhaitez modifier la politique.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

#### Étapes de document

- `aws:executeScript`- Modifie la politique du compartiment et vérifie que les principales déclarations de politique comportant des caractères génériques ont été supprimées du compartiment Amazon S3 que vous spécifiez dans le paramètre. `BucketName`

## **AWSConfigRemediation-RestrictBucketSSLRequestsOnly**

### Description

Le `AWSConfigRemediation-RestrictBucketSSLRequestsOnly` runbook crée une déclaration de politique relative au compartiment Amazon Simple Storage Service (Amazon S3) qui refuse explicitement les requêtes HTTP adressées au compartiment Amazon S3 que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

### Automatisation

### Propriétaire



## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- BucketName

Type : chaîne

Description : (Obligatoire) Nom du compartiment S3 auquel vous souhaitez refuser les requêtes HTTP.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3>DeleteBucketPolicy
- s3:GetBucketPolicy
- s3:PutEncryptionConfiguration
- s3:PutBucketPolicy

### Étapes de document

- aws:executeScript- Crée une politique de compartiment pour le compartiment S3 spécifié dans le BucketName paramètre qui refuse explicitement les requêtes HTTP.

# AWSSupport-TroubleshootS3PublicRead

## Description

Le `AWSSupport-TroubleshootS3PublicRead` runbook diagnostique les problèmes de lecture des objets du compartiment public Amazon Simple Storage Service (Amazon S3) que vous spécifiez dans le paramètre. `S3BucketName` Un sous-ensemble de paramètres est également analysé pour les objets du compartiment S3.

[Exécuter cette automatisation \(console\)](#)

## Limites

- Cette automatisation ne vérifie pas les points d'accès qui permettent au public d'accéder aux objets.
- Cette automatisation n'évalue pas les clés de condition dans la politique du compartiment S3.
- Si vous l'utilisez AWS Organizations, cette automatisation n'évalue pas les politiques de contrôle des services pour confirmer que l'accès à Amazon S3 est autorisé.

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `CloudWatchLogGroupName`

Type : chaîne

Description : (Facultatif) Le groupe de CloudWatch journaux Amazon Logs dans lequel vous souhaitez envoyer le résultat d'automatisation. Si aucun groupe de journaux correspondant à la valeur que vous spécifiez n'est trouvé, l'automatisation créera un groupe de journaux à l'aide de cette valeur de paramètre. La période de conservation du groupe de journaux créé par cette automatisation est de 14 jours.

- `CloudWatchLogStreamName`

Type : chaîne

Description : (Facultatif) Le flux du journal CloudWatch des journaux dans lequel vous souhaitez envoyer la sortie d'automatisation. Si aucun flux de journal correspondant à la valeur que vous spécifiez n'est trouvé, l'automatisation créera un flux de journal à l'aide de cette valeur de paramètre. Si vous ne spécifiez pas de valeur pour ce paramètre, l'automatisation utilisera le `ExecutionId` pour le nom du flux de journal.

- `HttpGet`

Type : booléen

Valeurs valides : `true` | `false`

Valeur par défaut : `true`

Description : (Facultatif) Si ce paramètre est défini sur `true`, l'automatisation envoie une requête HTTP partielle aux objets `S3BucketName` que vous spécifiez. Seul le premier octet de l'objet est renvoyé à l'aide de l'en-tête HTTP `Range`.

- `IgnoreBlockPublicAccess`

Type : booléen

Valeurs valides : `true` | `false`

Valeur par défaut : `false`

Description : (Facultatif) Si ce paramètre est défini sur `true`, l'automatisation ignore les paramètres de blocage d'accès public du compartiment S3 que vous spécifiez dans le `S3BucketName` paramètre. Il n'est pas recommandé de modifier ce paramètre par rapport à la valeur par défaut.

- **MaxObjects**

Type : entier

Valeurs valides : 1 à 25

Par défaut: 5

Description : (Facultatif) Le nombre d'objets à analyser dans le compartiment S3 que vous spécifiez dans le `S3BucketName` paramètre.

- **S3 BucketName**

Type : chaîne

Description : (Obligatoire) Nom du compartiment S3 à dépanner.

- **S3 PrefixName**

Type : chaîne

Description : (Facultatif) Le préfixe du nom clé des objets que vous souhaitez analyser dans votre compartiment S3. Pour plus d'informations, consultez la section [Clés d'objet](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

- **StartAfter**

Type : chaîne

Description : (Facultatif) Nom de la clé d'objet dans laquelle vous souhaitez que l'automatisation commence à analyser les objets de votre compartiment S3.

- **ResourcePartition**

Type : chaîne

Valeurs valides : `aws` | `aws-us-gov` | `aws-cn`

Par défaut : `aws`

Description : (Obligatoire) La partition dans laquelle se trouve votre compartiment S3.

- **Détaillée**

Type : booléen

Valeurs valides : true | false

Valeur par défaut : false

Description : (Facultatif) Pour renvoyer des informations plus détaillées lors de l'automatisation, définissez ce paramètre sur `true`. Seuls les messages d'avertissement et d'erreur seront renvoyés si le paramètre est défini sur `false`.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Les `logs:PutLogEvents` autorisations `logs:CreateLogGroup`, `logs:CreateLogStream`, et ne sont requises que si vous souhaitez que l'automatisation envoie des données de journal à CloudWatch Logs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:SimulateCustomPolicy",
        "iam:GetContextKeysForCustomPolicy",
        "s3:ListAllMyBuckets",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",
```

```
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketRequestPayment",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPolicy",
            "s3:GetBucketAcl"
        ],
        "Resource": "arn:aws:s3:::awsexamplebucket1",
        "Effect": "Allow"
    }
]
}
```

## Étapes de document

- `aws:assertAwsResourceProperty`- Confirme que le compartiment S3 existe et qu'il est accessible.
- `aws:executeScript`- Renvoie l'emplacement du compartiment S3 et votre ID utilisateur canonique.
- `aws:executeScript`- Renvoie les paramètres de blocage de l'accès public pour votre compte et le compartiment S3.
- `aws:assertAwsResourceProperty`- Confirme que le payeur du compartiment S3 est réglé sur `BucketOwner`. S'il `Requester Pays` est activé sur le compartiment S3, l'automatisation prend fin.
- `aws:executeScript`- Renvoie l'état de la politique du compartiment S3 et détermine s'il est considéré comme public. Pour plus d'informations sur les compartiments S3 publics, consultez [La signification du terme « public »](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.
- `aws:executeAwsApi`- Renvoie la politique du compartiment S3.
- `aws:executeAwsApi`- Renvoie toutes les clés de contexte présentes dans la politique du compartiment S3.
- `aws:assertAwsResourceProperty`- Confirme s'il existe un refus explicite dans la politique du compartiment S3 pour l'action d'`GetObjectAPI`.
- `aws:executeAwsApi`- Renvoie la liste de contrôle d'accès (ACL) pour le compartiment S3.

- `aws:executeScript`- Crée un groupe de CloudWatch journaux et un flux de journaux si vous spécifiez une valeur pour le `CloudWatchLogGroupName` paramètre.
- `aws:executeScript`- Sur la base des valeurs que vous spécifiez dans les paramètres d'entrée du runbook, évalue si l'un des paramètres du compartiment S3 collectés lors de l'automatisation empêche le public d'accéder aux objets. Ce script exécute les fonctions suivantes :
  - Évalue les paramètres de blocage de l'accès public
  - Renvoie les objets de votre compartiment S3 en fonction des valeurs que vous spécifiez dans les `StartAfter` paramètres `MaxObjectsS3PrefixName`, et.
  - Renvoie la politique du compartiment S3 pour simuler une politique IAM personnalisée pour les objets renvoyés par votre compartiment S3.
  - Exécute une requête HTTP partielle vers les objets renvoyés si le `HttpGet` paramètre est défini sur `true`. Seul le premier octet de l'objet est renvoyé à l'aide de l'en-tête HTTP `Range`.
  - Vérifie le nom de clé de l'objet renvoyé pour confirmer s'il se termine par un ou deux points. Les noms de clés d'objet qui se terminent par des points ne peuvent pas être téléchargés depuis la console Amazon S3.
  - Vérifie si le propriétaire de l'objet renvoyé correspond au propriétaire du compartiment S3.
  - Vérifie si l'ACL de l'objet accorde `READ FULL_CONTROL` ou autorise des utilisateurs anonymes.
  - Renvoie les balises associées à l'objet.
  - Utilise la stratégie IAM simulée pour confirmer s'il existe un refus explicite pour cet objet dans la politique du compartiment S3 pour l'action d'`GetObjectAPI`.
  - Renvoie les métadonnées de l'objet pour confirmer que la classe de stockage est prise en charge.
  - Vérifie les paramètres de chiffrement côté serveur de l'objet pour vérifier si l'objet est chiffré à l'aide d'une clé gérée par le client AWS Key Management Service (AWS KMS).

## Sorties

`AnalyzeObjects.seau`

`AnalyzeObjects.objet`

# SageMaker

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon SageMaker. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-DisableSageMakerNotebookRootAccess](#)

## AWS-DisableSageMakerNotebookRootAccess

### Description

Le AWS-DisableSageMakerNotebookRootAccess runbook désactive l'accès root sur une instance de SageMaker bloc-notes Amazon. Pendant l'automatisation, l'instance du bloc-notes est arrêtée pour apporter les modifications requises. SageMaker Les instances de bloc-notes Studio ne sont pas prises en charge.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.



- `NotebookInstanceName`

Type : chaîne

Description : (Obligatoire) Nom de l'instance de SageMaker bloc-notes sur laquelle désactiver l'accès root.

- `StartInstanceAfterUpdate`

Type : booléen

Valeur par défaut : `true`

Description : (Facultatif) Détermine si l'instance du bloc-notes est démarrée après la désactivation de l'accès root. Le réglage par défaut de ce paramètre est `true`. Si ce paramètre est défini sur `true`, l'instance est démarrée après la désactivation de l'accès root. Si ce paramètre est défini sur `false`, l'instance reste dans `stopped` cet état une fois que l'accès root est désactivé.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le `runbook`.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

### Étapes de document

- `CheckNotebookInstanceStatus` (`aws:executeAwsApi`) : Vérifie l'état actuel de l'instance de bloc-notes.
- `StopOrUpdateNotebookInstance` (`aws:branch`) : branches basées sur le statut de l'instance du bloc-notes.
- `StopNotebookInstance` (`aws:executeAwsApi`) : Démarre l'instance si le statut est `stopped`.
- `WaitForInstanceToStop` (`aws:waitForAwsResourceProperty`) : Vérifie que l'instance est `stopped`.

- `UpdateNotebookInstance` (`aws :executeAwsApi`) : désactive l'accès root sur l'instance du bloc-notes.
- `WaitForNotebookUpdate` (`aws : waitForAwsResourceProperty`) : Vérifie que l'accès root a été désactivé et que l'instance possède un `stopped` statut.
- `ChooseInstanceStart` (`aws:branch`) : Branche selon que l'instance doit être démarrée ou non.
- `StartNotebookInstance` (`aws :executeAwsApi`) : Démarre l'instance du bloc-notes.
- `VerifyNotebookInstanceStatus` (`aws : waitForAwsResourceProperty`) : Vérifie si l'instance existe `available` avant de désactiver l'accès root.
- `VerifyNotebookInstanceRootAccess` (`aws : assertAwsResource Propriété`) : Vérifie que le paramètre d'accès root à l'instance du bloc-notes est correctement désactivé.

## Secrets Manager

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Secrets Manager. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSConfigRemediation-DeleteSecret](#)
- [AWSConfigRemediation-RotateSecret](#)

## AWSConfigRemediation-DeleteSecret

### Description

Le `AWSConfigRemediation-DeleteSecret` runbook supprime un secret et toutes les versions qui y sont stockées. AWS Secrets Manager Vous pouvez éventuellement spécifier la fenêtre de restauration au cours de laquelle vous pouvez restaurer le secret. Si vous ne spécifiez aucune valeur pour le `RecoveryWindowInDays` paramètre, l'opération est par défaut de 30 jours.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- RecoveryWindowInDays

Type : entier

Valeurs valides : 7-30

Valeur par défaut : 30

Description : (Facultatif) Le nombre de jours pendant lesquels vous pouvez restaurer le secret.

- SecretId

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du secret que vous souhaitez supprimer.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- secretsmanager:DeleteSecret

- `secretsmanager:DescribeSecret`

### Étapes de document

- `aws:executeAwsApi`- Supprime le secret que vous spécifiez dans le `SecretId` paramètre.
- `aws:executeScript`- Vérifie que la suppression du secret a été planifiée.

## AWSConfigRemediation-RotateSecret

### Description

Le `AWSConfigRemediation-RotateSecret` runbook fait pivoter un secret qui y est stocké. AWS Secrets Manager

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `RotationInterval`

Type : Intervalle

Valeurs valides : 1 à 365

Description : (Obligatoire) Le nombre de jours entre les rotations du secret.

- `RotationLambdaArn`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) de la AWS Lambda fonction qui peut faire pivoter le secret.

- `SecretId`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du secret que vous souhaitez faire pivoter.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

### Étapes de document

- `aws:executeAwsApi`- Fait pivoter le secret que vous spécifiez dans le `SecretId` paramètre.
- `aws:executeScript`- Vérifie que la rotation a été activée sur le secret.

## Security Hub

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Security Hub. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWSConfigRemediation-EnableSecurityHub](#)

# AWSConfigRemediation-EnableSecurityHub

## Description

Le AWSConfigRemediation-EnableSecurityHub runbook active AWS Security Hub (Security Hub) le Compte AWS et l' Région AWS endroit où vous exécutez l'automatisation. Pour plus d'informations sur Security Hub, consultez [Qu'est-ce que c'est AWS Security Hub ?](#) dans le guide de AWS Security Hub l'utilisateur.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- EnableDefaultStandards

Type : booléen

Valeur par défaut : true

Description : (Obligatoire) Si ce paramètre est défini sur `true`, les normes de sécurité par défaut définies par Security Hub sont activées.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

## Étapes de document

- `aws:executeAwsApi`- Active Security Hub dans le compte courant et dans la région.
- `aws:executeAwsApi`- Vérifie que Security Hub a été activé.

## AWS Shield

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS Shield. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWSPremiumSupport-DDoSResiliencyAssessment](#)

## **AWSPremiumSupport-DDoSResiliencyAssessment**

### Description

Le `AWSPremiumSupport-DDoSResiliencyAssessment` manuel AWS Systems Manager d'automatisation vous aide à vérifier les vulnérabilités DDoS et à configurer les ressources conformément à la AWS Shield Advanced protection de votre. Compte AWS Il fournit un rapport sur les paramètres de configuration pour les ressources vulnérables aux attaques par déni de

service distribué (DDoS). Il est utilisé pour collecter, analyser et évaluer les ressources suivantes : Amazon Route 53, Amazon Load Balancers, Amazon CloudFront distributions AWS Global Accelerator et adresses IP AWS élastiques pour leurs paramètres de configuration conformément aux meilleures pratiques recommandées en matière de AWS Shield Advanced protection. Le rapport de configuration final est disponible dans un compartiment Amazon S3 de votre choix sous forme de fichier HTML.

Comment fonctionne-t-il ?

Ce manuel contient une série de vérifications pour vérifier les différents types de ressources accessibles au public et pour vérifier si leurs protections sont configurées conformément aux recommandations du livre blanc sur les [meilleures pratiques AWS DDoS](#). Le runbook effectue les opérations suivantes :

- Vérifie si un abonnement à AWS Shield Advanced est activé.
- Si cette option est activée, elle détecte s'il existe des ressources protégées par Shield Advanced.
- Il trouve toutes les ressources mondiales et régionales dans le Compte AWS et vérifie si elles sont protégées par le Shield.
- Il nécessite les paramètres du type de ressource pour l'évaluation, le nom du compartiment Amazon S3 et l'ID du compte AWS du compartiment Amazon S3 (S3BucketOwner).
- Il renvoie les résultats sous forme de rapport HTML stocké dans le compartiment Amazon S3 fourni.

Les paramètres d'AssessmentTypeentree déterminent si les contrôles sur toutes les ressources seront effectués. Par défaut, le runbook vérifie tous les types de ressources. Si seul le RegionalResources paramètre GlobalResources ou le paramètre est sélectionné, le runbook effectue des vérifications uniquement sur les types de ressources sélectionnés.

#### Important

- L'accès aux AWSPremiumSupport- \* runbooks nécessite un abonnement Enterprise ou Business Support. Pour plus d'informations, voir [Comparer les AWS Support forfaits](#).
- Ce runbook nécessite un ACTIVE [AWS Shield Advancedabonnement](#).

[Exécuter cette automatisation \(console\)](#)



## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux, macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- AssessmentType

Type : chaîne

Description : (Facultatif) Détermine le type de ressources à évaluer pour l'évaluation de la résilience DDoS. Par défaut, le runbook évaluera les ressources mondiales et régionales. Pour les ressources régionales, le runbook décrit tous les équilibreurs de charge d'application (ALB) et de réseau (NLB) ainsi que l'ensemble du groupe Auto Scaling de votre /region. Compte AWS

Valeurs valides : ['Global Resources', 'Regional Resources', 'Global and Regional Resources']

Par défaut : Ressources mondiales et régionales

- S3 BucketName

Type : AWS::S3::Bucket::Name

Description : (Obligatoire) Nom du compartiment Amazon S3 dans lequel le rapport sera chargé.

Modèle autorisé : `^[0-9a-z][a-z0-9\-\.\.]{3,63}$`

- S3 BucketOwnerAccount

Type : chaîne

Description : (Facultatif) Le Compte AWS propriétaire du compartiment Amazon S3. Spécifiez ce paramètre si le compartiment Amazon S3 appartient à un autre compartimentCompte AWS, sinon vous pouvez laisser ce paramètre vide.

Modèle autorisé : `^$|^[\0-9]{12,13}$`

- S3 BucketOwnerRoleArn

Type : `AWS::IAM::Role::Arn`

Description : (Facultatif) L'ARN d'un rôle IAM autorisé à décrire le compartiment Amazon S3 et à Compte AWS bloquer la configuration de l'accès public si le compartiment se trouve dans un autreCompte AWS. Si ce paramètre n'est pas spécifié, le runbook utilise l'utilisateur `AutomationAssumeRole` ou l'utilisateur IAM qui démarre ce runbook (s'il n'`AutomationAssumeRole`est pas spécifié). Consultez la section relative aux autorisations requises dans la description du runbook.

Modèle autorisé : `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[\0-9]{12,13}:role/.*$`

- S3 BucketPrefix

Type : chaîne

Description : (Facultatif) Le préfixe du chemin dans Amazon S3 pour le stockage des résultats.

Modèle autorisé : `^[a-zA-Z0-9][-.\/a-zA-Z0-9]{0,255}$|^$`

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

Exemple de politique IAM pour le rôle Automation Assume

```
{
  "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"
  }
]
}

```

## Instructions

1. Accédez au [AWSPremiumSupport-DDoS ResiliencyAssessment](#) dans la AWS Systems Manager console.
2. Sélectionnez Exécuter l'automatisation
3. Pour les paramètres d'entrée, entrez ce qui suit :
  - AutomationAssumeRole (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- AssessmentType (Facultatif) :

Détermine le type de ressources à évaluer pour l'évaluation de la résilience DDoS. Par défaut, le runbook évalue les ressources mondiales et régionales.

- S3 BucketName (obligatoire) :

Nom du compartiment Amazon S3 dans lequel enregistrer le rapport d'évaluation au format HTML.

- S3 BucketOwner (facultatif) :

L'Compte AWSID du compartiment Amazon S3 pour la vérification de propriété.

L'Compte AWSID est obligatoire si le rapport doit être publié dans un compartiment Amazon S3 multi-comptes et facultatif si le compartiment Amazon S3 se trouve dans le même compartiment Compte AWS que le lancement de l'automatisation.

- S3 BucketPrefix (facultatif) :

Tout préfixe pour le chemin dans Amazon S3 pour le stockage des résultats.

**Input parameters**

<p><b>AutomationAssumeRole</b> (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Select an existing IAM Role</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">ssm-admin arn:aws:iam::[redacted]:role/ssm-admin</div> <div style="text-align: right; margin-top: 5px;">↻</div>	<p><b>ResourceType</b> (Required) Determines the type of resources to be evaluated for DDoS resiliency assessment. By default, the runbook will evaluate both global and regional resources.</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Global and Regional Resources</div>
<p><b>S3BucketName</b> (Required) The name of the Amazon S3 bucket to save the assessment report in HTML format.</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Select an existing S3 Bucket</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">[redacted]</div> <div style="text-align: right; margin-top: 5px;">↻</div>	<p><b>S3BucketOwner</b> (Required) The Account ID of the Amazon S3 bucket for ownership verification.</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">[redacted]</div>
<p><b>S3BucketPrefix</b> (Optional) Any prefix for the path inside Amazon S3 for storing the results. Example path with prefix: S3://&lt;BucketName&gt;/&lt;Prefix&gt;</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">String</div>	

4. Sélectionnez Exécuter.

5. L'automatisation démarre.

6. Le document exécute les étapes suivantes :

- CheckShieldAdvancedState:

Vérifie si le compartiment Amazon S3 spécifié dans le « S3 BucketName » autorise les autorisations d'accès anonymes ou publiques en lecture ou en écriture, si le chiffrement au repos est activé sur le compartiment et si l'Compte AWSidentifiant fourni dans BucketOwner « S3 » est le propriétaire du compartiment Amazon S3.

- S3 BucketSecurityChecks :

Vérifie si le compartiment Amazon S3 spécifié dans le « S3 BucketName » autorise les autorisations d'accès anonymes ou publiques en lecture ou en écriture, si le chiffrement au repos est activé sur le compartiment et si l'Compte AWSidentifiant fourni dans BucketOwner « S3 » est le propriétaire du compartiment Amazon S3.

- BranchOnShieldAdvancedStatus:

Les succursales documentent les étapes en fonction du statut de l'AWS Shield Advancedabonnement et/ou du statut de propriétaire du compartiment Amazon S3.

- ShieldAdvancedConfigurationReview:

Révisé les configurations Shield Advanced pour s'assurer que le minimum de détails requis est présent. Par exemple : l'équipe IAM Access for AWS Shield Response Team (SRT), les détails de la liste de contacts et le statut d'engagement proactif de la SRT.

- ListShieldAdvancedProtections:

Répertorie les ressources protégées par le Shield et crée un groupe de ressources protégées pour chaque service.

- BranchOnResourceTypeAndCount:

Les branches documentent les étapes en fonction de la valeur du paramètre Resource Type et du nombre de ressources globales protégées par le Shield.

- ReviewGlobalResources:

Examine les ressources mondiales protégées par Shield Advanced, telles que les zones hébergées Route 53, CloudFront les distributions et les accélérateurs mondiaux.

- BranchOnResourceType:

Les branches documentent les étapes en fonction des types de ressources sélectionnés, qu'ils soient mondiaux, régionaux ou les deux.

- ReviewRegionalResources:

Examine les ressources régionales protégées par Shield Advanced, telles que les équilibreurs de charge d'application, les équilibreurs de charge réseau, les équilibreurs de charge classiques, les instances Amazon Elastic Compute Cloud (Amazon EC2) (adresses IP élastiques).

- SendReportToS3 :

Télécharge les détails du rapport d'évaluation DDoS dans le compartiment Amazon S3.

7. Une fois terminé, l'URI du fichier HTML du rapport d'évaluation est fourni dans le compartiment Amazon S3 :

Lien vers la console S3 et URI Amazon S3 pour le rapport sur l'exécution réussie du runbook

**▼ Outputs**

SendReportToS3.AssessmentReportS3ConsoleUrl  
[https://s3.console.aws.amazon.com/s3/object/ddos-readiness-review?region=us-east-1&prefix=ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24\\_04.08.37.html](https://s3.console.aws.amazon.com/s3/object/ddos-readiness-review?region=us-east-1&prefix=ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html)

SendReportToS3.AssessmentReportS3Uri  
[S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24\\_04.08.37.html](S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html)

---

**Execution status**

Overall status 🟢 Success	All executed steps 9	# Succeeded 9
# Failed 0	# Cancelled 0	# TimedOut 0

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

### AWSdocumentation de service

- [AWS Shield Advanced](#)

## Amazon SNS

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Simple Notification Service. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWS-EnableSNSTopicDeliveryStatusLogging](#)



- [AWSConfigRemediation-EncryptSNSTopic](#)
- [AWS-PublishSNSNotification](#)

## AWS-EnableSNSTopicDeliveryStatusLogging

### Description

Le `AWS-EnableSNSTopicDeliveryStatusLogging` runbook configure la journalisation de l'état de livraison pour un HTTP point de terminaison Amazon Data Firehose, Lambda ou Amazon Simple Platform application Queue Service (Amazon SQS). Cela permet à Amazon SNS de consigner les alertes ayant échoué et un échantillon de pourcentage de notifications d'alerte réussies envoyées à Amazon. CloudWatch Si la journalisation de l'état de livraison est déjà configurée pour le sujet, le runbook remplace la configuration existante par les nouvelles valeurs que vous spécifiez pour les paramètres d'entrée.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- EndpointType

Type : chaîne

Valeurs valides :

- HTTP
- Firehose
- Lambda
- Application
- SQS

Description : (Obligatoire) Type de point de terminaison de rubrique Amazon SNS pour lequel vous souhaitez enregistrer les messages de notification d'état de livraison.

- TopicArn

Type : chaîne

Description : (Obligatoire) L'ARN de la rubrique Amazon SNS pour laquelle vous souhaitez configurer la journalisation de l'état de livraison.

- SuccessFeedbackRoleArn

Type : chaîne

Description : (Obligatoire) L'ARN du rôle IAM utilisé par Amazon SNS pour envoyer les journaux des messages de notification réussis. CloudWatch

- SuccessFeedbackSampleRate

Type : chaîne

Valeurs valides : 0 à 100

Description : (Obligatoire) Pourcentage de messages réussis à échantillonner pour la rubrique Amazon SNS spécifiée.

- FailureFeedbackRoleArn

Type : chaîne

Description : (Obligatoire) L'ARN du rôle IAM utilisé par Amazon SNS pour envoyer les journaux des messages de notification d'échec. CloudWatch

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

## Étapes de document

- `aws:executeAwsApi`- Applique la valeur du `SuccessFeedbackRoleArn` paramètre à la rubrique Amazon SNS.
- `aws:executeAwsApi`- Applique la valeur du `SuccessFeedbackSampleRate` paramètre à la rubrique Amazon SNS.
- `aws:executeAwsApi`- Applique la valeur du `FailureFeedbackRoleArn` paramètre à la rubrique Amazon SNS.
- `aws:executeScript`- Confirme que l'enregistrement du statut de livraison est activé dans la rubrique Amazon SNS.

## Sorties

`VerifyDeliveryStatusLoggingEnabled`. `GetTopicAttributesResponse` - Réponse des opérations de `GetTopicAttributes` l'API.

`VerifyDeliveryStatusLoggingEnabled`. `VerifyDeliveryStatusLoggingEnabled` - Message indiquant la réussite de la vérification de l'enregistrement de l'état de livraison.

## **AWSConfigRemediation-EncryptSNSTopic**

### Description

Le `AWSConfigRemediation-EncryptSNSTopic` runbook active le chiffrement sur la rubrique Amazon Simple Notification Service (Amazon SNS) que vous spécifiez à l'aide d'une clé gérée par

le client AWS Key Management Service (AWS KMS). Ce runbook ne doit être utilisé que comme référence pour garantir que vos sujets Amazon SNS sont chiffrés conformément aux meilleures pratiques de sécurité minimales recommandées. Nous recommandons de chiffrer plusieurs sujets avec différentes clés gérées par le client.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- KmsKeyArn

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) de la clé gérée par le AWS KMS client que vous souhaitez utiliser pour chiffrer la rubrique Amazon SNS.

- TopicArn

Type : chaîne

Description : (Obligatoire) L'ARN de la rubrique Amazon SNS que vous souhaitez chiffrer.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

#### Étapes de document

- `aws:executeAwsApi`- Chiffre la rubrique Amazon SNS que vous spécifiez dans le `TopicArn` paramètre.
- `aws:assertAwsResourceProperty`- Confirme que le chiffrement est activé dans la rubrique Amazon SNS.

## AWS - PublishSNSNotification

### Description

Publiez une notification sur Amazon SNS.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Message

Type : chaîne

Description : (Obligatoire) message à inclure dans la notification SNS.

- TopicArn

Type : chaîne

Description : (Obligatoire) ARN de la rubrique SNS pour publier la notification.

## Amazon SQS

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Simple Queue Service (Amazon SQS). Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

Rubriques

- [AWS-EnableSQSEncryption](#)

### **AWS-EnableSQSEncryption**

Description

Le `AWS-EnableSQSEncryption` runbook active le chiffrement au repos pour une file d'attente Amazon Simple Queue Service (Amazon SQS). Une file d'attente Amazon SQS peut être chiffrée avec des clés gérées Amazon SQS (SSE-SQS) ou AWS Key Management Service avec des clés gérées AWS KMS (SSE-KMS). La clé que vous attribuez à votre file d'attente doit avoir une politique clé qui inclut des autorisations pour tous les principaux autorisés à utiliser la file d'attente. Lorsque le chiffrement est activé, les demandes anonymes `SendMessage` et les `ReceiveMessage` demandes adressées à la file d'attente cryptée sont rejetées.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- QueueUrl

Type : chaîne

Description : (Obligatoire) URL de la file d'attente Amazon SQS sur laquelle vous souhaitez activer le chiffrement.

- KmsKeyId

Type : chaîne

Description : (Facultatif) La AWS KMS clé à utiliser pour le chiffrement. Cette valeur peut être un identifiant unique global, un ARN associé à un alias ou à une clé, ou un nom d'alias préfixé par « alias/ ». Vous pouvez également utiliser la clé AWS gérée en spécifiant l'alias aws/sqs.

- KmsDataKeyReusePeriodSeconds

Type : chaîne

Valeurs valides : 60-86400

Valeur par défaut : 300

Description : (Facultatif) Durée, en secondes, pendant laquelle une file d'attente Amazon SQS peut réutiliser une clé de données pour chiffrer ou déchiffrer des messages avant de réappeler. AWS KMS

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

### Étapes de document

- `SelectKeyType` (aws:branch) : branches basées sur la clé spécifiée.
- `PutAttributeSseKms` (aws :executeAwsApi) - Met à jour la file d'attente Amazon SQS afin d'utiliser la AWS KMS clé spécifiée pour le chiffrement.
- `PutAttributeSseSqs` (aws :executeAwsApi) - Met à jour la file d'attente Amazon SQS afin d'utiliser la clé par défaut pour le chiffrement.
- `VerifySqsEncryptionKms` (aws : assertAwsResource Propriété) - Vérifie que le chiffrement est activé dans la file d'attente Amazon SQS.
- `VerifySqsEncryptionDefault` (aws : assertAwsResource Propriété) - Vérifie que le chiffrement est activé dans la file d'attente Amazon SQS.

## Step Functions

AWS Systems Manager Automation fournit des runbooks prédéfinis pour AWS Step Functions (Step Functions). Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).



## Rubriques

- [AWS-EnableStepFunctionsStateMachineLogging](#)

# AWS-EnableStepFunctionsStateMachineLogging

## Description

Le `AWS-EnableStepFunctionsStateMachineLogging` runbook active ou met à jour la journalisation sur la machine AWS Step Functions d'état que vous spécifiez. Le niveau de journalisation minimum doit être défini sur `ALLERROR`, ou `FATAL`.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux, macOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `Niveau`

Type : chaîne

Valeurs valides : `ALL` | `ERROR` | `FATAL`

Description : (Obligatoire) URL de la file d'attente Amazon SQS sur laquelle vous souhaitez activer le chiffrement.

- LogGroupArn

Type : chaîne

Description : (Obligatoire) L'ARN du groupe de CloudWatch journaux Amazon Logs auquel vous souhaitez envoyer des journaux State Machine.

- StateMachineArn

Type : chaîne

Description : (Obligatoire) L'ARN de la machine à états à laquelle vous souhaitez activer la connexion.

- IncludeExecutionData

Type : booléen

Par défaut : false

Description : (Facultatif) Détermine si les données d'exécution sont incluses dans les journaux.

- TracingConfiguration

Type : booléen

Par défaut : false

Description : (Facultatif) Détermine si le AWS X-Ray suivi est activé.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- states:DescribeStateMachine
- states:UpdateStateMachine

## Étapes de document

- `EnableStepFunctionsStateMachineLogging` (`aws:executeAwsApi`)- Met à jour la machine à états spécifiée avec la configuration de journalisation spécifiée.
- `VerifyStepFunctionsStateMachineLoggingEnabled` (`aws:assertAwsResourceProperty`)- Vérifie que la journalisation a été activée pour la machine à états spécifiée.

## Sorties

- `EnableStepFunctionsStateMachineLogging.Response` - Réponse de l'appel `UpdateStateMachine` d'API.

# Systems Manager

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Systems Manager. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [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

### Description

Le `AWS-BulkDeleteAssociation` runbook vous permet de supprimer jusqu'à 50 associations de Systems Manager State Manager à la fois.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `AssociationIds`

Type : `StringList`

Description : (Obligatoire) Liste séparée par des virgules des identifiants des associations que vous souhaitez supprimer.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:DeleteAssociation`

### Étapes de document

- `aws:executeScript`- Supprime les associations que vous spécifiez dans le `AssociationIds` paramètre.

## AWS-BulkEditOpsItems

### Description

Le `AWS-BulkEditOpsItems` runbook vous permet de modifier le statut, la gravité, la catégorie ou la priorité de AWS Systems Manager OpsItems. Cette automatisation peut en modifier un maximum de 50 OpsItems à la fois.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre

nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- **Catégorie**

Type : chaîne

Valeurs valides :

- Disponibilité
- Coût
- Pas de modification
- Performance
- Récupération
- Sécurité

Par défaut : aucune modification

Description : (Facultatif) La nouvelle catégorie que vous souhaitez spécifier pour les modifications OpsItems.

- **OpsItemIds**

Type : StringList

Description : (Obligatoire) Liste séparée par des virgules des OpsItems identifiants que vous souhaitez modifier (par exemple, OI-xxxxxxxxxxxxx, OI-xxxxxxxxxxxxx).

- **Priorité**

Type : chaîne

Valeurs valides :

- Pas de modification
- 1
- 2
- 3
- 4
- 5

Par défaut : aucune modification

Description : (Facultatif) L'importance de l'édition OpsItems par rapport OpsItems aux autres éléments du système.

- Sévérité

Type : chaîne

Valeurs valides :

- Pas de modification
- 1
- 2
- 3
- 4

Par défaut : aucune modification

Description : (Facultatif) La gravité de la modification OpsItems.

- WaitTimeBetweenEditsInSecs

Type : chaîne

Valeurs valides : 0,0-2,0

Valeur par défaut : 0,8

Description : (Facultatif) Le temps d'attente de l'automatisation entre deux appels à l'UpdateOpsItemsopération.

- Statut

Type : chaîne

Valeurs valides :

- InProgress
- Pas de modification
- Ouvrir

Par défaut : aucune modification

Description : (Facultatif) Le nouveau statut de la version modifiée OpsItems.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

### Étapes de document

- `aws:executeScript`- Modifie ce OpsItems que vous avez spécifié dans le `OpsItemIds` paramètre en fonction des valeurs que vous spécifiez pour les `Status` paramètres `CategoryPriority`, `Severity`, et.

## AWS-BulkResolveOpsItems

### Description

Le `AWS-BulkResolveOpsItems` runbook résout les problèmes AWS Systems Manager OpsItems qui correspondent au filtre que vous spécifiez. Vous pouvez également spécifier un `OpsItemId` à ajouter à la résolution à OpsItems l'aide du `OpsInsightsId` paramètre. Si vous spécifiez une valeur pour le `S3BucketName` paramètre, un résumé des résultats est envoyé au compartiment Amazon Simple Storage Service (Amazon S3). Pour recevoir une notification une fois que le résumé des résultats a été envoyé au compartiment Amazon S3, spécifiez une valeur pour le `SnsTopicArn` paramètre. Cette automatisation permettra d'en résoudre un maximum de 1 000 OpsItems à la fois.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire



## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Filtres

Type : chaîne

Description : (Obligatoire) Les paires clé-valeur de filtres permettant de renvoyer le résultat que OpsItems vous souhaitez résoudre. Par exemple, [{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]. Pour en savoir plus sur les options disponibles pour filtrer OpsItems les réponses, consultez [OpsItemFilters](#) la référence des AWS Systems Manager API.

- OpsInsightId

Type : chaîne

Description : (Facultatif) L'identifiant de ressource associé que vous souhaitez ajouter est résolu OpsItems.

- S3 BucketName

Type : chaîne

Description : (Facultatif) Nom du compartiment Amazon S3 auquel vous souhaitez envoyer le résumé des résultats.

- SnsMessage

Type : chaîne

Description : (Facultatif) La notification que vous souhaitez qu'Amazon Simple Notification Service (Amazon SNS) envoie une fois l'automatisation terminée.

- SnsTopicArn

Type : chaîne

Description : (Facultatif) L'ARN de la rubrique Amazon SNS que vous souhaitez notifier lorsque le résumé des résultats a été envoyé à Amazon S3.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `s3:GetBucketAcl`
- `s3:PutObject`
- `sns:Publish`
- `ssm:DescribeOpsItems`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

### Étapes de document

- `aws:executeScript`- Rassemble et résout les problèmes `OpsItems` en fonction des filtres que vous spécifiez. Si vous avez spécifié une valeur pour le `OpsInsightId` paramètre, la valeur est ajoutée en tant que ressource associée.
- `aws:executeScript`- Si vous avez spécifié une valeur pour le `S3BucketName` paramètre, un résumé des résultats est ensuite envoyé au compartiment Amazon S3.
- `aws:executeScript`- Si vous avez spécifié une valeur pour le `SnsTopicArn` paramètre, une notification est envoyée à la rubrique Amazon SNS une fois que le résumé des résultats a été envoyé à Amazon S3, y compris la valeur du `SnsMessage` paramètre si elle est spécifiée.

# AWS-ConfigureMaintenanceWindows

## Description

Le AWS-ConfigureMaintenanceWindows runbook vous permet d'activer ou de désactiver plusieurs fenêtres de maintenance de Systems Manager.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- MaintenanceWindows

Type : StringList

Description : (Obligatoire) Liste séparée par des virgules des identifiants des fenêtres de maintenance que vous souhaitez activer ou désactiver.

- MaintenanceWindowsStatus

Type : chaîne

Valeurs valides : « Vrai » | « Faux »

Par défaut : « False »

Description : (Obligatoire) Détermine si les fenêtres de maintenance sont activées ou désactivées. Spécifiez « True » pour activer les fenêtres de maintenance et « False » pour les désactiver.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

#### Étapes de document

- `aws:executeScript`- Recueille l'état des fenêtres de maintenance que vous spécifiez dans le `MaintenanceWindows` paramètre et active ou désactive les fenêtres de maintenance.

## AWS-CreateManagedLinuxInstance

### Description

Créez une instance EC2 pour Linux configurée pour Systems Manager.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

Linux

Paramètres

- `Amild`

Type : chaîne

Description : AMI ID (obligatoire) à utiliser pour lancer l'instance.

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- GroupName

Type : chaîne

Par défaut : SSM SecurityGroupForLinuxInstances

Description : (Obligatoire) nom du groupe de sécurité à créer.

- HttpTokens

Type : chaîne

Valeurs valides : facultatif | obligatoire

Par défaut : optionnel

Description : (Facultatif) IMDSv2 utilise des sessions basées sur des jetons. Définissez l'utilisation des jetons HTTP sur `optional` ou `required` pour déterminer si IMDSv2 est facultatif ou obligatoire.

- InstanceType

Type : chaîne

Par défaut : t2.medium

Description : (Obligatoire) type d'instance à lancer. La valeur par défaut est t2.medium.

- KeyPairName

Type : chaîne

Description : (Obligatoire) paire de clés à utiliser lors de la création de l'instance.

- RemoteAccessCidr

Type : chaîne

Par défaut : 0.0.0.0/0

Description : (Obligatoire) crée un groupe de sécurité avec le port SSH (plage de ports 22) ouvert pour les adresses IP spécifiées par CIDR (la valeur par défaut est 0.0.0.0/0). Si le groupe de sécurité existe déjà, il ne sera pas modifié et les règles ne changeront pas.

- RoleName

Type : chaîne

Par défaut : SSM ManagedInstanceProfileRole

Description : (Obligatoire) nom du rôle à créer.

- StackName

Type : chaîne

Par défaut : CreateManagedInstanceStack {{Automation:Execution\_ID}}

Description : (Facultatif) Spécifiez le nom de la pile utilisée par ce runbook

- SubnetId

Type : chaîne

Par défaut : Default

Description : (Obligatoire) la nouvelle instance sera déployée dans ce sous-réseau ou dans le sous-réseau par défaut si aucune valeur n'est spécifiée.

- VpcId

Type : chaîne

Par défaut : Default

Description : (Obligatoire) La nouvelle instance sera déployée dans cet Amazon Virtual Private Cloud (Amazon VPC) ou dans l'Amazon VPC par défaut si elle n'est pas spécifiée.

# AWS-CreateManagedWindowsInstance

## Description

Créez une instance EC2 pour une Windows Server instance configurée pour Systems Manager.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Windows

## Paramètres

### Paramètres

- Amild

Type : chaîne

Par défaut : `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

Description : AMI ID (obligatoire) à utiliser pour lancer l'instance.

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- GroupName

Type : chaîne

Par défaut : `SSM SecurityGroupForLinuxInstances`

Description : (Obligatoire) nom du groupe de sécurité à créer.

- `HttpTokens`

Type : chaîne

Valeurs valides : facultatif | obligatoire

Par défaut : optionnel

Description : (Facultatif) IMDSv2 utilise des sessions basées sur des jetons. Définissez l'utilisation des jetons HTTP sur `optional` ou `required` pour déterminer si IMDSv2 est facultatif ou obligatoire.

- `InstanceType`

Type : chaîne

Par défaut : `t2.medium`

Description : (Obligatoire) type d'instance à lancer. La valeur par défaut est `t2.medium`.

- `KeyPairName`

Type : chaîne

Description : (Obligatoire) paire de clés à utiliser lors de la création de l'instance.

- `RemoteAccessCidr`

Type : chaîne

Par défaut : `0.0.0.0/0`

Description : (Obligatoire) crée un groupe de sécurité avec le port RDP (plage de ports 3389) ouvert pour les adresses IP spécifiées par CIDR (la valeur par défaut est `0.0.0.0/0`). Si le groupe de sécurité existe déjà, il ne sera pas modifié et les règles ne changeront pas.

- `RoleName`

Type : chaîne

Par défaut : `SSM ManagedInstanceProfileRole`



Description : (Obligatoire) nom du rôle à créer.

- StackName

Type : chaîne

Par défaut : CreateManagedInstanceStack {{Automation:Execution\_ID}}

Description : (Facultatif) Spécifiez le nom de la pile utilisée par ce runbook

- SubnetId

Type : chaîne

Par défaut : Default

Description : (Obligatoire) la nouvelle instance sera déployée dans ce sous-réseau ou dans le sous-réseau par défaut si aucune valeur n'est spécifiée.

- VpcId

Type : chaîne

Par défaut : Default

Description : (Obligatoire) La nouvelle instance sera déployée dans cet Amazon Virtual Private Cloud (Amazon VPC) ou dans l'Amazon VPC par défaut si elle n'est pas spécifiée.

## **AWSConfigRemediation-EnableCWLoggingForSessionManager**

Description

Le `AWSConfigRemediation-EnableCWLoggingForSessionManager` runbook permet aux AWS Systems Manager sessions du gestionnaire de session (gestionnaire de session) de stocker les journaux de sortie dans un groupe de journaux Amazon CloudWatch (CloudWatch).

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

## Amazon

### Plateformes

Linux macOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- DestinationLogGroup

Type : chaîne

Description : (Obligatoire) Nom du groupe de CloudWatch journaux.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:UpdateDocument
- ssm:CreateDocument
- ssm:UpdateDefaultDocumentVersion
- ssm:DescribeDocument

### Étapes de document

- aws:executeScript- Accepte le groupe de CloudWatch journaux pour mettre à jour le document qui stocke les préférences des journaux de sortie de session du Gestionnaire de session, ou en crée un s'il n'existe pas.

## AWS-ExportOpsDataToS3

### Description

Ce runbook extrait une liste de OpsData résumés dans AWS Systems Manager Explorer et les exporte vers un objet situé dans un compartiment Amazon Simple Storage Service (Amazon S3) spécifié.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- columnFields

Type : StringList

Description : (Obligatoire) Champs de colonne à écrire dans le fichier de sortie.

- filtres

Type : chaîne

Description : (Facultatif) Filtres pour la getOpsSummary demande.

- **resultAttribute**

Type : chaîne

Description : (Facultatif) L'attribut de résultat de la getOpsSummary demande.

- **s3 BucketName**

Type : chaîne

Description : (obligatoire) compartiment S3 où vous souhaitez télécharger le fichier de sortie.

- **snsSuccessMessage**

Type : chaîne

Description : (Facultatif) Message à envoyer lorsque le runbook sera terminé.

- **snsTopicArn**

Type : chaîne

Description : (Obligatoire) ARN de la rubrique Amazon Simple Notification Service (Amazon SNS) pour avertir lorsque le téléchargement est terminé.

- **syncName**

Type : chaîne

Description : (Facultatif) Nom de la synchronisation des données de la ressource.

## Étapes de document

getOpsSummaryÉtape — Récupère jusqu'à 5 000 résumés d'opérations à exporter dans un fichier CSV dès maintenant.

## Sorties

OpsData object — Si le runbook s'exécute correctement, vous trouverez l' OpsData objet exporté dans votre compartiment S3 cible.

## **AWS-ExportPatchReportToS3**

### Description

Ce runbook extrait les listes des données récapitulatives et des détails des correctifs dans le gestionnaire de AWS Systems Manager correctifs et les exporte vers des fichiers .csv dans un compartiment Amazon Simple Storage Service (Amazon S3) spécifié.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `assumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui exécute ce document.

- `s3 BucketName`

Type : chaîne

Description : (Obligatoire) Le compartiment S3 dans lequel vous souhaitez télécharger le fichier de sortie.

- `snsTopicArn`

Type : chaîne

Description : (Facultatif) La rubrique Amazon Simple Notification Service (Amazon SNS) intitulée Amazon Resource Name (ARN) doit être notifiée lorsque le téléchargement est terminé.

- `snsSuccessMessage`

Type : chaîne

Description : (Facultatif) Texte du message à envoyer à la fin du runbook.

- targets

Type : chaîne

Description : (Obligatoire) L'ID de l'instance ou un caractère générique (\*) pour indiquer s'il convient de signaler les données de correctif pour une instance spécifique ou pour toutes les instances.

## Étapes de document

ExportReportStep — L'action de cette étape dépend de la valeur du targets paramètre. S'il targets est au format deinstanceids=\*, l'étape permet de récupérer jusqu'à 10 000 résumés de correctifs pour les instances de votre compte et d'exporter les données vers un fichier .csv.

S'il targets est au formatinstanceids=<instance-id>, l'étape récupère à la fois le résumé des correctifs et tous les correctifs pour l'instance spécifiée dans votre compte et les exporte vers un fichier .csv.

## Sorties

PatchSummaryObjet /Patches : si le runbook s'exécute correctement, l'objet du rapport de correctif exporté est téléchargé dans votre compartiment S3 cible.

# AWS-SetupInventory

## Description

Créez une association Systems Manager Inventory pour une ou plusieurs instances gérées. Le système recueille les métadonnées à partir de vos instances selon la planification dans l'association. Pour plus d'informations, consultez [AWS Systems Manager Inventaire](#).

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

Propriétaire

## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- Applications

Type : chaîne

Par défaut : Enabled

Description : (Facultatif) collectez des métadonnées sur les applications installées.

- AssociatedDocName

Type : chaîne

Par défaut : AWS-GatherSoftwareInventory

Description : (Facultatif) Nom du runbook utilisé pour collecter l'inventaire à partir de l'instance gérée.

- AssociationName

Type : chaîne

Description : (Facultatif) nom de l'association d'inventaire qui sera attribuée à l'instance.

- AssocWaitTime

Type : chaîne

Valeur par défaut : PT5M

Description : (Facultatif) durée pendant laquelle la collecte de l'inventaire doit s'interrompre l'association lorsque l'heure de début de l'association d'inventaire est atteinte. L'heure utilise le format ISO 8601.

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `AwsComponents`

Type : chaîne

Par défaut : Enabled

Description : (Facultatif) Collectez des métadonnées pour AWS des composants tels que amazon-ssm-agent.

- `CustomInventory`

Type : chaîne

Par défaut : Enabled

Description : (Facultatif) collectez des métadonnées d'inventaire personnalisées.

- `Dépôt de`

Type : chaîne

Description : (Facultatif) collectez des métadonnées sur les fichiers de vos instances.

Pour plus d'informations sur la collecte de ce type de données d'inventaire, voir

[Utilisation de l'inventaire des fichiers et du registre Windows](#). Nécessite SSMAgent

version 2.2.64.0 ou ultérieure. Exemple 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`

Type : chaîne

Par défaut : Enabled

Description : (Facultatif) collectez des informations supplémentaires sur l'instance, y compris le modèle d'UC, la vitesse et le nombre de cœurs, pour n'en citer que quelques-unes.



- **InstanceIds**

Type : chaîne

Par défaut : \*

Description : (obligatoire) Instances EC2 que vous souhaitez inventorier.

- **LambdaAssumeRole**

Type : chaîne

Description : (Facultatif) ARN du rôle qui autorise la fonction Lambda créée par Automation à effectuer des actions en votre nom. Si vous ne spécifiez pas cette valeur, un rôle transitoire est créé pour exécuter la fonction Lambda.

- **NetworkConfig**

Type : chaîne

Par défaut : Enabled

Description : (Facultatif) collectez des métadonnées sur les configurations réseau.

- **Sorties 3 BucketName**

Type : chaîne

Description : (Facultatif) Nom d'un compartiment Amazon S3 dans lequel vous souhaitez écrire les données du journal d'inventaire.

- **Sorties 3 KeyPrefix**

Type : chaîne

Description : (Facultatif) Un préfixe de clé Amazon S3 (sous-dossier) dans lequel vous souhaitez écrire les données du journal d'inventaire.

- **OutputS3Region**

Type : chaîne

Description : (Facultatif) Le nom de l' Région AWS endroit où se trouve l'Amazon S3.

- **Planificateur**

Type : chaîne

Par défaut : cron(0 \*/30 \* \* \* ? \*)

Description : (Facultatif) expression cron pour la planification de l'association d'inventaire. La valeur par défaut est toutes les 30 minutes.

- Services

Type : chaîne

Par défaut : Enabled

Description : (Facultatif, système d'exploitation Windows uniquement, nécessite SSMAgent version 2.2.64.0 ou ultérieure) collecte de données pour les configurations de service.

- WindowsRegistry

Type : chaîne

Description : (Facultatif) collecte des métadonnées sur les clés de registre Microsoft Windows. Pour plus d'informations sur la collecte de ce type de données d'inventaire, voir [Utilisation de l'inventaire des fichiers et du registre Windows](#). Nécessite SSM Agent version 2.2.64.0 ou ultérieure. Exemple : [{"Chemin » » HKEY\_CURRENT\_CONFIG \ System », "Recursive » :true}, {"Chemin » » HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Amazon \ «, " « : [" aminame "]}] MachinelImage ValueNames

- WindowsRoles

Type : chaîne

Par défaut : Enabled

Description : (Facultatif) collecte des informations sur les rôles Windows sur l'instance. S'applique aux systèmes d'exploitation Windows uniquement. Nécessite SSMAgent version 2.2.64.0 ou ultérieure.

- WindowsUpdates

Type : chaîne

Par défaut : Enabled

Description : (Facultatif) collecte des données sur toutes les mises à jour Windows de l'instance.

## AWS-SetupManagedInstance

### Description

Configurez une instance dotée d'un rôle AWS Identity and Access Management (IAM) pour accéder à Systems Manager.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- InstanceId

Type : chaîne

Description : (obligatoire) ID de l'instance EC2 à configurer.

- LambdaAssumeRole

Type : chaîne

Description : (Facultatif) ARN du rôle qui autorise la fonction Lambda créée par Automation à effectuer des actions en votre nom. Si vous ne spécifiez pas cette valeur, un rôle transitoire est créé pour exécuter la fonction Lambda.

- RoleName

Type : chaîne

Par défaut : SSM RoleForManagedInstance

Description : (facultatif) nom du rôle IAM de l'instance EC2. Si ce rôle n'existe pas, il est créé. Lorsque vous spécifiez cette valeur, vérifiez que le rôle contient la politique ManagedInstanceCore gérée par AmazonSSM.

## AWS-SetupManagedRoleOnEC2Instance

Description

Configurez une instance avec le rôle IAM RoleForManagedInstance géré par SSM pour l'accès à Systems Manager.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre

nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- InstanceId

Type : chaîne

Description : (obligatoire) ID de l'instance EC2 à configurer.

- LambdaAssumeRole

Type : chaîne

Description : (Facultatif) ARN du rôle qui autorise la fonction Lambda créée par Automation à effectuer des actions en votre nom. Si vous ne spécifiez pas cette valeur, un rôle transitoire est créé pour exécuter la fonction Lambda.

- RoleName

Type : chaîne

Par défaut : SSM RoleForManagedInstance

Description : (facultatif) nom du rôle IAM de l'instance EC2. Si ce rôle n'existe pas, il est créé. Lorsque vous spécifiez cette valeur, vérifiez que le rôle contient la politique ManagedInstanceCore gérée par AmazonSSM.

## AWSSupport-TroubleshootManagedInstance

### Description

Le AWSSupport-TroubleshootManagedInstance runbook vous aide à déterminer pourquoi une instance Amazon Elastic Compute Cloud (Amazon EC2) n'est pas signalée comme étant gérée par AWS Systems Manager. Ce manuel passe en revue la configuration VPC de l'instance, y compris les règles du groupe de sécurité, les points de terminaison VPC, les règles de la liste de contrôle d'accès réseau (ACL) et les tables de routage. Cela confirme également qu'un profil d'instance AWS Identity and Access Management (IAM) contenant les autorisations requises est attaché à l'instance.

#### Important

Ce manuel d'automatisation n'évalue pas les règles IPv6.

## [Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- InstanceId

Type : chaîne

Description : (Obligatoire) L'ID de l'instance Amazon EC2 qui n'est pas signalée comme étant gérée par Systems Manager.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

## Étapes de document

- `aws:executeScript`- Rassemble le numéro `PingStatus` de l'instance.
- `aws:branch`- Branches basées sur le fait que l'instance fournit déjà des rapports tels que gérés par Systems Manager.
- `aws:executeAwsApi`- Recueille des informations sur l'instance, y compris la configuration du VPC.
- `aws:executeScript`- Le cas échéant, collecte des informations supplémentaires relatives aux points de terminaison VPC qui ont été déployés pour être utilisés avec Systems Manager, et confirme que les groupes de sécurité attachés au point de terminaison VPC autorisent le trafic entrant sur le port TCP 443 depuis l'instance.
- `aws:executeScript`- Vérifie si la table de routage autorise le trafic vers le point de terminaison du VPC ou vers les points de terminaison publics de Systems Manager.
- `aws:executeScript`- Vérifie si les règles ACL du réseau autorisent le trafic vers le point de terminaison du VPC ou vers les points de terminaison publics de Systems Manager.
- `aws:executeScript`- Vérifie si le trafic sortant vers le point de terminaison du VPC ou les points de terminaison publics de Systems Manager est autorisé par le groupe de sécurité associé à l'instance.
- `aws:executeScript`- Vérifie si le profil d'instance attaché à l'instance inclut une politique gérée fournissant les autorisations requises.

- `aws:branch`- Branches basées sur le système d'exploitation de l'instance.
- `aws:executeScript`- Fournit une référence au script `ssmagent-toolkit-linux` shell.
- `aws:executeScript`- Fournit une référence au `ssmagent-toolkit-windows` PowerShell script.
- `aws:executeScript`- Génère le résultat final pour l'automatisation.
- `aws:executeScript`- Si `PingStatus` l'instance `estOnline`, indique que l'instance est déjà gérée par Systems Manager.

## AWSSupport-TroubleshootPatchManagerLinux

### Description

Le `AWSSupport-TroubleshootPatchManagerLinux` runbook permet de résoudre les problèmes courants susceptibles de provoquer l'échec d'un correctif sur les nœuds gérés basés sur Linux à l'aide de la AWS Systems Manager fonctionnalité « Patch Manager ». L'objectif principal de ce manuel est d'identifier la cause première de l'échec de la commande de correctif et de suggérer un plan de correction.

### Comment fonctionne-t-il ?

Le `AWSSupport-TroubleshootPatchManagerLinux` runbook prend en compte le couple ID d'instance et ID de commande que vous avez fourni pour le dépannage. Si aucun ID de commande n'est fourni, il sélectionne la dernière commande de correctif ayant échoué au cours des 30 derniers jours sur l'instance fournie. Après avoir vérifié l'état de la commande, le respect des conditions requises et la distribution du système d'exploitation, le runbook télécharge et exécute un package d'analyse de journaux. Le résultat inclut la cause première du problème ainsi que les mesures nécessaires pour le résoudre.

### Types de document

Automatisation

Propriétaire

Amazon

Plateformes

- Amazon Linux 2 et 2023



- Red Hat Enterprise Linux 8.X et 9.X
- Centos 8.X et 9.X
- SUSE 15.X

## Paramètres

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

## Instructions

Pour configurer l'automatisation, procédez comme suit :

1. Accédez au [AWSSupport-TroubleshootPatchManagerLinux](#) dans la AWS Systems Manager console.
2. Sélectionnez `Execute automation` (Exécuter l'automatisation).
3. Pour les paramètres d'entrée, entrez ce qui suit :
  - `InstanceId` (Obligatoire) :  
  
Utilisez le sélecteur d'instance interactif pour choisir l'ID du nœud géré par SSM basé sur Linux (Amazon Elastic Compute Cloud (Amazon EC2) ou serveur Hybrid Activated) contre lequel la commande de correctif a échoué, ou entrez manuellement l'ID de l'instance gérée par SSM.
  - `AutomationAssumeRole` (Facultatif) :

Entrez l'ARN du rôle IAM qui permet à Automation d'effectuer des actions en votre nom. Si aucun rôle n'est spécifié, Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- **RunCommandId (Facultatif) :**

Entrez l'ID de commande ayant échoué du `AWS-RunPatchBaseline` document. Si vous ne fournissez pas d'ID de commande, le runbook recherchera la dernière commande de correctif ayant échoué au cours des 30 derniers jours sur l'instance sélectionnée.

**Input parameters**

---

**InstanceId**  
(Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.  
 Show interactive instance picker

i-0[REDACTED]

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

Choose an option

**RunCommandId**  
(Optional) Failed Run Command ID of AWS-RunPatchBaseline. If not provided, we look for the latest unsuccessful execution of AWS-RunPatchBaseline for the instance and evaluate it. To confirm the command ID, look under Command History tab in the Run Command Console under AWS Systems Manager.

42[REDACTED]e

4. Sélectionnez Exécuter.

5. L'automatisation démarre.

6. Le document exécute les étapes suivantes :

- **CheckConcurrency:**

Garantit qu'il n'y a qu'une seule exécution de ce runbook ciblant la même instance. Si le runbook trouve une autre exécution en cours ciblant la même instance, il renvoie une erreur et se termine.

- **ValidateCommandIdentifiant :**

Valide si l'ID de commande fourni, en tant que paramètre d'entrée, a été exécuté pour le document `AWS-RunPatchBaseline SSM`. Si aucun ID de commande n'est fourni, le runbook prendra en compte le dernier échec d'exécution survenu `AWS-RunPatchBaseline` au cours des 30 derniers jours sur l'instance sélectionnée.

- **BranchOnCommandStatus:**

Confirme que l'état de la commande fournie est un échec. Dans le cas contraire, le runbook met fin à l'exécution et génère un rapport indiquant que la commande fournie a été exécutée avec succès.

- **VerifyPrerequisites:**

Confirmez que les prérequis mentionnés ci-dessus sont remplis.

- **GetPlatformDetails:**

Récupère la distribution et la version du système d'exploitation (OS).

- **GetDownloadAdresse URL :**

Récupère l'URL de téléchargement du package PatchManager Log Analyzer.

- **EvaluatePatchManagerLogs:**

Télécharge et exécute le package python PatchManager Log Analyzer sur l'instance pour évaluer le fichier journal.

- **GenerateReport:**

Génère un rapport final sur l'exécution du runbook qui inclut le problème identifié et la solution suggérée.

7. Une fois terminé, consultez la section Sorties pour obtenir les résultats détaillés de l'exécution :

```

▼ Outputs

GenerateReportOutput
Starting 'python3 main.py i-0[REDACTED] 3e016680-82f4-45f4-845c-aa4685b4fab0 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-aa4685b4fab0/awssrunShellScript/PatchLinux/stdout is :

Unable to download payload: https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz.failed to run commands: exit status 156

[ SOLUTION ] :
-----
Here are some suggestions to troubleshoot the issue:

Possible reasons for the above error are :

1. Network connectivity issue while accessing the s3 service endpoint from the instance to download the payload.
2. Instance doesn't have the required permissions to access the specified Amazon Simple Storage Service (Amazon S3) bucket.
3. No space left on the Instance.

To resolve this, ensure network connectivity to S3 endpoint from the instance. For more details, see information about required access to S3 buckets for Patch Manager in https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent-minimum-s3-permissions.

For testing purpose, try to manually access the above payload URL using curl or wget from within Instance. Command to run:

curl https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz --output payload.tar.gz

```

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)
- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

# AWSSupport-TroubleshootSessionManager

## Description

Le `AWSSupport-TroubleshootSessionManager` runbook vous aide à résoudre les problèmes courants qui vous empêchent de vous connecter à des instances Amazon Elastic Compute Cloud (Amazon EC2) gérées à l'aide du gestionnaire de session. Le gestionnaire de session est une fonctionnalité de AWS Systems Manager. Ce runbook vérifie les points suivants :

- Vérifie si l'instance est en cours d'exécution et génère des rapports tels que gérés par Systems Manager.
- Exécute le `AWSSupport-TroubleshootManagedInstance` runbook si l'instance n'est pas signalée comme étant gérée par Systems Manager.
- Vérifie la version de l'agent SSM installée sur l'instance.
- Vérifie si un profil d'instance contenant une politique recommandée AWS Identity and Access Management (IAM) pour le gestionnaire de session est attaché à l'instance Amazon EC2.
- Collecte les journaux de l'agent SSM à partir de l'instance.
- Analyse les préférences de votre gestionnaire de session.
- Exécute le `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook pour analyser la connectivité de l'instance aux points de terminaison de Session Manager AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3) et CloudWatch Amazon Logs (Logs). CloudWatch

## Considérations

- Les nœuds gérés hybrides ne sont pas pris en charge.
- Ce runbook vérifie uniquement si une politique IAM gérée recommandée est attachée au profil d'instance. Il n'analyse pas l'IAM ni AWS KMS les autorisations contenues dans votre profil d'instance.

### Important

Le `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook utilise [VPC Reachability Analyzer](#) pour analyser la connectivité réseau entre une source et un point de

terminaison de service. Vous êtes facturé par analyse effectuée entre une source et une destination. Pour plus de détails, consultez la section [Tarification d'Amazon VPC](#).

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- InstanceId

Type : chaîne

Description : (Obligatoire) L'ID de l'instance Amazon EC2 à laquelle vous ne pouvez pas vous connecter à l'aide du gestionnaire de session.

- SessionPreferenceDocument

Type : chaîne

Par défaut : SSM- SessionManagerRunShell

Description : (Facultatif) Le nom de votre document de préférences de session. Si vous ne spécifiez pas de document de préférences de session personnalisé lors du démarrage des sessions, utilisez la valeur par défaut.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

1. `aws:waitForAwsResourceProperty`: attend jusqu'à 6 minutes que votre instance cible passe les vérifications de statut.
2. `aws:executeScript`: analyse le document des préférences de session.
3. `aws:executeAwsApi`: obtient l'ARN du profil d'instance attaché à votre instance.
4. `aws:executeAwsApi`: Vérifie si votre instance est signalée comme étant gérée par Systems Manager.
5. `aws:branch`: Branches selon que votre instance produit ou non des rapports tels que gérés par Systems Manager.
6. `aws:executeScript`: Vérifie si l'agent SSM installé sur votre instance prend en charge le gestionnaire de session.
7. `aws:branch`: Branches basées sur la plate-forme de votre instance pour collecter `ssm-cli` les logs.
8. `aws:runCommand`: collecte la sortie des journaux à `ssm-cli` partir d'une macOS instance Linux or.
9. `aws:runCommand`: collecte les résultats des journaux à `ssm-cli` partir d'une Windows instance.
10. `aws:executeScript`: analyse les `ssm-cli` journaux.
11. `aws:executeScript`: Vérifie si une politique IAM recommandée est attachée au profil d'instance.



12. `aws:branch`: Détermine s'il faut évaluer la connectivité des `ssmmessages` terminaux sur la base `ssm-cli` des journaux.
13. `aws:executeAutomation`: Évalue si l'instance peut se connecter à un `ssmmessages` point de terminaison.
14. `aws:branch`: Détermine s'il convient d'évaluer la connectivité du point de terminaison Amazon S3 en fonction `ssm-cli` des journaux et de vos préférences de session.
15. `aws:executeAutomation`: Évalue si l'instance peut se connecter à un point de terminaison Amazon S3.
16. `aws:branch`: Détermine s'il convient d'évaluer la connectivité des AWS KMS terminaux en fonction `ssm-cli` des journaux et de vos préférences de session.
17. `aws:executeAutomation`: Évalue si l'instance peut se connecter à un AWS KMS point de terminaison.
18. `aws:branch`: détermine s'il faut évaluer la connectivité CloudWatch des terminaux Logs en fonction `ssm-cli` des journaux et de vos préférences de session.
19. `aws:executeAutomation`: Évalue si l'instance peut se connecter à un point de terminaison CloudWatch Logs.
20. `aws:executeAutomation`: Exécute le `AWSsupport-TroubleshootManagedInstance` runbook.
21. `aws:executeScript`: Compile le résultat des étapes précédentes et produit un rapport.

## Sorties

- `generateReport.EvalReport`- Les résultats des vérifications effectuées par le runbook en texte brut.

## Tierce

AWS Systems Manager Automation fournit des runbooks prédéfinis pour les produits et services tiers. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-CreateJiraIssue](#)

- [AWS-CreateServiceNowIncident](#)
- [AWS-RunPacker](#)

## AWS-CreateJiraIssue

### Description

Création d'un problème de Jira.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AssigneeName

Type : chaîne

Description : (Facultatif) nom d'utilisateur de la personne à laquelle le problème doit être attribué.

- DueDate

Type : chaîne

Description : (Facultatif) Date d'échéance du problème au yyyy-mm-dd format.

- IssueDescription

Type : chaîne

Description : (Obligatoire) description détaillée du problème.

- IssueSummary

Type : chaîne

Description : (Obligatoire) bref résumé du problème.

- IssueTypeName

Type : chaîne

Description : (Obligatoire) nom du type de problème que vous souhaitez créer (par exemple, Task, sous-tâche, Bug, etc.).

- JiraURL

Type : chaîne

Description : (Obligatoire) URL de l'instance Jira.

- JiraUsername

Type : chaîne

Description : (Obligatoire) nom de l'utilisateur avec lequel le problème sera créé.

- PriorityName

Type : chaîne

Description : (Facultatif) nom de la priorité du problème.

- ProjectKey

Type : chaîne

Description : (Obligatoire) clé du projet dans lequel le problème doit être créé.

- SSM ParameterName

Type : chaîne

Description : (Obligatoire) nom d'un paramètre SSM chiffré contenant la clé d'API ou un mot de passe pour l'utilisateur Jira.

## Étapes de document

`aws:createStack`- Créez une CloudFormation pile pour créer le rôle et la fonction Lambda IAM.

`aws:invokeLambdaFunction`- Invoquez la fonction Lambda pour créer le problème Jira

`aws:deleteStack`- Supprimez la CloudFormation pile créée.

Sorties

Issued: ID du problème Jira nouvellement créé

## **AWS-CreateServiceNowIncident**

Description

Créez un incident dans le tableau des ServiceNow incidents.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Catégorie

Type : chaîne

Description : (Facultatif) Catégorie de l'incident.

Valeurs valides : Aucune | Demande/Aide | Logiciel | Matériel | Réseau | Base de données

Valeur par défaut : Aucun

- Description

Type : chaîne

Description : (Obligatoire) Explication détaillée de l'incident.

- Impact

Type : chaîne

Description : (Facultatif) Effet d'un incident sur l'activité.

Valeurs valides : Haute | Moyenne | Faible

Valeur par défaut : Faible

- ServiceNowInstanceUsername

Type : chaîne

Description : (Obligatoire) Nom de l'utilisateur avec lequel l'incident sera créé.

- ServiceNowInstancePassword

Type : chaîne

Description : (Obligatoire) Nom d'un paramètre SSM crypté contenant le mot de passe de l'ServiceNow utilisateur.

- ServiceNowInstanceURL

Type : chaîne

Description : (Obligatoire) URL de l' ServiceNow instance

- ShortDescription

Type : chaîne

Description : (Obligatoire) Brève description de l'incident.

- Sous-catégorie

Type : chaîne

Description : (Facultatif) Sous-catégorie de l'incident.

Valeurs valides : Aucune | Antivirus | E-mail | Application interne | Système d'exploitation | Processeur | Disque | Clavier | Matériel | Mémoire | Moniteur | Souris | DHCP | DNS | Adresse IP | VPN | Sans fil | DB2 | MS SQL Server | Oracle

Valeur par défaut : Aucun

## Étapes de document

Push\_incident — Transfère les informations relatives à l'incident vers. ServiceNow

## Sorties

Push\_incident.incidentId — ID d'incident créé.

# AWS-RunPacker

## Description

Ce runbook utilise l'outil HashiCorp [Packer](#) pour valider, corriger ou créer des modèles de packer utilisés pour créer des images de machine. Ce runbook utilise Packer v1.7.2.

### Note

Si vous spécifiez une valeur `vpc_id`, vous devez également spécifier la valeur `subnet_id` d'un sous-réseau public. Sauf si vous modifiez l'attribut d'adressage public IPv4 de votre sous-réseau, vous devez également définir `associate_public_ip_address` avec la valeur `true`.

## [Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Force

Type : booléen

Description : Option Packer pour forcer un générateur à s'exécuter lorsque des artefacts d'une version précédente empêchent l'exécution d'une build.

- Mode

Type : chaîne

Description : Mode, ou commande, d'utilisation de Packer lors de la validation par rapport au modèle. Les options incluent BuildValidate, etFix.

- TemplateFileName

Type : chaîne

Description : Nom, ou clé, du fichier modèle dans le compartiment S3.

- Modèles 3 BucketName

Type : chaîne

Description : Nom du compartiment S3 contenant le modèle de packer.

## Étapes de document

`RunPackerProcessTemplate` — Exécute le mode sélectionné par rapport au modèle à l'aide de l'outil Packer.

## Sorties

`RunPackerProcessTemplate.output` — La sortie standard de l'outil Packer.

`RunPackerProcessTemplate.fixed_template_key` — Le nom du modèle stocké dans un compartiment S3 à utiliser uniquement lors de l'exécution en mode « Fix ».

`RunPackerProcessTemplate.s3_bucket` : nom du compartiment S3 qui contient le modèle fixe à utiliser uniquement lors de l'exécution en mode « Fix ».

## Amazon VPC

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon Virtual Private Cloud. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [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

### Description

Ce runbook supprime toutes les règles d'entrée et de sortie du groupe de sécurité que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre

nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- SecurityGroupId

Type : chaîne

Description : (Obligatoire) L'ID du groupe de sécurité que vous souhaitez fermer.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

### Étapes de document

- aws:executeScript- Supprime toutes les règles d'entrée et de sortie du groupe de sécurité que vous spécifiez dans le SecurityGroupId paramètre.

## AWSSupport-ConfigureDNSQueryLogging

### Description

Le AWSSupport-ConfigureDNSQueryLogging runbook configure la journalisation des requêtes DNS provenant de votre cloud privé virtuel (VPC) ou des zones hébergées sur Amazon Route 53. Vous pouvez choisir de publier les journaux de requêtes sur Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3) ou Amazon Data Firehose. Pour plus d'informations sur la journalisation des requêtes et les journaux des requêtes du résolveur, consultez les sections [Journalisation des requêtes DNS publiques et Journalisation](#) des [requêtes du résolveur](#).

[Exécuter cette automatisation \(console\)](#)

### Type de document

#### Automatisation

## Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- LogDestinationArn

Type : chaîne

Description : (Facultatif) L'ARN du groupe de CloudWatch journaux, du compartiment Amazon S3 ou du flux Firehose auquel vous souhaitez envoyer les journaux de requêtes. Notez que la journalisation des requêtes DNS publiques de Route 53 ne prend en charge que CloudWatch les groupes de journaux. Si vous ne spécifiez aucune valeur pour ce paramètre, l'automatisation crée un groupe de CloudWatch journaux au format `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID }` et une politique de ressources IAM pour publier les journaux de requêtes. Le groupe CloudWatch Logs créé par l'automatisation a une période de conservation de 14 jours.

- QueryLogType

Type : chaîne

Description : (Facultatif) Les types de requêtes que vous souhaitez enregistrer.

Valeurs valides : Public | Résolveur/Privé

Par défaut : Public

- ResourceId

## Type : chaîne

Description : (Obligatoire) L'ID de la ressource dont vous souhaitez enregistrer les requêtes. Si vous spécifiez `Public` le `QueryLogType` paramètre, la ressource doit être l'ID d'une zone hébergée privée Route 53. Si vous spécifiez `Resolver/Private` le `QueryLogType` paramètre, la ressource doit être l'ID d'un VPC.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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`

### Étapes de document

- `aws:executeScript`- Vérifie que la ressource que vous spécifiez pour le `ResourceId` paramètre existe et vérifie si le type de ressource correspond à l'`QueryLogTypeoption` requise.
- `aws:executeScript`- Vérifie que la valeur que vous spécifiez pour le `LogDestinationArn` paramètre correspond à la valeur requise. `QueryLogType`
- `aws:executeScript`- Vérifie les autorisations requises pour que Route 53 publie des journaux dans le groupe de CloudWatch journaux Logs et crée la politique de ressources IAM requise si elle n'existe pas.
- `aws:executeScript`- Active l'enregistrement des requêtes DNS sur la destination sélectionnée.

## **AWSsupport-ConfigureTrafficMirroring**

### Description

Le `AWSsupport-ConfigureTrafficMirroring` runbook configure la mise en miroir du trafic pour vous aider à résoudre les problèmes de connectivité entre un équilibreur de charge et les instances Amazon Elastic Compute Cloud (Amazon EC2). La mise en miroir du trafic copie le trafic entrant et sortant des interfaces réseau associées à vos instances. Pour configurer la mise en miroir du trafic, ce runbook crée les cibles, les filtres et les sessions requis. Par défaut, le runbook configure la mise en miroir de tout le trafic entrant et sortant pour tous les protocoles, à l'exception d'Amazon DNS. Si vous souhaitez refléter le trafic provenant de sources et de destinations spécifiques, vous pouvez modifier les règles entrantes et sortantes une fois l'automatisation terminée.

### [Exécuter cette automatisation \(console\)](#)

#### Type de document

Automatisation

#### Propriétaire

Amazon

#### Plateformes

LinuxmacOS, Windows

#### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `Source` : ENI

Type : chaîne

Description : (Obligatoire) L'interface Elastic network pour laquelle vous souhaitez configurer la mise en miroir du trafic.

- `Cible`

Type : chaîne

Description : (Obligatoire) Destination du trafic reflété. Vous devez spécifier l'ID d'une interface réseau, d'un Network Load Balancer ou d'un point de terminaison Gateway Load Balancer. Si vous spécifiez un Network Load Balancer, il doit y avoir des écouteurs UDP sur le port 4789.

- SessionNumber

Type : chaîne

Valeurs valides : 1-32766

Description : (Obligatoire) Numéro de la session miroir que vous souhaitez utiliser.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ec2:CreateTrafficMirrorTarget
- ec2:CreateTrafficMirrorFilter
- ec2:CreateTrafficMirrorFilterRule
- ec2:CreateTrafficMirrorSession
- ec2>DeleteTrafficMirrorSession
- ec2>DeleteTrafficMirrorFilter
- ec2>DeleteTrafficMirrorSession
- ec2>DeleteTrafficMirrorFilterRule
- iam:ListRoles
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

### Étapes de document

- aws:executeScript- Exécute un script pour créer une cible.
- aws:executeAwsApi- Crée une règle de filtrage.
- aws:executeAwsApi- Crée une règle de filtre miroir pour tout le trafic entrant.
- aws:executeAwsApi- Crée une règle de filtre miroir pour tout le trafic sortant.

- `aws:executeAwsApi`- Crée une session de miroir du trafic.
- `aws:executeAwsApi`- Supprime le filtre en cas d'échec de la création du filtre ou de la session.
- `aws:executeAwsApi`- Supprime la cible en cas d'échec de la création du filtre ou de la session.

## Sorties

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget. Sortie d'ID cible

# AWSSupport-ConnectivityTroubleshooter

## Description

Le `AWSSupport-ConnectivityTroubleshooter` runbook diagnostique les problèmes de connectivité entre les éléments suivants :

- AWS ressources au sein d'un Amazon Virtual Private Cloud (Amazon VPC)
- AWS ressources dans différents VPC Amazon au sein d'un même Région AWS VPC connectés à l'aide du peering VPC
- AWS ressources d'un Amazon VPC et d'une ressource Internet à l'aide d'une passerelle Internet
- AWS ressources d'un Amazon VPC et d'une ressource Internet à l'aide d'une passerelle de traduction d'adresses réseau (NAT)

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes



## LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- IP de destination

Type : chaîne

Description : (Obligatoire) Adresse IPv4 de la ressource à laquelle vous souhaitez vous connecter.

- DestinationPort

Type : chaîne

Valeur par défaut : true

Description : (Obligatoire) Le numéro de port auquel vous souhaitez vous connecter sur la ressource de destination.

- DestinationVpc

Type : chaîne

Par défaut : Tous

Description : (Facultatif) L'ID du VPC Amazon auquel vous souhaitez tester la connectivité.

- SourceIP

Type : chaîne

Description : (Obligatoire) Adresse IPv4 privée de la AWS ressource de votre Amazon VPC à partir de laquelle vous souhaitez tester la connectivité.

- SourcePortRange

Type : chaîne

Description : (Facultatif) La plage de ports utilisée par la AWS ressource de votre Amazon VPC à partir de laquelle vous souhaitez tester la connectivité.

- SourceVpc

Type : chaîne

Par défaut : Tous

Description : (Facultatif) L'ID du VPC Amazon à partir duquel vous souhaitez tester la connectivité.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcPeeringConnections

### Étapes de document

- aws:executeScript- Rassemble des informations sur la AWS ressource que vous spécifiez dans le SourceIP paramètre.
- aws:executeScript- Détermine la destination du trafic réseau provenant de la AWS ressource en utilisant les itinéraires collectés à l'étape précédente.
- aws:branch- Branches basées sur la destination du trafic réseau.
- aws:executeAwsApi- Recueille des informations sur la ressource de destination.
- aws:executeScript- Confirme que l'ID renvoyé pour le VPC Amazon de destination correspond à la valeur spécifiée, le cas échéant, dans le DestinationVpc paramètre.
- aws:executeAwsApi- Rassemble les règles du groupe de sécurité pour les ressources source et de destination.

- `aws:executeScript`- Confirme si les règles du groupe de sécurité autorisent le trafic nécessaire entre les ressources source et de destination.
- `aws:executeAwsApi`- Rassemble les listes de contrôle d'accès réseau (NACL) associées aux sous-réseaux pour les ressources source et de destination.
- `aws:executeScript`- Confirme si les NACL autorisent le trafic nécessaire entre les ressources source et de destination.
- `aws:executeScript`- Confirme si la source possède une adresse IP publique associée à la ressource, si la destination de la route est une passerelle Internet.
- `aws:executeAwsApi`- Rassemble les règles du groupe de sécurité pour la ressource source.
- `aws:executeScript`- Confirme si les règles du groupe de sécurité autorisent le trafic nécessaire entre la source et la ressource de destination.
- `aws:executeAwsApi`- Regroupe les NACL associés au sous-réseau de la ressource source.
- `aws:executeScript`- Confirme si les NACL autorisent le trafic nécessaire depuis la ressource source.
- `aws:executeAwsApi`- Recueille des informations sur la passerelle NAT.
- `aws:executeAwsApi`- Regroupe les NACL associés au sous-réseau pour la passerelle NAT.
- `aws:executeScript`- Confirme si les NACL autorisent le trafic nécessaire depuis le sous-réseau pour la passerelle NAT.
- `aws:executeScript`- Rassemble les routes associées au sous-réseau pour la passerelle NAT.
- `aws:executeScript`- Confirme si la passerelle NAT dispose d'une route vers une passerelle Internet.
- `aws:executeAwsApi`- Recueille des informations sur la connexion d'appairage VPC.
- `aws:executeScript`- Confirme que les deux VPC se trouvent dans la même région et que l'ID renvoyé pour le VPC de destination correspond à la valeur spécifiée, le cas échéant, dans `DestinationVpc` le paramètre.
- `aws:executeAwsApi`- Renvoie le sous-réseau de la ressource de destination.
- `aws:executeScript`- Regroupe les routes associées au sous-réseau pour le VPC homologue.
- `aws:executeScript`- Confirme si le VPC apparenté possède une route vers la connexion d'appairage.
- `aws:executeScript`- Confirme si le trafic est autorisé depuis la ressource source si la destination n'est pas prise en charge par l'automatisation.

# AWSSupport-TroubleshootVPN

## Description

Le AWSSupport-TroubleshootVPN runbook vous aide à suivre et à résoudre les erreurs dans une AWS Site-to-Site VPN connexion. L'automatisation comprend plusieurs contrôles automatisés conçus pour détecter les IKEv1 IKEv2 erreurs liées aux tunnels de AWS Site-to-Site VPN connexion. L'automatisation essaie de faire correspondre des erreurs spécifiques et la résolution correspondante forme une liste de problèmes courants.

Remarque : Cette automatisation ne corrige pas les erreurs. Il s'exécute pendant la période mentionnée et analyse le groupe de journaux à la recherche d'erreurs dans le [groupe de CloudWatch journaux VPN](#).

## Comment fonctionne-t-il ?

Le runbook exécute une validation des paramètres pour confirmer si le groupe de CloudWatch journaux Amazon inclus dans le paramètre d'entrée existe, si le groupe de journaux contient des flux de journaux correspondant à la journalisation du tunnel VPN, si l'identifiant de connexion VPN existe et si l'adresse IP du tunnel existe. Il effectue des appels d'API Logs Insights sur votre groupe de CloudWatch journaux qui sont configurés pour la journalisation VPN.

## Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre

nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- LogGroupName

Type : chaîne

Description : (Obligatoire) Le nom du groupe de CloudWatch journaux Amazon configuré pour la journalisation des AWS Site-to-Site VPN connexions

Modèle autorisé : `^[\\.\-_\/#A-Za-z0-9]{1,512}`

- VpnConnectionId

Type : chaîne

Description : (Obligatoire) L'identifiant de AWS Site-to-Site VPN connexion à résoudre.

Modèle autorisé : `^vpn-[0-9a-f]{8,17}$`

- Adresse IP du tunnel

Type : chaîne

Description : (Obligatoire) L'adresse IPv4 du tunnel numéro 1 associée à votre AWS Site-to-Site VPN.

Modèle autorisé : `^((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}$`

- Adresse IP du tunnel

Type : chaîne

Description : (Facultatif) L'adresse IPv4 du tunnel numéro 2 associée à votre AWS Site-to-Site VPN.

Modèle autorisé : `^((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}|^$`

- Version IKE

Type : chaîne

Description : (Obligatoire) Sélectionnez la version IKE que vous utilisez. Valeurs autorisées :

`IKEv1`, `IKEv2`

Valeurs valides : [ 'IKEv1', 'IKEv2' ]

- StartTimeinEpoch

Type : chaîne

Description : (Facultatif) Heure de début de l'analyse du journal. Vous pouvez utiliser StartTimeinEpoch/EndTimeinEpoch ou LookBackPeriod pour l'analyse des journaux

Modèle autorisé : ^\d{10}\$

- EndTimeinEpoch

Type : chaîne

Description : (Facultatif) Heure de fin de l'analyse du journal. Vous pouvez utiliser StartTimeinEpoch/EndTimeinEpoch ou LookBackPeriod pour l'analyse des journaux. Si on donne à la fois « StartTimeinEpoch/» EndTimeinEpoch et « LookBackPeriod then » LookBackPeriod ont la priorité

Modèle autorisé : ^\d{10}\$

- LookBackPeriod

Type : chaîne

Description : (Facultatif) Durée à deux chiffres en heures de consultation rétrospective pour l'analyse du journal. Plage valide : 01 - 99. Cette valeur est prioritaire si vous indiquez StartTimeinEpoch également et EndTime

Modèle autorisé : ^(\d?[1-9] | [1-9]0)\$

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

- `ec2:DescribeVpnConnections`

## Instructions

Remarque : Cette automatisation fonctionne sur les groupes de CloudWatch journaux configurés pour la journalisation de votre tunnel VPN, lorsque le format de sortie de journalisation est JSON.

Pour configurer l'automatisation, procédez comme suit :

1. Accédez au [AWSSupport-TroubleshootVPN](#) dans la console. AWS Systems Manager
2. Pour les paramètres d'entrée, entrez ce qui suit :

- `AutomationAssumeRole` (Facultatif) :

Amazon Resource Name (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `LogGroupName` (Obligatoire) :

Le nom du groupe de CloudWatch journaux Amazon à valider. Il doit s'agir du groupe de CloudWatch journaux configuré pour que le VPN envoie des journaux.

- `VpnConnectionId` (Obligatoire) :

L'identifiant de AWS Site-to-Site VPN connexion dont le groupe de journaux est tracé pour détecter une erreur VPN.

- Adresse IP du tunnel (obligatoire) :

Le tunnel Une adresse IP associée à votre AWS Site-to-Site VPN connexion.

- Adresse IP du tunnel (facultatif) :

Adresse IP du tunnel B associée à votre AWS Site-to-Site VPN connexion.

- `Version IKE` (obligatoire) :

Sélectionnez la version d'`IkeVersion` que vous utilisez. Valeurs autorisées : IKEv1, IKEv2.

- `StartTimeinEpoch` (Facultatif) :

Début de l'intervalle de temps pour rechercher une erreur. La plage étant inclusive, l'heure de début spécifiée est incluse dans la requête. Spécifié comme heure de l'époque, le nombre de secondes écoulées depuis le 1er janvier 1970, 00:00:00 UTC.

- EndTimeinEpoch (Facultatif) :

Fin de l'intervalle de temps pour rechercher des erreurs. La plage étant inclusive, l'heure de fin spécifiée est incluse dans la requête. Spécifié comme heure de l'époque, le nombre de secondes écoulées depuis le 1er janvier 1970, 00:00:00 UTC.

- LookBackPeriod (Obligatoire) :

Temps, en heures, nécessaire pour revenir sur la requête afin de détecter une erreur.

Remarque : Configurez un StartTimeinEpoch EndTimeinEpoch, ou LookBackPeriod pour fixer la plage de temps pour l'analyse des journaux. Donnez un nombre à deux chiffres en heures pour vérifier les erreurs passées depuis le début de l'automatisation. Ou, si l'erreur s'est produite dans le passé dans un intervalle de temps spécifique, incluez StartTimeinEpoch et EndTimeinEpoch, au lieu de LookBackPeriod.

Input parameters	
<b>AutomationAssumeRole</b> <small>(Optional) The ARN of the role that allows Automation to perform the actions on your behalf.</small> <input type="text" value="Choose an option"/>	<b>LogGroupName</b> <small>(Required) The Amazon CloudWatch log group name to be validated. This must be the CloudWatch log group which is destined for VPN logs</small> <input type="text" value="vpnlog"/>
<b>VpnConnectionId</b> <small>(Required) The AWS Site-to-Site VPN connection id to be validated.</small> <input type="text" value="vpn-123abc456zxc"/>	<b>Tunnel1IPAddress</b> <small>(Required) The tunnel number 1 IP address associated with your AWS Site-to-Site VPN to be validated.</small> <input type="text" value="1.1.1.1"/>
<b>Tunnel2IPAddress</b> <small>(Optional) The tunnel number 2 IP address associated with your AWS Site-to-Site VPN to be validated.</small> <input type="text" value="String"/>	<b>IKEVersion</b> <small>(Required) Select what IKE Version you are using. Allowed values : IKEv1, IKEv2 or both</small> <input type="text" value="IKEv1"/>
<b>StartTimeinEpoch</b> <small>(Optional) Start time for log analysis. You can either use StartTimeinEpoch/EndTimeinEpoch or LookBackPeriod for logs analysis</small> <input type="text" value="String"/>	<b>EndTimeinEpoch</b> <small>(Optional) End time for log analysis. You can either use StartTimeinEpoch/EndTimeinEpoch or LookBackPeriod for logs analysis</small> <input type="text" value="String"/>
<b>LookBackPeriod</b> <small>(Required) Time in hours to look back for log analysis</small> <input type="text" value="05"/>	

3. Sélectionnez Exécuter.

4. L'automatisation démarre.

5. Le runbook d'automatisation exécute les étapes suivantes :

- Validation des paramètres :

Exécute une série de validations sur les paramètres d'entrée inclus dans l'automatisation.

- branchOnValidationOfLogGroup:

Vérifie si le groupe de logs mentionné dans le paramètre est valide. S'il n'est pas valide, il arrête le lancement ultérieur des étapes d'automatisation.

- branchOnValidationOfLogStream:



Vérifie si le flux de journaux existe dans le groupe de CloudWatch journaux inclus. S'il n'est pas valide, il arrête le lancement ultérieur des étapes d'automatisation.

- `branchOnValidationOfVpnConnectionId`:

Vérifie si l'identifiant de connexion VPN inclus dans le paramètre est valide. S'il n'est pas valide, il arrête le lancement ultérieur des étapes d'automatisation.

- `branchOnValidationOfVpnIp`:

Vérifie si l'adresse IP du tunnel mentionnée dans le paramètre est valide ou non. S'il n'est pas valide, il arrête l'exécution ultérieure des étapes d'automatisation.

- Erreur de trace :

Fait un appel à l'API Logs Insight dans le groupe de CloudWatch journaux inclus et recherche l'erreur liée à IKEv1/IKEv2 ainsi qu'une solution suggérée associée.

6. Une fois terminé, consultez la section Sorties pour connaître les résultats détaillés de l'exécution.

```

▼ Outputs
parameterValidation.LogGroupName
LogGroupName

parameterValidation.VpnConnection
validVpnConnection

traceErrorTunnelIkeV2
{"IKEv2ErrorCount":0}

traceErrorTunnelIkeV1
{"IKEv1ErrorCount":0}

traceErrorTunnelIkeV1
{"Error related to : AMS tunnel received DELETE for Phase 2 SA:"
Please treat below as Potential resolution of this error :
AMS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent Delete_SA message for Phase 2. When AMS 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-ikev2-tunnel-instability-rekey/
[2] Phase 2 Troubleshooting: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-phase-2-ipsec/
}

"Error related to : AMS tunnel received DELETE for IKE_SA from CGW:"
Please treat below as Potential resolution of this error :
AMS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent the Delete_SA message for Parent/IKE_SA. When AMS 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 :
AMS 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.

```

## Références

### Systems Manager Automation

- [Exécuter cette automatisation \(console\)](#)

- [Exécuter une automatisation](#)
- [Configuration d'une automatisation](#)
- [Page d'accueil de Support Automation Workflows](#)

AWSdocumentation de service

- [Contenu des journaux du VPN de site à site](#)

## **AWSConfigRemediation-DeleteEgressOnlyInternetGateway**

Description

Le AWSConfigRemediation-DeleteEgressOnlyInternetGateway runbook supprime la passerelle Internet de sortie uniquement que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- EgressOnlyInternetGatewayId

Type : chaîne

Description : (Obligatoire) L'ID de la passerelle Internet de sortie uniquement que vous souhaitez supprimer.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2>DeleteEgressOnlyInternetGateway`
- `ec2:DescribeEgressOnlyInternetGateways`

### Étapes de document

- `aws:executeScript`- Supprime la passerelle Internet de sortie uniquement spécifiée dans le paramètre. `EgressOnlyInternetGatewayId`
- `aws:executeScript`- Vérifie que la passerelle Internet de sortie uniquement a été supprimée.

## **AWSConfigRemediation-DeleteUnusedENI**

### Description

Le `AWSConfigRemediation-DeleteUnusedENI` runbook supprime une Elastic Network Interface (ENI) dont le statut de pièce jointe est de. `detached`

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- NetworkInterfaceId

Type : chaîne

Description : (Obligatoire) L'ID de l'ENI que vous souhaitez supprimer.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2>DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces

### Étapes de document

- aws:executeAwsApi- Supprime l'ENI que vous spécifiez dans le NetworkInterfaceId paramètre.
- aws:executeScript- Vérifie que l'ENI a été supprimée.

## **AWSConfigRemediation-DeleteUnusedSecurityGroup**

### Description

Le AWSConfigRemediation-DeleteUnusedSecurityGroup runbook supprime le groupe de sécurité que vous spécifiez dans le GroupId paramètre. Si vous tentez de supprimer un groupe de sécurité associé à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou référencé par un

autre groupe de sécurité, l'automatisation échoue. Cette automatisation ne supprime pas de groupe de sécurité par défaut.

### [Exécuter cette automatisation \(console\)](#)

#### Type de document

Automatisation

#### Propriétaire

Amazon

#### Plateformes

LinuxmacOS, Windows

#### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- GroupId

Type : chaîne

Description : (Obligatoire) L'ID du groupe de sécurité que vous souhaitez supprimer.

#### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups

- `ec2:DeleteSecurityGroup`

## Étapes de document

- `aws:executeAwsApi`- Renvoie le nom du groupe de sécurité en utilisant la valeur que vous indiquez dans le `GroupId` paramètre.
- `aws:branch`- Confirme que le nom du groupe n'est pas « par défaut ».
- `aws:executeAwsApi`- Supprime le groupe de sécurité spécifié dans le `GroupId` paramètre.
- `aws:executeScript`- Confirme que le groupe de sécurité a été supprimé.

## **AWSConfigRemediation-DeleteUnusedVPCNetworkACL**

### Description

Le `AWSConfigRemediation-DeleteUnusedVPCNetworkACL` runbook supprime une liste de contrôle d'accès réseau (ACL) qui n'est pas associée à un sous-réseau.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- **NetworkAcIID**

Type : chaîne

Description : (Obligatoire) L'ID de l'ACL réseau que vous souhaitez supprimer.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2>DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

#### Étapes de document

- `aws:executeAwsApi`- Supprime l'ACL réseau spécifiée dans le `NetworkAclId` paramètre.
- `aws:executeScript`- Confirme que l'ACL réseau spécifiée dans le `NetworkAclId` paramètre a été supprimée.

## **AWSConfigRemediation-DeleteVPCFlowLog**

### Description

Le `AWSConfigRemediation-DeleteVPCFlowLog` runbook supprime le journal de flux du cloud privé virtuel (VPC) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- FlowLogId

Type : chaîne

Description : (Obligatoire) L'ID du journal de flux que vous souhaitez supprimer.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2>DeleteFlowLogs
- ec2:DescribeFlowLogs

## Étapes de document

- aws:executeAwsApi- Supprime le journal de flux que vous spécifiez dans le FlowLogId paramètre.
- aws:executeScript- Vérifie que le journal de flux a été supprimé.

# **AWSConfigRemediation-DetachAndDeleteInternetGateway**

## Description



Le `AWSConfigRemediation-DetachAndDeleteInternetGateway` runbook détache et supprime la passerelle Internet que vous spécifiez. Si des adresses IP élastiques ou des adresses IPv4 publiques sont associées à des instances Amazon EC2 de votre cloud privé virtuel (VPC), le runbook échoue.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `InternetGatewayId`

Type : chaîne

Description : (Obligatoire) L'ID de la passerelle Internet que vous souhaitez supprimer.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

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

- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

## Étapes de document

- `aws:waitForAwsResourceProperty`- Accepte l'ID de la passerelle privée virtuelle et attend que la propriété d'état de la passerelle privée virtuelle `available` soit modifiée ou expire.
- `aws:executeAwsApi`- Récupère une configuration de passerelle privée virtuelle spécifiée.
- `aws:branch`- Branches basées sur la valeur du paramètre `VpcAttachments .state`.
  
- `aws:waitForAwsResourceProperty`- Accepte l'ID de la passerelle privée virtuelle et attend que la propriété `VpcAttachments .state` de la passerelle privée virtuelle soit modifiée `attached` ou `expire`.
- `aws:executeAwsApi`- Accepte l'ID de la passerelle privée virtuelle et l'ID de l'Amazon VPC en entrée, et détache la passerelle privée virtuelle de l'Amazon VPC.
- `aws:waitForAwsResourceProperty`- Accepte l'ID de la passerelle privée virtuelle et attend que la propriété `VpcAttachments .state` de la passerelle privée virtuelle soit modifiée `detached` ou `expire`.
  
- `aws:executeAwsApi`- Accepte l'ID de la passerelle privée virtuelle en entrée et le supprime.
  
- `aws:waitForAwsResourceProperty`- Accepte l'ID de la passerelle privée virtuelle en entrée et vérifie sa suppression.  
  
`aws:executeAwsApi`- Recueille l'ID VPC à partir de l'ID de passerelle Internet.
- `aws:executeAwsApi`- Détache l'ID de passerelle Internet du VPC.
- `aws:executeAwsApi`- Supprime la passerelle Internet.

## **AWSConfigRemediation- DetachAndDeleteVirtualPrivateGateway**

### Description

Le `AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` runbook détache et supprime une passerelle privée virtuelle Amazon Elastic Compute Cloud (Amazon EC2) donnée attachée à un cloud privé virtuel (VPC) créé avec Amazon Virtual Private Cloud (Amazon VPC).

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `VpnGatewayId`

Type : chaîne

Description : (Obligatoire) L'ID de la passerelle privée virtuelle à supprimer.

Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2>DeleteVpnGateway`

- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

### Étapes de document

- `aws:waitForAwsResourceProperty`- Accepte l'ID de la passerelle privée virtuelle et attend que la propriété d'état de la passerelle privée virtuelle `available` soit modifiée ou expire.
- `aws:executeAwsApi`- Récupère une configuration de passerelle privée virtuelle spécifiée.
- `aws:branch`- Branches basées sur la valeur du paramètre `VpcAttachments.state`.
- `aws:waitForAwsResourceProperty`- Accepte l'ID de la passerelle privée virtuelle et attend que la propriété `VpcAttachments.state` de la passerelle privée virtuelle soit modifiée `attached` ou `expire`.
- `aws:executeAwsApi`- Accepte l'ID de la passerelle privée virtuelle et l'ID de l'Amazon VPC en entrée, et détache la passerelle privée virtuelle de l'Amazon VPC.
- `aws:waitForAwsResourceProperty`- Accepte l'ID de la passerelle privée virtuelle et attend que la propriété `VpcAttachments.state` de la passerelle privée virtuelle soit modifiée `detached` ou `expire`.
- `aws:executeAwsApi`- Accepte l'ID de la passerelle privée virtuelle en entrée et le supprime.
- `aws:waitForAwsResourceProperty`- Accepte l'ID de la passerelle privée virtuelle en entrée et vérifie sa suppression.

## AWS-DisableIncomingSSHOnPort22

### Description

Le `AWS-DisableIncomingSSHOnPort22` runbook supprime les règles qui autorisent le trafic SSH entrant illimité sur le port TCP 22 pour les groupes de sécurité.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `SecurityGroupIds`

Type : chaîne

Description : (Obligatoire) Liste séparée par des virgules des identifiants des groupes de sécurité pour lesquels vous souhaitez restreindre le trafic SSH.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

## Étapes de document

- `aws:executeAwsApi`- Supprime toutes les règles autorisant le trafic SSH entrant sur le port TCP 22 à partir des groupes de sécurité que vous spécifiez dans le `SecurityGroupIds` paramètre.

## Sorties

DisableIncomingModèle SSH. RestrictedSecurityGroupIds - Une liste des identifiants des groupes de sécurité dont les règles SSH entrantes ont été supprimées.

## AWS-DisablePublicAccessForSecurityGroup

### Description

Ce runbook désactive les ports SSH et RDP par défaut ouverts à toutes les adresses IP.

#### Important

Ce runbook échoue avec un « »InvalidPermission. NotFound« erreur pour les groupes de sécurité qui répondent aux deux critères suivants : 1) Le groupe de sécurité est situé dans un VPC autre que celui par défaut ; et 2) Les règles entrantes du groupe de sécurité ne spécifient pas les ports ouverts selon les quatre modèles suivants :

- 0.0.0.0/0
- ::/0
- SSH or RDP port + 0.0.0.0/0
- SSH or RDP port + ::/0

#### Note

Ce runbook n'est pas disponible Régions AWS en Chine.

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- GroupId

Type : chaîne

Description : (Obligatoire) ID du groupe de sécurité pour lequel les ports doivent être désactivés.

- IpAddressToBlock

Type : chaîne

Description : (Facultatif) Adresses IPv4 supplémentaires à partir desquelles l'accès doit être bloqué, au format 1.2.3.4/32.

## **AWSConfigRemediation-DisableSubnetAutoAssignPublicIP**

### Description

Le AWSConfigRemediation-DisableSubnetAutoAssignPublicIP runbook désactive l'attribut d'adressage public IPv4 pour le sous-réseau que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- SubnetId

Type : chaîne

Description : (Obligatoire) L'ID du sous-réseau sur lequel vous souhaitez désactiver l'attribut d'adresse IPv4 public attribué automatiquement.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSubnets
- ec2:ModifySubnetAttribute

### Étapes de document

- aws:executeAwsApi- Désactive l'attribut d'adresse IPv4 public attribué automatiquement au sous-réseau que vous avez spécifié dans le paramètre. SubnetId
- aws:assertAwsResourceProperty- Vérifie que l'attribut a été désactivé.

## AWSSupport - EnableVPCFlowLogs

### Description

Le AWSSupport - EnableVPCFlowLogs runbook crée les journaux de flux Amazon Virtual Private Cloud (Amazon VPC) pour les sous-réseaux, les interfaces réseau et les VPC de votre. Compte AWS



Si vous créez un journal de flux pour un sous-réseau ou un VPC, chaque interface réseau élastique de ce sous-réseau ou d'Amazon VPC est surveillée. Les données des journaux de flux sont publiées dans le groupe de CloudWatch journaux Amazon Logs ou dans le compartiment Amazon Simple Storage Service (Amazon S3) que vous spécifiez. Pour plus d'informations sur les journaux de flux, consultez la section [Journaux de flux VPC](#) dans le guide de l'utilisateur Amazon VPC.

 Important

Les frais d'ingestion de données et d'archivage pour les journaux vendus s'appliquent lorsque vous publiez des journaux de flux sur CloudWatch Logs ou sur Amazon S3. Pour plus d'informations, voir la [tarification de Flow Logs](#)

[Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- DeliverLogsPermissionArn

Type : chaîne

Description : (Facultatif) L'ARN du rôle IAM qui permet à Amazon Elastic Compute Cloud (Amazon EC2) de publier des journaux de flux dans le groupe de journaux Logs de votre CloudWatch compte. Si vous spécifiez `s3` le `LogDestinationType` paramètre, ne fournissez pas de valeur pour ce paramètre. Pour plus d'informations, consultez [Publier des journaux de flux dans des CloudWatch journaux](#) dans le guide de l'utilisateur Amazon VPC.

- `LogDestinationARN`

Type : chaîne

Description : (Facultatif) L'ARN de la ressource sur laquelle les données du journal de flux sont publiées. Si le `LogDestinationType` paramètre `cloud-watch-logs` est spécifié, indiquez l'ARN du groupe de CloudWatch journaux de journaux dans lequel vous souhaitez publier les données des journaux de flux. Vous pouvez également utiliser `LogGroupName` à la place. Si le `LogDestinationType` paramètre `s3` est spécifié, vous devez spécifier l'ARN du compartiment Amazon S3 dans lequel vous souhaitez publier les données du journal de flux pour ce paramètre. Vous pouvez également spécifier un dossier dans le compartiment.

- `LogDestinationType`

Type : chaîne

Valeurs valides : `cloud-watch-logs` | `s3`

Description : (Obligatoire) Détermine où les données du journal de flux sont publiées. Si vous spécifiez `LogDestinationType` comme `s3`, ne spécifiez pas `DeliverLogsPermissionArn` ou `LogGroupName`.

- `LogFormat`

Type : chaîne

Description : (Facultatif) Les champs à inclure dans le journal de flux et l'ordre dans lequel ils doivent apparaître dans l'enregistrement. Pour obtenir la liste des champs disponibles, consultez la section [Enregistrements du journal de flux](#) dans le guide de l'utilisateur Amazon VPC. Si vous ne fournissez aucune valeur pour ce paramètre, le journal de flux est créé selon le format par défaut. Si vous spécifiez ce paramètre, vous devez spécifier au moins un champ.

- `LogGroupName`

Type : chaîne

Description : (Facultatif) Nom du groupe de CloudWatch journaux dans lequel les données des journaux de flux sont publiées. Si vous spécifiez s3 le `LogDestinationType` paramètre, ne fournissez pas de valeur pour ce paramètre.

- `ResourceIds`

Type : `StringList`

Description : (Obligatoire) Liste séparée par des virgules des identifiants des sous-réseaux, des interfaces réseau élastiques ou des VPC pour lesquels vous souhaitez créer un journal de flux.

- `TrafficType`

Type : chaîne

Valeurs valides : `ACCEPTER` | `REJETER` | `TOUT`

Description : (Obligatoire) Type de trafic à enregistrer. Vous pouvez consigner le trafic que la ressource accepte ou rejette, ou tout le trafic.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le 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:GetBucketAcl`

#### Étapes de document

- `aws:branch`- Branches basées sur la valeur spécifiée pour le `LogDestinationType` paramètre.
- `aws:executeScript`- Crée un groupe de journaux si aucune valeur n'est spécifiée pour le `LogDestinationARN` paramètre, mais elle `cloud-watch-logs` est spécifiée pour le `LogDestinationType` paramètre.
- `aws:executeScript`- Crée des journaux de flux en fonction des valeurs spécifiées dans les paramètres du runbook.

## **AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch**

### Description

Le `AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch` runbook remplace un journal de flux Amazon VPC existant qui publie les données du journal de flux sur Amazon Simple Storage Service (Amazon S3) par un journal de flux qui publie les données du journal de flux dans le groupe de journaux CloudWatch Amazon Logs CloudWatch (Logs) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

## Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- DestinationLogGroup

Type : chaîne

Description : (Obligatoire) Nom du groupe de CloudWatch journaux dans lequel vous souhaitez publier les données des journaux de flux.

- DeliverLogsPermissionArn

Type : chaîne

Description : (Obligatoire) L'ARN du rôle AWS Identity and Access Management (IAM) que vous souhaitez utiliser et qui fournit à Amazon Elastic Compute Cloud (Amazon EC2) les autorisations requises pour publier les données des journaux de flux dans Logs. CloudWatch

- FlowLogId

Type : chaîne

Description : (Obligatoire) L'ID du journal de flux publié sur Amazon S3 que vous souhaitez remplacer.

- MaxAggregationInterval

Type : entier

Valeurs valides : 60 | 600

Description : (Facultatif) Intervalle de temps maximal, en secondes, pendant lequel un flux de paquets est capturé et agrégé dans un enregistrement de journal de flux.

- TrafficType

Type : chaîne

Valeurs valides : ACCEPTER | REJETER | TOUT

Description : (Obligatoire) Type de données du journal de flux que vous souhaitez enregistrer et publier.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2>DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

### Étapes de document

- `aws:executeAwsApi`- Recueille des informations sur votre VPC à partir de la valeur que vous spécifiez dans `FlowLogId` le paramètre.
- `aws:executeAwsApi`- Crée un journal de flux basé sur les valeurs que vous spécifiez pour les paramètres du runbook.
- `aws:assertAwsResourceProperty`- Vérifie que le journal de flux nouvellement créé est publié dans CloudWatch Logs.
- `aws:executeAwsApi`- Supprime le journal de flux publié sur Amazon S3.
- `aws:executeScript`- Confirme que le journal de flux publié sur Amazon S3 a été supprimé.

# AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

## Description

Le AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket runbook remplace un journal de flux Amazon VPC existant qui publie les données du journal de flux sur CloudWatch Amazon Logs CloudWatch (Logs) par un journal de flux qui publie les données du journal de flux dans le compartiment Amazon Simple Storage Service (Amazon S3) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- Destinations 3 BucketArn

Type : chaîne

Description : (Obligatoire) L'ARN du compartiment Amazon S3 dans lequel vous souhaitez publier les données du journal de flux.

- FlowLogId

Type : chaîne

Description : (Obligatoire) L'ID du journal de flux publié dans les CloudWatch journaux que vous souhaitez remplacer.

- MaxAggregationInterval

Type : entier

Valeurs valides : 60 | 600

Description : (Facultatif) Intervalle de temps maximal, en secondes, pendant lequel un flux de paquets est capturé et agrégé dans un enregistrement de journal de flux.

- TrafficType

Type : chaîne

Valeurs valides : ACCEPTER | REJETER | TOUT

Description : (Obligatoire) Type de données du journal de flux que vous souhaitez enregistrer et publier.

### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2>DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

### Étapes de document

- `aws:executeAwsApi`- Recueille des informations sur votre VPC à partir de la valeur que vous spécifiez dans `FlowLogId` le paramètre.
- `aws:executeAwsApi`- Crée un journal de flux basé sur les valeurs que vous spécifiez pour les paramètres du runbook.



- `aws:assertAwsResourceProperty`- Vérifie que le journal de flux nouvellement créé est publié sur Amazon S3.
- `aws:executeAwsApi`- Supprime le journal de flux publié dans CloudWatch Logs.
- `aws:executeScript`- Confirme que le journal de flux publié dans CloudWatch Logs a été supprimé.

## AWS-ReleaseElasticIP

### Description

Libérer l'adresse IP Elastic spécifiée à l'aide de l'ID d'allocation

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- `AllocationId`

Type : chaîne

Description : (Obligatoire) ID d'allocation de l'adresse IP Elastic.

## AWS-RemoveNetworkACLUnrestrictedSSHRDP

### Description

Le AWS-RemoveNetworkACLUnrestrictedSSHRDP runbook supprime toutes les règles de liste de contrôle d'accès réseau (ACL) de l'ACL réseau spécifiée qui autorisent le trafic entrant depuis toutes les adresses sources vers les ports SSH et RDP par défaut. Les règles qui incluent des plages de ports qui se chevauchent avec les ports SSH et RDP par défaut ne sont pas supprimées.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- NetworkAcId

Type : chaîne

Description : (Obligatoire) ID de l'ACL réseau dont vous souhaitez supprimer les règles illimitées qui autorisent le trafic entrant de toutes les adresses source vers les ports SSH et RDP par défaut.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAclEntry`
- `ec2:DescribeNetworkAcls`

## Étapes de document

- `aws:executeScript`- Supprime toutes les règles d'entrée qui autorisent le trafic depuis toutes les adresses sources du groupe de sécurité que vous avez spécifié dans le `SecurityGroupId` paramètre.

## Sorties

`RemoveNACLEntriesAndVerify.VerificationMessage` - Messages de vérification des règles ACL du réseau supprimées avec succès.

`RemoveNACLEntriesAndVerify.RulesDeletedAndApiResponses` - Les règles ACL du réseau qui ont été supprimées et les réponses aux opérations de `DeleteNetworkAclEntryAPI`.

# **AWSConfigRemediation- RemoveUnrestrictedSourceIngressRules**

## Description

Le `AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules` runbook supprime toutes les règles d'entrée du groupe de sécurité que vous spécifiez qui autorisent le trafic provenant de toutes les adresses sources.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `SecurityGroupId`

Type : chaîne

Description : (Obligatoire) L'ID du groupe de sécurité dont vous souhaitez supprimer les règles d'entrée qui autorisent le trafic provenant de toutes les adresses sources.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

## Étapes de document

- `aws:executeScript`- Supprime toutes les règles d'entrée qui autorisent le trafic depuis toutes les adresses sources du groupe de sécurité que vous avez spécifié dans le `SecurityGroupId` paramètre.

# AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

## Description

Le `AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` runbook supprime toutes les règles du groupe de sécurité par défaut du cloud privé virtuel (VPC) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- `AutomationAssumeRole`

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `GroupId`

Type : chaîne

Description : (Obligatoire) L'ID du groupe de sécurité dont vous souhaitez supprimer toutes les règles.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

### Étapes de document

- `aws:assertAwsResourceProperty`- Confirme que le groupe de sécurité que vous avez spécifié dans le `GroupId` paramètre est nommé par défaut.
- `aws:executeScript`- Supprime toutes les règles du groupe de sécurité que vous avez spécifié dans le `GroupId` paramètre.

## AWSSupport-SetupIPMonitoringFromVPC

### Description

`AWSSupport-SetupIPMonitoringFromVPC` crée une instance Amazon Elastic Compute Cloud (Amazon EC2) dans le sous-réseau spécifié et surveille les adresses IP cibles sélectionnées (IPv4 ou IPv6) en exécutant en permanence des tests ping, MTR, traceroute et tracetcp. Les résultats sont stockés dans les CloudWatch journaux Amazon Logs et des filtres métriques sont appliqués pour visualiser rapidement les statistiques de latence et de perte de paquets dans un CloudWatch tableau de bord.

### Informations supplémentaires

Les données CloudWatch des journaux peuvent être utilisées pour le dépannage du réseau et l'analyse des modèles/tendances. En outre, vous pouvez configurer des CloudWatch alarmes avec les notifications Amazon SNS lorsque la perte de paquets et/ou la latence atteignent un seuil. Les données peuvent également être utilisées lors de l'ouverture d'un dossier AWS Support, afin d'isoler rapidement un problème et de réduire le temps de résolution lors de l'enquête sur un problème réseau.

#### Note

Pour nettoyer les ressources créées par `AWSSupport-SetupIPMonitoringFromVPC`, vous pouvez utiliser le runbook `AWSSupport-TerminateIPMonitoringFromVPC`. Pour plus d'informations, consultez [AWSSupport-TerminateIPMonitoringFromVPC](#).

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- CloudWatchLogGroupNamePrefix

Type : chaîne

Par défaut :/AWSSupport-SetupIPMonitoringFromVPC

Description : (Facultatif) Préfixe utilisé pour chaque groupe de CloudWatch journaux créé pour les résultats du test.

- CloudWatchLogGroupRetentionInDays

Type : chaîne

Valeurs valides : 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

Valeur par défaut : 7

Description : (Facultatif) nombre de jours pendant lesquels vous souhaitez conserver les résultats de la surveillance du réseau.

- InstanceType

Type : chaîne

Valeurs valides : t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

Par défaut : t2.micro

Description : (Facultatif) type d'instance EC2 pour l'instance EC2Rescue. Taille recommandée : t2.micro.

- SubnetId

Type : chaîne

Description : (Obligatoire) ID de sous-réseau pour l'instance de surveillance. Sachez que si vous spécifiez un sous-réseau privé, vous devez vous assurer qu'il existe un accès Internet pour permettre à l'instance de surveillance de configurer le test (c'est-à-dire d'installer l'agent CloudWatch Logs, d'interagir avec Systems Manager et CloudWatch).

- TargetIPs

Type : chaîne

Description : (Obligatoire) liste séparée par des virgules des adresses IPv4 et/ou IPv6 à surveiller. Les espaces ne sont pas autorisés. La taille maximale est de 255 caractères. Sachez que si vous fournissez une adresse IP non valide, l'automatisation échoue et restaure la configuration du test.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Il est recommandé que l'utilisateur qui exécute l'automatisation dispose de la politique gérée par AmazonSSM AutomationRole IAM attachée. En outre, l'utilisateur doit disposer de la stratégie suivante associée à son compte utilisateur, groupe ou rôle :

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



```

{
  "Action": [
    "iam:CreateRole",
    "iam:CreateInstanceProfile",
    "iam:GetRole",
    "iam:GetInstanceProfile",
    "iam:DetachRolePolicy",
    "iam:AttachRolePolicy",
    "iam:PassRole",
    "iam:AddRoleToInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam>DeleteRole",
    "iam>DeleteInstanceProfile",
    "iam:PutRolePolicy",
    "iam>DeleteRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::
    AWS_account_ID
    :role/AWSSupport/SetupIPMonitoringFromVPC_*",
    "arn:aws:iam::
    AWS_account_ID
    :instance-profile/AWSSupport/SetupIPMonitoringFromVPC_*"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "iam:DetachRolePolicy",
    "iam:AttachRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
  ],
  "Effect": "Allow"
},
{
  "Action": [
    "cloudwatch:DeleteDashboards"
  ],
  "Resource": [
    "*"
  ],
  "Effect": "Allow"
}

```

```

    },
    {
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypes",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:AssignIpv6Addresses",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "ssm:GetParameter",
        "ssm:SendCommand",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}

```

## Étapes de document

1. **aws:executeAwsApi**- décrivez le sous-réseau fourni.
2. **aws:branch**- évaluer l'entrée TargetTips.

(IPv6) Si TargetIPs contient un IPv6 :

**aws:assertAwsResourceProperty**- vérifiez qu'un pool IPv6 est associé au sous-réseau fourni

3. **aws:executeScript**- obtenez l'architecture du type d'instance et le chemin des paramètres publics pour la dernière version d'Amazon Linux 2AMI.
4. **aws:executeAwsApi**- procurez-vous la dernière version d'Amazon Linux 2 AMI sur Parameter Store.
5. **aws:executeAwsApi**- créez un groupe de sécurité pour le test dans le VPC du sous-réseau.

(Nettoyage) Si la création du groupe de sécurité échoue :

**aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

6. **aws:executeAwsApi**- autoriser tout le trafic sortant dans le groupe de sécurité de test.

(Nettoyage) Si la création de la règle de sortie du groupe de sécurité échoue :

**aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

7. **aws:executeAwsApi**- crée un rôle IAM pour l'instance EC2 de test

(Nettoyage) Si la création du rôle échoue :

a. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation, s'il existe.

b. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

8. **aws:executeAwsApi**- joindre la politique gérée par AmazonSSM ManagedInstanceCore

(Nettoyage) Si l'attachement de la stratégie échoue :

a. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation, si elle est attachée.

b. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.

c. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

9. **aws:executeAwsApi**- joindre une politique en ligne pour permettre de définir les rétentions des groupes de CloudWatch journaux et de créer un tableau de bord CloudWatch

(Nettoyage) Si l'attachement de la stratégie en ligne échoue :

a. **aws:executeAwsApi**- supprimez la politique CloudWatch en ligne du rôle créé par l'automatisation, s'il a été créé.

- b. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
- c. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
- d. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

10 **aws:executeAwsApi**- créer un profil d'instance IAM.

(Nettoyage) Si la création du profil d'instance échoue :

- a. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation, s'il existe.
- b. **aws:executeAwsApi**- supprimez la politique CloudWatch intégrée du rôle créé par l'automatisation.
- c. **aws:executeAwsApi**- supprimez la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
- d. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
- e. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

11 **aws:executeAwsApi**- associe le profil d'instance IAM au rôle IAM.

(Nettoyage) Si l'association du profil d'instance et du rôle échoue :

- a. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle, s'il est associé.
- b. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
- c. **aws:executeAwsApi**- supprimez la politique CloudWatch intégrée du rôle créé par l'automatisation.
- d. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
- e. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
- f. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

12 **aws:sleep**- attendez que le profil d'instance soit disponible.

13 **aws:runInstances**- crée l'instance de test dans le sous-réseau spécifié, en y attachant le profil d'instance créé précédemment.

(Nettoyage) Si l'étape échoue :

- a. **aws:changeInstanceState**- arrête l'instance de test.
- b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.

- d. **aws:executeAwsApi**- supprimez la politique CloudWatch intégrée du rôle créé par l'automatisation.
- e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
- f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
- g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

14 **aws:branch**- évaluer l'entrée TargetTips.

(IPv6) Si TargetIPs contient un IPv6 :

**aws:executeAwsApi**- attribuer un IPv6 à l'instance de test.

15 **aws:waitForAwsResourceProperty**- attendez que l'instance de test devienne une instance gérée.

(Nettoyage) Si l'étape échoue :

- a. **aws:changeInstanceState**- arrête l'instance de test.
- b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
- c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
- d. **aws:executeAwsApi**- supprimez la politique CloudWatch intégrée du rôle créé par l'automatisation.
- e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
- f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
- g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

16 **aws:runCommand**- installer les prérequis de test :

(Nettoyage) Si l'étape échoue :

- a. **aws:changeInstanceState**- arrête l'instance de test.
- b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
- c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
- d. **aws:executeAwsApi**- supprimez la politique CloudWatch intégrée du rôle créé par l'automatisation.
- e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.

f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.

g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

17 **aws:runCommand**- vérifiez que les adresses IP fournies sont syntaxiquement correctes (IPv4 et/ou IPv6) :

(Nettoyage) Si l'étape échoue :

a. **aws:changeInstanceState**- arrête l'instance de test.

b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.

c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.

d. **aws:executeAwsApi**- supprimez la politique CloudWatch intégrée du rôle créé par l'automatisation.

e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.

f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.

g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

18 **aws:runCommand**- définissez le test MTR pour chacune des adresses IP fournies.

(Nettoyage) Si l'étape échoue :

a. **aws:changeInstanceState**- arrête l'instance de test.

b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.

c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.

d. **aws:executeAwsApi**- supprimez la politique CloudWatch intégrée du rôle créé par l'automatisation.

e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.

f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.

g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

19 **aws:runCommand**- définissez le premier test de ping pour chacune des adresses IP fournies.

(Nettoyage) Si l'étape échoue :

a. **aws:changeInstanceState**- arrête l'instance de test.

b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.

c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.

- d. **aws:executeAwsApi**- supprimez la politique CloudWatch intégrée du rôle créé par l'automatisation.
  - e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
  - f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
  - g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.
- 20 **aws:runCommand**- définissez le deuxième test de ping pour chacune des adresses IP fournies.

(Nettoyage) Si l'étape échoue :

- a. **aws:changeInstanceState**- arrête l'instance de test.
  - b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
  - c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
  - d. **aws:executeAwsApi**- supprimez la politique CloudWatch en ligne du rôle créé par l'automatisation.
  - e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
  - f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
  - g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.
- 21 **aws:runCommand**- définissez le test de tracepath pour chacune des adresses IP fournies.

(Nettoyage) Si l'étape échoue :

- a. **aws:changeInstanceState**- arrête l'instance de test.
  - b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
  - c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
  - d. **aws:executeAwsApi**- supprimez la politique CloudWatch en ligne du rôle créé par l'automatisation.
  - e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
  - f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
  - g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.
- 22 **aws:runCommand**- définissez le test traceroute pour chacune des adresses IP fournies.

- a. **aws:changeInstanceState**- arrête l'instance de test.
  - b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
  - c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
  - d. **aws:executeAwsApi**- supprimez la politique CloudWatch en ligne du rôle créé par l'automatisation.
  - e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
  - f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
  - g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.
- 23**aws:runCommand**- configurez CloudWatch les journaux.

(Nettoyage) Si l'étape échoue :

- a. **aws:changeInstanceState**- arrête l'instance de test.
  - b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
  - c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
  - d. **aws:executeAwsApi**- supprimez la politique CloudWatch en ligne du rôle créé par l'automatisation.
  - e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
  - f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
  - g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.
- 24**aws:runCommand**- programmez des cronjobs pour exécuter chaque test toutes les minutes.

(Nettoyage) Si l'étape échoue :

- a. **aws:changeInstanceState**- arrête l'instance de test.
- b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
- c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
- d. **aws:executeAwsApi**- supprimez la politique CloudWatch en ligne du rôle créé par l'automatisation.
- e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
- f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.



- g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.
- 25 **aws:sleep**- attendez que les tests génèrent des données.
- 26 **aws:runCommand**- définissez les rétentions de groupes de CloudWatch journaux souhaitées.

(Nettoyage) Si l'étape échoue :

- a. **aws:changeInstanceState**- arrête l'instance de test.
  - b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
  - c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
  - d. **aws:executeAwsApi**- supprimez la politique CloudWatch en ligne du rôle créé par l'automatisation.
  - e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
  - f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
  - g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.
- 27 **aws:runCommand**- définissez les filtres métriques des groupes de CloudWatch logs.

(Nettoyage) Si l'étape échoue :

- a. **aws:changeInstanceState**- arrête l'instance de test.
  - b. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
  - c. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.
  - d. **aws:executeAwsApi**- supprimez la politique CloudWatch en ligne du rôle créé par l'automatisation.
  - e. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
  - f. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
  - g. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.
- 28 **aws:runCommand**- créer le CloudWatch tableau de bord.

(Nettoyage) Si l'étape échoue :

- a. **aws:executeAwsApi**- supprimez le CloudWatch tableau de bord, s'il existe.
- b. **aws:changeInstanceState**- arrête l'instance de test.
- c. **aws:executeAwsApi**- supprime le profil d'instance IAM du rôle.
- d. **aws:executeAwsApi**- supprimez le profil d'instance IAM créé par l'automatisation.

- e. **aws:executeAwsApi**- supprimez la politique CloudWatch en ligne du rôle créé par l'automatisation.
- f. **aws:executeAwsApi**- détache la politique ManagedInstanceCore gérée par AmazonSSM du rôle créé par l'automatisation.
- g. **aws:executeAwsApi**- supprimez le rôle IAM créé par l'automatisation.
- h. **aws:executeAwsApi**- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

## Sorties

createCloudWatchDashboards.Output : URL du tableau de bord. CloudWatch

createManagedInstance. InstanceIds - l'ID de l'instance de test.

## **AWSSupport-TerminateIPMonitoringFromVPC**

### Description

AWSSupport-TerminateIPMonitoringFromVPCmet fin à un test de surveillance IP précédemment lancé parAWSSupport-SetupIPMonitoringFromVPC. Les données relatives à l'ID de test spécifié sont supprimées.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- AutomationExecutionId

Type : chaîne

Description : (Obligatoire) L'ID d'exécution de l'automatisation utilisé lors de l'exécution précédente du `AWSSupport-SetupIPMonitoringFromVPC` runbook. Toutes les ressources associées à cet ID d'exécution sont supprimées.

- InstanceId

Type : chaîne

Description : (Obligatoire) ID de l'instance de surveillance.

- SubnetId

Type : chaîne

Description : (Obligatoire) ID de sous-réseau pour l'instance de surveillance.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

Il est recommandé que l'utilisateur qui exécute l'automatisation dispose de la politique gérée par `AmazonSSM AutomationRole` IAM attachée. En outre, la politique suivante doit être attachée à l'utilisateur, au groupe ou au rôle de l'utilisateur :

```
{
  "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"
}
]

```

```
}
```

## Étapes de document

1. `aws:assertAwsResourceProperty`- vérifient `AutomationExecutionId` et `InstanceId` sont liés au même test.
2. `aws:assertAwsResourceProperty`- vérifient `SubnetId` et `InstanceId` sont liés au même test.
3. `aws:executeAwsApi`- récupérer le groupe de sécurité de test.
4. `aws:executeAwsApi`- supprimez le CloudWatch tableau de bord.
5. `aws:changeInstanceState`- arrête l'instance de test.
6. `aws:executeAwsApi`- supprime le profil d'instance IAM du rôle.
7. `aws:executeAwsApi`- supprimez le profil d'instance IAM créé par l'automatisation.
8. `aws:executeAwsApi`- supprimez la politique CloudWatch intégrée du rôle créé par l'automatisation.
9. `aws:executeAwsApi`- détache la politique `ManagedInstanceCore` gérée par AmazonSSM du rôle créé par l'automatisation.
10. `aws:executeAwsApi`- supprimez le rôle IAM créé par l'automatisation.
11. `aws:executeAwsApi`- supprimez le groupe de sécurité créé par l'automatisation, s'il existe.

## Sorties

Aucun

# AWS WAF

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS WAF. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-AddWAFRegionalRuleToRuleGroup](#)
- [AWS-AddWAFRegionalRuleToWebAcl](#)
- [AWSConfigRemediation-EnableWAFClassicLogging](#)
- [AWSConfigRemediation-EnableWAFClassicRegionalLogging](#)
- [AWSConfigRemediation-EnableWAFV2Logging](#)

# AWS-AddWAFRegionalRuleToRuleGroup

## Description

Le `AWS-AddWAFRegionalRuleToRuleGroup` runbook ajoute une règle AWS WAF régionale existante à un groupe de règles AWS WAF régional. Seuls les groupes de règles régionaux AWS WAF classiques sont pris en charge. Les groupes de règles régionaux classiques peuvent comporter un maximum de 10 règles.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- RuleGroupId

Type : chaîne

Description : (Obligatoire) L'ID du groupe de règles que vous souhaitez mettre à jour.

- RulePriority

Type : entier

Description : (Obligatoire) Priorité de la nouvelle règle. La priorité des règles détermine l'ordre dans lequel les règles d'un groupe régional sont évaluées. Les règles dont la valeur est inférieure sont prioritaires par rapport aux règles dont la valeur est supérieure. Cette valeur doit correspondre à un nombre entier unique. Si vous ajoutez plusieurs règles à un groupe de règles régional, les valeurs ne doivent pas nécessairement être consécutives.

- RuleId

Type : chaîne

Description : (Obligatoire) L'ID de la règle que vous souhaitez ajouter à votre groupe de règles régional.

- RuleAction

Type : chaîne

Description : (Obligatoire) Spécifie l'action à effectuer lorsqu'une requête Web répond aux conditions de la règle. AWS WAF

Valeurs valides : ALLOW | BLOCK | COUNT

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

## Étapes de document

- `GetWAF ChangeToken (aws :executeAwsApi)` - Récupère un jeton de AWS WAF modification pour s'assurer que le runbook n'envoie pas de demandes contradictoires au service.

- **AddWAF WAF RegionalRuleGroup (RuleToAWS:ExecuteScript)** - Ajoute la règle spécifiée au groupe de règles régional. AWS WAF
- **VerifyChangeTokenPropagating (aws : waitForAwsResourceProperty)** - Vérifie que le jeton de modification a le statut PENDING ouINSYNC.
- **VerifyRuleAddedToRuleGroup (AWS:ExecuteScript)** - Vérifie que la AWS WAF règle spécifiée a été ajoutée au groupe de règles régional cible.

## Sorties

- **VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse** - Résultat de l'étape de vérification de l'ajout de la nouvelle règle au groupe de règles régional.
- **VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse** - Résultat de l'opération `ListActivatedRulesInRuleGroup` d'API.

# AWS-AddWAFRegionalRuleToWebAcl

## Description

Le `AWS-AddWAFRegionalRuleToWebAcl` runbook ajoute une règle AWS WAF régionale existante, un groupe de règles ou une règle basée sur le taux à une liste de contrôle d'accès Web (ACL) régionale AWS WAF classique. Ce runbook ne met pas à jour les ACL Web régionaux AWS WAF classiques existants qui sont gérés par AWS Firewall Manager.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- `AutomationAssumeRole`



Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- WebACLIId

Type : chaîne

Description : (Obligatoire) L'ID de l'ACL Web que vous souhaitez mettre à jour.

- ActivatedRulePriority

Type : entier

Description : (Obligatoire) Priorité de la nouvelle règle. La priorité des règles détermine l'ordre dans lequel les règles d'une ACL Web sont évaluées. Les règles dont la valeur est inférieure sont prioritaires par rapport aux règles dont la valeur est supérieure. Cette valeur doit correspondre à un nombre entier unique. Si vous ajoutez plusieurs règles à une ACL Web régionale, les valeurs ne doivent pas nécessairement être consécutives.

- ActivatedRuleRuleId

Type : chaîne

Description : (Obligatoire) L'ID de la règle normale, de la règle basée sur le taux ou du groupe que vous souhaitez ajouter à l'ACL Web.

- ActivatedRuleAction

Type : chaîne

Valeurs valides : ALLOW | BLOCK | COUNT

Description : (Facultatif) Spécifie l'action à effectuer lorsqu'une requête Web répond aux conditions de la règle. AWS WAF

- ActivatedRuleType

Type : chaîne

Valeurs valides : REGULAR | RATE\_BASED | GROUP

Par défaut : REGULAR

Description : (Facultatif) Type de règle que vous ajoutez à l'ACL Web. Bien que ce champ soit facultatif, notez que si vous essayez d'ajouter une RATE\_BASED règle à une ACL Web sans définir le type, la demande échoue car elle utilise par défaut une REGULAR règle.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

### Étapes de document

- `DetermineWebACL NotIn FMS AndRulePriority` (AWS:ExecuteScript) - Vérifie si l'ACL AWS WAF Web figure dans une politique de sécurité de Firewall Manager et vérifie que l'ID de priorité n'est pas en conflit avec une ACL existante.
- `AddRuleOrRuleGroupToWebACL` (AWS:ExecuteScript) - Ajoute la règle spécifiée à l'ACL Web. AWS WAF
- `VerifyRuleOrRuleGroupAddedToWebAcl` (AWS:ExecuteScript) - Vérifie que la AWS WAF règle spécifiée a été ajoutée à l'ACL Web cible.

### Sorties

- `DetermineWebACL NotIn FM. AndRulePriority PrereqResponse`: sortie de l'`DetermineWebACLNotInFMSAndRulePriority` étape.
- `VerifyRuleOrRuleGroupAddedToWebAcl. VerifyRuleOrRuleGroupAddedToWebACLResponse` : sortie de l'`AddRuleOrRuleGroupToWebACL` étape.
- `VerifyRuleOrRuleGroupAddedToWebAcl. ListActivatedRulesOrRuleGroupsInWebACLResponse` : sortie de l'`VerifyRuleOrRuleGroupAddedToWebAcl` étape.

# AWSConfigRemediation-EnableWAFClassicLogging

## Description

Le AWSConfigRemediation-EnableWAFClassicLogging runbook permet de se connecter à Amazon Data Firehose (Firehose) pour la liste de contrôle d'accès Web ( AWS WAF ACL Web) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

## Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

LinuxmacOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- DeliveryStreamName

Type : chaîne

Description : (Obligatoire) Nom du flux de diffusion Firehose auquel vous souhaitez envoyer des journaux.

- WebACLId

Type : chaîne

Description : (Obligatoire) L'ID de l'ACL AWS WAF Web à laquelle vous souhaitez activer la connexion.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

## Étapes de document

- `aws:executeAwsApi`- Confirme que le flux de diffusion que vous avez spécifié `DeliveryStreamName` existe.
- `aws:executeAwsApi`- Rassemble l'ARN de l'ACL AWS WAF Web spécifiée dans le `WebACLId` paramètre.
- `aws:executeAwsApi`- Active la journalisation pour l'ACL Web.
- `aws:assertAwsResourceProperty`- Vérifie que la journalisation a été activée sur l'ACL AWS WAF Web.

## **AWSConfigRemediation-EnableWAFClassicRegionalLogging**

### Description

Le `AWSConfigRemediation-EnableWAFClassicRegionalLogging` runbook permet de se connecter à Amazon Data Firehose (Firehose) pour la liste de contrôle d'accès Web (AWS WAF ACL) que vous spécifiez.

[Exécuter cette automatisation \(console\)](#)

### Type de document

### Automatisation

### Propriétaire

## Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- LogDestinationConfigs

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du flux de diffusion Firehose auquel vous souhaitez envoyer des journaux.

- WebACLIId

Type : chaîne

Description : (Obligatoire) L'ID de l'ACL AWS WAF Web à laquelle vous souhaitez activer la connexion.

### Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:CreateServiceLinkedRole
- waf-regional:GetLoggingConfiguration
- waf-regional:GetWebAcl
- waf-regional:PutLoggingConfiguration

## Étapes de document

- `aws:executeAwsApi`- Rassemble l'ARN de l'ACL AWS WAF Web spécifiée dans le `WebACLId` paramètre.
- `aws:executeAwsApi`- Active la journalisation pour l'ACL Web.
- `aws:assertAwsResourceProperty`- Vérifie que la journalisation a été activée sur l'ACL AWS WAF Web.

## AWSConfigRemediation-EnableWAFV2Logging

### Description

Le `AWSConfigRemediation-EnableWAFV2Logging` runbook permet de consigner une liste de contrôle d'accès Web AWS WAF (ACL Web) (AWS WAF V2) avec le flux de diffusion Amazon Data Firehose (Firehose) spécifié.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- `AutomationAssumeRole`


Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- `LogDestinationConfigs`

Type : chaîne

Description : (Obligatoire) L'ARN du flux de diffusion Firehose que vous souhaitez associer à l'ACL Web.

 Note

L'ARN du flux de diffusion Firehose doit commencer par le préfixe. `aws-waf-logs-` Par exemple, `aws-waf-logs-us-east-2-analytics`. Pour plus d'informations, consultez [Amazon Data Firehose](#).

- `WebAclArn`

Type : chaîne

Description : ARN (obligatoire) de l'ACL Web pour laquelle la journalisation sera activée.

#### Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

#### Étapes de document

- `aws:executeScript`- Active la journalisation pour l'ACL Web AWS WAF V2 et vérifie que la journalisation a la configuration spécifiée.

# Amazon WorkSpaces

AWS Systems Manager Automation fournit des runbooks prédéfinis pour Amazon WorkSpaces. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

## Rubriques

- [AWS-CreateWorkSpace](#)
- [AWSSupport-RecoverWorkSpace](#)

## AWS-CreateWorkSpace

### Description

Le AWS-CreateWorkSpace runbook crée un nouveau bureau WorkSpaces virtuel Amazon, appelé a Workspace, sur la base des valeurs que vous spécifiez pour les paramètres d'entrée. Pour plus d'informations WorkSpaces, consultez [Qu'est-ce qu'Amazon WorkSpaces ?](#) dans le guide d'WorkSpaces administration Amazon.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

### Propriétaire

Amazon

### Plateformes

LinuxmacOS, Windows

### Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre



nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- **BundleId**

Type : chaîne

Description : (Obligatoire) L'ID du bundle à utiliser pour WorkSpace.

- **ComputeTypeName**

Type : chaîne

Valeurs valides : VALEUR | STANDARD | PERFORMANCE | PUISSANCE | GRAPHISMES | POWERPRO | GRAPHICSPRO

Description : (Facultatif) Type de calcul pour votre WorkSpace.

- **DirectoryId**

Type : chaîne

Description : (Obligatoire) L'ID du répertoire auquel vous souhaitez WorkSpace ajouter votre nom.

- **RootVolumeEncryptionEnabled**

Type : booléen

Valeurs valides : true | false

Valeur par défaut : false

Description : (Facultatif) Détermine si le volume racine du WorkSpace est chiffré.

- **RootVolumeSizeGib**

Type : entier

Description : (Obligatoire) Taille du volume racine du WorkSpace.

- **RunningMode**

Type : chaîne

Valeurs valides : ALWAYS\_ON | AUTO\_STOP

Description : (Obligatoire) Le mode de fonctionnement du WorkSpace.

- `RunningModeAutoStopTimeoutInMinutes`

Type : entier

Description : (Facultatif) Temps écoulé entre la fermeture de session d'un utilisateur et son WorkSpaces arrêt. Spécifiez une valeur par intervalles de 60 minutes.

- `Balises`

Type : chaîne

Description : (Facultatif) Balises que vous souhaitez appliquer au Workspace.

- `UserName`

Type : chaîne

Description : (Obligatoire) Le nom d'utilisateur à associer au Workspace.

- `UserVolumeEncryptionEnabled`

Type : booléen

Valeurs valides : true | false

Valeur par défaut : false

Description : (Facultatif) Détermine si le volume utilisateur du Workspace est chiffré.

- `UserVolumeSizeGib`

Type : entier

Description : (Obligatoire) Taille du volume utilisateur pour le Workspace.

- `VolumeEncryptionKey`

Type : chaîne

Description : (Facultatif) La AWS Key Management Service clé symétrique que vous souhaitez utiliser pour chiffrer les données stockées sur votre Workspace

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

### Étapes de document

- `aws:executeScript`- Crée un `WorkSpace` en fonction des valeurs que vous spécifiez pour les paramètres d'entrée.
- `aws:waitForAwsResourceProperty`- Vérifie l'état du système d'exploitation `WorkSpace` .  
`AVAILABLE`

### Sorties

`CreateWorkspace.WorkspaceId`

## AWSSupport - RecoverWorkSpace

### Description

Le `AWSSupport - RecoverWorkSpace` runbook exécute les étapes de restauration sur le bureau `WorkSpaces` virtuel Amazon, connu sous le nom de `WorkSpace`, que vous spécifiez. Le runbook redémarre le `WorkSpace`, et si l'état est toujours le cas `UNHEALTHY`, le restaure ou le reconstruit en `WorkSpace` fonction des valeurs que vous spécifiez pour les paramètres d'entrée. Avant d'utiliser ce runbook, nous vous recommandons de consulter le guide d' `WorkSpaces` administration Amazon consacré [WorkSpaces aux problèmes de résolution](#) des problèmes.

#### Important

La restauration ou la reconstruction d'un `WorkSpace` est une action potentiellement destructrice qui peut entraîner la perte de données. Cela est dû au fait que les `WorkSpace` données sont restaurées à partir du dernier instantané disponible et que les données récupérées à partir des instantanés peuvent dater de 12 heures.

L'option de restauration recrée à la fois le volume racine et le volume utilisateur en fonction des instantanés les plus récents. L'option de reconstruction recrée le volume utilisateur à partir de l'instantané le plus récent et le recrée `WorkSpace` à partir de l'image associée au bundle à partir duquel `WorkSpace` il a été créé. Les applications installées ou les paramètres

système modifiés après leur WorkSpace création sont perdus. Pour plus d'informations sur la restauration et la reconstruction WorkSpaces, consultez [Restore a WorkSpace](#) et [Rebuild a WorkSpace](#) dans le Guide d' WorkSpaces administration Amazon.

### [Exécuter cette automatisation \(console\)](#)

Type de document

Automatisation

Propriétaire

Amazon

Plateformes

LinuxmacOS, Windows

Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Facultatif) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Si aucun rôle n'est spécifié, Systems Manager Automation utilise les autorisations de l'utilisateur qui lance ce runbook.

- Reconnaître

Type : chaîne

Valeurs valides : Oui

Description : (Obligatoire) Si vous entrez Oui, vous comprenez que les actions de restauration et de reconstruction tenteront de récupérer les données à WorkSpace partir de l'instantané le plus récent et que les données restaurées à partir de ces instantanés peuvent dater de 12 heures seulement.

- Redémarrer

Type : chaîne

Valeurs valides : Oui | Non

Par défaut : Oui

Description : (Obligatoire) Détermine si le WorkSpace est redémarré.

- Reconstruire

Type : chaîne

Valeurs valides : Oui | Non

Par défaut : Non

Description : (Obligatoire) Détermine si le WorkSpace est reconstruit.

- Restaurer

Type : chaîne

Valeurs valides : Oui | Non

Par défaut : Non

Description : (Obligatoire) Détermine si le WorkSpace est restauré.

- Workspaceld

Type : chaîne

Description : (Obligatoire) L'ID du WorkSpace fichier que vous souhaitez récupérer.

## Autorisations IAM requises

Le `AutomationAssumeRole` paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`

- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

## Étapes de document

- `aws:executeAwsApi`- Rassemble l'état de ce WorkSpace que vous spécifiez dans le `WorkspaceId` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie l'état du WorkSpace isAVAILABLE,ERROR,IMPAIREDSTOPPED, ouUNHEALTHY.
- `aws:branch`- Branches basées sur l'état du WorkSpace.
- `aws:executeAwsApi`- Démarre le WorkSpace.
- `aws:branch`- Branches basées sur la valeur que vous spécifiez pour le `Action` paramètre.
- `aws:waitForAwsResourceProperty`- Attend le WorkSpace statut après avoir démarré.
- `aws:waitForAwsResourceProperty`- Attend que l' WorkSpace état passe à AVAILABLE,ERRORIMPAIRED, ou UNHEALTHY après avoir été démarré.
- `aws:executeAwsApi`- Recueille l'état de la machine WorkSpace après le démarrage.
- `aws:branch`- Branches basées sur l'état de la WorkSpace machine après le démarrage.
- `aws:executeAwsApi`- Rassemble les instantanés disponibles pour restaurer ou reconstruire le WorkSpace
- `aws:branch`- Branches basées sur la valeur que vous spécifiez pour le `Reboot` paramètre.
- `aws:executeAwsApi`- Redémarre le WorkSpace
- `aws:executeAwsApi`- Recueille l'état de la machine WorkSpace après le démarrage.
- `aws:waitForAwsResourceProperty`- Attend que l'état du WorkSpace passe àREBOOTING.
- `aws:waitForAwsResourceProperty`- Attend que l' WorkSpace état passe à AVAILABLE,ERROR, ou UNHEALTHY après avoir été redémarré.
- `aws:executeAwsApi`- Recueille l'état du WorkSpace après le redémarrage.
- `aws:branch`- Branches basées sur l'état du WorkSpace après le redémarrage.
- `aws:branch`- Branches basées sur la valeur que vous spécifiez pour le `Restore` paramètre.
- `aws:executeAwsApi`- Restaure le WorkSpace. Si la restauration échoue, le runbook essaie de reconstruire le WorkSpace.
- `aws:waitForAwsResourceProperty`- Attend que l'état du WorkSpace passe àRESTORING.

- `aws:waitForAwsResourceProperty`- Attend que l' Workspace état passe à `AVAILABLEERROR`, ou `UNHEALTHY` après avoir été restauré.
- `aws:executeAwsApi`- Rassemble l'état de l' Workspace objet restauré.
- `aws:branch`- Branches basées sur l'état de l' Workspace après restauration.
- `aws:branch`- Branches basées sur la valeur que vous spécifiez pour le `Rebuild` paramètre.
- `aws:executeAwsApi`- Reconstitue le Workspace
- `aws:waitForAwsResourceProperty`- Attend que l'état du Workspace passe à `REBUILDING`.
- `aws:waitForAwsResourceProperty`- Attend que l' Workspace État change ou `UNHEALTHY` après avoir été reconstruit. `AVAILABLE ERROR`
- `aws:executeAwsApi`- Rassemble l'état de l' Workspace après sa reconstruction.
- `aws:assertAwsResourceProperty`- Confirme l'état du Workspace si `AVAILABLE`.

## X-Ray

AWS Systems Manager L'automatisation fournit des runbooks prédéfinis pour AWS X-Ray. Pour plus d'informations sur les runbooks, consultez la section [Utilisation des runbooks](#). Pour plus d'informations sur la façon d'afficher le contenu du runbook, consultez [Afficher le contenu du runbook](#).

### Rubriques

- [AWSConfigRemediation-UpdateXRayKMSKey](#)

## AWSConfigRemediation-UpdateXRayKMSKey

### Description

Le `AWSConfigRemediation-UpdateXRayKMSKey` runbook permet de chiffrer vos AWS X-Ray données à l'aide d'une clé AWS Key Management Service (AWS KMS). Ce runbook ne doit être utilisé que comme référence pour garantir que vos AWS X-Ray données sont cryptées conformément aux meilleures pratiques de sécurité minimales recommandées. Nous recommandons de chiffrer plusieurs ensembles de données avec différentes clés KMS.

[Exécuter cette automatisation \(console\)](#)

### Type de document

Automatisation

## Propriétaire

Amazon

## Plateformes

Linux macOS, Windows

## Paramètres

- AutomationAssumeRole

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom.

- KeyId

Type : chaîne

Description : (Obligatoire) Le nom de ressource Amazon (ARN), l'ID de clé ou l'alias de clé KMS que vous AWS X-Ray souhaitez utiliser pour chiffrer les données.

## Autorisations IAM requises

Le AutomationAssumeRole paramètre nécessite les actions suivantes pour utiliser correctement le runbook.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:DescribeKey
- xray:GetEncryptionConfig
- xray:PutEncryptionConfig

## Étapes de document

- aws:executeAwsApi- Active le chiffrement de vos données X-Ray à l'aide de la clé KMS que vous spécifiez dans le KeyId paramètre.



- `aws:waitForAwsResourceProperty`- Attend que l'état de la configuration de chiffrement de votre X-Ray soit ACTIVE atteint.
- `aws:executeAwsApi`- Rassemble l'ARN de la clé que vous spécifiez dans le `KeyId` paramètre.
- `aws:assertAwsResourceProperty`- Vérifie que le chiffrement a été activé sur votre X-Ray.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.