



Guía del usuario de

AWS Systems Manager Referencia del manual de automatización



AWS Systems Manager Referencia del manual de automatización: Guía del usuario de

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Referencia del manual de procedimientos de Automatización	1
Cómo ver contenido del manual de procedimientos	4
API Gateway	4
AWSConfigRemediation-DeleteAPIGatewayStage	5
AWSConfigRemediation-EnableAPIGatewayTracing	6
AWSConfigRemediation-UpdateAPIGatewayMethodCaching	7
AWSSupport-TroubleshootAPIGatewayHttpErrors	9
AWS Batch	14
AWSSupport-TroubleshootAWSBatchJob	14
CloudFormation	20
AWS-DeleteCloudFormationStack	21
AWS-EnableCloudFormationSNSNotification	22
AWS-RunCfnLint	24
AWSSupport-TroubleshootCFNCustomResource	26
AWS-UpdateCloudFormationStack	28
CloudFront	29
AWSConfigRemediation-EnableCloudFrontDefaultRootObject	29
AWSConfigRemediation-EnableCloudFrontAccessLogs	31
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity	33
AWSConfigRemediation-EnableCloudFrontOriginFailover	35
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS	36
CloudTrail	38
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail	39
AWS-EnableCloudTrail	40
AWS-EnableCloudTrailCloudWatchLogs	42
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS	43
AWS-EnableCloudTrailKmsEncryption	45
AWSConfigRemediation-EnableCloudTrailLogFileValidation	46
AWS-EnableCloudTrailLogFileValidation	48
AWS-QueryCloudTrailLogs	49
CloudWatch	51
AWS-ConfigureCloudWatchOnEC2Instance	51
AWS-EnableCWAlarm	53
AWSSupport-TroubleshootCloudWatchAgent	55

AWSSupport-TroubleshootCloudWatchAlarm	62
Amazon DocumentDB	70
AWS-EnableDocDbClusterBackupRetentionPeriod	70
CodeBuild	72
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMScmk	73
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject	74
AWS CodeDeploy	76
AWSSupport-TroubleshootCodeDeploy	76
AWS Config	78
AWSSupport-SetupConfig	78
Amazon Connect	81
AWSSupport-AssociatePhoneNumbersToConnectContactFlows	82
AWSSupport-CollectAmazonConnectContactFlowLog	90
AWS Directory Service	96
AWS-CreateDSManagementInstance	97
AWSSupport-TroubleshootADConnectorConnectivity	102
AWSSupport-TroubleshootDirectoryTrust	105
AWS AppSync	109
AWS-EnableAppSyncGraphQLApiLogging	109
Amazon Athena	112
AWS-EnableAthenaWorkGroupEncryptionAtRest	112
DynamoDB	114
AWS-ChangeDDBRWCapacityMode	115
AWS-CreateDynamoDBBackup	117
AWS-DeleteDynamoDbBackup	118
AWSConfigRemediation-DeleteDynamoDbTable	119
AWS-DeleteDynamoDbTableBackups	120
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable	122
AWSConfigRemediation-EnablePITRForDynamoDbTable	123
AWS-EnableDynamoDbAutoscaling	125
AWS-RestoreDynamoDBTable	128
AWS Database Migration Service	131
AWSSupport-TroubleshootDMSTableErrors	131
AWSSupport-TroubleshootDMSEndpointConnection	137
Amazon EBS	148
AWSSupport-AnalyzeEBSResourceUsage	148

AWS-ArchiveEBSSnapshots	155
AWS-AttachEBSVolume	157
AWSSupport-CalculateEBSPerformanceMetrics	158
AWS-CopySnapshot	165
AWS-CreateSnapshot	166
AWS-DeleteSnapshot	167
AWSConfigRemediation-DeleteUnusedEBSVolume	168
AWS-DeregisterAMIs	170
AWS-DetachEBSVolume	172
AWSConfigRemediation-EnableEbsEncryptionByDefault	173
AWS-ExtendEbsVolume	174
AWSSupport-ModifyEBSSnapshotPermission	176
AWSConfigRemediation-ModifyEBSVolumeType	179
Amazon EC2	180
AWS-ASGEnterStandby	183
AWS-ASGExitStandby	184
AWS-CreateImage	185
AWS-DeleteImage	186
AWS-PatchAsgInstance	188
AWS-PatchInstanceWithRollback	191
AWS-QuarantineEC2Instance	193
AWS-ResizeInstance	195
AWS-RestartEC2Instance	196
AWS-SetupJupyter	197
AWS-StartEC2Instance	201
AWS-StopEC2Instance	202
AWS-TerminateEC2Instance	202
AWS-UpdateLinuxAmi	203
AWS-UpdateWindowsAmi	207
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck	212
AWSConfigRemediation-EnforceEC2InstanceIMDSv2	213
AWSEC2-CloneInstanceAndUpgradeSQLServer	215
AWSEC2-CloneInstanceAndUpgradeWindows	219
AWSEC2-PatchLoadBalancerInstance	223
AWSEC2-SQLServerDBRestore	224
AWSSupport-ActivateWindowsWithAmazonLicense	230

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2	233
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD	238
AWSSupport-CheckXenToNitroMigrationRequirements	244
AWSSupport-CloneXenEC2InstanceAndMigrateToNitro	247
AWSSupport-CollectSAPHANALogs	255
AWSSupport-ConfigureEC2Metadata	261
AWSSupport-ContainEC2Instance	265
AWSSupport-CopyEC2Instance	276
AWSPremiumSupport-DiagnoseDiskUsageOnLinux	281
AWSSupport-EnableWindowsEC2SerialConsole	285
AWSPremiumSupport-ExtendVolumesOnWindows	293
AWSSupport-ExecuteEC2Rescue	298
AWSSupport-ListEC2Resources	301
AWSSupport-ManageRDPSettings	304
AWSSupport-ManageWindowsService	306
AWSSupport-MigrateEC2ClassicToVPC	308
AWSSupport-MigrateXenToNitroLinux	315
AWSSupport-ResetAccess	327
AWSSupport-ResetLinuxUserPassword	330
AWSSupport-RunEC2RescueForWindowsTool	337
AWSPremiumSupport-ResizeNitroInstance	341
AWSSupport-ShareEncryptedAMIOrEBSSnapshot	349
AWSSupport-RestoreEC2InstanceFromSnapshot	354
AWSSupport-SendLogBundleToS3Bucket	358
AWSSupport-StartEC2RescueWorkflow	360
AWSSupport-TroubleshootActiveDirectoryReplication	371
AWSPremiumSupport-TroubleshootEC2DiskUsage	376
AWSSupport-TroubleshootEC2InstanceConnect	381
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs	388
AWSSupport-TroubleshootRDP	391
AWSSupport-TroubleshootSSH	397
AWSSupport-TroubleshootSUSERegistration	401
AWSSupport-TroubleshootWindowsPerformance	403
AWSSupport-TroubleshootWindowsUpdate	411
AWSSupport-UpgradeWindowsAWSDrivers	418
Amazon ECS	422

AWSSupport-CollectECSInstanceLogs	423
AWS-InstallAmazonECSAgent	425
AWS-ECSRunTask	427
AWSSupport-TroubleshootECSContainerInstance	431
AWSSupport-TroubleshootECSTaskFailedToStart	433
AWS-UpdateAmazonECSAgent	438
Amazon EFS	440
AWSSupport-CheckAndMountEFS	440
Amazon EKS	443
AWS-CreateEKSClusterWithFargateProfile	444
AWS-CreateEKSClusterWithNodegroup	448
AWS-DeleteEKSCluster	451
AWS-MigrateToNewEKSSelfManagedNodeGroup	454
AWSPremiumSupport-TroubleshootEKSCluster	460
AWSSupport-TroubleshootEKSWorkerNode	464
AWS-UpdateEKSCluster	467
AWS-UpdateEKSMangedNodeGroup	468
AWS-UpdateEKSSelfManagedLinuxNodeGroups	472
AWSSupport-CollectEKSLinuxNodeStatistics	476
AWSSupport-CollectEKSInstanceLogs	482
AWSSupport-SetupK8sApiProxyForEKS	486
AWSSupport-TroubleshootEbsCsiDriversForEks	497
AWSSupport-TroubleshootEKSSALBControllerIssues	506
AWSSupport-TroubleshootEKSDNSFailure	518
Elastic Beanstalk	524
AWSSupport-CollectElasticBeanstalkLogs	525
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ..	528
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications	529
AWSSupport-TroubleshootElasticBeanstalk	531
Elastic Load Balancing	534
AWSConfigRemediation-DropInvalidHeadersForALB	534
AWS-EnableCLBAccessLogs	536
AWS-EnableCLBConnectionDraining	538
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing	540
AWSConfigRemediation-EnableELBDeletionProtection	541
AWSConfigRemediation-EnableLoggingForALBAndCLB	543

AWSSupport-TroubleshootCLBConnectivity	544
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing	548
AWS-UpdateALBDesyncMitigationMode	549
AWS-UpdateCLBDesyncMitigationMode	551
AWSSupport-TroubleshootELBHealthChecks	553
Amazon EMR	558
AWSSupport-AnalyzeEMRLogs	558
AWSSupport-DiagnoseEMRLogsWithAthena	564
OpenSearch Servicio Amazon	573
AWSConfigRemediation-DeleteOpenSearchDomain	574
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain	575
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups	577
AWSSupport-TroubleshootOpenSearchRedYellowCluster	578
AWSSupport-TroubleshootOpenSearchHighCPU	585
EventBridge	592
AWS-AddOpsItemDedupStringToEventBridgeRule	592
AWS-DisableEventBridgeRule	593
AWS Glue	595
AWSSupport-TroubleshootGlueConnection	595
Amazon FSx	606
AWSSupport-ValidateFSxWindowsADConfig	607
GuardDuty	621
AWSConfigRemediation-CreateGuardDutyDetector	621
IAM	622
AWSSupport-TroubleshootIAMAccessDeniedEvents	623
AWS-AttachIAMToInstance	630
AWS-DeleteIAMInlinePolicy	632
AWSConfigRemediation-DeleteIAMRole	633
AWSConfigRemediation-DeleteIAMUser	635
AWSConfigRemediation-DeleteUnusedIAMGroup	638
AWSConfigRemediation-DeleteUnusedIAMPolicy	639
AWSConfigRemediation-DetachIAMPolicy	640
AWSConfigRemediation-EnableAccountAccessAnalyzer	642
AWSSupport-GrantPermissionsToIAMUser	643
AWSConfigRemediation-RemoveUserPolicies	648
AWSConfigRemediation-ReplaceIAMInlinePolicy	650

AWSConfigRemediation-RevokeUnusedIAMUserCredentials	652
AWSConfigRemediation-SetIAMPasswordPolicy	654
AWSSupport-ContainIAMPrincipal	657
AWSSupport-TroubleshootSAMLIssues	672
Detección y respuesta a incidentes	677
AWSPremiumSupport-OnboardWorkloadToIDR	678
Amazon Kinesis Data Streams	685
AWS-EnableKinesisStreamEncryption	686
AWS KMS	687
AWSConfigRemediation-CancelKeyDeletion	688
AWSConfigRemediation-EnableKeyRotation	689
Lambda	691
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing	691
AWSConfigRemediation-DeleteLambdaFunction	693
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK	694
AWSConfigRemediation-MoveLambdaToVPC	696
AWSSupport-RemediateLambdaS3Event	697
AWSSupport-TroubleshootLambdaInternetAccess	700
AWSSupport-TroubleshootLambdaS3Event	704
Amazon Managed Workflows para Apache Airflow	706
AWSSupport-TroubleshootMWAAEnvironmentCreation	706
Neptune	713
AWS-EnableNeptuneDbAuditLogsToCloudWatch	713
AWS-EnableNeptuneDbBackupRetentionPeriod	715
AWS-EnableNeptuneClusterDeletionProtection	717
Amazon RDS	718
AWS-CreateEncryptedRdsSnapshot	719
AWS-CreateRdsSnapshot	722
AWSConfigRemediation-DeleteRDSCluster	723
AWSConfigRemediation-DeleteRDSClusterSnapshot	725
AWSConfigRemediation-DeleteRDSInstance	726
AWSConfigRemediation-DeleteRDSInstanceSnapshot	728
AWSConfigRemediation-DisablePublicAccessToRDSInstance	730
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster	731
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance	733
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance	735

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance	737
AWSConfigRemediation-EnableMultiAZOnRDSInstance	738
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance	740
AWSConfigRemediation-EnableRDSClusterDeletionProtection	743
AWSConfigRemediation-EnableRDSInstanceBackup	744
AWSConfigRemediation-EnableRDSInstanceDeletionProtection	746
AWSConfigRemediation-ModifyRDSInstancePortNumber	748
AWSSupport-ModifyRDSSnapshotPermission	750
AWSPremiumSupport-PostgreSQLWorkloadReview	752
AWS-RebootRdsInstance	769
AWSSupport-ShareRDSSnapshot	770
AWS-StartRdsInstance	774
AWS-StartStopAuroraCluster	775
AWS-StopRdsInstance	777
AWSSupport-TroubleshootConnectivityToRDS	778
AWSSupport-TroubleshootRDSIAMAuthentication	780
AWSSupport-ValidateRdsNetworkConfiguration	788
Amazon Redshift	794
AWSConfigRemediation-DeleteRedshiftCluster	794
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster	796
AWSConfigRemediation-EnableRedshiftClusterAuditLogging	797
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot	799
AWSConfigRemediation-EnableRedshiftClusterEncryption	801
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting	802
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster	804
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings	805
AWSConfigRemediation-ModifyRedshiftClusterNodeType	807
Amazon S3	809
AWS-ArchiveS3BucketToIntelligentTiering	810
AWS-ConfigureS3BucketLogging	812
AWS-ConfigureS3BucketVersioning	815
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock	816
AWSConfigRemediation-ConfigureS3PublicAccessBlock	818
AWS-CreateS3PolicyToExpireMultipartUploads	821
AWS-DisableS3BucketPublicReadWrite	823
AWS-EnableS3BucketEncryption	823

AWS-EnableS3BucketKeys	825
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy	827
AWSConfigRemediation-RestrictBucketSSLRequestsOnly	828
AWSSupport-TroubleshootS3PublicRead	829
AWSSupport-ConfigureS3ReplicationSameAndCrossAccount	835
AWSSupport-EmptyS3Bucket	854
AWSSupport-TroubleshootS3EventNotifications	861
AWSSupport-ContainS3Resource	868
Amazon SES	877
AWSSupport-AnalyzeSESMessagesSendingStatus	878
AWSSupport-DeploySESSendingLogsToCloudWatchLogs	882
SageMaker IA	889
AWS-DisableSageMakerNotebookRootAccess	889
AWSSupport-RequestSageMakerLimitIncrease	891
Secrets Manager	895
AWSConfigRemediation-DeleteSecret	895
AWSConfigRemediation-RotateSecret	897
CSPM de Security Hub	898
AWSConfigRemediation-EnableSecurityHub	899
AWS Shield	900
AWSPremiumSupport-DDoSResiliencyAssessment	900
Amazon SNS	909
AWS-EnableSNSTopicDeliveryStatusLogging	910
AWSConfigRemediation-EncryptSNSTopic	912
AWS-PublishSNSNotification	914
Amazon SQS	915
AWS-EnableSQSEncryption	915
Step Functions	917
AWS-EnableStepFunctionsStateMachineLogging	918
Systems Manager	920
AWS-BulkDeleteAssociation	921
AWS-BulkEditOpsItems	922
AWS-BulkResolveOpsItems	925
AWS-ConfigureMaintenanceWindows	927
AWS-CreateManagedLinuxInstance	929
AWS-CreateManagedWindowsInstance	931

AWSConfigRemediation-EnableCWLoggingForSessionManager	934
AWS-ExportOpsDataToS3	935
AWS-ExportPatchReportToS3	937
AWS-SetupInventory	939
AWS-SetupManagedInstance	943
AWS-SetupManagedRoleOnEC2Instance	945
AWSSupport-TroubleshootManagedInstance	946
AWSSupport-TroubleshootPatchManagerLinux	949
AWSSupport-TroubleshootSessionManager	952
De terceros	958
AWS-CreateJiraIssue	958
AWS-CreateServiceNowIncident	961
AWS-RunPacker	963
Amazon VPC	965
AWS-CloseSecurityGroup	966
AWSSupport-ConfigureDNSQueryLogging	968
AWSSupport-ConfigureTrafficMirroring	971
AWSSupport-ConnectivityTroubleshooter	973
AWSSupport-TroubleshootVPN	977
AWSConfigRemediation-DeleteEgressOnlyInternetGateway	983
AWSConfigRemediation-DeleteUnusedENI	985
AWSConfigRemediation-DeleteUnusedSecurityGroup	986
AWSConfigRemediation-DeleteUnusedVPCNetworkACL	987
AWSConfigRemediation-DeleteVPCFlowLog	989
AWSConfigRemediation-DetachAndDeleteInternetGateway	990
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway	992
AWS-DisableIncomingSSHOnPort22	994
AWS-DisablePublicAccessForSecurityGroup	995
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP	997
AWSSupport-EnableVPCFlowLogs	998
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch	1005
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket	1007
AWS-ReleaseElasticIP	1009
AWS-RemoveNetworkACLUnrestrictedSSHRDP	1010
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules	1012
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules	1013

AWSSupport-SetupIPMonitoringFromVPC	1014
AWSSupport-TerminateIPMonitoringFromVPC	1023
AWS WAF	1026
AWS-AddWAFRegionalRuleToRuleGroup	1027
AWS-AddWAFRegionalRuleToWebAcl	1029
AWSConfigRemediation-EnableWAFClassicLogging	1032
AWSConfigRemediation-EnableWAFClassicRegionalLogging	1033
AWSConfigRemediation-EnableWAFV2Logging	1035
Amazon WorkSpaces	1037
AWS-CreateWorkSpace	1037
AWSSupport-RecoverWorkSpace	1040
X-Ray	1044
AWSConfigRemediation-UpdateXRayKMSKey	1045
.....	mxlvii

Referencia del manual de procedimientos de Automatización de Systems Manager

Para ayudarle a empezar rápidamente, AWS Systems Manager proporciona manuales de ejecución predefinidos. Estos manuales son mantenidos por Amazon Web Services, AWS Support, y AWS Config. La referencia del manual describe cada uno de los manuales de ejecución predefinidos proporcionados por Systems Manager Soporte, y. AWS Config

Important

Si ejecuta un flujo de trabajo de automatización que invoca otros servicios mediante un rol de servicio de AWS Identity and Access Management (IAM), tenga en cuenta que el rol de servicio debe configurarse con el permiso necesario para invocar dichos servicios. Este requisito se aplica a todos los manuales de procedimientos de Automatización de AWS (manuales de AWS- *), como los manuales de procedimientos AWS-ConfigureS3BucketLogging, AWS-CreateDynamoDBBackup y AWS-RestartEC2Instance, por nombrar algunos. Este requisito también se aplica a todos los manuales de automatización personalizados que cree y que invoquen otros AWS servicios mediante acciones que llamen a otros servicios. Por ejemplo, si utiliza las acciones `aws:executeAwsApi`, `aws:createStack` o `aws:copyImage`, debe configurar el rol de servicio con el permiso necesario para invocar esos servicios. Puedes habilitar los permisos para otros AWS servicios añadiendo una política integrada de IAM al rol. Para obtener más información, consulte [Añadir una política integrada de automatización para invocar otros servicios](#). AWS

Esta referencia incluye temas que describen cada uno de los manuales de ejecución de Systems Manager propiedad de AWS AWS Support, y AWS Config. Los manuales están organizados por los correspondientes. Servicio de AWS Cada página proporciona una explicación de los parámetros obligatorios y opcionales que se pueden especificar al utilizar el manual de procedimientos. Cada página también muestra una lista de los pasos que se indican en el manual de procedimientos y la salida de la automatización, si la hay.

Esta referencia no incluye una página separada para los manuales que requieren aprobación, como el manual de procedimientos AWS-CreateManagedLinuxInstanceWithApproval o AWS-StopEC2InstanceWithApproval. Cualquier nombre de manual de procedimientos que incluya

WithApproval significa que el manual de procedimientos incluye la acción [aws:approve](#). Esta acción detiene temporalmente una automatización hasta que las entidades principales designadas aprueben o rechacen la acción. Después de que se alcanza el número necesario de aprobaciones, se reanuda la automatización.

Para obtener información acerca de la ejecución de las automatizaciones, consulte [Ejecución de una automatización sencilla](#). Para obtener información sobre cómo ejecutar automatizaciones en varios objetivos, consulte [Running automations that use targets and rate controls](#).

Temas

- [Cómo ver contenido del manual de procedimientos](#)
- [API Gateway](#)
- [AWS Batch](#)
- [CloudFormation](#)
- [CloudFront](#)
- [CloudTrail](#)
- [CloudWatch](#)
- [Amazon DocumentDB](#)
- [CodeBuild](#)
- [AWS CodeDeploy](#)
- [AWS Config](#)
- [Amazon Connect](#)
- [AWS Directory Service](#)
- [AWS AppSync](#)
- [Amazon Athena](#)
- [DynamoDB](#)
- [AWS Database Migration Service](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [Amazon ECS](#)
- [Amazon EFS](#)
- [Amazon EKS](#)

- [Elastic Beanstalk](#)
- [Elastic Load Balancing](#)
- [Amazon EMR](#)
- [OpenSearch Servicio Amazon](#)
- [EventBridge](#)
- [AWS Glue](#)
- [Amazon FSx](#)
- [GuardDuty](#)
- [IAM](#)
- [Detección y respuesta a incidentes](#)
- [Amazon Kinesis Data Streams](#)
- [AWS KMS](#)
- [Lambda](#)
- [Amazon Managed Workflows para Apache Airflow](#)
- [Neptune](#)
- [Amazon RDS](#)
- [Amazon Redshift](#)
- [Amazon S3](#)
- [Amazon SES](#)
- [SageMaker IA](#)
- [Secrets Manager](#)
- [CSPM de Security Hub](#)
- [AWS Shield](#)
- [Amazon SNS](#)
- [Amazon SQS](#)
- [Step Functions](#)
- [Systems Manager](#)
- [De terceros](#)
- [Amazon VPC](#)

- [AWS WAF](#)
- [Amazon WorkSpaces](#)
- [X-Ray](#)

Cómo ver contenido del manual de procedimientos

Puede ver el contenido de los manuales de procedimientos en la consola de Systems Manager.

Cómo ver el contenido del manual de procedimientos

1. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>
2. En el panel de navegación, elija Documentos.

-o bien-

Si la página de AWS Systems Manager inicio se abre primero, elija el icono de menú () para abrir el panel de navegación y, a continuación, elija Documentos en el panel de navegación.

3. En la sección Categorías, seleccione Documentos de automatización.
4. Elija un manual de procedimientos y, a continuación, elija View details (Ver detalles).
5. Elija la pestaña Content.

API Gateway

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon API Gateway. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

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

AWSConfigRemediation-DeleteAPIGatewayStage

Descripción

El AWSConfigRemediation-DeleteAPIGatewayStage runbook elimina una etapa de Amazon API Gateway (API Gateway). AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- StageArn

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) de la etapa API Gateway que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`: elimina la etapa de API Gateway especificada en el parámetro `StageArn`.

AWSConfigRemediation-EnableAPIGatewayTracing

Descripción

El `AWSConfigRemediation-EnableAPIGatewayTracing` runbook permite el rastreo en una etapa de Amazon API Gateway (API Gateway). AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- StageArn

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) de la etapa de API Gateway en la que desea habilitar el seguimiento.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- aws:executeScript: habilita el rastreo en la etapa API Gateway especificada en el parámetro StageArn.

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

Descripción

El manual de procedimientos AWSConfigRemediation-UpdateAPIGatewayMethodCaching actualiza la configuración del método de caché para un recurso de etapa de Amazon API Gateway.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- CachingAuthorizedMethods

Tipo: StringList

Descripción: (obligatorio) los métodos autorizados para habilitar el almacenamiento en caché. La lista debe ser una combinación de DELETE, GET, HEAD, OPTIONS, PATCH, POST y PUT. El almacenamiento en caché está habilitado para los métodos seleccionados y deshabilitado para los métodos no seleccionados. El almacenamiento en caché está habilitado para todos los métodos si ANY está seleccionado y está deshabilitado para todos los métodos si NONE está seleccionado.

- StageArn

Tipo: cadena

Descripción: (obligatorio) el ARN de la etapa API Gateway para la API REST.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`: acepta el ID de recurso de la etapa como entrada, actualiza la configuración del método de caché para una etapa de API Gateway mediante la acción de la API `UpdateStage` y verifica la actualización.

AWSSupport-TroubleshootAPIGatewayHttpErrors

Descripción

El `AWSSupport-TroubleshootAPIGatewayHttpErrors` manual ayuda a solucionar los errores 5XX/4XX al invocar una API REST de Amazon API Gateway implementada mediante el análisis de los registros de ejecución de and/or acceso y el análisis de los errores para proporcionar medidas de corrección mediante los artículos y la documentación de Re:post. AWS

Important

Este manual tiene las siguientes limitaciones:

- El registro debe estar habilitado. Consulte [Configurar el registro de CloudWatch API de Amazon mediante la consola API Gateway](#).
- Los registros deben estar habilitados antes de que se produjeran los errores. La captura y el análisis de los registros no se pueden realizar de forma retrospectiva.
- Errores cubiertos: 500, 502, 503, 504, 401, 403, 429.
- Solo APIs se admiten REST. WebSocket y HTTP (v2) no están incluidos en este manual.

Important

El uso de este runbook puede generar cargos adicionales en su AWS cuenta por los Amazon CloudWatch Logs capturados por su API REST y por CloudWatch los Logs Insights utilizados en el análisis. Consulta [CloudWatch los precios de Amazon](#) para obtener más información sobre los cargos en los que se puede incurrir. Si el `aws:deletestack` paso no funciona, ve a la CloudFormation consola para eliminar manualmente la pila. El nombre de la pila creado por este manual de procedimientos comienza por `AWSSupport-TroubleshootAPIGatewayHttpErrors`. Para obtener información sobre la eliminación de CloudFormation pilas, consulte [Eliminar una pila](#) en la Guía del AWS CloudFormation usuario.

¿Cómo funciona?

El manual de ejecución realiza los siguientes pasos de validación y análisis:

- Valida que la API REST especificada existe y que usted tiene los permisos necesarios.
- Valida que la etapa especificada existe en la API.
- Valida que la ruta de recursos especificada existe en la API.
- Valida que el método HTTP especificado existe para el recurso.
- Analiza CloudWatch los registros en busca de los parámetros y el intervalo de tiempo especificados para identificar los errores y proporcionar recomendaciones de corrección.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `apigateway:GET`
- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:PutLogEvents`
- `logs:StartQuery`
- `logs:GetQueryResults`

Política de IAM de ejemplo:

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

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSsupport-TroubleshootAPIGatewayHttpErrors](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a SSM Automation realizar las acciones en su nombre. Si no se especifica ningún rol, SSM Automation utiliza los permisos del usuario que inicia este manual.
 - Tipo: `AWS::IAM::Role::Arn`
 - RestApild (Obligatorio):

- Descripción: (obligatorio) El ID de API de la API que requiere la solución de problemas. Debe ser una cadena alfanumérica de 10 caracteres.
- Tipo: String
- Valor permitido: `^[a-zA-Z0-9]{10}$`
- StageName (Obligatorio):
 - Descripción: (Obligatorio) El nombre de la etapa desplegada. Debe tener entre 1 y 128 caracteres y contener letras, números, guiones bajos o guiones.
 - Tipo: String
 - Valor permitido: `^[a-zA-Z0-9_\\-]{1,128}$`
- ResourcePath (Opcional):
 - Descripción: (opcional) La ruta del recurso para la que se configura el método. Ejemplos: `/`, `/store/items`, `/resource`.
 - Tipo: String
 - Valor predeterminado: `/`
- HttpMethod (Opcional):
 - Descripción: (opcional) El método de la ruta de recursos configurada.
 - Tipo: String
 - Valores permitidos: `[ANY, DELETE, HEAD, OPTIONS, GET, POST, PUT, PATCH]`
 - Valor predeterminado: `GET`
- StartTime (Opcional):
 - Descripción: (opcional) La fecha y hora de inicio de la consulta de los CloudWatch registros. Formato: `yyyy-MM-ddTHH:mm:ss` en la zona horaria UTC. Si no se especifica, el valor predeterminado es 3 días antes de la hora actual.
 - Tipo: String
 - Valor permitido: `^$|^([0-9]{4}-([01-9]|1[0-2])-([01-9]|1[0-2])[0-9]|3[0-1])T([0-3]|01)[0-9]:[0-5][0-9]:[0-5][0-9]$`
 - Valor predeterminado: `""`
- EndTime (Opcional):
 - Descripción: (opcional) Fecha y hora de finalización de la consulta de los CloudWatch registros. Formato: `yyyy-MM-ddTHH:mm:ss` en la zona horaria UTC. Si no se especifica, el valor predeterminado es la hora actual.
 - Tipo: String

- Valor permitido: `^$|^([0-9]{4}-([01-9]|1[0-2])-([01-9]|1[0-2][0-9]|3[0-1])T(2[0-3]|([01][0-9])):[0-5][0-9]:[0-5][0-9])$`
- Valor predeterminado: `""`
- AccessLogs (Opcional):
 - Descripción: (opcional) Si se deben analizar los registros de acceso.
 - Tipo: `Boolean`
 - Valores permitidos: `[true, false]`
 - Valor predeterminado: `false`
- RequestId (Opcional):
 - Descripción: (opcional) El identificador de la solicitud en la que se observó un error. Debe tener un formato de UUID válido.
 - Tipo: `String`
 - Valor permitido: `^$|^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})$`
 - Valor predeterminado: `""`

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- CheckApiExists:

Valida que la API REST proporcionada existe y que tienes los permisos necesarios para acceder a ella.

- CheckStageExists:

Valida que el nombre de etapa proporcionado existe en la API en cuestión y recupera la información del grupo de registros de acceso.

- CheckResourceExists:

Valida que la ruta de recurso proporcionada existe en la API y recupera el ID del recurso.

- CheckMethodExists:

Valida que el método HTTP proporcionado existe para el recurso especificado.

- AnalyseLogs:

Busca registros con los parámetros proporcionados y devuelve recomendaciones en función de los errores encontrados. Este paso analiza los registros de ejecución y acceso (si están habilitados) para identificar los errores 4XX y 5XX y proporciona una guía de corrección específica.

7. Una vez finalizado, consulte la sección de resultados para ver los resultados detallados de la ejecución, incluidos el análisis de errores y las recomendaciones de corrección.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWS Batch

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Batch Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-TroubleshootAWSBatchJob](#)

AWSSupport - TroubleshootAWSBatchJob

Descripción

El AWSSupport-TroubleshootAWSBatchJob manual le ayuda a solucionar los problemas que impiden que un AWS Batch trabajo pase de un estado a RUNNABLE otro. STARTING

¿Cómo funciona?

Este manual realiza las siguientes comprobaciones:

- Si el entorno informático está en DISABLED estado INVALID o.
- Si el Max vCPU parámetro del entorno de cómputo es lo suficientemente grande como para acomodar el volumen de trabajos de la cola de trabajos.
- Si los trabajos requieren más recursos de memoria CPUs o v de los que pueden proporcionar los tipos de instancias del entorno de cómputo.
- Si los trabajos deben ejecutarse en instancias basadas en GPU, pero el entorno de procesamiento no está configurado para usar instancias basadas en GPU.
- Si el grupo de Auto Scaling del entorno de cómputo no pudo lanzar las instancias.
- Si las instancias lanzadas pueden unirse al clúster subyacente de Amazon Elastic Container Service (Amazon ECS); de lo contrario, ejecuta [AWSSupport-TroubleshootECSContainerInstance](#) el runbook.
- Si hay algún problema con los permisos que bloquea acciones específicas necesarias para ejecutar el trabajo.

Important

- Este manual debe iniciarse en la misma AWS región en la que se encuentra el trabajo cuyo RUNNABLE estado está estancado.
- Este manual se puede iniciar para los AWS Batch trabajos programados en instancias de Amazon ECS AWS Fargate o Amazon Elastic Compute Cloud (Amazon EC2). Si se inicia la automatización para un AWS Batch trabajo en Amazon Elastic Kubernetes Service (Amazon EKS), la iniciación se detiene.
- Si hay instancias disponibles para ejecutar el trabajo pero no registran el clúster de Amazon ECS, este manual de ejecución inicia el manual de [AWSSupport-TroubleshootECSContainerInstance](#) automatización para intentar determinar el motivo. Para obtener más información, consulte el manual de ejecución. [AWSSupport-TroubleshootECSContainerInstance](#)

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- JobId

Tipo: cadena

Descripción: (Obligatorio) El ID del AWS Batch Job cuyo RUNNABLE estado está atascado.

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

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Instrucciones

1. Navegue hasta [AWSSupport-TroubleshootAWSBatchJob](#) la AWS Systems Manager consola.

2. Elija Ejecutar automatización

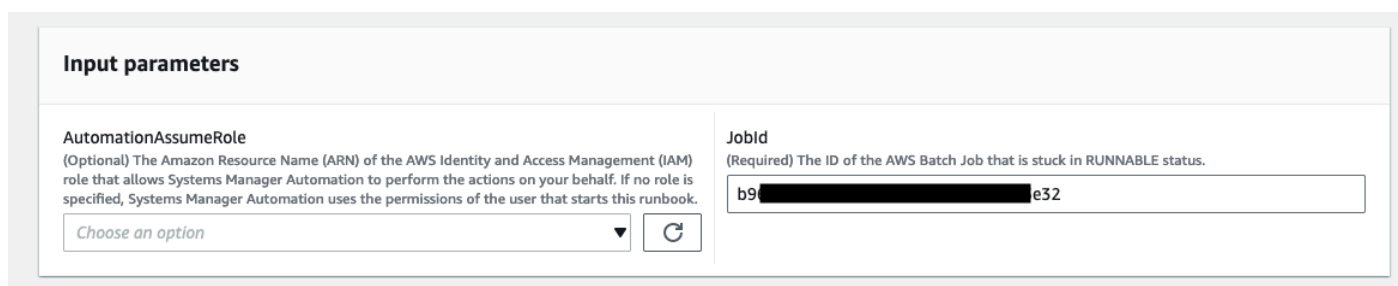
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole(Opcional):

El nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- JobId(Obligatorio):

El ID del AWS Batch Job que está atascado en el RUNNABLE estado.



Input parameters

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

4. Seleccione Ejecutar.

5. Observe que se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- PreflightPermissionChecks:

Realiza comprobaciones previas a la verificación de los permisos de IAM con el usuario o rol iniciador. Si falta algún permiso, en este paso se indican las acciones de la API que faltan en la sección de resultados globales.

- ProceedOnlyIfUserHasPermission:

Se ramifica en función de si tiene permisos para realizar todas las acciones necesarias para el manual.

- AWSBatchJobEvaluation:

Realiza comprobaciones con respecto al AWS Batch Job para comprobar que existe y se encuentra en ese RUNNABLE estado.

- ProceedOnlyIfBatchJobExistsAndIsinRunnableEstado:

~~Las sucursales se basan en si el trabajo existe y se encuentra en ese RUNNABLE estado.~~

- `BatchComputeEnvironmentEvaluation`:

Realiza comprobaciones con respecto al entorno AWS Batch informático.

- `ProceedOnlyIfComputeEnvironmentChecksAreDe acuerdo`:

Las ramas se basan en si las comprobaciones del entorno de cómputo se realizaron correctamente.

- `UnderlyingInfraEvaluation`:

Realiza comprobaciones con respecto a la solicitud subyacente de Auto Scaling Group o Spot Fleet.

- `ProceedOnlyIfInstancesNotJoiningEcsCluster`:

Las sucursales se basan en si hay instancias que no se unen al clúster de Amazon ECS.

- `EcsAutomationRunner`:

Ejecuta la automatización de Amazon ECS para las instancias que no se unen al clúster.

- `ExecutionResults`:

Genera resultados en función de los pasos anteriores.

7. Una vez completados, se proporciona el URI del archivo HTML del informe de evaluación:

Enlace a la consola S3 y URI de Amazon S3 para el informe sobre la ejecución correcta del manual de procedimientos

▼ Outputs

ExecutionResults.message

```
#####
EXECUTION RESULT SUMMARY
#####
```

Here is the summary of the execution of this runbook:

```

[INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY":
[ERROR]: Job "411-XXXXXXXXXXXXXXXXXXXX-606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnNEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/creating-compute-environments.html
! [WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html
[ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.

```

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

+++++

STEP:PreflightPermissionChecks

+++++

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

+++++

STEP:AWSBatchJobEvaluation

+++++

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

+++++

STEP:BatchComputeEnvironmentEvaluation

+++++

```

[INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY":
[ERROR]: Job "411-XXXXXXXXXXXXXXXXXXXX-606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnNEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/creating-compute-environments.html
! [WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnNEEWmt8eY".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html
[ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.

```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

CloudFormation

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS CloudFormation Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

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

AWS-DeleteCloudFormationStack

Descripción

Elimina una CloudFormation pila.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- StackNameOrId

Tipo: cadena

Descripción: (obligatorio) Nombre o identificador único de la CloudFormation pila que se va a eliminar

AWS-EnableCloudFormationSNSNotification

Descripción

El AWS-EnableCloudFormationSNSNotification runbook habilita las notificaciones del Amazon Simple Notification Service (Amazon SNS) para la pila AWS CloudFormation (CloudFormation) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- StackArn

Tipo: cadena

Descripción: (obligatorio) El ARN o el nombre de la CloudFormation pila para la que desea habilitar las notificaciones de Amazon SNS.

- NotificationArn

Tipo: cadena

Descripción: (obligatorio) El ARN del tema de Amazon SNS que desea asociar a la pila.
CloudFormation

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm: GetAutomationExecution`
- `ssm: StartAutomationExecution`
- formación de nubes: `DescribeStacks`
- formación de nubes: `UpdateStack`
- `kms:Decrypt`
- `kms: GenerateDataKey`
- `sns:Publish`
- `sqs: GetQueueAttributes`

Pasos de documentos

- `CheckCfnSnsLimits` (`aws:executeScript`) - Verifica el número máximo de temas de Amazon SNS que aún no se han asociado a CloudFormation la pila que especifique.
- `EnableCfnSnsNotification` (`aws:executeAwsApi`) - Activa las notificaciones de Amazon SNS para la CloudFormation pila.
- `VerificationCfnSnsNotification` (`aws:executeScript`) - Verifica que las notificaciones de Amazon SNS estén habilitadas para CloudFormation la pila.

Salidas

`CheckCfnSnsLimits`. `NotificationArnList` - Una lista de los ARNs que reciben notificaciones de Amazon SNS para la CloudFormation pila.

VerificationCfnSnsNotification. VerifySnsTopicsResponse - Respuesta de la operación de API que confirma que las notificaciones de Amazon SNS están habilitadas para la CloudFormation pila.

AWS-RunCfnLint

Descripción

Este runbook usa un [AWS CloudFormation Linter](#) (cfn-python-lint) para validar las plantillas YAML y JSON según la especificación del recurso. CloudFormation El manual de procedimientos AWS-RunCfnLint realiza comprobaciones adicionales, como asegurarse de que se han introducido valores válidos para las propiedades de los recursos. Si la validación no se realiza correctamente, el paso RunCfnLintAgainstTemplate produce un error y la salida de la herramienta de linter se proporciona en un mensaje de error. Este manual de procedimientos utiliza cfn-lint v0.24.4.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ConfigureRuleFlag

Tipo: cadena

Descripción: (opcional) opciones de configuración que una regla pasará al parámetro `--configure-rule`.

Ejemplo: `E2001:strict=false,E3012:strict=false`.

- `FormatFlag`

Tipo: cadena

Descripción: (opcional) valor que se pasa al parámetro `--format` para especificar el formato de salida.

Valores válidos: Predeterminado | inactividad | analizable | json

Valor predeterminado: Default

- `IgnoreChecksFlag`

Tipo: cadena

Descripción: (opcional) IDs de las reglas que se van a pasar al parámetro `--ignore-checks`. Estas reglas no se comprueban.

Ejemplo: `E1001, E1003, W7001`

- `IncludeChecksFlag`

Tipo: cadena

Descripción: (opcional) IDs de las reglas que se van a transferir al parámetro. `--include-checks` Estas reglas se comprueban.

Ejemplo: `E1001, E1003, W7001`

- `InfoFlag`

Tipo: cadena

Descripción: (opcional) opción para el parámetro `--info`. Incluya la opción para habilitar información adicional de registro sobre el procesamiento de la plantilla.

Predeterminado: false

- `TemplateFileName`

Tipo: cadena

Descripción: el nombre, o clave, del archivo de plantilla en el bucket de S3.

- Plantillas (3) BucketName

Tipo: cadena

Descripción: el nombre del bucket de S3 que contiene la plantilla de empaquetador.

- RegionsFlag

Tipo: cadena

Descripción: (opcional) Valores que se van a pasar al `--regions` parámetro for para probar la plantilla con los valores especificados. Regiones de AWS

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

Pasos de documentos

`RunCfnLintAgainstTemplate` — Ejecuta la `cfn-python-lint` herramienta en la CloudFormation plantilla especificada.

Salidas

`RunCfnLintAgainstTemplate.output`: la salida estándar de la herramienta. `cfn-python-lint`

AWSSupport-TroubleshootCFNCustomResource

Descripción

El manual de procedimientos `AWSSupport-TroubleshootCFNCustomResource` ayuda a diagnosticar por qué una pila de AWS CloudFormation no pudo crear, actualizar o eliminar un recurso personalizado. El manual de procedimientos comprueba el token de servicio utilizado para el recurso personalizado y el mensaje de error devuelto. Tras revisar los detalles del recurso personalizado, el resultado del manual de procedimientos proporciona una explicación del comportamiento de la pila y los pasos para solucionar el problema del recurso personalizado.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `StackName`

Tipo: cadena

Descripción: (obligatorio) El nombre de la CloudFormation pila en la que se produjo un error en el recurso personalizado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `cloudformation:ListStackResources`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`

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

Pasos de documentos

- `validateCloudFormationStack`- Comprueba que la CloudFormation pila existe en la misma Cuenta de AWS y Región de AWS.
- `checkCustomResource`- Analiza la CloudFormation pila, comprueba el recurso personalizado que ha fallado y genera información sobre cómo solucionar el problema del recurso personalizado que ha fallado.

AWS-UpdateCloudFormationStack

Descripción

Actualice una AWS CloudFormation pila mediante una CloudFormation plantilla almacenada en un bucket de Amazon S3.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `LambdaAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el ARN del rol asumido por Lambda.

- `StackNameOrId`

Tipo: cadena

Descripción: (obligatorio) Nombre o ID único de la CloudFormation pila que se va a actualizar

- `TemplateUrl`

Tipo: cadena

Descripción: (Obligatoria) ubicación del depósito de S3 que contiene la CloudFormation plantilla actualizada (p. ej. `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`)

CloudFront

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon CloudFront. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

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

AWSConfigRemediation-EnableCloudFrontDefaultRootObject

Descripción

El `AWSConfigRemediation-EnableCloudFrontDefaultRootObject` runbook configura el objeto raíz predeterminado para la distribución Amazon CloudFront (CloudFront) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `CloudFrontDistributionId`

Tipo: cadena

Descripción: (obligatorio) El ID de la CloudFront distribución para la que desea configurar el objeto raíz predeterminado.

- `DefaultRootObject`

Tipo: cadena

Descripción: (obligatorio) El objeto que deseas CloudFront devolver cuando una solicitud de un espectador apunte a tu URL raíz.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Configura el objeto raíz predeterminado para la CloudFront distribución que especifique en el `CloudFrontDistributionId` parámetro.

AWSConfigRemediation-EnableCloudFrontAccessLogs

Descripción

El `AWSConfigRemediation-EnableCloudFrontAccessLogs` runbook permite el registro de acceso para la distribución de Amazon CloudFront (CloudFront) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de Amazon Simple Storage Service (Amazon S3) en el que desea almacenar los registros de acceso. No se admiten los buckets de la Región de AWS af-south-1, ap-east-1, eu-south-1 y me-south-1.

- CloudFrontId

Tipo: cadena

Descripción: (obligatorio) El ID de la CloudFront distribución a la que quieres habilitar el acceso al iniciar sesión.

- IncludeCookies

Tipo: Booleano

Valores válidos: true | false

Descripción: (Obligatorio) Defina este parámetro en true, si desea que las cookies se incluyan en los registros de acceso.

- Prefijo

Tipo: cadena

Descripción: (opcional) Una cadena opcional que desee CloudFront añadir como prefijo al registro filenames de acceso de su distribución, por ejemplo. myprefix/

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

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

 Note

La `s3:GetBucketLocation` API solo se puede usar para los buckets de S3 de la misma cuenta. No puedes usarla para buckets de S3 entre cuentas.

Pasos de documentos

- `aws:executeScript`- Habilita el registro de acceso para la CloudFront distribución que especifique en el `CloudFrontDistributionId` parámetro.

AWSConfigRemediation- EnableCloudFrontOriginAccessIdentity

Descripción

El `AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity` manual habilita la identidad de acceso de origen para la distribución de Amazon CloudFront (CloudFront) que especifiques. Esta automatización asigna la misma identidad de acceso de CloudFront origen a todos los orígenes del tipo de origen de Amazon Simple Storage Service (Amazon S3) sin identidad de acceso de origen para CloudFront la distribución que especifique. Esta automatización no concede permiso de lectura a la identidad de acceso de origen para acceder CloudFront a los objetos de su bucket de Amazon S3. Debe actualizar los permisos de su bucket de Amazon S3 para permitir el acceso.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- CloudFrontDistributionId

Tipo: cadena

Descripción: (obligatorio) El ID de la CloudFront distribución en la que quieres habilitar la conmutación por error de Origin.

- OriginAccessIdentityId

Tipo: cadena

Descripción: (obligatorio) El ID de la identidad de acceso al CloudFront origen que se va a asociar al origen.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Activa la identidad de acceso de origen para la CloudFront distribución que especifique en el `CloudFrontDistributionId` parámetro y verifica que se haya asignado la identidad de acceso de origen.

AWSConfigRemediation-EnableCloudFrontOriginFailover

Descripción

El `AWSConfigRemediation-EnableCloudFrontOriginFailover` manual permite la conmutación por error de origen para la distribución de Amazon CloudFront (CloudFront) que especifiques.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `CloudFrontDistributionId`

Tipo: cadena

Descripción: (obligatorio) El ID de la CloudFront distribución en la que quieres habilitar la conmutación por error de Origin.

- `OriginGroupId`

Tipo: cadena

Descripción: (obligatorio) ID del grupo original.

- `PrimaryOriginId`

Tipo: cadena

Descripción: (obligatorio) el ID del origen principal en el grupo de origen.

- `SecondaryOriginId`

Tipo: cadena

Descripción: (obligatorio) el ID del origen secundario en el grupo de origen.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Activa la conmutación por error de origen para la CloudFront distribución que especifique en el `CloudFrontDistributionId` parámetro y verifica que la conmutación por error esté habilitada.

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

Descripción

El `AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS` manual habilita la política de protocolo de visualización para la distribución de Amazon CloudFront (CloudFront) que especifiques.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `CloudFrontDistributionId`

Tipo: cadena

Descripción: (obligatorio) El ID de la CloudFront distribución en la que desea habilitar la política de protocolo de visualización.

- `ViewerProtocolPolicy`

Tipo: cadena

Valores válidos: solo https, redirect-to-https

Descripción: (obligatorio) el protocolo que los lectores pueden utilizar para acceder a los archivos en el origen.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Activa la política de protocolo de visualización para la CloudFront distribución que especifique en el `CloudFrontDistributionId` parámetro y verifica que la política se haya asignado.

CloudTrail

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS CloudTrail Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

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

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

Descripción

El AWSConfigRemediation-CreateCloudTrailMultiRegionTrail runbook crea un registro AWS CloudTrail (CloudTrail) que envía los archivos de registro de varios Regiones de AWS al depósito de Amazon Simple Storage Service (Amazon S3) que elija.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BucketName

Tipo: cadena

Descripción: (obligatorio) nombre del bucket de Amazon S3 en el que desea cargar registros.

- KeyPrefix

Tipo: cadena

Descripción: (opcional) el prefijo de clave de Amazon S3 que viene después el nombre del bucket que ha designado para la entrega del archivo de registros.

- TrailName

Tipo: cadena

Descripción: (Obligatorio) El nombre de la CloudTrail ruta que se va a crear.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- aws:executeAwsApi- Acepta el nombre de la ruta y el nombre del bucket de Amazon S3 como entrada y crea una CloudTrail ruta.
- aws:executeAwsApi: permite iniciar sesión en la ruta creada e inicia la entrega de registros en el bucket de Amazon S3 que especificó.
- aws:assertAwsResourceProperty- Verifica que se haya creado el CloudTrail sendero.

AWS-EnableCloudTrail

Descripción

Cree un AWS CloudTrail rastro y configure el registro en un bucket de S3.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- S3 BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de S3 designado para la publicación de archivos de registro.

Note

El bucket S3 debe existir y la política del bucket debe conceder CloudTrail permiso para escribir en él. Para obtener más información, consulte la [Política de buckets de Amazon S3 para CloudTrail](#).

- TrailName

Tipo: cadena

Descripción: (obligatorio) el nombre del nuevo registro de seguimiento.

AWS-EnableCloudTrailCloudWatchLogs

Descripción

Este runbook actualiza la configuración de una o más AWS CloudTrail rutas para enviar eventos a un grupo de CloudWatch registros de Amazon Logs.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- CloudWatchLogsLogGroupArn

Tipo: cadena

Descripción: (obligatorio) El ARN del grupo de CloudWatch registros al que se entregarán los CloudTrail registros.

- CloudWatchLogsRoleArn

Tipo: cadena

Descripción: (obligatorio) El ARN del rol de IAM Logs Logs asume que escribe en el grupo de CloudWatch registros especificado.

- TrailNames

Tipo: StringList

Descripción: (Obligatorio) Lista separada por comas con los nombres de las CloudTrail rutas cuyos eventos quieres enviar a Logs. CloudWatch

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- cloudtrail:UpdateTrail
- iam:PassRole

Pasos de documentos

- aws:executeScript- Actualiza las CloudTrail rutas especificadas para enviar los eventos al grupo de CloudWatch registros especificado.

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

Descripción

El AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS runbook cifra un rastro AWS CloudTrail (CloudTrail) con la clave gestionada por el cliente AWS Key Management Service (AWS KMS) que especifique. Este manual solo debe usarse como referencia para garantizar que sus CloudTrail rutas estén cifradas de acuerdo con las mejores prácticas de seguridad mínimas recomendadas. Recomendamos cifrar varias rutas con diferentes claves de KMS. CloudTrail los archivos de resumen no están cifrados. Si ya ha establecido el EnableLogFileValidation parámetro como true para la ruta, consulte la sección «Uso del cifrado del lado del servidor con claves AWS KMS administradas» del tema sobre [prácticas recomendadas de seguridad CloudTrail preventiva](#) de la Guía del AWS CloudTrail usuario para obtener más información.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- KMSKeyId

Tipo: cadena

Descripción: (obligatorio) el ARN, el ID de clave o el alias de la clave gestionada por el cliente que desea utilizar para cifrar la ruta que especifique en el parámetro `TrailName`.

- TrailName

Tipo: cadena

Descripción: (obligatorio) el ARN o el nombre de la ruta que quieres actualizar para cifrarla.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- `cloudtrail:UpdateTrail`

Pasos de documentos

- `aws:executeAwsApi`: habilita el cifrado en la ruta que especifique en el parámetro `TrailName`.
- `aws:executeAwsApi`: recopila el ARN de la clave gestionada por el cliente que especifique en el parámetro `KMSKeyId`.
- `aws:assertAwsResourceProperty`- Verifica que el cifrado esté habilitado en la CloudTrail ruta.

AWS-EnableCloudTrailKmsEncryption

Descripción

Este manual actualiza la configuración de una o más AWS CloudTrail rutas para utilizar el cifrado AWS Key Management Service (AWS KMS).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **KMSKeyId**

Tipo: cadena

Descripción: (obligatorio) El identificador de la clave gestionada por el cliente que desea utilizar para cifrar la ruta que especifique en el `TrailName` parámetro. El valor puede ser un nombre de alias con el prefijo «alias/», un ARN completamente especificado para un alias o un ARN completamente especificado para una clave.

- **TrailNames**

Tipo: `StringList`

Descripción: (Obligatorio) Una lista separada por comas de las rutas que desea actualizar para cifrarlas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Permite el AWS KMS cifrado de las rutas que especifique en el `TrailName` parámetro.

AWSConfigRemediation-EnableCloudTrailLogFileValidation

Descripción

El `AWSConfigRemediation-EnableCloudTrailLogFileValidation` libro de rutas permite la validación del archivo de registro de su AWS CloudTrail sendero.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- TrailName

Tipo: cadena

Descripción: (obligatorio) el nombre o nombre de recurso de Amazon (ARN) de la ruta para la que desea habilitar la validación de registros.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- aws:executeAwsApi: permite la validación del registro de la ruta de AWS CloudTrail que especifique en el parámetro TrailName.

- `aws:assertAwsResourceProperty`: verifica que la validación del registro esté habilitada para su ruta.

AWS-EnableCloudTrailLogFileValidation

Descripción

El `AWS-EnableCloudTrailLogFileValidation` libro de rutas permite la validación del archivo de registro de los AWS CloudTrail senderos que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `TrailNames`

Tipo: `StringList`

Descripción: (Obligatorio) Una lista separada por comas con los nombres de los CloudTrail senderos para los que desea habilitar la validación de registros.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Permite la validación del registro de las AWS CloudTrail rutas que especifique en el `TrailNames` parámetro.

AWS-QueryCloudTrailLogs

Descripción

El `AWS-QueryCloudTrailLogs` runbook crea una tabla de Amazon Athena a partir del depósito de Amazon Simple Storage Service (Amazon S3) de su elección que contiene registros (). AWS CloudTrail CloudTrail Tras crear la tabla, la automatización ejecuta las consultas SQL que especifique y, a continuación, elimina la tabla.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Consultar

Tipo: cadena

Descripción: (obligatoria) la consulta SQL que desea ejecutar.

- SourceBucketPath

Tipo: cadena

Descripción: (Obligatorio) El nombre del depósito de Amazon S3 que contiene los archivos de CloudTrail registro que desea consultar.

- TableName

Tipo: cadena

Descripción: (opcional) el nombre de la tabla Athena creada por la automatización.

Predeterminado: cloudtrail_logs

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Pasos de documentos

- `aws:executeAwsApi`: crea una tabla de Athena.
- `aws:executeAwsApi`: ejecuta la cadena de consulta que especifique en el parámetro Query.
- `aws:executeScript`: sondea y espera a que se complete la consulta.
- `aws:executeAwsApi`: obtiene los resultados de la consulta.
- `aws:executeAwsApi`: elimina la tabla creada por la automatización.

CloudWatch

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon CloudWatch. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

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

AWS-ConfigureCloudWatchOnEC2Instance

Descripción

Activa o desactiva la supervisión CloudWatch detallada de Amazon en las instancias gestionadas.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) El ID de la EC2 instancia de Amazon en la que quieres habilitar la CloudWatch supervisión.

- propiedades

Tipo: cadena

Descripción: (opcional) no se admite este parámetro. Se enumera aquí por motivos de compatibilidad con versiones anteriores.

- status

Valores válidos: ENABLED | DISABLED

Descripción: (Opcional) especifica si desea habilitar o deshabilitar CloudWatch.

Valor predeterminado: Enabled

Pasos de documentos

configureCloudWatch - Se configura CloudWatch en la EC2 instancia de Amazon con el estado indicado.

Salidas

Esta automatización no tiene salidas.

AWS-EnableCWAlarm

Descripción

El AWS-EnableCWAlarm runbook crea alarmas de Amazon CloudWatch (CloudWatch) para AWS los recursos suyos Cuenta de AWS que aún no tienen una. CloudWatch las alarmas se crean para los siguientes AWS recursos:

- Instancias de Amazon Elastic Compute Cloud (Amazon EC2)
- Volúmenes de Amazon Elastic Block Store (Amazon EBS)
- Buckets de Amazon Simple Storage Service (Amazon S3)
- Clústeres de Amazon Relational Database Service (Amazon RDS)

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ComparisonOperator

Tipo: cadena

Valores válidos: GreaterThanOrEqualToThreshold | GreaterThanThreshold | GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpperThreshold | LessThanLowerThreshold | LessThanOrEqualToThreshold | LessThanThreshold

Descripción: (Obligatoria) La operación aritmética que se utilizará al comparar la estadística y el umbral especificados.

- MetricName

Tipo: cadena

Descripción: (obligatorio) Nombre de la métrica asociada a la alarma.

- Periodo

Tipo: entero

Valores válidos: 10 | 30 | 60 | Un múltiplo de 60

Descripción: (Obligatorio) El período, en segundos, durante el que se aplica la estadística.

- Recurso ARNs

Tipo: StringList

Descripción: (Obligatorio) Una lista separada por comas ARNs de los recursos para los que se debe crear una CloudWatch alarma

- Estadística

Tipo: cadena

Valores válidos: Promedio | Máximo | Mínimo | SampleCount | Suma

Descripción: (Obligatorio) La estadística de la métrica asociada a la alarma.

- Threshold

Tipo: entero

Descripción: (Obligatorio) El valor que se va a comparar con la estadística especificada.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudwatch:PutMetricAlarm`

Pasos de documentos

- `aws:executeScript`- Crea una CloudWatch alarma según los valores especificados en los parámetros del manual para los recursos que especifique en el `ResourceARNs` parámetro.

Salidas

Habilitar. `CWAlarm FailedResources`: una lista cartográfica de los recursos ARNs para los que no se creó una CloudWatch alarma y el motivo del error.

Habilitar. `CWAlarm SuccessfulResources`: una lista de recursos ARNs para los que se creó correctamente una CloudWatch alarma.

AWSSupport-TroubleshootCloudWatchAgent

Descripción

El `AWSSupport-TroubleshootCloudWatchAgent` manual automatiza la solución de problemas del Amazon CloudWatch Agent en sus instancias de Amazon Elastic Compute Cloud (Amazon EC2). El manual realiza esta solución de problemas mediante una serie de comprobaciones básicas y ampliadas (opcionales).

Las comprobaciones básicas incluyen las siguientes:

- Compruebe si hay un AWS Identity and Access Management perfil de instancia (IAM)

- Compruebe si los permisos de IAM de Amazon CloudWatch Agent necesarios están adjuntos a la instancia Amazon EC2

Las comprobaciones ampliadas solo se realizan si el ID de instancia de Amazon EC2 proporcionado es una instancia gestionada por Systems Manager. Entre estas comprobaciones ampliadas se incluyen las siguientes:

- Compruebe el estado del CloudWatch agente de Amazon en la instancia
- Analice los registros del Amazon CloudWatch Agent para ver los problemas comunes y los pasos de solución de problemas relevantes
- Comprima los registros y archivos de configuración pertinentes en la instancia de Amazon EC2 y, si lo desea, cárguelos en el depósito de Amazon Simple Storage Service (Amazon S3) que prefiera
- Realice una comprobación de conectividad entre la instancia y los puntos de enlace necesarios

Important

Cuando el `RunVpcReachabilityAnalyzer` parámetro esté establecido en `true`, este manual determinará si es necesario llamar al `runbook` secundario, `AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2`. El manual secundario utiliza el `Reachability Analyzer` de VPC, que tiene un costo asociado. Para obtener más información sobre los precios, consulte la documentación de [precios de Amazon VPC](#).

Important

Este manual solo comprueba el rol de su perfil de instancia de IAM para ver si tiene los permisos necesarios. Si, por el contrario, se basa en las credenciales definidas en un `.aws/credentials` archivo, es posible que los resultados del `verifyIamPermissions` paso no sean precisos.

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- `getInstanceProfile`: Comprueba si la instancia Amazon EC2 proporcionada tiene un perfil de instancia de IAM adjunto.

- `verifyIamPermissions`: Comprueba el perfil de instancia asociado a la instancia para determinar si se han aplicado los permisos de IAM necesarios.
- `getInstanceInformation`: Comprueba si la instancia tiene un agente de Systems Manager activo y busca el tipo de sistema operativo de la instancia.
- `getAgentStatus`: Comprueba el estado del CloudWatch agente de Amazon en la instancia (comprobación ampliada).
- `AnalyzeLogs/ analyzeLogsWindows`: analiza y genera los resultados de los registros de Amazon CloudWatch Agent en función del tipo de sistema operativo.
- `CollectLogs/ collectLogsWindows`: agrupa y genera los archivos de solución de problemas de Amazon CloudWatch Agent correspondientes en función del tipo de sistema operativo.
- `checkEndpointReachability/checkEndpointReachabilityWindows`: comprueba si la instancia puede alcanzar los puntos finales requeridos en función del tipo de sistema operativo.
- `analyzeAwsEndpointReachabilityFromEC2`: Consulta el manual de automatización secundario para comprobar si la instancia seleccionada es accesible a los puntos finales necesarios (si está activado).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2: DescribeInstances`
- objetivo: `GetInstanceProfile`
- objetivo: `GetRole`

- objetivo: ListAttachedRolePolicies
- objetivo: ListRolePolicies
- objetivo: GetRolePolicy
- objetivo: GetPolicy
- objetivo: GetPolicyVersion
- objetivo: SimulatePrincipalPolicy
- ssm: DescribeInstanceInformation
- ssm: SendCommand
- ssm: GetCommandInvocation
- ssm: DescribeInstanceAssociationsStatus
- ssm: StartAutomationExecution

Ejemplo de política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:SimulatePrincipalPolicy",
        "ssm:DescribeInstanceInformation",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:StartAutomationExecution"
      ],
      "Resource": "*"
    }
  ]
}
```

}

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootCloudWatchAgent](#) Systems Manager en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El ARN del rol de IAM que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
 - Tipo: `AWS::IAM::Role::Arn`
 - InstanceId (Obligatorio):
 - Descripción: (Obligatorio) El ID de la instancia de Amazon EC2 en la que desea solucionar los problemas del Amazon CloudWatch Agent.
 - Tipo: `AWS::EC2::Instance::Id`
 - Patrón de permisos: `^i-[0-9a-f]{8,17}$`
 - S3 UploadBucket (opcional):
 - Descripción: (opcional) El nombre de un depósito de Amazon S3 para cargar los registros de Amazon CloudWatch Agent recopilados. El perfil de instancia de Amazon EC2 debe tener los permisos correctos para cargar archivos en este bucket. Esto también requiere que la instancia Amazon EC2 de destino sea una instancia gestionada por Systems Manager.
 - Tipo: `AWS::S3::Bucket::Name`
 - Patrón de permisos: `^$|^[a-z0-9][a-z0-9.-]{1,61}[a-z0-9]$`
 - Valor predeterminado: `""`
 - S3 BucketOwnerAccountId (opcional):
 - Descripción: (opcional) El número de AWS cuenta propietario del depósito de Amazon S3 en el que desea cargar los registros de Amazon CloudWatch Agent. Si no modificas este parámetro, los manuales utilizan el ID de AWS cuenta del usuario o rol en el que se ejecuta la automatización.
 - Tipo: `String`

- Patrón de permisos: `^\\{\\{ global:ACCOUNT_ID \\}\\}$|^[0-9]{12}$`
- Valor predeterminado: `{{ global:ACCOUNT_ID }}`
- Compruebe el EC2 punto final (opcional):
 - Descripción: (opcional) Especifique `true` si la configuración de su agente utiliza la opción de `append_dimensions` añadir las dimensiones métricas de Amazon EC2 a las métricas recopiladas por el agente. Cuando `append_dimensions` se utiliza, el Amazon CloudWatch Agent requiere conectividad con el punto final de la API de Amazon EC2, por lo que se realizarán pruebas de conectividad adicionales mediante las comprobaciones ampliadas.
 - Tipo: `String`
 - Valores permitidos: `[true, false]`
 - Valor predeterminado: `false`
- `RunVpcReachabilityAnalyzer` (Opcional):
 - Descripción: (opcional) Especifique `true` que se ejecute la automatización `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` secundaria si las comprobaciones ampliadas determinan un problema de red o si el ID de instancia especificado no es una instancia administrada.
 - Tipo: `Boolean`
 - Valor predeterminado: `false`
- `RetainVpcReachabilityAnalysis` (Opcional):
 - Descripción: (opcional) Solo es relevante si lo `RunVpcReachabilityAnalyzer` es `true`. Especifique si desea `true` conservar la ruta de conocimiento de la red y los análisis relacionados creados por el Reachability Analyzer de VPC. De forma predeterminada, esos recursos se eliminan después de un análisis exitoso.
 - Tipo: `Boolean`
 - Valor predeterminado: `false`

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `getInstanceProfile`:

Comprueba si la instancia Amazon EC2 proporcionada tiene un perfil de instancia de IAM adjunto.

- `branchOnInstanceProfileStatus`:

Ramifica la automatización para comprobar los permisos de perfil de instancia necesarios si el perfil de instancia está adjunto a la instancia.

- `verifyIamPermissions`:

Comprueba el perfil de instancia asociado a la instancia para determinar si se han aplicado los permisos de IAM necesarios.

- `getInstanceInformation`:

Comprueba si la instancia tiene un agente de Systems Manager activo y busca el tipo de sistema operativo de la instancia.

- `branchOnManagedInstance`:

Ramifica la automatización para realizar comprobaciones ampliadas si la instancia está gestionada.

- `getAgentStatus`:

Comprueba el estado del Amazon CloudWatch Agent en la instancia.

- `branchOnInstanceOsType`:

Ramifica la automatización para ejecutar un `collection/analysis` comando de registro específico en función del sistema operativo.

- Analice los registros/ `analyzeLogsWindows`:

Analiza y genera los resultados de los registros de Amazon CloudWatch Agent en función del tipo de sistema operativo.

- `CollectLogs/ collectLogsWindows`:

Agrupar y genera los archivos de solución de problemas de Amazon CloudWatch Agent correspondientes en función del tipo de sistema operativo.

- `checkEndpointReachability/checkEndpointReachabilityWindows`:

Comprueba si la instancia puede alcanzar los puntos finales necesarios en función del tipo de sistema operativo.

- `branchOnRunVpcReachabilityAnalyzer`:

Ramifica la automatización para ejecutar el análisis de accesibilidad de la VPC si está habilitada y se detectan problemas de red.

- Genere puntos finales:

Genera un punto final para comprobar los errores de comprobación prolongados y el valor de `CheckEC2Endpoint`

- `analyzeAwsEndpointReachabilityFromEC2`:

Llama al manual de automatización `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` para comprobar la accesibilidad de la instancia seleccionada a los puntos finales necesarios.

- Hallazgos de salida:

Genera los resultados de los pasos de ejecución de la automatización.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWSSupport-TroubleshootCloudWatchAlarm

Descripción

El `AWSSupport-TroubleshootCloudWatchAlarm` manual ayuda a identificar y solucionar problemas relacionados con las alarmas Amazon CloudWatch () CloudWatch problemáticas o mal configuradas. Utiliza una lógica de evaluación de alarmas pública AWS APIs y conocida para detectar puntos de datos retrasados o ausentes en las métricas monitoreadas, lo que puede provocar que se omitan o se retrasen las acciones de alarma. Este manual proporciona un enfoque estructurado para investigar y resolver los problemas relacionados con Amazon CloudWatch (CloudWatch) Alarm.

¿Cómo funciona?

El manual de ejecución `AWSSupport-TroubleshootCloudWatchAlarm` lleva a cabo los siguientes pasos:

- Verifica los detalles de la alarma de Amazon CloudWatch (CloudWatch) y el valor del `AlarmTriggerTimestamp` parámetro para comprobar si está dentro de 2 592 000 segundos (30 días).
- Comprueba si una alarma se basa en una métrica o matemática métrica o si se trata de una alarma detectora de anomalías.
- Comprueba si una alarma tiene un estado de datos insuficiente.
- Comprueba si las métricas utilizadas en la alarma coinciden con el `ListMetrics` valor.
- Verifica si a una métrica le faltaban puntos de datos en una marca de tiempo determinada.
- Obtiene el historial más reciente de una marca de tiempo determinada.
- Comprueba si una alarma no se ha activado debido a un retraso o a un error en las métricas.
- Comprueba si se han realizado las acciones habilitadas de una `was/were` alarma.
- Genera un informe de solución de problemas que combina todos los resultados del diagnóstico.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudwatch:DescribeAlarms`

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

JSON

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

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSsupport-TroubleshootCloudWatchAlarm](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Tipo: String

- Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.
- CloudWatchMetricAlarmName(Obligatorio):
 - Tipo: String
 - Descripción: (Obligatorio) El nombre de la alarma métrica de Amazon CloudWatch (CloudWatch) para solucionar el problema.
 - Valor permitido: `^[a-zA-Z0-9.:;,\_\&() ]{1,255}$`
- AlarmTriggerTimestamp (Obligatorio):
 - Tipo: String
 - Descripción: (Obligatorio) La marca horaria UTC en la que se produjo el problema de la alarma. Esta información es crucial para solucionar el problema y comprender el contexto en el que ocurrió. El valor de la marca de tiempo debe ser una hora de los últimos 30 días a partir de hoy y estar en ese formato. YYYY-MM-DDTHH:mm:ssZ Ejemplo: 2024-10-29T09:04:00Z
 - Valor permitido: `^((\d{4})-(\d{2})-(\d{2}))T(\d{2}):(\d{2}):(\d{2})Z$`

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **VerifyRunbookInputs**

Verifica los detalles de la alarma de Amazon CloudWatch (CloudWatch) y el valor del AlarmTriggerTimestamp parámetro para comprobar si está dentro de 2 592 000 segundos (30 días).

- **UpdateSSMDocumentInputChecksVariable**

Actualiza la variable SSMDocumentInputChecks con el valor SSMDocumentInputChecks del paso. VerifyRunbookInputs

- **BranchOnAlarmIsVerified**

Se basa en la verificación de entradas de Runbook AlarmTriggerTimestamp yCloudWatchAlarmName.

- **CheckMetricAlarmType**

Comprueba si una alarma se basa en una métrica o matemática métrica o si es una alarma detectora de anomalías.

- **CheckAlarmInInsufficientDataState**

Comprueba si una alarma tiene un estado de datos insuficiente.

- **UpdateInsufficientDataChecksVariable**

Actualiza la variable `InsufficientDataChecks` con el valor `InsufficientDataChecks` del `CheckAlarmInInsufficientDataState` paso.

- **BranchOnAlarmHasInsufficientData**

Se ramifica según el `AlarmHasInsufficientData` valor del `CheckAlarmInInsufficientDataState` paso, el paso por defecto es `CheckMetricMismatch`.

- **CheckMetricMismatch**

Comprueba si las métricas utilizadas en la alarma coinciden con el `ListMetrics` valor.

- **UpdateMetricMismatchChecksVariable**

Actualiza la variable `MetricMismatchChecks` con el valor `MetricMismatchChecks` del `CheckMetricMismatch` paso.

- **BranchOnMetricsMatched**

Se ramifica según el `MetricsMatched` valor del `CheckMetricMismatch` paso, el paso por defecto es `CheckMissingDatapoint`.

- **CheckMissingDatapoint**

Comprueba si a una métrica le faltaban puntos de datos en una marca de tiempo determinada.

- **UpdateMetricMissingDatapointsChecksVariable**

Actualiza la variable `MetricMissingDatapointsChecks` con el valor del paso.
`MetricMissingDatapointsChecks` `CheckMissingDatapoint`

- **BranchOnMetricMissingDatapoint**

Se ramifica según el `MetricMissingDatapoint` valor del `CheckMissingDatapoint` paso, el paso por defecto es `GetAlarmHistoryDetails`.

Obtiene el historial más reciente de una marca de tiempo determinada.

- **UpdateAlarmHistoryChecksVariable**

Actualiza la variable AlarmHistoryChecks con el valor AlarmHistoryChecks del GetAlarmHistoryDetails paso.

- **BranchOnAlarmHistoryFound**

Se ramifica según el AlarmHistoryFound valor del GetAlarmHistoryDetails paso, el paso por defecto esCheckDelayedMetric.

- **CheckDelayedMetric**

Comprueba si una alarma no se ha activado debido a un retraso o a un error en las métricas.

- **UpdateDelayedMetricChecksVariable**

Actualiza la variable DelayedMetricChecks con el valor DelayedMetricChecks del CheckDelayedMetric paso.

- **BranchOnMetricDelayedAndDatapointsMeetThreshold**

Se ramifica en los DatapointsMeetThreshold valores MetricDelayed y del CheckDelayedMetric paso; el paso por defecto esGenerateReport.

- **CheckActionDelivered**

Comprueba si se han realizado las acciones activadas por una was/were alarma.

- **UpdateActionDeliveredChecksVariable**

Actualiza la variable ActionDeliveredChecks con la salida ActionDeliveredChecks del CheckActionDelivered paso.

- **GenerateReport**

Compila el resultado de los pasos anteriores y genera un informe.

7. Una vez completada la ejecución, revise la sección de resultados para ver los resultados detallados de la ejecución:

- GenerateReport.Informe

Un informe de la alarma métrica de Amazon CloudWatch (CloudWatch) proporcionada.

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

```
=====
1. Validating SSM Document input parameters:
=====
# [PASSED]: Found a metric alarm with name Demo-Alarm

=====
2. Checking alarm's data state:
=====
# [PASSED]: The alarm is not in INSUFFICIENT_DATA state, alarm's
state is: ALARM

=====
3. Checking if the alarm experienced metric mismatches:
=====
# [PASSED]: Metric matches with the configured metric for Alarm.
```

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

# [PASSED]: Metric has datapoints

=====

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

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

=====

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

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

=====

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

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

-----

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

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

Amazon DocumentDB

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon DocumentDB (con compatibilidad con MongoDB). Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-EnableDocDbClusterBackupRetentionPeriod](#)

AWS-EnableDocDbClusterBackupRetentionPeriod

Descripción

El AWS-EnableDocDbClusterBackupRetentionPeriod runbook habilita un período de retención de copias de seguridad para el clúster de Amazon DocumentDB que especifique. Esta función establece el número total de días durante los que se conserva una copia de seguridad automática. Para modificar un clúster, el clúster debe estar en el estado disponible con un tipo de motor dedocdb.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `DBClusterResourceId`

Tipo: cadena

Descripción: (obligatorio) El ID de recurso del clúster de Amazon DocumentDB para el que desea habilitar el período de retención de copias de seguridad.

- `BackupRetentionPeriod`

Tipo: entero

Descripción: (obligatorio) El número de días durante los que se conservan las copias de seguridad automatizadas. Debe tener un valor de 7 a 35 días.

- `PreferredBackupWindow`

Tipo: cadena

Descripción: (opcional) Un intervalo de tiempo diario en hora universal coordinada (UTC) con el formato hh24:mm-hh24:mm, por ejemplo, 07:14-07:44. El valor debe ser de al menos 30 minutos y no puede entrar en conflicto con el período de mantenimiento preferido.

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

- `rds:ModifyDBCluster`

Pasos de documentos

- `GetDocDbClusterIdentifier` (`aws:executeAwsApi`) - Devuelve el identificador del clúster de Amazon DocumentDB utilizando el ID de recurso proporcionado.
- `VerifyDocDbEngine` (`aws:assertAwsResourceProperty`) - Comprueba que el tipo de motor de Amazon DocumentDB `docdb` es para evitar cambios inadvertidos en otros tipos de motor de Amazon RDS.
- `VerifyDocDbStatus` (`aws:waitAwsResourceProperty`) - Verifica que el estado del clúster de Amazon DocumentDB sea `available`.
- `ModifyDocDbRetentionPeriod` (`aws:executeAwsApi`) - Establece el período de retención mediante los valores proporcionados para el clúster de Amazon DocumentDB especificado.
- `VerifyDocDbBackupsEnabled` (`aws:executeScript`) - Verifica que el período de retención del clúster de Amazon DocumentDB y la ventana de respaldo preferida, si se especificó, se hayan establecido correctamente.

Salidas

`ModifyDocDbRetentionPeriod`. `ModifyDbClusterResponse` - Respuesta de la operación de la `ModifyDBCluster` API.

`VerifyDocDbBackupsEnabled`. `VerifyDbClusterBackupsEnabledResponse` - Resultado del `VerifyDocDbBackupsEnabled` paso que confirma la modificación correcta del clúster de Amazon DocumentDB.

CodeBuild

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS CodeBuild Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK](#)

- [AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject](#)

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

Descripción

El AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK manual cifra los artefactos de construcción de un proyecto AWS CodeBuild (CodeBuild) con la clave administrada por el cliente AWS Key Management Service (AWS KMS) que especifiques. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- KMSKeyId

Tipo: cadena

Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) de la clave gestionada por el AWS KMS cliente que desea utilizar para cifrar el CodeBuild proyecto que especifique en el parámetro. ProjectId

- ProjectId

Tipo: cadena

Descripción: (obligatorio) El ID del CodeBuild proyecto cuyos artefactos de construcción desea cifrar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`- Recopila el nombre del CodeBuild proyecto a partir del ID del proyecto.
- `aws:executeAwsApi`- Habilita el cifrado en el CodeBuild proyecto que especifique en el `ProjectId` parámetro.
- `aws:assertAwsResourceProperty`- Verifica que el cifrado esté habilitado en el CodeBuild proyecto.

Salidas

`UpdateLambdaConfig`. `UpdateFunctionConfigurationResponse` - Respuesta de la llamada a la `UpdateFunctionConfiguration` API.

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

Descripción

El `AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject` runbook elimina las variables de `AWS_SECRET_ACCESS_KEY` entorno `AWS_ACCESS_KEY_ID` y las variables de entorno

del proyecto AWS CodeBuild (CodeBuild) que especifiques. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- ResourceId

Tipo: cadena

Descripción: (obligatorio) El ID del CodeBuild proyecto cuyas variables de entorno clave de acceso desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

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

Pasos de documentos

- `aws:executeScript`- Elimina las variables de entorno clave de acceso del CodeBuild proyecto especificadas en el `ResourceId` parámetro.

AWS CodeDeploy

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS CodeDeploy Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-TroubleshootCodeDeploy](#)

AWSSupport-TroubleshootCodeDeploy

Descripción

El `AWSSupport-TroubleshootCodeDeploy` manual ayuda a diagnosticar por qué ha fallado una AWS CodeDeploy implementación en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). El manual de procedimientos proporciona pasos para ayudarle a resolver el problema o a resolver problemas adicionales. También CodeDeploy se proporcionan las mejores prácticas para ayudarlo a evitar problemas similares en el futuro.

Este manual de procedimientos puede ayudarle a resolver los siguientes problemas:

- El CodeDeploy agente no está instalado o no se está ejecutando en la EC2 instancia de Amazon
- La EC2 instancia de Amazon no tiene un perfil de instancia AWS Identity and Access Management (IAM) adjunto
- El perfil de instancia de IAM adjunto a la EC2 instancia de Amazon no tiene los permisos necesarios de Amazon Simple Storage Service (Amazon S3)

- Falta una revisión almacenada en Amazon S3 o el bucket de Amazon S3 utilizado está en una Región de AWS EC2 instancia diferente a la de Amazon
- Problemas con el archivo de especificaciones de la aplicación (AppSpec)
- Errores de tipo “File already exists at location”
- Los enganches de eventos del ciclo de vida CodeDeploy administrado
- Enlaces de eventos fallidos del ciclo de vida gestionados por el cliente
- Eventos de escalado durante una implementación

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DeploymentId

Tipo: cadena

Descripción: (obligatorio) el ID de la implementación que falló.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) El ID de la EC2 instancia de Amazon en la que se produjo un error en la implementación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`: verifica los valores proporcionados para los parámetros `DeploymentId` y `InstanceId`.
- `aws:executeScript`- Recopila información de la EC2 instancia de Amazon, como el estado de la instancia y los detalles del perfil de la instancia de IAM.
- `aws:executeScript`: revisa la implementación especificada y regresa un análisis sobre los motivos por los que se ha producido un error en la implementación.

AWS Config

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Config Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-SetupConfig](#)

AWSSupport-SetupConfig

Descripción

El `AWSsupport-SetupConfig` runbook crea un rol vinculado a un servicio AWS Identity and Access Management (IAM), un registrador de configuración con tecnología y un canal de entrega con un bucket de Amazon Simple Storage Service (Amazon S3) desde el que se AWS Config envían las instantáneas de la configuración y los archivos del historial de la configuración. AWS Config Si especifica valores para los `AggregatorAccountRegion` parámetros `AggregatorAccountId` y, el runbook también crea autorizaciones para la agregación de datos a fin de recopilar datos de AWS Config configuración y conformidad de varios y varios. Cuentas de AWS Regiones de AWS Para obtener más información sobre la agregación de datos de varias cuentas y regiones, consulte la sección [Agregación de datos multicuenta y multirregionales](#) en la Guía para desarrolladores de AWS Config .

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `AggregatorAccountId`

Tipo: cadena

Descripción: (opcional) El ID del Cuenta de AWS lugar donde se agregará un agregador para agregar los datos de AWS Config configuración y cumplimiento de varias cuentas y Regiones de AWS. El agregador también utiliza esta cuenta para autorizar las cuentas de origen.

- **AggregatorAccountRegion**

Tipo: cadena

Descripción: (opcional) La región en la que se agregará un agregador para agregar los datos de AWS Config configuración y cumplimiento de varias cuentas y regiones.

- **IncludeGlobalResourcesRegion**

Tipo: cadena

Predeterminado: us-east-1

Descripción: (obligatorio) para evitar registrar los datos de los recursos globales en cada región, especifique una región desde la que registrar los datos de los recursos globales.

- **Partición**

Tipo: cadena

Valor predeterminado: aws

Descripción: (obligatoria) la partición de la que desea recopilar datos de AWS Config de configuración y conformidad.

- **S3 BucketName**

Tipo: cadena

Valor predeterminado: aws-config-delivery-channel

Descripción: (opcional) el nombre que desea aplicar al bucket de Amazon S3 creado para el canal de entrega. El ID de la cuenta se adjunta al final del nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeScript`: crea un rol de IAM vinculada a un servicio para AWS Config si aún no existe ninguna.
- `aws:executeScript`: crea un grabador de configuración si aún no existe ninguno.
- `aws:executeScript`: crea un bucket de Amazon S3 para que lo utilice el canal de entrega si aún no existe ninguno.
- `aws:executeScript`: crea un canal de entrega con los recursos creados por el manual de procedimientos.
- `aws:executeAwsApi`: detiene o inicia el registro de configuración.
- `aws:executeScript`: si ha especificado valores para los parámetros `AggregatorAccountId` y `AggregatorAccountRegion`, se configuran las autorizaciones para la agregación de datos de varias cuentas y regiones.

Amazon Connect

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Connect. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

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

AWSSupport-AssociatePhoneNumbersToConnectContactFlows

Descripción

AWSSupport-AssociatePhoneNumbersToConnectContactFlows Esto le ayuda a asociar números de teléfono a los flujos de contactos de su instancia de Amazon Connect. Al proporcionar las asignaciones de números de teléfono y flujos de contactos en un archivo de entrada de valores separados por comas (CSV), el manual asocia tantos números de teléfono a los flujos de contactos como sea posible en 14,5 minutos. El manual genera un archivo CSV con todos los pares de números de teléfono y flujos de contactos que no ha podido asociar dentro del límite de tiempo para que puedas introducirlos en la siguiente ejecución.

¿Cómo funciona?

El manual le AWSSupport-AssociatePhoneNumbersToConnectContactFlows ayuda a asociar números de teléfono a los flujos de contactos de su instancia de Amazon Connect mediante un archivo CSV de datos de mapeo que se almacena en un depósito de Amazon Simple Storage Service (Amazon S3). El archivo CSV de entrada debe alinearse con el siguiente formato, con `PhoneNumber` los valores en formato [E.164](#).

Ejemplo del archivo CSV de entrada

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

El manual de automatización también crea los siguientes archivos en la ubicación de destino especificada en `DestinationFileBucket` y `DestinationFilePath`.

- **automation:EXECUTION_ID/ResourceIdList.csv**: un archivo temporal que contiene los `ContactFlowId` pares `PhoneNumberId` y necesarios para la `AssociatePhoneNumberContactFlow` API.
- **automation:EXECUTION_ID/ErrorResourceList.csv**: un archivo que contiene los pares de números de teléfono y flujo de contactos que no se pudieron procesar

debido a un error, por ejemplo, `ResourceNotFoundException` en el formato `dePhoneNumber,ContactFlowName,ErrorMessage`.

- **automation:EXECUTION_ID/NonProcessedResourceList.csv**: un archivo que contiene los pares de número de teléfono y flujo de contactos que no se procesaron. El manual intenta procesar tantos números de teléfono y flujos de contactos como sea posible en 14,5 minutos (15 minutos después del tiempo de espera de la AWS Lambda función, 30 segundos de búfer). Si hay algunos números de teléfono o flujos de contactos que no se han podido procesar por falta de tiempo, el runbook los incluye en un archivo CSV para usarlos como entrada en la siguiente ejecución del runbook.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

```
{
  "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"
}
]
}

```

Si proporciona un `LambdaRoleArn` parámetro, el rol requiere las siguientes acciones para usar el runbook correctamente.

JSON

```

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

```

```

    "connect:AssociatePhoneNumberContactFlow"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "s3:PutObject",
    "s3:GetObject"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/DESTINATION_FILE_PATH*",
  "Effect": "Allow"
}
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-AssociatePhoneNumbersToConnectContactFlows](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional)

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- ConnectInstanceId (Obligatorio)

El ID de tu instancia de Amazon Connect.

- SourceFileBucket (Obligatorio)

El depósito de Amazon S3 que almacena el archivo CSV que contiene los pares de número de teléfono y flujo de contacto.

- SourceFilePath (Obligatorio)

La clave de objeto de Amazon S3 del archivo CSV que contiene los pares de número de teléfono y flujo de contacto. Por ejemplo, `path/to/input.csv`.

- `DestinationFileBucket` (Obligatorio)

El depósito de Amazon S3 en el que la automatización colocará un archivo intermedio y un informe de resultados.

- `DestinationFilePath` (Opcional)

La ruta del objeto de Amazon S3 en `DestinationFileBucket` la que se deben almacenar un archivo intermedio y un informe de resultados. Por ejemplo, si lo especifica `path/to/files/`, los archivos se almacenan en `s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`.

- `S3 BucketOwnerAccount` (opcional)

El número de AWS cuenta propietario del bucket de Amazon S3 en el que desea cargar el registro de flujo de contactos. Si no especificas este parámetro, los manuales utilizan el ID de AWS cuenta del usuario o rol en el que se ejecuta la automatización.

- `S3 BucketOwnerRoleArn` (opcional)

El ARN de la función de IAM con permisos para obtener la configuración de acceso público del bucket y el bloqueo de cuentas de Amazon S3, la configuración de cifrado del bucket, el bucket ACLs, el estado de la política del bucket y cargar objetos al bucket. Si no se especifica este parámetro, el runbook utiliza el runbook `AutomationAssumeRole` (si se especifica) o el usuario que inicia este runbook (si no `AutomationAssumeRole` se especifica). Por favor consulte la sección de permisos necesarios en la descripción del manual de procedimientos.

- `LambdaRoleArn` (Opcional)

El ARN de la función de IAM que permite a la AWS Lambda función acceder a los AWS servicios y recursos necesarios. Si no se especifica ningún rol, esta automatización creará un rol de IAM para Lambda en su cuenta.

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `CheckConnectInstanceExistence`

Comprueba si la instancia de Amazon Connect proporcionada `ConnectInstanceId` existe.

- Comprueba [S3] BucketPublicStatus

Comprueba si los buckets de Amazon S3 especificados en `SourceFileBucket` y `DestinationFileBucket` permiten permisos de acceso de lectura o escritura públicos o anónimos.

- CheckSourceFileExistenceAndSize

Comprueba si el archivo CSV de origen especificado en el `SourceFilePath` existe y si el tamaño del archivo supera el límite de 25 MiB.

- GenerateResourceIdMap

Descarga el archivo CSV de origen especificado en el `SourceFilePath` identificador `PhoneNumberId` y `ContactFlowId` para cada recurso. Una vez hecho esto, carga un archivo CSV que contiene `PhoneNumber`, `PhoneNumberIdContactFlowName`, y `ContactFlowId` al bucket Amazon S3 de destino especificado en `DestinationFileBucket`. Si `PhoneNumberId` no se puede identificar con un número determinado, el archivo estará vacío en el archivo CSV.

- AssociatePhoneNumbersToContactFlows

Crea una AWS Lambda función en tu cuenta mediante una AWS CloudFormation pila. La AWS Lambda función asocia cada número a un flujo de contactos que aparece en el archivo CSV de origen especificado en `SourceFileBucket` `SourceFilePath` y, a continuación, la AWS CloudFormation pila invoca la función. La AWS Lambda función asigna tantos números de teléfono a los flujos de contactos como sea posible antes de que se agote el tiempo de espera (15 minutos). Se carga la lista de números de teléfono y flujos de contactos que no se pudieron procesar debido a un error `[automation:EXECUTION_ID]/ErrorResourceList.csv`. Se cargan los que no se han podido procesar debido a que se ha superado el número máximo de números de teléfono que se pueden procesar en una sola ejecución `[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. Si se produce un error en este paso, se pasa al `DescribeCloudFormationErrorFromStackEvents` paso siguiente para mostrar el motivo del error debido a los eventos de la AWS CloudFormation pila.

- WaitForPhoneNumberContactFlowAssociationCompletion

Espera hasta que se cree la AWS Lambda función que asigna números de teléfono a los flujos de contactos y la AWS CloudFormation pila complete su invocación.

- GenerateReport

Genera el informe que contiene el número de números de teléfono asignados a los flujos de contactos, los que no se pudieron procesar debido a un error y los que no se pudieron procesar debido a un exceso del número máximo de números de teléfono que se pueden procesar en una sola ejecución. El informe también muestra la ubicación (URI de Amazon S3 y URL de la consola de Amazon S3) de `[automation:EXECUTION_ID]/ErrorResourceList.csv` o `[automation:EXECUTION_ID]/NonProcessedResourceList.csv`, si corresponde.

- **DeleteCloudFormationStack**

Elimina la AWS CloudFormation pila, incluida la función Lambda para el mapeo.

- **DescribeCloudFormationErrorFromStackEvent**

Describe los errores de la AWS CloudFormation pila del `AssociatePhoneNumbersToContactFlows` paso.

7. Una vez finalizado, revise la sección de resultados para ver los resultados detallados de la ejecución:

- `GenerateReport.OutputPayload`

Resultado de las asociaciones de números de teléfono y flujo de contactos. Este informe contiene la siguiente información:

- El número de pares de números de teléfono y flujo de contactos que aparecen en el archivo CSV de entrada
- El número de números de teléfono asociados a los flujos de contactos, tal como se especifica en el archivo CSV de entrada
- El número de números de teléfono que no se pudieron asociar a los flujos de contactos debido a un error
- El número de números de teléfono que no estaban asociados a los flujos de contactos por falta de tiempo
- La ubicación (URI de Amazon S3 y URL de la consola de Amazon S3) del archivo CSV que contiene los pares de número de teléfono y flujo de contactos que no se pudieron asociar debido a un error
- La ubicación (URI de Amazon S3 y URL de la consola de Amazon S3) del archivo CSV que contiene los pares de números de teléfono y flujo de contactos que no estaban asociados por falta de tiempo
- `DescribeCloudFormationErrorFromStackEvents.Eventos`

Resultado que muestra los eventos de la AWS CloudFormation pila si el AssociatePhoneNumbersToContactFlows paso falla.

Resultado de la ejecución con un número reducido de números de teléfono y flujos de contactos

```

▼ 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
"}

```

Resultado de la ejecución con una gran cantidad de números de teléfono y flujos de contactos y números de teléfono que no estaban asociados debido a un error o a una limitación de tiempo

```

▼ 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.
"}

```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSSupport-CollectAmazonConnectContactFlowLog

Descripción

El manual de `AWSSupport-CollectAmazonConnectContactFlowLog` automatización se utiliza para recopilar los registros del flujo de contactos de Amazon Connect para un ID de contacto específico. Al proporcionar su ID de instancia y su ID de contacto de Amazon Connect, el runbook busca en los registros de flujo de contactos el contacto del grupo de CloudWatch registros de Amazon y los carga en el depósito de Amazon Simple Storage Service (Amazon S3) que se especifica en el parámetro de solicitud. El runbook genera un resultado que proporciona la URL de la consola Amazon S3 y el comando AWS CLI para que pueda descargar los registros.

¿Cómo funciona?

El manual de `AWSSupport-CollectAmazonConnectContactFlowLog` automatización ayuda a recopilar los registros de flujo de contactos de Amazon Connect para un ID de contacto específico almacenados en el grupo de CloudWatch registros configurado y los carga en un bucket de Amazon S3 específico. Para mejorar la seguridad de los registros recopilados del flujo de contactos de Amazon Connect, la automatización evalúa la configuración del bucket de Amazon S3 para determinar si el bucket concede permisos públicos `read` o de `write` acceso y si es propiedad de la AWS cuenta especificada en el `S3BucketOwnerAccountId` parámetro. Si su bucket de Amazon S3 utiliza cifrado con AWS Key Management Service claves del lado del servidor (SSE-KMS), asegúrese de que el usuario o rol AWS Identity and Access Management (IAM) que ejecuta esta automatización tenga los permisos sobre la `kms:GenerateDataKey` clave. AWS KMS Para obtener más información sobre los registros generados por su instancia de Amazon Connect, consulte [Registros de flujo almacenados en un grupo de CloudWatch registros de Amazon](#).

Important

Las consultas de CloudWatch Logs Insights se cobran en función de la cantidad de datos consultados. A los clientes de capa gratuita solo se les cobra por el uso que superar las cuotas de servicio. Para obtener más información, consulte [Precios de Amazon CloudWatch](#).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

```
{
  "Statement": [
    {
      "Action": [
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectAttributes",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "connect:DescribeInstance",
        "connect:DescribeContact",
        "ds:DescribeDirectories"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ]
    }
  ]
}
```

```
        "Resource": "*",
        "Effect": "Allow"
    }
]
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-CollectAmazonConnectContactFlowLog](#) Systems Manager en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- ConnectInstanceId (Obligatorio):

El ID de tu instancia de Amazon Connect.

- ContactId (Obligatorio):

El ID del contacto para el que quieres recopilar el registro de flujo de contactos.

- S3 BucketName (obligatorio):

El nombre del bucket de Amazon S3 de su cuenta en la que desea cargar el registro del flujo de contactos. Asegúrese de que la política de buckets no conceda permisos de lectura/escritura innecesarios a las partes que no necesiten acceder a los registros recopilados.

- S3 ObjectPrefix (opcional):

La ruta del objeto de Amazon S3 en el bucket de Amazon S3 para un registro de flujo de contactos cargado. Por ejemplo, si lo especifica CollectedLogs, el registro se cargará como `s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId][AWSAccountId].gz`. Si no especifica este parámetro, se utilizará el ID de ejecución de Systems Manager Automation, por ejemplo: `s3://your-s3-bucket/`

[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz.

Nota: si especifica un valor para esta automatización S3objectPrefix y la ejecuta con el mismo [ContactId], se sobrescribirá el registro del flujo de contactos.

- S3 BucketOwnerAccount (opcional):

El número de AWS cuenta propietario del bucket de Amazon S3 en el que desea cargar el registro del flujo de contactos. Si no especifica este parámetro, el runbook utilizará el ID de AWS cuenta del usuario o rol en el que se ejecuta la automatización.

- S3 BucketOwnerRoleArn (opcional):

El ARN de la función de IAM con permisos para obtener la configuración de acceso público del bucket y el bloqueo de cuentas de Amazon S3, la configuración de cifrado del bucket ACLs, el estado de la política del bucket y cargar objetos al bucket. Si no se especifica este parámetro, el runbook usa el runbook AutomationAssumeRole (si se especifica) o el usuario que inicia este runbook (si no AutomationAssumeRole se especifica). Consulte la sección de permisos necesarios en la descripción del manual.

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

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- CheckConnectInstanceExistence

Comprueba si la instancia de Amazon Connect proporcionada en el ConnectInstanceId esACTIVE.

- Comprueba S3 BucketPublicStatus

Comprueba si el bucket de Amazon S3 especificado en la S3BucketName permite permisos de acceso de lectura o escritura públicos o anónimos.

- GenerateLogSearchTimeRange

Genera `StartTime` y `EndTime` para el `StartQuery` paso en función de la `DescribeContact` API `InitiationTimestamp` y lo `LastUpdateTimestamp` devuelve. `StartTime` será una hora antes `InitiationTimestamp` y `EndTime` una hora después `LastUpdateTimestamp`.

- `StartQuery`

Inicia un registro de consultas para lo proporcionado `ContactId` en el grupo de CloudWatch registros asociado a la instancia de Amazon Connect proporcionada en `ConnectInstanceId`. Las consultas caducan tras 60 minutos de ejecución. Si se agota el tiempo de espera de la consulta, reduzca el intervalo de tiempo en el que se busca. Puede ver las consultas que se están realizando actualmente, así como su historial de consultas recientes en la CloudWatch consola. Para obtener más información, [consulta Ver las consultas en ejecución o el historial de consultas](#).

- `WaitForQueryCompletion`

Espera a que se complete el registro de consultas de los CloudWatch registros proporcionado `ContactId`. Observe que la consulta agota el tiempo de espera después de 60 minutos de ejecución. Si se agota el tiempo de espera de la consulta, reduzca el intervalo de tiempo en el que se busca. Puede ver las consultas en curso actualmente, así como su historial de consultas recientes, en la consola de Amazon Connect. Para obtener más información, consulte [Ver las consultas en curso o el historial de consultas](#).

- `UploadContactFlowLog`

Obtiene el resultado de la consulta y carga el registro del flujo de contactos en el bucket de Amazon S3 especificado en `S3BucketName`.

- `GenerateReport`

Devuelve la URL de la consola Amazon S3 en la que se cargó el registro del flujo de contactos y un ejemplo de comando AWS CLI que puede utilizar para descargar el archivo de registro.

7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución:

- `GenerateReport.OutputPayload`

Resultado que indica que el manual ha recuperado correctamente los registros del flujo de contactos del contacto especificado. Este informe también contiene la URL de la consola

Amazon S3 y un ejemplo de comando AWS CLI para que pueda descargar el archivo de registro.

▼ Outputs

GenerateReport.OutputPayload

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

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

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

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

- S3 Console URL for the Contact Flow Log file

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

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

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

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS Directory Service

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Directory Service Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

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

AWS-CreateDSManagementInstance

Descripción

El AWS-CreateDSManagementInstance runbook crea una instancia de Windows de Amazon Elastic Compute Cloud (Amazon EC2) que puede usar para administrar el directorio. AWS Directory Service La instancia de administración no se puede usar para administrar los directorios del conector de AD.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AmiID

Tipo: cadena

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

Descripción: (Opcional) Amazon Machine Image (AMI) id que se utilizará para lanzar la instancia. De forma predeterminada, la instancia se lanzará con la última AMI básica de Microsoft Windows Server 2019.

- DirectoryId

Tipo: cadena

Descripción: (obligatorio) El identificador de directorio de su Directory Service directorio.

- IamInstanceProfileName

Tipo: cadena

Descripción: (opcional) nombre del perfil de la instancia de IAM. De forma predeterminada, si no existe ningún perfil de instancia con el nombre Amazon SSMDirectoryServiceInstanceProfileRole, se SSMDirectory ServiceInstanceProfileRole creará un perfil de instancia con el nombre Amazon.

Predeterminado: Amazon SSMDirectory ServiceInstanceProfileRole

- InstanceType

Tipo: cadena

Valor predeterminado: t3.medium

Valores permitidos:

- 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

Descripción: (opcional) Tipo de instancia que se va a lanzar. El valor predeterminado es t3.medium.

- KeyPairName

Tipo: cadena

Descripción: (opcional) Par de claves que se utilizará al lanzar la instancia. Windows no admite pares de ED25519 claves. De forma predeterminada, la instancia se lanza sin un key pair (NoKeyPair).

Predeterminado: NoKeyPair

- RemoteAccessCidr

Tipo: cadena

Descripción: (opcional) Crea un grupo de seguridad con un puerto para RDP (rango de puertos 3389) abierto según lo IPs especificado por el CIDR (el valor predeterminado es 0.0.0.0/0). Si el grupo de seguridad ya existe no será modificado y no se cambiarán las reglas.

Valor predeterminado: 0.0.0.0/0

- SecurityGroupName

Tipo: cadena

Descripción: (opcional) Nombre del grupo de seguridad. De forma predeterminada, si no existe ningún grupo de seguridad con el nombre Amazon SSMDirectoryServiceSecurityGroup, se SSMDirectory ServiceSecurityGroup creará un grupo de seguridad con el nombre Amazon.

Predeterminado: Amazon SSMDirectory ServiceSecurityGroup

- Tags

Tipo: MapList

Descripción: (opcional) un par clave-valor que desee aplicar a los recursos creados por la automatización.

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

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeAwsApi`: recopila detalles sobre el directorio que especifique en el parámetro `DirectoryId`.
- `aws:executeAwsApi`: obtiene el bloque CIDR de la nube privada virtual (VPC) en la que se lanzó el directorio.
- `aws:executeAwsApi`: crea un grupo de seguridad con el valor que especifique en el parámetro `SecurityGroupName`.
- `aws:executeAwsApi`: crea una regla de entrada para el grupo de seguridad recién creado que permite el tráfico RDP desde el CIDR que especifique en el parámetro `RemoteAccessCidr`.
- `aws:executeAwsApi`: crea un rol de IAM y un perfil de instancia con el valor que especifique en el parámetro `IamInstanceProfileName`.
- `aws:executeAwsApi`: lanza una instancia de Amazon EC2 en función de los valores que especifique en los parámetros del manual de procedimientos.
- `aws:executeAwsApi`: Crea un AWS Systems Manager documento para unir la instancia recién lanzada a su directorio.
- `aws:runCommand`: une la nueva instancia a su directorio.
- `aws:runCommand`: instala herramientas de administración remota del servidor en la nueva instancia.

AWSSupport-TroubleshootADConnectorConnectivity

Descripción

El manual de procedimientos AWSSupport-TroubleshootADConnectorConnectivity verifica los siguientes requisitos previos para el conector de AD:

- Comprueba si el grupo de seguridad y las reglas de la lista de control de acceso (ACL) de la red asociados a su conector de AD permiten el tráfico necesario.
- Comprueba si los puntos de enlace de la VPC de la CloudWatch interfaz AWS Systems Manager AWS Security Token Service, y de Amazon se encuentran en la misma nube privada virtual (VPC) que el AD Connector.

Cuando las comprobaciones de requisitos previos se completen correctamente, el runbook lanza dos instancias t2.micro de Amazon Elastic Compute Cloud (Amazon EC2) Linux en las mismas subredes que el AD Connector. Después se realizan las pruebas de conectividad de red con las utilidades netcat y nslookup.

[Ejecuta esta automatización \(consola\)](#)

Important

El uso de este manual puede suponer cargos adicionales Cuenta de AWS para las EC2 instancias de Amazon, los volúmenes de Amazon Elastic Block Store y Amazon Machine Image (AMI) creado durante la automatización. Para obtener más información, consulte [Precios de Amazon Elastic Compute Cloud](#) y [Precios de Amazon Elastic Block Store](#).

Si el `aws:deletestack` paso no se realiza correctamente, vaya a la AWS CloudFormation consola para eliminar manualmente la pila. El nombre de la pila creado por este manual de procedimientos comienza por AWSSupport-TroubleshootADConnectorConnectivity. Para obtener información sobre la eliminación de CloudFormation pilas, consulte [Eliminar una pila](#) en la Guía del AWS CloudFormation usuario.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DirectoryId

Tipo: cadena

Descripción: (obligatorio) el ID del directorio del conector de AD con el que desea solucionar los problemas de conectividad.

- Ec2 InstanceProfile

Tipo: cadena

Máximo de caracteres: 128

Descripción: (obligatorio) el nombre del perfil de instancia que desea asignar a las instancias que se lanzan para realizar pruebas de conectividad. El perfil de instancia que especifique debe tener la política AmazonSSMManagedInstanceCore o los permisos equivalentes adjuntos.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el directorio especificado en el parámetro `DirectoryId` es un conector de AD.
- `aws:executeAwsApi`: recopila información sobre el conector de AD.
- `aws:executeAwsApi`: recopila información sobre los grupos de seguridad asociados al conector de AD.
- `aws:executeAwsApi`: recopila información sobre las reglas de ACL de la red asociadas a las subredes del conector de AD.
- `aws:executeScript`: evalúa las reglas del grupo de seguridad del conector de AD para verificar que se permite el tráfico saliente necesario.

- `aws:executeScript`: evalúa las reglas de ACL de la red del conector de AD para verificar que se permite el tráfico de red saliente y entrante requerido.
- `aws:executeScript`- Comprueba si los AWS Systems Manager puntos finales de la CloudWatch interfaz AWS Security Token Service y de Amazon se encuentran en la misma VPC que el AD Connector.
- `aws:executeScript`: compila los resultados de las comprobaciones realizadas en los pasos anteriores.
- `aws:branch`: ramifica la automatización en función del resultado de los pasos anteriores. La automatización se detiene aquí si faltan las reglas de entrada y salida requeridas para los grupos de seguridad y la red. ACLs
- `aws:createStack`- Crea una CloudFormation pila para lanzar EC2 instancias de Amazon para realizar pruebas de conectividad.
- `aws:executeAwsApi`- Reúne las EC2 instancias IDs de Amazon recién lanzadas.
- `aws:waitForAwsResourceProperty`- Espera a que la primera EC2 instancia de Amazon recién lanzada muestre que está gestionada por AWS Systems Manager.
- `aws:waitForAwsResourceProperty`- Espera a que la segunda EC2 instancia de Amazon recién lanzada muestre que está gestionada por AWS Systems Manager.
- `aws:runCommand`- Realiza pruebas de conectividad de red con las direcciones IP del servidor DNS local desde la primera EC2 instancia de Amazon.
- `aws:runCommand`- Realiza pruebas de conectividad de red con las direcciones IP del servidor DNS local desde la segunda EC2 instancia de Amazon.
- `aws:changeInstanceState`- Detiene las EC2 instancias de Amazon utilizadas para las pruebas de conectividad.
- `aws:deleteStack`- Elimina la CloudFormation pila.
- `aws:executeScript`- Muestra instrucciones sobre cómo eliminar manualmente la CloudFormation pila si la automatización no logra eliminarla.

AWSsupport-TroubleshootDirectoryTrust

Descripción

El `AWSsupport-TroubleshootDirectoryTrust` manual diagnostica los problemas de creación de confianza entre un AWS Managed Microsoft AD y un Active Directory de Microsoft. La automatización garantiza que el tipo de directorio sea compatible con las confianzas y, a

continuación, comprueba las reglas de los grupos de seguridad asociados, las listas de control de acceso a la red (red ACLs) y las tablas de enrutamiento para detectar posibles problemas de conectividad.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DirectoryId

Tipo: cadena

Valor permitido: `^d-[a-z0-9]{10}$`

Descripción: (obligatorio) El identificador del que se va AWS Managed Microsoft AD a solucionar el problema.

- RemoteDomainCidrs

Tipo: StringList

Valores permitidos: `^(((0-9){1-9}(0-9){1-9}1(0-9){2}2(0-4)(0-9){25}(0-5))\.\.){3}((0-9){1-9}(0-9){1-9}1(0-9){2}2(0-4)(0-9){25}(0-5))(\.(3(0-2)(1-2)(0-9){1-9}))$`

Descripción: (obligatorio) los CIDR del dominio remoto con el que intenta establecer una relación de confianza. Puede añadir varios valores separados CIDRs por comas. Por ejemplo, 172.31.48.0/20, 192.168.1.10/32.

- RemoteDomainName

Tipo: cadena

Descripción: (obligatorio) nombre completo del dominio remoto con el que está estableciendo una relación de confianza.

- RequiredTrafficACL

Tipo: cadena

Descripción: (obligatorio) Los requisitos de puerto predeterminados para AWS Managed Microsoft AD. En la mayoría de los casos, no debe modificar el valor predeterminado.

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

- RequiredTrafficSG

Tipo: cadena

Descripción: (Obligatorio) Los requisitos de puerto predeterminados para AWS Managed Microsoft AD. En la mayoría de los casos, no debe modificar el valor predeterminado.

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

- TrustId

Tipo: cadena

Descripción: (opcional) ID de la relación de confianza para solucionar el problema.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el tipo de directorio sea AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Obtiene información sobre AWS Managed Microsoft AD.
- `aws:branch`: ramifica la automatización si se proporciona un valor para el parámetro `TrustId` de entrada.
- `aws:executeAwsApi`: obtiene información sobre la relación de confianza.
- `aws:executeAwsApi`: obtiene las direcciones IP DNS del reenviador condicional para el `RemoteDomainName`.
- `aws:executeAwsApi`: obtiene información acerca de las rutas IP que se han agregado a AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Obtiene CIDRs las AWS Managed Microsoft AD subredes.
- `aws:executeAwsApi`: obtiene información acerca de los grupos de seguridad asociados con AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Obtiene información sobre la red ACLs asociada a. AWS Managed Microsoft AD
- `aws:executeScript`: confirma que `RemoteDomainCidrs` son valores válidos. Confirma que AWS Managed Microsoft AD tiene reenviadores condicionales y que las `RemoteDomainCidrs` rutas IP requeridas se han agregado a las direcciones IP que no `RemoteDomainCidrs` son de la RFC 1918. AWS Managed Microsoft AD
- `aws:executeScript`: evalúa las reglas de los grupos de seguridad.

- `aws:executeScript`- Evalúa la red. ACLs

Salidas

`evalDirectorySecuritygroup.output`: resulta de evaluar si las reglas del grupo de seguridad asociadas al mismo AWS Managed Microsoft AD permiten el tráfico necesario para la creación de confianza.

`evalAclEntries.output`: resulta de evaluar si la red ACLs asociada al mismo AWS Managed Microsoft AD permite el tráfico necesario para la creación de confianza.

`evaluateRemoteDomainCIDR.output`: resulta de evaluar si los valores son válidos.

`RemoteDomainCidrs` Confirma que AWS Managed Microsoft AD tiene reenviadores condicionales y que las `RemoteDomainCidrs` rutas IP requeridas se han agregado a las direcciones IP que no `RemoteDomainCidrs` son de la AWS Managed Microsoft AD RFC 1918.

AWS AppSync

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS AppSync Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-EnableAppSyncGraphQLApiLogging](#)

AWS-EnableAppSyncGraphQLApiLogging

Descripción

El `AWS-EnableAppSyncGraphQLApiLogging` runbook permite el registro a nivel de campo y el registro a nivel de solicitud para la API AWS AppSync GraphQL que especifique. El runbook aplicará los cambios a la API GraphQL especificada aunque el registro ya esté habilitado.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ApiId

Tipo: cadena

Descripción: (obligatorio) El ID de la API para la que quieres habilitar el registro.

- FieldLogLevel

Tipo: cadena

Valores válidos: ERROR | TODOS

Descripción: (obligatorio) El nivel de registro del campo.

- CloudWatchLogsRoleArn

Tipo: cadena

Descripción: (obligatorio) El ARN del rol de servicio que AWS AppSync asume publicar en Amazon CloudWatch Logs.

- ExcludeVerboseContent

Tipo: Booleano

Valor predeterminado: False

Descripción: (opcional) Se configura True para excluir información como los encabezados, el contexto y las plantillas de mapeo evaluadas, independientemente del nivel de registro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws: executeAwsApi` - Recopila el tipo de autenticación y la información de configuración relevante para el tipo de autenticación principal.
- `aws:branch`: se ramifica según el tipo de autenticación.
- `aws: executeAwsApi` - Actualiza la configuración de registro de la API AWS AppSync GraphQL en función de los valores especificados para los parámetros de entrada del runbook.

Salidas

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Respuesta de la `UpdateGraphQLApi` llamada.
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Respuesta de la `UpdateGraphQLApi` llamada.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Respuesta de la `UpdateGraphQLApi` llamada.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Respuesta de la `UpdateGraphQLApi` llamada.

Amazon Athena

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Athena. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-EnableAthenaWorkGroupEncryptionAtRest](#)

AWS-EnableAthenaWorkGroupEncryptionAtRest

Descripción

El AWS-EnableAthenaWorkGroupEncryptionAtRest runbook permite el cifrado en reposo para el grupo de trabajo de Amazon Athena que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- WorkGroup

Tipo: cadena

Descripción: (Obligatorio) El grupo de trabajo para el que desea habilitar el cifrado en reposo.

- EncryptionOption

Tipo: cadena

Valores válidos: SSE_S3 | SSE_KMS | CSE_KMS

Descripción: (obligatorio) Especifica qué opción de cifrado se utiliza. Puede elegir el cifrado del lado del servidor con claves administradas de Amazon S3 (SSE_S3), el cifrado del lado del servidor con claves administradas (SSE_KMS) o el cifrado del lado del cliente con claves AWS KMS administradas (CSE_KMS). AWS KMS

- KmsKeyId

Tipo: cadena

Descripción: (opcional) Si utiliza una opción de AWS KMS cifrado, especifique el ARN de la clave, el ID de la clave o el alias de la clave que desee utilizar.

- EnableMinimumEncryptionConfiguration

Tipo: Booleano

Valor predeterminado: True

Descripción: (opcional) Aplica un nivel mínimo de cifrado al grupo de trabajo para los resultados de consultas y cálculos que se escriben en Amazon S3. Cuando está habilitada, los usuarios del grupo de trabajo solo pueden establecer el cifrado en el nivel mínimo establecido por el administrador o en un nivel superior al enviar consultas. Esta configuración no se aplica a los grupos de trabajo habilitados para Spark.

- EnforceWorkGroupConfiguration

Tipo: Booleano

Valor predeterminado: True

Descripción: (Opcional) Si se establece en `True`, la configuración del grupo de trabajo anulará la configuración del lado del cliente. Si se establece en `False`, se utiliza la configuración del lado del cliente.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:branch`: se ramifica según la opción de cifrado especificada en el parámetro. `EncryptionOption`
- `aws:executeAwsApi` - Este paso actualiza el Athena Work Group con la configuración de cifrado especificada.
- `aws:executeAwsApi` - Actualiza el Grupo de Trabajo de Athena con la configuración de cifrado especificada.
- `aws:assertAwsResourceProperty`: verifica que se haya habilitado el cifrado para el grupo de trabajo.

DynamoDB

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para Amazon DynamoDB. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-ChangeDDBRWCapacityMode](#)

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

AWS-ChangeDDBRWCapacityMode

Descripción

El AWS-ChangeDDBRWCapacityMode runbook cambia el modo de capacidad de lectura/escritura de una o más tablas de Amazon DynamoDB (DynamoDB) al modo bajo demanda o al modo aprovisionado.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- CapacityMode

Tipo: cadena

Valores válidos: PROVISIONED | PAY_PER_REQUEST

Descripción: (Obligatorio) El modo de capacidad de lectura/escritura deseado. Al cambiar de la capacidad bajo demanda (pay-per-request) a la aprovisionada, se deben establecer los valores iniciales de la capacidad aprovisionada. Los valores de la capacidad aprovisionada inicial se estiman en función de la capacidad de lectura y escritura consumida por la tabla y los índices secundarios globales durante los últimos 30 minutos.

- ReadCapacityUnits

Tipo: entero

Predeterminado: 0

Descripción: (opcional) El número máximo de lecturas muy consistentes que se consumen por segundo antes de que DynamoDB devuelva una excepción de limitación.

- TableNames

Tipo: cadena

Descripción: (Obligatoria) Lista de nombres de tablas de DynamoDB separados por comas para cambiar el modo de capacidad de lectura/escritura de...

- WriteCapacityUnits

Tipo: entero

Predeterminado: 0

Descripción: (opcional) El número máximo de escrituras consumidas por segundo antes de que DynamoDB devuelva una excepción de limitación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Cambia el modo de capacidad de lectura/escritura de las tablas de DynamoDB especificadas en el parámetro. `TableNames`

Salidas

Modo de `DDBRWCapacity` cambio. `SuccessesTables` - Lista de nombres de tablas de DynamoDB en las que se ha cambiado correctamente el modo de capacidad

Modo de cambio. `DDBRWCapacity FailedTables` - Lista cartográfica de los nombres de las tablas de DynamoDB en las que se ha producido un error al cambiar el modo de capacidad y el motivo del error.

AWS-CreateDynamoDBBackup

Descripción

Creación de una tabla de Amazon DynamoDB.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BackupName

Tipo: cadena

Descripción: (obligatorio) nombre de la copia de seguridad que se va a crear.

- LambdaAssumeRole

Tipo: cadena

Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- TableName

Tipo: cadena

Descripción: (obligatorio) nombre de la tabla de DynamoDB.

AWS-DeleteDynamoDbBackup

Descripción

Elimina la copia de seguridad de una tabla de Amazon DynamoDB.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BackupArn

Tipo: cadena

Descripción: (obligatorio) ARN de la copia de seguridad de la tabla de DynamoDB que eliminar.

AWSConfigRemediation-DeleteDynamoDbTable

Descripción

El manual de procedimientos AWSConfigRemediation-DeleteDynamoDbTable elimina la tabla de Amazon DynamoDB (DynamoDB) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- TableName

Tipo: cadena

Descripción: (obligatorio) nombre de la tabla de DynamoDB que quiere eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- aws:executeScript: elimina la tabla de DynamoDB especificada en el parámetro TableName.
- aws:executeScript: comprueba que se ha eliminado la tabla de DynamoDB.

AWS-DeleteDynamoDbTableBackups

Descripción

Elimine las copias de seguridad de tabla de DynamoDB basadas en días de retención o al recuento.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LambdaAssumeRole

Tipo: cadena

Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- RetentionCount

Tipo: cadena

Valor predeterminado: 10

Descripción: (opcional) el número de copias de seguridad que conservar para la tabla. Si existen más copias de seguridad que el número especificado de copias de seguridad, se eliminarán las copias de seguridad más antiguas. RetentionDays Se puede usar uno RetentionCount o ambos, no ambos.

- RetentionDays

Tipo: cadena

Descripción: (opcional) el número de días que conservar las copias de seguridad para la tabla. Las copias de seguridad más antiguas que el número de días especificado se eliminarán.

RetentionDays Se puede usar una RetentionCount o las dos, no ambas.

- TableName

Tipo: cadena

Descripción: (obligatorio) nombre de la tabla de DynamoDB.

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

Descripción

El AWSConfigRemediation-EnableEncryptionOnDynamoDbTable runbook cifra una tabla de Amazon DynamoDB (DynamoDB) mediante la clave gestionada por el cliente AWS KMS() que especifique para AWS Key Management Service el parámetro. KMSKeyId

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- KMSKeyID

Tipo: cadena

Descripción: (obligatorio) el ARN de la clave administrada por el cliente que desea utilizar para cifrar la tabla de DynamoDB que especifica en el parámetro `TableName`.

- `TableName`

Tipo: cadena

Descripción: (obligatorio) el nombre de la tabla de DynamoDB que quiere encriptar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`: cifra la tabla de DynamoDB que especifique en el parámetro `TableName`.
- `aws:waitForAwsResourceProperty`: comprueba que la propiedad de `Enabled` de la tabla DynamoDB de `SSESpecification` esté establecida en `true`.
- `aws:assertAwsResourceProperty`: comprueba que la tabla de DynamoDB esté cifrada con la clave gestionada por el cliente especificada en el parámetro `KMSKeyId`.

AWSConfigRemediation-EnablePITRForDynamoDbTable

Descripción

El `AWSConfigRemediation-EnablePITRForDynamoDbTable` runbook habilita la point-in-time recuperación (PITR) en la tabla de Amazon DynamoDB que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- TableName

Tipo: cadena

Descripción: (obligatorio) El nombre de la tabla de DynamoDB en la que se va a point-in-time habilitar la recuperación.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`- Permite la point-in-time recuperación en la tabla de DynamoDB que especifique en el parámetro. `TableName`
- `aws:assertAwsResourceProperty`- Confirma que point-in-time la recuperación está habilitada en la tabla de DynamoDB.

AWS-EnableDynamoDbAutoscaling

Descripción

El `AWS-EnableDynamoDbAutoscaling` runbook habilita Application Auto Scaling para la tabla de Amazon DynamoDB de capacidad aprovisionada que especifique. Application Auto Scaling ajusta dinámicamente la capacidad de rendimiento aprovisionada en respuesta a los patrones de tráfico. Para obtener más información, consulte [Administrar la capacidad de rendimiento automáticamente con el escalado automático de DynamoDB en la Guía](#) para desarrolladores de Amazon DynamoDB.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `TableName`

Tipo: cadena

Descripción: (Obligatorio) El nombre de la tabla de DynamoDB en la que desea activar Application Auto Scaling.

- MinReadCapacity

Tipo: entero

Descripción: (Obligatorio) El número mínimo de unidades de capacidad de lectura de rendimiento aprovisionadas para la tabla de DynamoDB.

- MaxReadCapacity

Tipo: entero

Descripción: (obligatorio) El número máximo de unidades de capacidad de lectura de rendimiento aprovisionadas para la tabla de DynamoDB.

- TargetReadCapacityUtilization

Tipo: entero

Descripción: (Obligatorio) El objetivo de utilización de la capacidad de lectura deseado. La utilización objetivo es el porcentaje del rendimiento aprovisionado consumido en un momento dado. Puede establecer los valores de utilización objetivo del escalado automático entre el 20 y el 90 por ciento.

- ReadScaleOutCooldown

Tipo: entero

Descripción: (Obligatorio) Cantidad de tiempo en segundos que se tarda en esperar a que surta efecto una actividad anterior de ampliación de la capacidad de lectura.

- ReadScaleInCooldown

Tipo: entero

Descripción: (Obligatorio) El tiempo en segundos transcurrido desde que se completa una actividad de ampliación de la capacidad de lectura antes de que se pueda iniciar otra actividad de ampliación horizontal.

- MinWriteCapacity

Tipo: entero

Descripción: (Obligatorio) El número mínimo de unidades de escritura de rendimiento provisionadas para la tabla de DynamoDB.

- `MaxWriteCapacity`

Tipo: entero

Descripción: (obligatorio) El número máximo de unidades de escritura de rendimiento provisionadas para la tabla de DynamoDB.

- `TargetWriteCapacityUtilization`

Tipo: entero

Descripción: (Obligatorio) El uso deseado de la capacidad de escritura objetivo. La utilización objetivo es el porcentaje del rendimiento provisionado consumido en un momento dado. Puede establecer los valores de utilización objetivo del escalado automático entre el 20 y el 90 por ciento.

- `WriteScaleOutCooldown`

Tipo: entero

Descripción: (Obligatorio) Cantidad de tiempo en segundos que se tarda en esperar a que surta efecto una actividad anterior de ampliación de la capacidad de escritura.

- `WriteScaleInCooldown`

Tipo: entero

Descripción: (Obligatorio) El tiempo en segundos transcurrido desde que se completa una actividad de ampliación de la capacidad de escritura antes de que se pueda iniciar otra actividad de ampliación horizontal.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `application-autoscaling:DescribeScalableTargets`

- `application-autoscaling:DescribeScalingPolicies`
 - `application-autoscaling:PutScalingPolicy`
 - `application-autoscaling:RegisterScalableTarget`
-
- `RegisterAppAutoscalingTargetWrite` (`aws:executeAwsApi`) - Configura Application Auto Scaling en la tabla de DynamoDB que especifique.
 - `RegisterAppAutoscalingTargetWriteDelay` (`aws:sleep`) - Se suspende para evitar la limitación de la API.
 - `PutScalingPolicyWrite` (`aws:executeAwsApi`): configura la utilización de la capacidad de escritura objetivo para la tabla de DynamoDB.
 - `PutScalingPolicyWriteDelay` (`aws:sleep`) - Se suspende para evitar la limitación de la API.
 - `RegisterAppAutoscalingTargetRead` (`aws:executeAwsApi`): configura las unidades de capacidad de lectura mínima y máxima para la tabla de DynamoDB.
 - `RegisterAppAutoscalingTargetReadDelay` (`aws:sleep`) - Se suspende para evitar la limitación de la API.
 - `PutScalingPolicyRead` (`aws:executeAwsApi`): configura la utilización de la capacidad de lectura objetivo para la tabla de DynamoDB.
 - `VerifyDynamoDbAutoscalingEnabled` (`aws:executeScript`) - Verifica que Application Auto Scaling esté habilitado para la tabla de DynamoDB según los valores que especifique.

Salidas

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

AWS-RestoreDynamoDBTable

Descripción

El `AWS-RestoreDynamoDBTable` runbook restaura la tabla de Amazon DynamoDB que point-in-time especifique mediante la recuperación (PITR).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- EnablePointInTimeRecoverAsNeeded

Tipo: Booleano

Predeterminado: true

Descripción: (opcional) Determina si la automatización activa la point-in-time recuperación según sea necesario para restaurar la tabla.

- GlobalSecondaryIndexOverride

Tipo: cadena

Descripción: (opcional) los nuevos índices secundarios globales sustituirán a los índices secundarios existentes en la nueva tabla.

- LocalSecondaryIndexOverride

Tipo: cadena

Descripción: (opcional) los nuevos índices secundarios locales sustituirán a los índices secundarios existentes de la nueva tabla.

- RestoreDateTime

Tipo: cadena

Descripción: (Obligatorio) La point-in-time recuperación a la que quieres restaurar la tabla durante los últimos 35 días. Especifique la fecha y hora en el siguiente formato: DD/MM/YYYY HH:MM:SS.

- SourceTableArn

Tipo: cadena

Descripción: (obligatorio) ID de la instancia de ARN que desea reiniciar.

- SseSpecificationOverride

Tipo: cadena

Descripción: (opcional) la configuración de cifrado del lado del servidor que se utilizará en la nueva tabla.

- TargetTableName

Tipo: cadena

Descripción: (obligatorio) el nombre de la tabla que se va a restaurar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- `dynamodb:Scan`
- `dynamodb:UpdateItem`

Pasos de documentos

- `aws:executeScript`- Restaura la tabla de DynamoDB que especifique en `TargetTableName` el parámetro mediante `recovery.point-in-time`

AWS Database Migration Service

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para AWS Database Migration Service. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

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

AWSSupport-TroubleshootDMSTableErrors

Descripción

El manual de AWS Systems Manager `AWSSupport-TroubleshootDMSTableErrors` automatización le ayuda a automatizar el proceso de solución de problemas en las tareas de migración de `Table errors` bases de datos o en la replicación sin servidor desde AWS Database Migration Service. Estos errores se producen cuando las tablas no se migran del punto final de origen (base de datos de origen) al punto final de destino (base de datos de destino) debido a la tarea de migración de la base de datos o a la replicación sin servidor creada en el servicio AWS DMS. Este manual analiza los mensajes de error de firma de los registros y se centra específicamente en CloudWatch los registros de tareas para las tareas tradicionales de migración de bases de datos y en los registros sin servidor para la replicación sin servidor. También proporciona sugerencias específicas y medidas de corrección para los mensajes de error más comunes que aparecen durante las migraciones. `Table error AWS DMS`

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Obtiene información sobre el AWS DMS ARN proporcionado, que puede ser una tarea de migración de base de datos o una replicación sin servidor.
- Comprueba si el AWS DMS recurso proporcionado se ha iniciado al menos una vez comprobando el `FreshStartDate` valor en la respuesta de la `DescribeReplicationTasks` API (para la tarea de migración de la base de datos) y de la `DescribeReplications` API (para la replicación sin servidor). Si el recurso no se ha iniciado, la automatización genera un error.
- Si el recurso se ha iniciado, la automatización comprueba las tablas de los `TableError` estados utilizando `TableStatistics` información. Si no se encuentra ningún error, la automatización finaliza el flujo de trabajo después de mostrar un mensaje que confirma que no se ha encontrado ningún error en la tabla en la tarea de migración de la base de datos especificada o en la replicación sin servidor.
- Si se encuentran tablas con `TableError` estados, la automatización comprueba si el CloudWatch registro está habilitado para el AWS DMS recurso especificado. Si el registro no está habilitado, la automatización finaliza el flujo de trabajo después de mostrar un mensaje que indica que el registro no está habilitado.

Nota: se espera que el CloudWatch registro esté habilitado, ya que la automatización se basa en estos registros para analizar e identificar los problemas relacionados con las tablas en `TableError` estado.

- Si el registro está habilitado, la automatización analiza los CloudWatch registros y genera un informe para cada tabla que esté en `TableError` estado. El informe incluye sugerencias sobre los mensajes de error más comunes y proporciona los registros de errores pertinentes para ayudar a identificar y resolver los problemas que impiden la correcta migración de la tabla del punto final de AWS DMS origen al punto final de AWS DMS destino.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DMSArn

Tipo: cadena

Descripción: (obligatorio) ARN de la tarea de migración de la base de datos o replicación sin servidor

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

- StartTimeRange

Tipo: cadena

Descripción: (opcional) Este parámetro define el inicio del intervalo de tiempo para el análisis de los CloudWatch registros de la tarea de migración de la base de datos o la replicación sin servidor determinada. Si se proporciona, solo se recopilarán y analizarán los registros generados a partir de ese momento específico. Tenga en cuenta que existe la posibilidad de que se agote el tiempo de espera del flujo de trabajo si el intervalo de tiempo entre `startDate` y `endDate` es demasiado largo. El valor debe proporcionarse en formato de fecha y hora ISO 6081.

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

- EndTimeRange

Tipo: cadena

Descripción: (opcional) Este parámetro establece el final del intervalo de tiempo para el análisis del CloudWatch registro de la tarea de migración de la base de datos determinada o la replicación

sin servidor. Si se proporciona, solo se recopilarán y analizarán los registros generados hasta ese momento específico. Tenga en cuenta que existe la posibilidad de que se agote el tiempo de espera del flujo de trabajo si el intervalo de tiempo entre `startDate` y `endDate` es demasiado largo. El valor debe proporcionarse en formato de fecha y hora ISO 6081.

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

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Ejemplo de política de IAM para el rol Automation Assume

JSON

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

```

        "dms:DescribeReplicationTasks",
        "dms:DescribeReplications"
    ],
    "Resource": "*"
}
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootDMSTableErrors](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- DMSArn

ARN de la tarea de migración de la base de datos o la replicación sin servidor que tiene errores de tabla.

- StartTimeRange

(Opcional) Formato de fecha y hora ISO 6081 que define el inicio del intervalo de tiempo para analizar los CloudWatch registros de la tarea de migración de la base de datos determinada o la replicación sin servidor.

- EndTimeRange

(Opcional) Formato de fecha y hora ISO 6081 que define el final del intervalo de tiempo para analizar los CloudWatch registros de la tarea de migración de la base de datos en cuestión o de la replicación sin servidor.

4. Seleccione el botón Ejecutar en la parte inferior de la página.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- validar DMSInput TypeAndGatherDetails

Valida la entrada del AWS DMS ARN dada y recopila los detalles básicos de la tarea de migración de la base de datos o la replicación sin servidor que se requieren en los siguientes pasos.

- branchOnTableErrores

Ramifica el flujo de trabajo en función del número de errores de tabla encontrados en el paso anterior. Si el recuento es superior a 0, continúe con el branchOnCWLoggingStatus paso -. De lo contrario, continúe con el outputNoTableErrors paso -.

- outputNoTableErrores

Muestra un mensaje que indica que los errores de la tabla no se encuentran en la tarea de migración de la base de datos determinada o en la replicación sin servidor.

- Estado de BranchOn CWLogging

Ramifica el flujo de trabajo en función del estado de CloudWatch registro que se encuentra en el paso anterior. Si está activado, continúe con el gatherTableDetails paso -. De lo contrario, continúe con el outputNoCWLoggingEnabled paso -.

- Salida No habilitada CWLogging

Muestra un mensaje que indica que el CloudWatch registro no está habilitado en la tarea de migración de la base de datos o en la replicación sin servidor en cuestión.

- gatherTableDetails

Recopila las FullLoadEndTime marcas temporales de las tablas fallidas y calcula los valores del intervalo de tiempo para analizar los registros. CloudWatch

- analyzeCloudWatchRegistros

Analiza los registros que se encuentran en el grupo de CloudWatch registros en función de los mensajes de error de firma y devuelve el informe al usuario.

7. Una vez completada la ejecución, revise la sección de resultados para ver los resultados detallados de la ejecución.

- Se encontraron errores en el resultado de No hay ninguna tabla

Si no se encuentra ningún error de tabla en la tarea de migración de base de datos proporcionada o en la replicación sin servidor, la automatización muestra el resultado con el mismo mensaje.

- Resultado de No se ha activado el inicio de CloudWatch sesión

Si el CloudWatch registro no está habilitado en la tarea de migración de bases de datos proporcionada o en la replicación sin servidor, la automatización muestra el resultado que indica lo mismo y proporciona los pasos para habilitar el registro.

- Informe de análisis de registros

Genera un informe que identifica las tablas en Table error estado correspondientes a la tarea de migración de bases de datos proporcionada o a la replicación sin servidor, diferenciando los tipos de error, enumerando los mensajes de error encontrados y proporcionando sugerencias y pasos de corrección específicos para cada tabla identificada.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSSupport-TroubleshootDMSEndpointConnection

Descripción

El AWSSupport-TroubleshootDMSEndpointConnection manual ayuda a diagnosticar y solucionar los problemas de conectividad entre AWS Database Migration Service las instancias de replicación y los puntos finales. AWS DMS La automatización utiliza las comprobaciones [del Reachability Analyzer](#) para probar la conectividad de la red y analiza la configuración de la red para identificar posibles problemas de conectividad que podrían impedir que las migraciones se realicen correctamente. AWS DMS

 Important

Debe haber probado la conectividad entre la instancia de AWS DMS replicación y el punto final mediante la AWS DMS consola o la API antes de ejecutar este manual. Si no ha probado la conexión, hágalo primero; de lo contrario, puede que tenga que volver a ejecutar este runbook. Tanto la instancia de AWS DMS replicación como el punto final deben estar disponibles para que las pruebas de conectividad sean precisas.

 Important

Este manual crea e invoca AWS Lambda funciones, que generarán cargos de Lambda. Cada ejecución de análisis del Reachability Analyzer también conlleva cargos. [Para obtener más información sobre los precios, consulte la página de precios de Amazon VPC en la pestaña Network Analysis y AWS Lambda precios.](#)

¿Cómo funciona?

El manual realiza un análisis sistemático de la AWS DMS conectividad a través de las siguientes fases:

Fase 1: Validación de recursos y requisitos previos

- Validación del punto final: verifica la existencia del AWS DMS punto final, recupera su configuración (nombre del servidor, puerto y tipo de motor) y confirma que el motor de base de datos es compatible para la solución de problemas.
- Estado de la prueba de conexión: recupera el estado actual de la prueba de conexión entre la instancia de replicación y el punto final mediante la AWS DMS DescribeConnections API, incluidos los mensajes de error de intentos de prueba anteriores.
- Análisis de instancias de replicación: recopila los detalles de la configuración de la red, incluidos el ID de Amazon VPC, la IDs subred y el IDs grupo de seguridad, e identifica la interfaz de red elástica (ENI) asociada a la instancia de replicación.

Fase 2: resolución de DNS y descubrimiento de rutas de red

- Resolución de DNS basada en Amazon VPC: crea una función Lambda temporal en la misma Amazon VPC que la instancia de replicación para convertir el nombre de host del punto final en su

dirección IP desde el contexto de Amazon VPC, lo que garantiza una resolución de DNS privada precisa.

- **Identificación del objetivo:** determina el objetivo adecuado para Reachability Analyzer en función de si el punto final se encuentra dentro de la misma Amazon VPC (usa ENI) o es externo (usa una dirección IP resuelta).
- **IPv6 Comprobación de compatibilidad:** valida que las direcciones resueltas lo estén IPv4, ya que Reachability Analyzer no admite direcciones IPv6

Fase 3: Análisis integral de la ruta de la red

- **Ejecución del Reachability Analyzer:** crea una ruta de Network Insights desde la instancia de replicación ENI hasta el destino (ENI del punto final o dirección IP) y ejecuta un análisis exhaustivo para probar la conectividad TCP en el puerto especificado.
- **Análisis de red multicapa:** examina la ruta de red completa, incluidas las tablas de enrutamiento, los grupos de seguridad, la red, las puertas de enlace de Internet ACLs, las puertas de enlace de NAT, las conexiones de emparejamiento de Amazon VPC y las puertas de enlace de tránsito para identificar las barreras de conectividad.
- **Generación de explicaciones detalladas:** en caso de problemas de conectividad, proporciona explicaciones específicas para cada componente de la red que bloquea el tráfico, incluidos los números de reglas exactos, los bloques de CIDR, los rangos de puertos y las restricciones de protocolo.

Fase 4: generación de informes y limpieza de recursos

- **Informes exhaustivos:** genera un informe detallado que contiene un resumen de las pruebas de conexión, los resultados del análisis de la ruta de la red y las explicaciones específicas de los fallos, junto con una guía de corrección.
- **Administración de recursos:** limpia automáticamente los recursos creados (función Lambda, funciones de IAM, rutas de Network Insights), a menos que `PersistReachabilityAnalyzerResults` el parámetro esté configurado para conservar los resultados del análisis para su posterior investigación.
- **Gestión de errores:** proporciona informes de errores específicos para diversos escenarios de error, como motores de bases de datos no compatibles, recursos faltantes, errores en la resolución del DNS y problemas de permisos.

El manual admite la solución de problemas de conectividad para varios motores de bases de datos, incluidos Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon Neptune, Amazon Redshift, Amazon S3, Azure SQL Database, MySQL, Oracle, PostgreSQL DB2, SQL Server y muchos otros.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `dms:DescribeEndpoints`
- `dms:DescribeReplicationInstances`
- `dms:DescribeConnections`
- `iam:GetRole`
- `iam:PassRole`
- `iam:SimulatePrincipalPolicy`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:GetFunction`
- `lambda:InvokeFunction`

- `lambda:ListTags`
- `lambda:TagResource`
- `lambda:UntagResource`
- `lambda:UpdateFunctionCode`

Permisos de IAM opcionales

Los siguientes permisos solo son necesarios dentro de la `AutomationAssumeRole` si no proporciona un `LambdaRoleArn` parámetro y desea que la automatización cree la función de ejecución de Lambda por usted:

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

Important

Además de las acciones mencionadas anteriormente, `AutomationAssumeRole` deben tener [Amazon VPCReachability AnalyzerFullAccessPolicy](#) como [política gestionada adjunta](#) para que las pruebas del [Reachability Analyzer](#) se realicen correctamente.

Ejemplo de política:

```
{
  "Version": "2012-10-17"      ,
  "Statement": [
    {
      "Sid": "AllowDMSTroubleshootingActions",
      "Effect": "Allow",
      "Action": [
        "dms:DescribeEndpoints",
        "dms:DescribeReplicationInstances",
```

```

        "dms:DescribeConnections",
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:TagRole",
        "iam:UntagRole"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowDMSLambdaInvocation",
    "Effect": "Allow",
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": "arn:*:lambda:*:function:AWSSupport-
TroubleshootDMSEndpointConnection-*"
},
{
    "Sid": "AllowPassRoleToDMSLambda",
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "arn:*:iam:*:role/AWSSupport-
TroubleshootDMSEndpointConnection-*",
    "Condition": {
        "StringLikeIfExists": {
            "iam:PassedToService": "lambda.amazonaws.com"
        }
    }
},

```

```

    {
      "Sid": "AllowRolePolicyManagement",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "iam:ResourceTag/AWSSupport-
TroubleshootDMSEndpointConnection": "true"
        }
      }
    }
  ]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootDMSEndpointConnection](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a SSM Automation realizar las acciones en su nombre. Si no se especifica ningún rol, SSM Automation utiliza los permisos del usuario que inicia este manual.
 - Tipo: `AWS::IAM::Role::Arn`
 - DmsEndpointArn (Obligatorio)
 - Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) del AWS Database Migration Service punto final.
 - Tipo: `String`

- Valor permitido: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+:\d{12}:endpoint:[A-Z0-9]{1,48}$`
- DmsReplicationInstanceArn (Obligatorio)
 - Descripción: (obligatorio) El nombre de recurso de Amazon (ARN) de la instancia de AWS Database Migration Service replicación.
 - Tipo: String
 - Valor permitido: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+:\d{12}:rep:[A-Z0-9]+$`
- PersistReachabilityAnalyzerResults (Opcional)
 - Descripción: (opcional) El indicador que informa si los resultados de la ejecución del análisis de Network Insights deben conservarse o no.
 - Tipo: Boolean
 - Valores permitidos: `[true, false]`
 - Valor predeterminado: `false`
- LambdaRoleArn (Opcional)
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a la AWS Lambda función acceder a los AWS servicios y recursos necesarios. Si no se especifica ninguna función, esta automatización de Systems Manager creará una función de IAM para Lambda en su cuenta.
 - Tipo: `AWS::IAM::Role::Arn`
 - Valor predeterminado: `""`
- Confirme (obligatorio)
 - Descripción: (Obligatorio) Introduzca esta información yes para confirmar que este manual creará una función Lambda en su cuenta y creará una función de IAM si no LambdaRoleArn se proporciona ninguna.
 - Tipo: String
 - Valor permitido: `^[Yy][Ee][Ss]$`

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- DescribeEndpointAndCheckEngine:

Recupera la configuración del AWS DMS punto final y valida si el tipo de motor de base de datos es compatible para la solución de problemas. Extrae el nombre del servidor, el puerto y el tipo de motor de la configuración del punto final.

- `BranchOnEndpointAndCheckEngineErrors`:

Ramifica la automatización en función de los errores de la validación del punto final. Si se encuentran errores, la automatización procede a generar un informe de errores; de lo contrario, continúa con las pruebas de conectividad.

- `GetTestConnectionStatus`:

Recupera el estado de la conexión y el mensaje de error del AWS DMS punto final mediante la `DescribeConnections` API. Este paso comprueba si se ha realizado una prueba de conexión y captura los mensajes de error.

- `BranchOnTestConnectionStatusErrors`:

Ramifica la automatización en función de los errores de estado de la prueba de conexión. Si se detectan errores, la automatización genera un informe de errores; de lo contrario, continúa con el análisis de las instancias de replicación.

- `DescribeReplicationInstance`:

Recupera los detalles de configuración de red de la instancia de AWS DMS replicación, incluidos el ID de Amazon VPC, la IDs subred y el IDs grupo de seguridad, e identifica la interfaz de red elástica (ENI) asociada.

- `ValidateResourcePermissions`:

Valida que la función de ejecución tenga los permisos necesarios para limpiar los recursos que se crearán durante el proceso de automatización.

- Cree `DNSResolver Lambda`:

Crea una AWS CloudFormation pila que contiene una función Lambda implementada en la misma Amazon VPC que la instancia de replicación. Esta función se utiliza para convertir nombres DNS en direcciones IP privadas desde el contexto de Amazon VPC.

- `DescribeCloudFormationErrorFromStackEvents`:

Si se produce un error en la creación de la CloudFormation pila, en este paso se describen los errores de los eventos de la pila para proporcionar información detallada sobre los errores y poder solucionarlos.

- **Obtenga DNSResolverLambdaName:**

Recupera el nombre de la función Lambda del solucionador de DNS de los resultados de CloudFormation la pila para su uso en los pasos siguientes.

- **ResolveDmsEndpoint:**

Invoca la función Lambda para convertir el nombre de host AWS DMS del punto final en su dirección IP desde Amazon VPC. Esto garantiza una resolución precisa del DNS privado y valida la compatibilidad. IPv4

- **BranchOnResolveDmsEndpointErrors:**

Ramifica la automatización en función de los errores de resolución del DNS. Si el punto final no se puede resolver o se resuelve en una IPv6 dirección, la automatización genera un informe de errores.

- **GetReachabilityAnalyzerTarget:**

Identifica el objetivo adecuado para el Reachability Analyzer en función de la configuración de Amazon VPC y la ubicación del punto final. Determina si se debe utilizar un ENI (para los mismos puntos de enlace de Amazon VPC) o una dirección IP (para los puntos de enlace externos) como destino.

- **GenerateErrors:**

Crea un informe de errores completo cuando se producen errores en los pasos anteriores. Incluye detalles sobre los errores de validación de los terminales, los fallos en las pruebas de conexión o los problemas de resolución del DNS, así como una guía de corrección específica.

- **GenerateReport:**

Crea un informe completo de solución de problemas que contiene el estado de la conexión, los resultados del análisis de la ruta de la red mediante el Reachability Analyzer, explicaciones detalladas de las barreras de conectividad y acciones recomendadas para su resolución.

- **CheckStackExists:**

Comprueba si la CloudFormation pila se creó correctamente y si es necesario eliminarla durante la limpieza. Este paso garantiza una gestión adecuada de los recursos, independientemente del éxito o el fracaso de la automatización.

- **Eliminar DNSResolver Lambda:**

Elimina la CloudFormation pila que contiene la función Lambda de resolución de DNS y los recursos asociados (`PersistReachabilityAnalyzerResults` a menos que esté configurada en), lo que garantiza `true` que no queden recursos residuales una vez finalizada la automatización.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución:

- `GetTestConnectionStatus.estado`

El estado actual de la prueba de conexión entre la instancia de AWS DMS replicación y el punto final (p. ej., correcta, fallida, en fase de prueba).

- `DescribeCloudFormationErrorFromStackEvents.Eventos`

Si se produce un error en la creación de la CloudFormation pila, este resultado contiene los eventos de error detallados del proceso de creación de la pila para ayudar a diagnosticar los problemas de implementación de la infraestructura.

- `GenerateReport.informe`

Un informe completo de solución de problemas que contiene los resultados del análisis de conexión, los hallazgos del Reachability Analyzer, el análisis de la ruta de la red, las barreras de conectividad específicas identificadas y recomendaciones de remediación detalladas con enlaces a la documentación relevante. AWS

- `GenerateErrors.informe`

Si se producen errores durante el proceso de automatización, este resultado proporciona un informe de errores detallado que incluye los motivos específicos del error, los recursos afectados y una guía para resolver los problemas antes de volver a intentar la automatización.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

Amazon EBS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic Block Store. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [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

Descripción

El manual de AWSSupport-AnalyzeEBSResourceUsage automatización se utiliza para analizar el uso de los recursos en Amazon Elastic Block Store (Amazon Block Store). Analiza el uso del volumen e identifica los volúmenes, imágenes e instantáneas abandonados en una región determinada. AWS

¿Cómo funciona?

El manual de ejecución realiza las cuatro tareas siguientes:

1. Comprueba que existe un bucket de Amazon Simple Storage Service (Amazon S3) o crea uno nuevo.
2. Reúne todos los volúmenes de Amazon EBS en el estado disponible.
3. Reúne todas las instantáneas de Amazon EBS para las que se ha eliminado el volumen de origen.
4. Reúne todas las imágenes de máquina de Amazon (AMI) que no estén siendo utilizadas por ninguna instancia no terminada de Amazon Elastic Compute Cloud (Amazon EC2).

El runbook genera informes CSV y los almacena en un bucket de Amazon S3 proporcionado por el usuario. El depósito proporcionado debe estar protegido siguiendo las mejores prácticas AWS de seguridad, tal como se describe al final. Si el bucket de Amazon S3 proporcionado por el usuario no existe en la cuenta, el runbook crea un nuevo bucket de Amazon S3 con el formato de nombre `<User-provided-name>-awssupport-YYYY-MM-DD`, cifrado con una clave personalizada AWS Key Management Service (AWS KMS), con el control de versiones de objetos habilitado, bloquea el acceso público y requiere solicitudes para usar SSL/TLS.

Si desea especificar su propio bucket de Amazon S3, asegúrese de que esté configurado siguiendo estas prácticas recomendadas:

- Bloquee el acceso público al bucket (establecido `IsPublic` en `False`).
- Active el registro de acceso a Amazon S3.
- [Permita solo las solicitudes de SSL en su bucket.](#)
- Activa el control de versiones de objetos.
- Usa una clave AWS Key Management Service (AWS KMS) para cifrar tu bucket.

Important

El uso de este manual puede implicar cargos adicionales en su cuenta por la creación de buckets y objetos de Amazon S3. Consulte los [precios de Amazon S3](#) para obtener más información sobre los cargos en los que se puede incurrir.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- S3 BucketName

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

Descripción: (obligatorio) El bucket de Amazon S3 de su cuenta en el que cargar el informe. Asegúrese de que la política de cubos no conceda read/write permisos innecesarios a las partes que no necesitan acceder a los registros recopilados. Si el depósito especificado no existe en la cuenta, la automatización crea un nuevo depósito en la región en la que se inicia la automatización con el formato de nombre <User-provided-name>-awssupport-YYYY-MM-DD, cifrado con una AWS KMS clave personalizada.

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

- CustomerManagedKmsKeyArn

Tipo: cadena

Descripción: (opcional) La AWS KMS clave personalizada Amazon Resource Name (ARN) para cifrar el nuevo bucket de Amazon S3 que se creará si el bucket especificado no existe en la cuenta. La automatización falla si se intenta crear el depósito sin especificar un ARN de AWS KMS clave personalizada.

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

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Ejemplo de política con los permisos de IAM mínimos necesarios para ejecutar este manual:

JSON

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



```

    "Statement": [{
      "Sid": "ReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ssm:DescribeAutomationExecutions"
      ],
      "Resource": "*"
    }, {
      "Sid": "KMSGeneratePermissions",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
      "Resource": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }, {
      "Sid": "S3ReadOnlyPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketAcl",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
        "arn:aws:s3:::amzn-s3-demo-bucket2/"
      ]
    }, {
      "Sid": "S3CreatePermissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketLogging",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "*"
    }
  ]
}

```

```
}
    }
}
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-AnalyzeEBSResourceUsage](#) la AWS Systems Manager consola.

2. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- S3 BucketName (obligatorio):

El bucket de Amazon S3 de su cuenta en el que cargar el informe.

- CustomerManagedKmsKeyArn(Opcional):

La AWS KMS clave personalizada Amazon Resource Name (ARN) para cifrar el nuevo bucket de Amazon S3 que se creará si el bucket especificado no existe en la cuenta.

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**.

Enter the name of an existing S3 Bucket

test-bucket-1

Example: s3-bucket-name

AutomationAssumeRole

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

Select an existing IAM Role

admin-my

arn:aws:iam:::role:

CustomerManagedKmsKeyArn

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

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

3. Seleccione Ejecutar.

4. Se inicia la automatización.

5. El manual de procedimientos de automatización realiza los siguientes pasos:

- Compruebe la simultaneidad:

Garantiza que solo haya una iniciación de este manual en la región. Si el runbook encuentra otra ejecución en curso, devuelve un error y finaliza.

- verifyOrCreateCubo S3:

Comprueba si existe el bucket de Amazon S3. De lo contrario, crea un nuevo bucket de Amazon S3 en la región en la que se inicia la automatización con el formato de nombre `<User-provided-name>-awssupport-YYYY-MM-DD`, cifrado con una AWS KMS clave personalizada.

- gatherAmiDetails:

Busca AMI que no estén siendo utilizadas por ninguna instancia de Amazon EC2, genera el informe con el formato `<region>-images.csv` de nombre y lo carga en el bucket de Amazon S3.

- gatherVolumeDetails:

Verifica los volúmenes de Amazon EBS en el estado disponible, genera el informe con el formato `<region>-volume.csv` de nombre y lo carga en un bucket de Amazon S3.

- gatherSnapshotDetails:

Busca las instantáneas de Amazon EBS de los volúmenes de Amazon EBS que ya se han eliminado, genera el informe con el formato `<region>-snapshot.csv` del nombre y lo carga en el bucket de Amazon S3.

6. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.

▼ 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.	

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS-ArchiveEBSSnapshots

Descripción

El manual de procedimientos AWS-ArchiveEBSSnapshots le ayuda a archivar las instantáneas de los volúmenes de Amazon Elastic Block Store (Amazon EBS) especificando la etiqueta que ha aplicado a sus instantáneas. Como alternativa, puede proporcionar el ID de un volumen si sus instantáneas no están etiquetadas.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Description (Descripción)

Tipo: cadena

Descripción: (opcional) una descripción para la instantánea de Amazon EBS.

- DryRun

Tipo: cadena

Valores válidos: Yes | No

Descripción: (obligatorio) comprueba si tiene los permisos necesarios para la acción, sin realizar realmente la solicitud, y proporciona una respuesta de error.

- RetentionCount

Tipo: cadena

Descripción: (opcional) el número de instantáneas que desea archivar. No especifique un valor para este parámetro si especifica un valor para RetentionDays.

- RetentionDays

Tipo: cadena

Descripción: (opcional) el número de días anteriores de instantáneas que desea archivar. No especifique un valor para este parámetro si especifica un valor para RetentionCount.

- SnapshotWithTag

Tipo: cadena

Valores válidos: Yes | No

Descripción: (obligatorio) especifica si las instantáneas que desea archivar están etiquetadas.

- TagKey

Tipo: cadena

Descripción: (opcional) la clave de la etiqueta asignada a las instantáneas que desea archivar.

- TagValue

Tipo: cadena

Descripción: (opcional) el valor de la etiqueta asignada a las instantáneas que desea archivar.

- Volumeld

Tipo: cadena

Descripción: (opcional) el ID del volumen cuyas instantáneas desea archivar. Utilice este parámetro si sus instantáneas no están etiquetadas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

`aws:executeScript`: archiva las instantáneas usando la etiqueta que especifique mediante los parámetros `TagKey` y `TagValue` o el parámetro `VolumeId`.

AWS-AttachEBSVolume

Descripción

Adjunte una Amazon Elastic Block Store (Amazon EBS) a una instancia Amazon Elastic Compute Cloud (Amazon EC2).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Dispositivo

Tipo: cadena

Descripción: (obligatorio) el nombre del dispositivo (por ejemplo, /dev/sdh o xvdh).

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia en la que desea asociar el volumen.

- VolumeId

Tipo: cadena

Descripción: (obligatorio) ID del volumen de Amazon EBS. El volumen y la instancia deben estar dentro de la misma zona de disponibilidad.

AWSsupport-CalculateEBSPerformanceMetrics

Descripción

El AWSsupport-CalculateEBSPerformanceMetrics manual ayuda a diagnosticar los problemas de rendimiento de Amazon EBS mediante el cálculo y la publicación de las métricas de rendimiento en un CloudWatch panel de control. El panel muestra las IOPS y el rendimiento medios estimados para un volumen de Amazon EBS objetivo o todos los volúmenes adjuntos a la instancia de Amazon Elastic Compute Cloud (Amazon EC2) de destino. En el caso de las instancias Amazon EC2, también muestra el rendimiento y las IOPS promedio de la instancia. El manual muestra el enlace al CloudWatch panel recién creado, que muestra las métricas calculadas relevantes. CloudWatch El CloudWatch panel se crea en su cuenta con el nombre:AWSsupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>.

¿Cómo funciona?

El manual realiza los siguientes pasos:

- Garantiza que las marcas de tiempo especificadas sean válidas.
- Valida si el ID de recurso (volumen de Amazon EBS o instancia de Amazon EC2) es válido.
- Al proporcionar un Amazon EC2 como ResourceID, se crea un CloudWatch panel con el total real de esa instancia de IOPS/Throughput Amazon EC2 y un gráfico de IOPs/rendimiento medio estimado para todos los volúmenes de Amazon EBS adjuntos a una instancia de Amazon EC2.
- Cuando proporcionas un volumen de Amazon EBS como ResourceID, se crea un panel con CloudWatch un gráfico de IOPS/Throughput promedio estimado para ese volumen.
- Una vez generado el CloudWatch panel, si las IOPS promedio estimadas o el rendimiento promedio estimado son superiores a las IOPS máximas o al rendimiento máximo, respectivamente, es posible realizar microráfagas para el volumen o los volúmenes adjuntos a una instancia de Amazon EC2.

Note

En el caso de los volúmenes con capacidad de ráfaga (gp2, sc2 y st1), se debe tener en cuenta el máximo hasta lograr un equilibrio de ráfagas. IOPS/throughput Una vez que el balance de ráfaga se haya utilizado por completo, es decir, cuando pase a ser cero, considere las métricas de referencia. IOPS/throughput

Important

La creación del CloudWatch panel de control puede conllevar cargos adicionales a su cuenta. Para obtener más información, consulta la [guía de CloudWatch precios de Amazon](#).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Ejemplo de política

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "cloudwatch:PutDashboard",
      "Resource": "arn:aws:cloudwatch::111122223333:dashboard/*-EBS-Performance-*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceTypes"
      ],
      "Resource": "*"
    }
  ]
}
```

```
]
}
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-CalculateEBSPerformanceMetrics](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- ResourceID (obligatorio):

El ID de la instancia de Amazon EC2 o del volumen de Amazon EBS.

- Hora de inicio (obligatorio):

Hora de inicio para ver los datos CloudWatch. La hora debe estar en el formato yyyy-mm-ddThh:mm:ss y en UTC.

- Hora de finalización (obligatoria):

Hora de finalización para ver los datos CloudWatch. La hora debe estar en el formato yyyy-mm-ddThh:mm:ss y en UTC.

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

4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:
 - CheckResourceIDAndTimeStamps:

Comprueba si la hora de finalización es superior a la hora de inicio en al menos un minuto y si el recurso proporcionado existe.

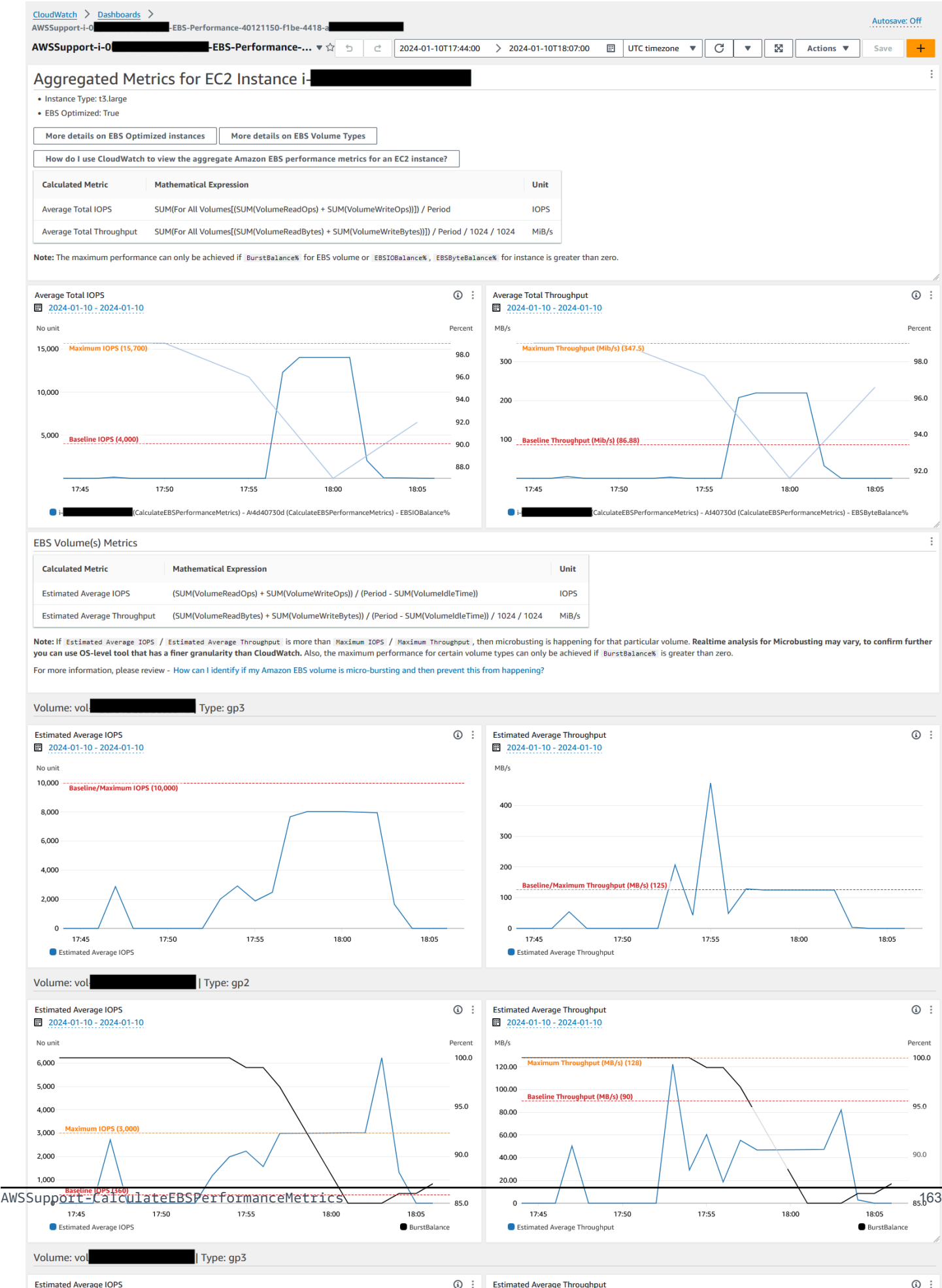
- **CreateCloudWatchDashboard:**

Calcula el rendimiento de Amazon EBS y muestra un gráfico basado en su ID de recurso. Si proporciona un ID de volumen de Amazon EBS para el parámetro ID de recurso, este manual crea un CloudWatch panel con el promedio estimado de IOPS y el rendimiento promedio estimado para el volumen de Amazon EBS. Si proporciona un ID de instancia de Amazon EC2 para el parámetro ID de recurso, este manual crea un CloudWatch panel con el promedio de IOPS totales y el rendimiento total promedio de la instancia de Amazon EC2 y con el promedio estimado de IOPS y el rendimiento promedio estimado para todos los volúmenes de Amazon EBS adjuntos a la instancia de Amazon EC2.

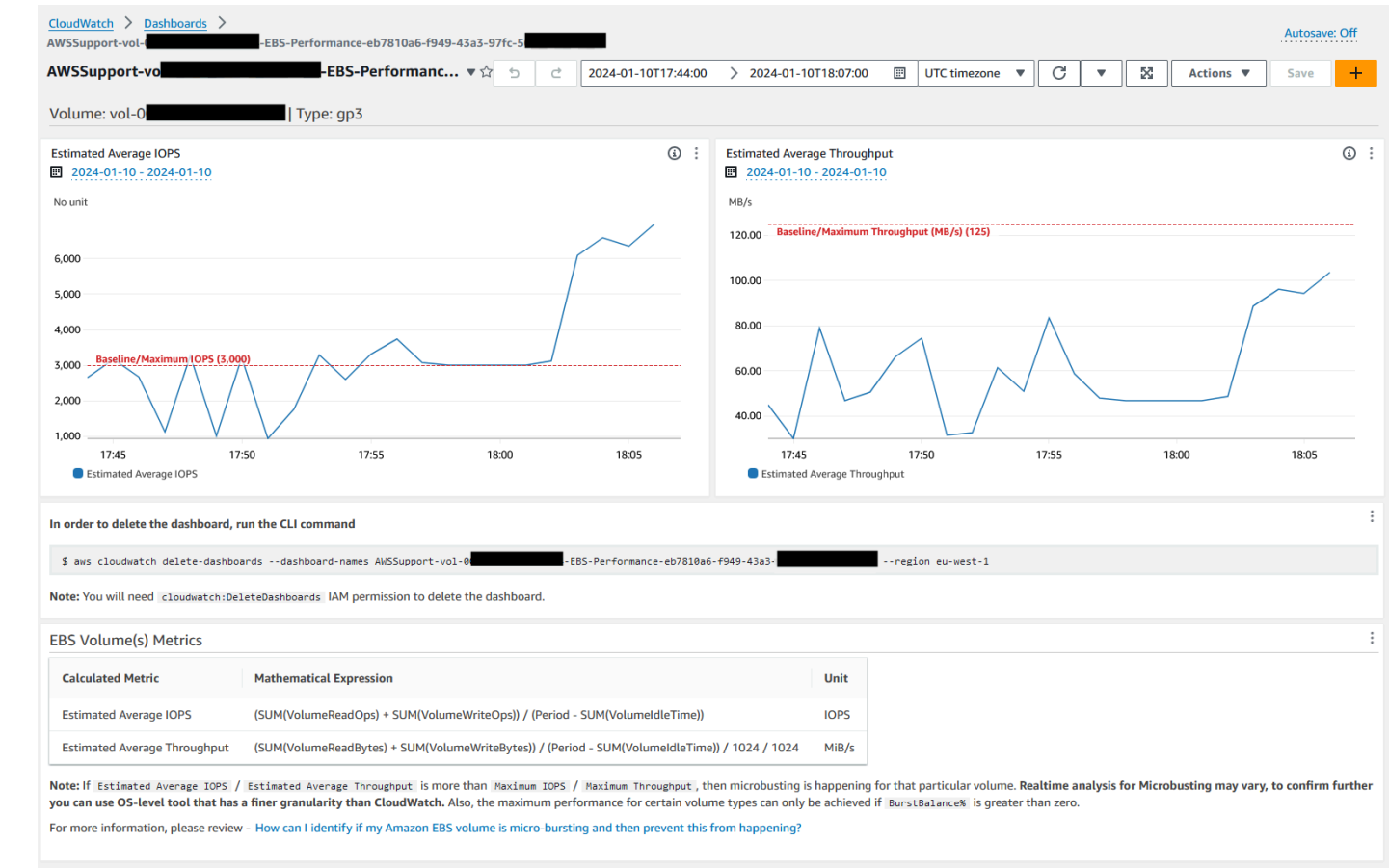
7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución:



Ejemplo de CloudWatch panel para el ID de recurso como instancia de Amazon EC2



Ejemplo de CloudWatch panel para el identificador de recurso como identificador de volumen de Amazon EBS



Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS documentación de servicio

- [¿Cómo puedo identificar si mi volumen de Amazon EBS tiene una microráfaga y evitar que esto suceda?](#)

- [¿Cómo puedo CloudWatch ver las métricas de rendimiento agregadas de Amazon EBS para una instancia EC2?](#)

AWS-CopySnapshot

Descripción

Copia una point-in-time instantánea de un volumen de Amazon Elastic Block Store (Amazon EBS). Puede copiar la instantánea dentro de la misma región Región de AWS o de una región a otra. Las copias de instantáneas de EBS cifradas permanecen cifradas. Las copias de instantáneas sin cifrar permanecen sin cifrar. Para copiar una instantánea cifrada que se compartió desde otra cuenta, debe tener permisos para la clave maestra del cliente (CMK) de KMS utilizada para cifrar la instantánea. Las instantáneas creadas mediante la copia de otra instantánea tienen un ID de volumen arbitrario que no debe utilizarse para ningún fin.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Description (Descripción)

Tipo: cadena

Descripción: (opcional) una descripción para la instantánea de Amazon EBS.

- SnapshotId

Tipo: cadena

Descripción: (obligatorio) ID de la instantánea de Amazon EBS que copiar.

- SourceRegion

Tipo: cadena

Descripción: (obligatorio) la región en la que se encuentra actualmente la instantánea de origen.

Pasos de documentos

copySnapshot: copia una instantánea de un volumen de Amazon EBS.

Salidas

CopySnapshot. SnapshotId - El ID de la nueva instantánea.

AWS-CreateSnapshot

Descripción

Cree una instantánea de un volumen de Amazon EBS.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Description (Descripción)

Tipo: cadena

Descripción: (opcional) una descripción de la instantánea.

- Volumeld

Tipo: cadena

Descripción: (obligatorio) ID del volumen.

AWS-DeleteSnapshot

Descripción

Elimina una instantánea de volumen de Amazon EBS.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- SnapshotId

Tipo: cadena

Descripción: (obligatorio) ID de la instantánea de EBS.

AWSConfigRemediation-DeleteUnusedEBSVolume

Descripción

El manual de procedimientos AWSConfigRemediation-DeleteUnusedEBSVolume elimina un volumen de Amazon Elastic Block Store (Amazon EBS) no utilizado.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- CreateSnapshot

Tipo: Booleano

Descripción: (opcional) si se establece en `true`, la automatización crea una instantánea del volumen de Amazon EBS antes de eliminarlo.

- VolumeId

Tipo: cadena

Descripción: (obligatorio) el ID del volumen de Amazon EBS que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`: verifica que el volumen de Amazon EBS que especifique en el parámetro `VolumeId` no esté en uso y crea una instantánea en función del valor que elija para el parámetro `CreateSnapshot`.
- `aws:branch`: se ramifica en función del valor que haya elegido para el parámetro `CreateSnapshot`.

- `aws:waitForAwsResourceProperty`: espera a que se complete la instantánea.
- `aws:executeAwsApi`: elimina la instantánea si la creación de la instantánea ha fallado.
- `aws:executeAwsApi`: elimina el volumen de Amazon EBS que especifique en el parámetro `VolumeId`.
- `aws:executeScript`: verifica que se haya eliminado el volumen de Amazon EBS.

AWS-DeregisterAMIs

Descripción

El manual de procedimientos AWS-DeregisterAMIs le ayuda a anular el registro Amazon Machine Images (AMIs) especificando la etiqueta que ha aplicado a su AMIs.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `DryRun`

Tipo: cadena

Valores válidos: Yes | No

Descripción: (obligatorio) comprueba si tiene los permisos necesarios para la acción, sin realizar realmente la solicitud, y proporciona una respuesta de error.

- RetainNumber

Tipo: cadena

Descripción: (opcional) el número de AMIs que desea retener. No especifique un valor para este parámetro si especifica un valor para Age.

- Antigüedad

Tipo: cadena

Descripción: (opcional) El número de días anteriores de AMIs que desea retener. No especifique un valor para este parámetro si especifica un valor para RetainNumber.

- TagKey

Tipo: cadena

Descripción: (obligatorio) la clave de la etiqueta asignada a la AMIs cuyo registro desea anular.

- TagValue

Tipo: cadena

Descripción: (obligatorio) el valor de la etiqueta asignada a la AMIs cuyo registro desea anular.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`: valida los valores que especifique para los parámetros de entrada del manual de procedimientos.
- `aws:executeAwsApi`: anula el registro AMIs con la etiqueta que especifique con los parámetros `TagKey` y `TagValue`.

AWS-DetachEBSVolume

Descripción

Separa un volumen de Amazon EBS de una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `LambdaAssumeRole`

Tipo: cadena

Descripción: (opcional) el ARN del rol asumido por Lambda.

- Volumeld

Tipo: cadena

Descripción: (obligatorio) ID del volumen de EBS. El volumen y la instancia deben estar dentro de la misma zona de disponibilidad.

AWSConfigRemediation-EnableEbsEncryptionByDefault

Descripción

El AWSConfigRemediation-EnableEbsEncryptionByDefault manual permite el cifrado de todos los volúmenes nuevos de Amazon Elastic Block Store (Amazon EBS) que se encuentren en el Región de AWS lugar donde se ejecute la Cuenta de AWS automatización. Los volúmenes que se crearon antes de ejecutar la automatización no están cifrados.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeAwsApi`: habilita la configuración de cifrado predeterminada de Amazon EBS en la cuenta y la región actual.
- `aws:assertAwsResourceProperty`: verifica que la configuración de cifrado predeterminada de Amazon EBS esté habilitada.

AWS-ExtendEbsVolume

Descripción

El manual de procedimientos `AWS-ExtendEbsVolume` aumenta el tamaño de un volumen de Amazon EBS y amplía el sistema de archivos. Esta automatización es compatible con los sistemas de archivos `xfs` y `ext4`.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DriveLetter

Tipo: cadena

Descripción: (opcional) la letra de la unidad cuyo sistema de archivos desea ampliar. Este parámetro es obligatorio para las instancias de Windows.

- InstanceId

Tipo: cadena

Descripción: (opcional) el ID de la instancia de Amazon EC2 a la que se adjunta el volumen de Amazon EBS que desea ampliar.

- KeepSnapshot

Tipo: Booleano

Predeterminado: true

Descripción: (opcional) determina si se debe conservar la instantánea creada antes de aumentar el tamaño del volumen de su Amazon EBS.

- MountPoint

Tipo: cadena

Descripción: (opcional) el punto de montaje de la unidad cuyo sistema de archivos desea ampliar. Este parámetro es obligatorio para las instancias de Linux.

- SizeGib

Tipo: cadena

Descripción: (obligatorio) el tamaño en GiB al que desea modificar su volumen de Amazon EBS.

- VolumeId

Tipo: cadena

Descripción: (obligatorio) el ID del volumen de EBS que desea ampliar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`: aumenta el tamaño del volumen hasta el valor que especifique en el parámetro `VolumeId` y amplía el sistema de archivos.

AWSSupport-ModifyEBSSnapshotPermission

Descripción

El manual de procedimientos `AWSSupport-ModifyEBSSnapshotPermission` le ayuda a modificar los permisos de varias instantáneas de Amazon Elastic Block Store (Amazon EBS). Con este manual de procedimientos, puede crear instantáneas `Public` o `Private` y compartirlas con otras Cuentas de AWS. Las instantáneas cifradas con una clave de KMS predeterminada no se pueden compartir con otras cuentas que utilicen este manual de procedimientos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AccountIds

Tipo: StringList

Predeterminado: none

Descripción: (opcional) La cuenta con IDs la que desea compartir las instantáneas. Este parámetro es obligatorio si especifica un valor No para el parámetro Private.

- AccountPermissionOperation

Tipo: cadena

Valores válidos: add | remove

Predeterminado: none

Descripción: (opcional) el tipo de operación que se va a realizar.

- Private

Tipo: cadena

Valores válidos: Yes | No

Descripción: (obligatorio) introduzca No para el valor si desea compartir instantáneas con cuentas específicas.

- SnapshotIds

Tipo: StringList

Descripción: (Obligatoria) Las instantáneas IDs de Amazon EBS cuyo permiso desee modificar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

1. aws:executeScript- Verifica IDs las instantáneas proporcionadas en el parámetro. SnapshotIds Tras verificarlas IDs, el script comprueba si hay instantáneas cifradas y genera una lista si encuentra alguna.
2. aws:branch: ramifica la automatización en función del valor que introduzca para el parámetro Private.
3. aws:executeScript: modifica los permisos de las instantáneas especificadas para compartirlas con las cuentas especificadas.
4. aws:executeScript: modifica los permisos de las instantáneas para cambiarlos de Public a Private.

Salidas

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Resultado

MakePrivate.Resultado

MakePrivate.Comandos

AWSConfigRemediation-ModifyEBSVolumeType

Descripción

El manual de procedimientos AWSConfigRemediation-ModifyEBSVolumeType modifica el tipo de volumen de un volumen de Amazon Elastic Block Store (Amazon EBS). Una vez modificado el tipo de volumen, el volumen entra en un estado optimizing. Para obtener información sobre la supervisión del progreso de las modificaciones de volumen, consulte [Supervisar el progreso de las modificaciones de volumen](#) en la Guía del usuario de Amazon EC2.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- EbsVolumeld

Tipo: cadena

Descripción: (obligatorio) el ID del volumen de Amazon EBS que desea modificar.

- EbsVolumeType

Tipo: cadena

Valores válidos: standard | io1 | io2 | gp2 | gp3 | sc1 | st1

Descripción: El tipo de volumen al que desea cambiar el volumen de Amazon EBS. Para obtener información sobre los tipos de volúmenes de Amazon EBS, consulte los tipos de [volúmenes de Amazon EBS](#) en la Guía del usuario de Amazon EC2.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- aws:waitForAwsResourceProperty: verifica que el estado del volumen es available o in-use.
- aws:executeAwsApi: modifica el volumen de Amazon EBS que especifique en el parámetro EbsVolumeId.
- aws:waitForAwsResourceProperty: verifica que el tipo de volumen se ha cambiado al valor que especificó en el parámetro EbsVolumeType.

Amazon EC2

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic Compute Cloud. Los manuales de Amazon Elastic Block Store se encuentran en la [Amazon EBS](#) sección de referencia del manual. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-ASGEnterStandby](#)
- [AWS-ASGExitStandby](#)
- [AWS-CreatImage](#)
- [AWS-DeletImage](#)
- [AWS-PatchAsgInstance](#)
- [AWS-PatchInstanceWithRollback](#)
- [AWS-QuarantineEC2Instance](#)
- [AWS-ResizeInstance](#)
- [AWS-RestartEC2Instance](#)
- [AWS-SetupJupyter](#)
- [AWS-StartEC2Instance](#)
- [AWS-StopEC2Instance](#)
- [AWS-TerminateEC2Instance](#)
- [AWS-UpdateLinuxAmi](#)
- [AWS-UpdateWindowsAmi](#)
- [AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck](#)
- [AWSConfigRemediation-EnforceEC2InstanceIMDSv2](#)
- [AWSEC2-CloneInstanceAndUpgradeSQLServer](#)
- [AWSEC2-CloneInstanceAndUpgradeWindows](#)
- [AWSEC2-PatchLoadBalancerInstance](#)
- [AWSEC2-SQLServerDBRestore](#)
- [AWSSupport-ActivateWindowsWithAmazonLicense](#)
- [AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2](#)
- [AWSPremiumSupport-ChangeInstanceTypeIntelToAMD](#)
- [AWSSupport-CheckXenToNitroMigrationRequirements](#)
- [AWSSupport-CloneXenEC2InstanceAndMigrateToNitro](#)
- [AWSSupport-CollectSAPHANALogs](#)
- [AWSSupport-ConfigureEC2Metadata](#)

- [AWSSupport-ContainEC2Instance](#)
- [AWSSupport-CopyEC2Instance](#)
- [AWSPremiumSupport-DiagnoseDiskUsageOnLinux](#)
- [AWSSupport-EnableWindowsEC2SerialConsole](#)
- [AWSPremiumSupport-ExtendVolumesOnWindows](#)
- [AWSSupport-ExecuteEC2Rescue](#)
- [AWSSupport-ListEC2Resources](#)
- [AWSSupport-ManageRDPSettings](#)
- [AWSSupport-ManageWindowsService](#)
- [AWSSupport-MigrateEC2ClassicToVPC](#)
- [AWSSupport-MigrateXenToNitroLinux](#)
- [AWSSupport-ResetAccess](#)
- [AWSSupport-ResetLinuxUserPassword](#)
- [AWSSupport-RunEC2RescueForWindowsTool](#)
- [AWSPremiumSupport-ResizeNitroInstance](#)
- [AWSSupport-ShareEncryptedAMIOrEBSSnapshot](#)
- [AWSSupport-RestoreEC2InstanceFromSnapshot](#)
- [AWSSupport-SendLogBundleToS3Bucket](#)
- [AWSSupport-StartEC2RescueWorkflow](#)
- [AWSSupport-TroubleshootActiveDirectoryReplication](#)
- [AWSPremiumSupport-TroubleshootEC2DiskUsage](#)
- [AWSSupport-TroubleshootEC2InstanceConnect](#)
- [AWSSupport-TroubleshootLinuxMGNDRSAgentLogs](#)
- [AWSSupport-TroubleshootRDP](#)
- [AWSSupport-TroubleshootSSH](#)
- [AWSSupport-TroubleshootSUSERegistration](#)
- [AWSSupport-TroubleshootWindowsPerformance](#)
- [AWSSupport-TroubleshootWindowsUpdate](#)
- [AWSSupport-UpgradeWindowsAWSDrivers](#)

AWS-ASGEnterStandby

Descripción

Cambie el estado de espera de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en un grupo de Auto Scaling.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: ID (obligatorio) de una EC2 instancia de Amazon para la que desea cambiar el estado de espera dentro de un grupo de Auto Scaling.

- LambdaRoleArn

Tipo: cadena

Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

AWS-ASGExitStandby

Descripción

Cambie el estado de espera de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en un grupo de Auto Scaling.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: ID (obligatorio) de una EC2 instancia para la que desea cambiar el estado de espera dentro de un grupo de Auto Scaling.

- LambdaRoleArn

Tipo: cadena

Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

AWS-CreateImage

Descripción

Lanza una Amazon Machine Image (AMI) nueva de una instancia Amazon Elastic Compute Cloud (Amazon EC2).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia EC2.

- NoReboot

Tipo: Booleano

Descripción: (opcional) no reinicie la instancia antes de crear la imagen.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

JSON

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

AWS-DeleteImage

Descripción

Elimine una Amazon Machine Image (AMI) y todas las instantáneas asociadas.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ImageId

Tipo: cadena

Descripción: (obligatorio) ID de la AMI.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

JSON

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

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

AWS-PatchAsgInstance

Descripción

Parchee instancias de Amazon Elastic Compute Cloud (Amazon EC2) en un grupo de escalado automático.

[Ejecuta esta automatización \(consola\)](#)

Important

Este runbook aplica una AutoPatchInstanceInASG etiqueta a la instancia de destino durante la ejecución. Esta etiqueta impide que el runbook se ejecute dos veces en la misma instancia simultáneamente; no es un indicador del cumplimiento de los parches. Si se produce un error en el paso de aplicación de parches, es posible que el valor de la etiqueta siga siendo el mismo Completed aunque se muestre el estado de ejecución del runbook.

Failed

Para verificar el cumplimiento del parche en la instancia, usa [DescribeInstancePatchStates](#) o [ListComplianceItems](#) en su lugar.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia que parchear. No especifique un ID de instancia que esté configurado para ejecutarse durante un período de mantenimiento.

- LambdaRoleArn

Tipo: cadena

Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función de Lambda.

- WaitForInstance

Tipo: cadena

Predeterminado: PT2 M

Descripción: (opcional) la duración que Automatización debería suspenderse para permitir a la instancia regresar al servicio.

- WaitForReboot

Tipo: cadena

Predeterminado: PT5 M

Descripción: (opcional) la duración que Automatización debería suspenderse para permitir el reinicio de una instancia parcheada.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Descripción

Hace que una EC2 instancia cumpla con la línea base del parche aplicable. Revierte el volumen raíz en caso de fallo.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `InstanceId`

Tipo: cadena

Descripción: (Obligatoria) EC2 InstanceId a la que aplicamos la línea base del parche.

- `LambdaAssumeRole`

Tipo: cadena

Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- ReportS3Bucket

Tipo: cadena

Descripción: (opcional) destino del bucket de Amazon S3 Bucket para el informe de conformidad generado durante el proceso.

Pasos de documentos

Número de paso	Nombre del paso	Acción de 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

Número de paso	Nombre del paso	Acción de Automation
10	DeleteSnapshot	aws:invokeLambdaFunction
11	deleteCloudFormationPlantilla	aws:deleteStack

Salidas

IdentifyRootVolume.Carga útil

PrePatchSnapshot.Salida

SaveComplianceReportToS3. Carga útil

RestoreFromSnapshot4. Carga útil

CheckCompliance.Carga útil

AWS-QuarantineEC2Instance

Descripción

Con el AWS-QuarantineEC2Instance runbook, puede asignar un grupo de seguridad a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que no permita ningún tráfico entrante o saliente.

Important

Los cambios en la configuración de RDP deben revisarse detenidamente antes de ejecutar este manual de procedimientos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia administrada para administrar la configuración de RDP.

- IsolationSecurityGroup

Tipo: cadena

Descripción: (obligatorio) el nombre del grupo de seguridad que desea asignar a la instancia para evitar el tráfico entrante o saliente.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

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

Pasos de documentos

- `aws:executeAwsApi`: recopila detalles sobre la instancia.
- `aws:executeScript`: verifica que la instancia no forma parte de un grupo de escalado automático.
- `aws:executeAwsApi`: crea una instantánea del volumen raíz adjunta a la instancia.
- `aws:waitForAwsResourceProperty`: espera a que el estado de la instantánea sea `completed`.
- `aws:executeAwsApi`: asigna el grupo de seguridad especificado en el parámetro `IsolationSecurityGroup` a su instancia.

Salidas

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

AWS-ResizeInstance

Descripción

Cambie el tipo de instancia de una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia.

- InstanceType

Tipo: cadena

Descripción: (obligatorio) tipo de instancia.

AWS-RestartEC2Instance

Descripción

Reinicie una o más instancias de Amazon Elastic Compute Cloud (Amazon EC2).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceIds

Tipo: StringList

Descripción: (Obligatoria) La IDs de las EC2 instancias de Amazon que se van a reiniciar.

AWS-SetupJupyter

Descripción

El AWS-SetupJupyter manual le ayuda a configurar Jupyter Notebook en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Puede especificar una instancia existente o proporcionar una Amazon Machine Image (AMI) ID de la automatización para lanzar y configurar una nueva instancia. Antes de comenzar, debe crear un parámetro SecureString en Parameter Store para usarlo como contraseña del cuaderno de Jupyter. Parameter Store es una herramienta en AWS Systems Manager. Para obtener más información acerca de la creación de parámetros, consulte [Creación de parámetros](#) en el Guía del usuario de AWS Systems Manager .

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Amild

Tipo: cadena

Descripción: (opcional) El identificador del AMI que desea usar para lanzar una nueva instancia y configurar Jupyter Notebook.

- Instanceld

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia en la que desea configurar el cuaderno de Jupyter.

- InstanceType

Tipo: cadena

Valor predeterminado: t3.medium

Descripción: (opcional) si va a lanzar una nueva instancia para configurar el cuaderno de Jupyter, especifique el tipo de instancia que desea usar.

- JupyterPasswordSSMKey

Tipo: cadena

Descripción: (obligatorio) el nombre del parámetro SecureString en Parameter Store que desea utilizar como contraseña para el cuaderno de Jupyter.

- KeyPairName

Tipo: cadena

Descripción: (opcional) el par de claves que desea asociar con la instancia recién lanzada.

- RemoteAccessCidr

Tipo: cadena

Valor predeterminado: 0.0.0.0/0

Descripción: (opcional) el rango de CIDR desde el que desea permitir el tráfico SSH.

- RoleName

Tipo: cadena

Predeterminado: SSMManged InstanceProfileRole

Descripción: (opcional) el nombre del perfil de instancia de la instancia recién lanzada.

- StackName

Tipo: cadena

Predeterminado: CreateManagedInstanceStack {{Automation:EXECUTION_ID}}

Descripción: (opcional) El nombre de la CloudFormation pila que quieres que utilice la automatización.

- SubnetId

Tipo: cadena

Valor predeterminado: Default

Descripción: (opcional) la subred en la que desea lanzar la instancia nueva para usarla.

- VpcId

Tipo: cadena

Valor predeterminado: Default

Descripción: (opcional) el ID de la nube privada virtual (VPC) en la que desea lanzar la instancia nueva.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeScript`: configura el cuaderno de Jupyter en la instancia que especifique, o en una instancia recién lanzada, utilizando los valores que especifique para los parámetros de entrada del manual de procedimientos.

AWS-StartEC2Instance

Descripción

Inicie una o más instancias de Amazon Elastic Compute Cloud (Amazon EC2).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `InstanceId`

Tipo: `StringList`

Descripción: EC2 instancias (obligatorias) para iniciar.

AWS-StopEC2Instance

Descripción

Detiene una o más instancias de Amazon Elastic Compute Cloud (Amazon EC2).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceIds

Tipo: StringList

Descripción: EC2 Instancias (obligatorias) para detener.

AWS-TerminateEC2Instance

Descripción

Finalice una o más instancias de Amazon Elastic Compute Cloud (Amazon EC2).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceIds

Tipo: StringList

Descripción: (Obligatoria) IDs de una o más EC2 instancias para terminar.

AWS-UpdateLinuxAmi

Descripción

Actualice un Amazon Machine Image (AMI) con los paquetes de distribución de Linux y el software de Amazon.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

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

- Debe ser un ARN de rol de IAM válido o una cadena vacía. La variable de sistema se `{global:ACCOUNT_ID}` puede utilizar en lugar del identificador de AWS cuenta en el arn.
- ExcludePackages

Tipo: cadena

Predeterminado: none

Descripción: (opcional) nombres de los paquetes a los que no se aplicarán las actualizaciones, en todas las condiciones. De forma predeterminada ("none"), no se excluye ningún paquete.

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

- Debe ser «ninguno» O debe ser una lista de elementos separados por comas compuesta por letras, números, espacios y los siguientes caracteres: `, . _ + : = < > ( ) [ ] / * -`
- IamInstanceProfileName

Tipo: cadena

Predeterminado: ManagedInstanceProfile

Descripción: (obligatorio) perfil de instancia que permite a Systems Manager administrar la instancia.

Valor permitido: `^[\w+=,.\@-]{1,128}$`

- Debe tener entre 1 y 128 caracteres y contener solo letras, números y los siguientes caracteres:
+ = , . @ - _

- IncludePackages

Tipo: cadena

Valor predeterminado: all

Descripción: (opcional) actualizar solo estos paquetes designados. De forma predeterminada ("all"), se aplican todas las actualizaciones disponibles.

Valor permitido: `^(all|[a-zA-Z0-9\s,._+:=<>()\[\]/*-]+)$`

- Debe ser «todos» O debe ser una lista de elementos separados por comas compuesta por letras, números, espacios y los siguientes caracteres: , . _ + : = < > () [] / * -

- InstanceType

Tipo: cadena

Valor predeterminado: t2.micro

Descripción: (opcional) tipo de instancia que se lanzará como el host de espacio de trabajo. Los tipos de instancia varían según la región.

Valor permitido: `^[a-z0-9]+(-[a-z0-9]+)*\.[a-z0-9]+$`

- Debe tener el formato prefix.suffix, donde ambas partes contienen letras minúsculas y números y el prefijo puede incluir guiones

- MetadataOptions

Tipo: StringMap

Predeterminado: {» HttpEndpoint «: «activado», "«: «opcional"} HttpTokens

Descripción: (opcional) las opciones de metadatos de la instancia. Para obtener más información, consulte [InstanceMetadataOptionsRequest](#).

Valor permitido: `^\{[^<>\$;|&\\]*\}$`

- Debe estar envuelta entre corchetes {} y no puede contener los siguientes caracteres: < > \$; | & \

- PostUpdateScript

Tipo: cadena

Predeterminado: none

Descripción: (opcional) URL de un script que se ejecutará después de que se apliquen las actualizaciones de paquete. El valor predeterminado (“none”) es no ejecutar un script.

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

- Debe ser «ninguno» O una URL válida HTTP/HTTPS

- PreUpdateScript

Tipo: cadena

Predeterminado: none

Descripción: (opcional) URL de un script que se ejecutará antes de que se apliquen las actualizaciones. El valor predeterminado (“none”) es no ejecutar un script.

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

- Debe ser «ninguno» O una HTTP/HTTPS URL válida

- SecurityGroupIds

Tipo: cadena

Descripción: (Obligatorio) Lista separada por comas IDs de los grupos de seguridad que desea aplicar alAMI.

Valor permitido: `^sg-[a-z0-9]{8,17}$`

- Debe empezar con «sg-» seguido de 8 a 17 letras minúsculas o números

- SourceAmild

Tipo: cadena

Descripción: (obligatorio) ID de la imagen de máquina de Amazon de origen.

Valor permitido: `^ami-[a-z0-9]{8,17}$`

- Debe empezar con «ami-» seguido de 8 a 17 letras minúsculas o números
- SubnetId

Tipo: cadena

Descripción: (opcional) el ID de la subred en la que quiere lanzar la instancia. Si ha eliminado la VPC predeterminada, se necesita este parámetro.

Valor permitido: `^$|^subnet-[a-z0-9]{8,17}$`

- Debe estar vacío O empezar por «subnet-» seguido de 8 a 17 letras minúsculas o números
- TargetAmiName

Tipo: cadena

Predeterminado: `UpdateLinuxAmi_from_{{}}_on_{{SourceAmiIdglobal:date_time}}`

Descripción: (opcional) nombre de la nueva AMI que se va a crear. El valor predeterminado es una cadena generada por el sistema que incluye el ID de la AMI de origen, así como la hora y la fecha de creación.

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

- Debe tener entre 3 y 128 caracteres y contener solo letras, números, espacios y los siguientes caracteres: () [] { } . / ' @ _ : -

AWS-UpdateWindowsAmi

Descripción

Actualice una Amazon Machine Image (AMI) de Microsoft Windows. De forma predeterminada, este manual de procedimientos instala todas las actualizaciones de Windows, el software de Amazon y los controladores de Amazon. A continuación, ejecuta Sysprep para crear una nueva AMI. Soporta desde Windows Server 2008 R2 hasta Windows Server 2022.

⚠ Important

Este manual no es compatible con Windows Server 2025 y versiones posteriores, ya que los controladores AWS Paravirtual no son compatibles con estas versiones. Para obtener más información, consulte [Controladores paravirtuales para](#) instancias de Windows.

⚠ Important

Si tus instancias se conectan AWS Systems Manager mediante puntos de enlace de VPC, este manual fallará a menos que se utilice en la región us-east-1. Las instancias deben tener habilitado TLS 1.2 para usar este manual de procedimientos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Categorías

Tipo: cadena

Descripción: (opcional) especificar una o más categorías de actualización. Puede filtrar las categorías usando valores separados por comas. Opciones: Aplicación, conectores, CriticalUpdates, DefinitionUpdates DeveloperKits, ControladoresFeaturePacks, Guía, Microsoft SecurityUpdates, ServicePacks, HerramientasUpdateRollups, Actualizaciones. Los formatos válidos incluyen una sola entrada, por ejemplo:CriticalUpdates. O puede especificar una lista separada por comas:CriticalUpdates,SecurityUpdates. NOTA: No puede haber ningún espacio ni antes ni después de las comas.

- ExcludeKbs

Tipo: cadena

Descripción: (opcional) Especifique uno o más artículos de Microsoft Knowledge Base (KB) IDs para excluirlos. Puede excluir varios IDs mediante valores separados por comas. Formatos válidos: KB9876543 o 9876543.

- IamInstanceProfileName

Tipo: cadena

Predeterminado: ManagedInstanceProfile

Descripción: (obligatorio) nombre del rol que permite a Systems Manager administrar la instancia.

- IncludeKbs

Tipo: cadena

Descripción: (opcional) Especifique uno o más artículos de Microsoft Knowledge Base (KB) IDs para incluirlos. Puede instalar varios IDs mediante valores separados por comas. Formatos válidos: KB9876543 o 9876543.

- InstanceType

Tipo: cadena

Valor predeterminado: t2.medium

Descripción: (opcional) tipo de instancia que se lanzará como el host de espacio de trabajo. Los tipos de instancia varían según la región. El valor predeterminado es t2.medium.

- MetadataOptions

Tipo: StringMap

Predeterminado: {» HttpEndpoint «: «activado», "HttpTokens«: «opcional"}

Descripción: (opcional) las opciones de metadatos de la instancia. Para obtener más información, consulte [InstanceMetadataOptionsRequest](#).

- PostUpdateScript

Tipo: cadena

Descripción: (opcional) script proporcionado como una cadena. Se ejecutará después de instalar las actualizaciones del SO.

- PreUpdateScript

Tipo: cadena

Descripción: (opcional) script proporcionado como una cadena. Se ejecutará antes de instalar las actualizaciones del SO.

- PublishedDateAfter

Tipo: cadena

Descripción: (opcional) especificar la fecha después de la cual deben haberse publicado las actualizaciones. Por ejemplo, si se especifica 01/01/2017, devolverá las actualizaciones que se encontraron durante la búsqueda de Windows Update y que se publicaron a partir del 01/01/2017.

- PublishedDateBefore

Tipo: cadena

Descripción: (opcional) especificar la fecha antes de la cual deben haberse publicado las actualizaciones. Por ejemplo, si se especifica 01/01/2017, devolverá las actualizaciones que se encontraron durante la búsqueda de Windows Update y que se publicaron antes del 01/01/2017.

- PublishedDaysOld

Tipo: cadena

Descripción: (opcional) especificar el número de días de antigüedad que tienen que tener las actualizaciones desde la fecha de publicación. Por ejemplo, si se especifica 10, devolverá todas

las actualizaciones que se encuentren durante la búsqueda de Windows Update y que se hayan publicado hace 10 o más días.

- **SecurityGroupIds**

Tipo: cadena

Descripción: (Obligatorio) Lista separada por comas IDs de los grupos de seguridad que desea aplicar a losAMI.

- **SeverityLevels**

Tipo: cadena

Descripción: (opcional) especificar uno o varios niveles de gravedad de MSRC asociados con una actualización. Puede filtrar los niveles de gravedad usando valores separados por comas. De forma predeterminada, se seleccionan parches para todos los niveles de seguridad. Si se suministra un valor, la lista de actualizaciones se filtrará por dichos valores. Opciones: Critical, Important, Low, Moderate o Unspecified. Los formatos válidos incluyen una sola entrada, por ejemplo: Critical. O bien, puede especificar una lista separada por comas: Critical,Important,Low.

- **SourceAmild**

Tipo: cadena

Descripción: (obligatorio) El AMI ID de la fuente.

- **SubnetId**

Tipo: cadena

Descripción: (opcional) el ID de la subred en la que quiere lanzar la instancia. Si ha eliminado la VPC predeterminada, se necesita este parámetro.

- **TargetAmiName**

Tipo: cadena

Predeterminado: UpdateWindowsAmi _from_ {{SourceAmild}} _on_ {{global:date_time}}

Descripción: (opcional) nombre de la nueva AMI que se va a crear. El valor predeterminado es una cadena generada por el sistema que incluye el ID de la AMI de origen, así como la hora y la fecha de creación.

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

Descripción

El AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck manual permite realizar comprobaciones de estado para el grupo de Amazon EC2 Auto Scaling (Auto Scaling) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- AutoScalingGroupARN

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del grupo de escalado automático en el que desea habilitar las comprobaciones de estado.

- HealthCheckGracePeriod

Tipo: entero

Predeterminado: 300

Descripción: (opcional) La cantidad de tiempo, en segundos, que Auto Scaling espera antes de comprobar el estado de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que ha entrado en servicio.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`: activa las comprobaciones de estado en el grupo de escalado automático que especifique en el parámetro `AutoScalingGroupARN`.

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

Descripción

El `AWSConfigRemediation-EnforceEC2InstanceIMDSv2` manual requiere la instancia de Amazon Elastic Compute Cloud (Amazon EC2) que especifique para usar Instance Metadata Service versión 2 (IMDSv2).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `InstanceId`

Tipo: cadena

Descripción: (Obligatorio) El ID de la EC2 instancia de Amazon que quieres usar IMDSv2.

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `HttpPutResponseHopLimit`

Tipo: entero

Descripción: (opcional) El límite de respuesta del servicio IMDS de vuelta al solicitante.

Establézcalo en 2 o más para las EC2 instancias que alojan contenedores. Establézcalo en 0 para no cambiarlo (predeterminado).

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

Predeterminado: 0

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Establece la `HttpTokens` opción `required` en la EC2 instancia de Amazon que especifique en el `InstanceId` parámetro.
- `aws:assertAwsResourceProperty`- Verifica `IMDSv2` es obligatorio en la EC2 instancia de Amazon.

AWSEC2-CloneInstanceAndUpgradeSQLServer

Descripción

Cree un AMI a partir de una EC2 instancia para Windows Server ejecutar SQL Server 2008 o una versión posterior y, a continuación, actualizar la AMI a una versión posterior de SQL Server. Solo se admiten las versiones en inglés de SQL Server.

Las rutas de actualización admitidas son las siguientes:

- SQL Server 2008 a SQL Server 2017, 2016 o 2014
- SQL Server 2008 R2 a SQL Server 2017, 2016 o 2014
- SQL Server 2012 a SQL Server 2019, 2017, 2016 o 2014
- SQL Server 2014 a SQL Server 2019, 2017 o 2016
- SQL Server 2016 a SQL Server 2019 o 2017

Si utiliza una versión anterior de Windows Server que no es compatible con SQL Server 2019, el documento de automatización debe actualizar su versión de Windows Server a 2016.

La actualización es un proceso de múltiples pasos que puede tardar 2 horas en completarse. La automatización crea la AMI a partir de la instancia y, a continuación, lanza una instancia temporal desde la nueva AMI en el especificado `SubnetID`. Los grupos de seguridad asociados a la instancia original se aplican a la instancia temporal. A continuación, la automatización realiza una actualización in situ a la `TargetSQLVersion` en la instancia temporal. Tras la actualización, la automatización crea una nueva AMI desde la instancia temporal y, a continuación, termina la instancia temporal.

Puede probar la funcionalidad de la aplicación lanzando la nueva AMI en tu VPC. Una vez que haya terminado las pruebas y antes de realizar otra actualización, programe el tiempo de inactividad de las aplicaciones antes de cambiar completamente a la instancia actualizada.

 Note

Si desea modificar el nombre de la computadora de la EC2 instancia lanzada desde la nueva AMI , consulte [Cambiar el nombre de un equipo que aloja una instancia independiente de SQL Server](#).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

Requisitos previos

- TLS versión 1.2.
- Solo se admiten las versiones en inglés de SQL Server.
- La EC2 instancia debe usar una versión de Windows Server es decir Windows Server 2008 R2 (o posterior) y SQL Server 2008 (o posterior).
- Compruebe que SSM Agent esté instalado en su instancia. Para obtener más información, consulte [Instalación y configuración del agente SSM en EC2 instancias de Windows Server](#).
- Configure la instancia para que utilice un rol de perfil de instancia AWS Identity and Access Management (IAM). Para obtener más información, consulte [Crear un perfil de instancias de IAM para Systems Manager](#).
- Verifique que la instancia tiene 20 GB de espacio libre en el disco de arranque de la instancia.
- Para las instancias que utilizan una versión Bring Your Own License (BYOL) de SQL Server, se aplican los siguientes requisitos previos adicionales:
 - Proporcione un ID de instantánea de EBS que incluya medios de instalación de destino de SQL Server. Para ello:

1. Compruebe que la EC2 instancia ejecute Windows Server 2008 R2 o una versión posterior.
2. Cree un volumen de EBS de 6 GB en la misma zona de disponibilidad en la que se ejecuta la instancia. Adjunte el volumen a la instancia. Móntelo, por ejemplo, como unidad D.
3. Haga clic con el botón derecho del ratón en la ISO y móntela en una instancia como, por ejemplo, la unidad E.
4. Copie el contenido de la ISO desde la unidad E:\ a la unidad D:\
5. Cree una instantánea de EBS del volumen de 6 GB creado en el paso 2.

Limitaciones

- La actualización solo se puede realizar en un SQL Server mediante la autenticación de Windows.
- Verifique que no exista ninguna actualización de parches de seguridad pendiente en las instancias. Abra Control Panel (Panel de control) y elija Check for updates (Buscar actualizaciones).
- No se admiten las implementaciones de SQL Server en HA y el modo de duplicación.

Parámetros

- `IamInstanceProfile`

Tipo: cadena

Descripción: (obligatorio) el perfil de instancia de IAM.

- `InstanceId`

Tipo: cadena

Descripción: (Obligatorio) La instancia en ejecución Windows Server 2008 R2 (o posterior) y SQL Server 2008 (o posterior).

- `KeepPreUpgradeImageBackUp`

Tipo: cadena

Descripción: (opcional) si se establece en `true`, la automatización no elimina la AMI creada a partir de la instancia antes de la actualización. Si se establece en `true`, debe eliminar la AMI. De forma predeterminada, se elimina la AMI.

- `SubnetId`

Tipo: cadena

Descripción: (obligatorio) proporcionar una subred para el proceso de actualización. Compruebe que la subred tenga conectividad saliente con los AWS servicios, Amazon S3 y Microsoft (para descargar los parches).

- SQLServerSnapshotId

Tipo: cadena

Descripción: (condicional) ID de instantánea para los medios de instalación de SQL Server. Este parámetro es necesario para las instancias que utilizan una versión BYOL de SQL Server. Este parámetro es opcional para las instancias con licencia incluida de SQL Server (instancias lanzadas con una imagen de máquina de AWS Amazon para Windows Server proporcionada con Microsoft SQL Server).

- RebootInstanceBeforeTakingImage

Tipo: cadena

Descripción: (opcional) si se establece en `true`, la automatización reinicia la instancia antes de crear una AMI previa a la actualización. De forma predeterminada, la automatización no se reinicia antes de la actualización.

- Destino SQLVersion

Tipo: cadena

Descripción: (opcional) seleccione la versión de SQL Server de destino.

Posibles objetivos:

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

Destino predeterminado: SQL Server 2016

Salidas

AMIId: el ID de la AMI creada a partir de la instancia que se actualizó a una versión posterior de SQL Server.

AWSEC2-CloneInstanceAndUpgradeWindows

Descripción

Cree una Amazon Machine Image (AMI) a partir de una instancia de Windows Server 2008 R2, 2012 R2, 2016, 2019 o 2022 y, a continuación, Windows Server actualícela AMI a 2016, 2019, 2022 o 2025. Las rutas de actualización admitidas son las siguientes.

- Windows Server2008 R2 a Windows Server 2016.
- Windows Server 2012 R2 a Windows Server 2016.
- Windows Server 2012 R2 a Windows Server 2019.
- Windows Server 2012 R2 a Windows Server 2022.
- Windows Server 2016 a Windows Server 2019.
- Windows Server 2016 a Windows Server 2022.
- Windows Server2016 a Windows Server 2025.
- Windows Server2019 a Windows Server 2022.
- Windows Server2019 a Windows Server 2025.
- Windows ServerDe 2022 a Windows Server 2025.

La operación de actualización es un proceso de múltiples pasos que puede tardar 2 horas en completarse. Recomendamos realizar una actualización del sistema operativo en instancias con al menos 2 V CPUs y 4 GB de RAM. La automatización crea una AMI a partir de la instancia y, a continuación, inicia una instancia temporal desde la AMI recién creada en la SubnetId especificada. Los grupos de seguridad asociados a la instancia original se aplican a la instancia temporal. A continuación, la automatización realiza una actualización in situ a la TargetWindowsVersion en la instancia temporal. Para actualizar la instancia de Windows Server 2008 R2 a Windows Server 2016, 2019 o 2022 es necesario realizar una actualización in situ dos veces, ya que no se puede actualizar directamente de Windows Server 2008 R2 a Windows Server 2016, 2019 o 2022. La automatización también actualiza o instala los controladores de AWS que necesita la instancia actualizada. Después de la actualización, la automatización crea una nueva AMI a partir de la instancia temporal y, después, termina la instancia temporal.

Puede probar la funcionalidad de la aplicación iniciando una instancia de prueba desde la AMI actualizada en la Amazon Virtual Private Cloud (Amazon VPC). Una vez que haya terminado las pruebas y antes de realizar otra actualización, programe el tiempo de inactividad de las aplicaciones antes de cambiar completamente a la instancia actualizada.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows ServerEdiciones Standard y Datacenter de 2008, 2012 R2, 2016, 2019 o 2022

Requisitos previos

- TLS versión 1.2.
- Compruebe que SSM Agent esté instalado en su instancia. Para obtener más información, consulte [Instalación y configuración de SSM Agent en instancias de EC2 para Windows Server](#).
- Debe estar instalado Windows PowerShell 3.0 o una versión posterior en la instancia.
- Para las instancias que están unidas a un dominio de Microsoft Active Directory, se recomienda especificar un SubnetId que no tenga conectividad con los controladores de dominio para evitar conflictos con nombres de host.
- La subred de la instancia debe tener conectividad saliente a Internet, lo que proporciona acceso a Servicios de AWS Amazon S3 y acceso a la descarga de parches de Microsoft. Este requisito se cumple si la subred es pública y la instancia tiene una dirección IP pública, o si la subred es una subred privada con una ruta que envía el tráfico de Internet a un dispositivo de NAT público.
- Esta automatización solo funciona con las Windows Server instancias 2008 R2, 2012 R2, 2016, 2019 y 2022.
- Configure la Windows Server instancia con un perfil de instancia AWS Identity and Access Management (IAM) que proporcione los permisos necesarios para Systems Manager. Para obtener más información, consulte [Crear un perfil de instancias de IAM para Systems Manager](#).
- Verifique que la instancia tiene 20 GB de espacio libre en el disco de arranque.

- Si la instancia no usa una licencia AWS de Windows proporcionada, especifique un ID de instantánea de Amazon EBS que incluya los medios de instalación de Windows Server 2012 R2. Para ello:
 - Compruebe que la instancia EC2 ejecuta Windows Server 2012 o una versión posterior.
 - Cree un volumen de EBS de 6 GB en la misma zona de disponibilidad en la que se ejecuta la instancia. Adjunte el volumen a la instancia. Móntelo, por ejemplo, como unidad D.
 - Haga clic con el botón derecho del ratón en la ISO y móntela en una instancia como, por ejemplo, la unidad E.
 - Copie el contenido de la ISO desde la unidad E:\ a la unidad D:\
 - Cree una instantánea de EBS del volumen de 6 GB creado en el paso 2 anterior.
- [Para las actualizaciones de Windows Server 2025, la instancia de origen debe estar basada en Nitro.](#)

Limitaciones

Esta Automatización no admite la actualización de controladores de dominio de Windows, clústeres o sistemas operativos de escritorio de Windows. Esta Automatización tampoco admite instancias EC2 para Windows Server con los siguientes roles instalados.

- Host de sesión de Escritorio remoto (RDSH)
- Agente de conexión a Escritorio remoto (RDCB)
- Host de virtualización de Escritorio remoto (RDVH)
- Acceso web de Escritorio remoto (RDWA)

Parámetros

- `AlternativeKeyPairName`

Tipo: cadena

Descripción: (opcional) el nombre de un par de claves alternativo que se utilizará durante el proceso de actualización. Esto resulta útil en situaciones en las que el key pair asignado a la instancia original no está disponible. Si a la instancia original no se le asignó un key pair, debe especificar un valor para este parámetro.

- `BYOLWindowsMediaSnapshotId`

Tipo: cadena

Descripción: (opcional) el ID de la instantánea de Amazon EBS para copiar lo que incluyen los medios de instalación de Windows Server 2012R2. Solo es necesario si se está actualizando una instancia BYOL.

- `IamInstanceProfile`

Tipo: cadena

Descripción: (obligatorio) el nombre del perfil de instancia de IAM que permite que Systems Manager administre la instancia.

- `InstanceId`

Tipo: cadena

Descripción: (Obligatoria) La instancia EC2 que ejecuta Windows Server 2008 R2, 2012 R2, 2016, 2019 o 2022.

- `KeepPreUpgradeImageBackUp`

Tipo: cadena

Descripción: (opcional) si se establece en True, la Automatización no elimina la AMI creada a partir de la instancia EC2 antes de la actualización. Si se establece en True, debe eliminar la AMI. De forma predeterminada, se elimina la AMI.

- `SubnetId`

Tipo: cadena

Descripción: (obligatorio) esta es la subred para el proceso de actualización y donde reside su instancia EC2 de origen. Compruebe que la subred tenga conectividad saliente con los AWS servicios, Amazon S3 y Microsoft (para descargar los parches).

- `TargetWindowsVersion`

Tipo: cadena

Descripción: (obligatorio) seleccionar la versión de Windows de destino.

Predeterminado: 2025

- `RebootInstanceBeforeTakingImage`

Tipo: cadena

Descripción: (opcional) si se establece en True, la Automatización reinicia la instancia antes de crear una AMI previa a la actualización. De forma predeterminada, la Automation no se reinicia antes de la actualización.

AWSEC2-PatchLoadBalancerInstance

Descripción

Actualice y parchee la versión secundaria de una EC2 instancia de Amazon (Windows o Linux) conectada a cualquier balanceador de carga (clásico, ALB o NLB). El tiempo de drenaje de conexiones predeterminado se aplica antes de parchear la instancia. Puede anular el tiempo de espera introduciendo el tiempo de carga personalizado en minutos (1-59) para el parámetro. ConnectionDrainTime

La automatización es la siguiente:

1. Se determina el equilibrador de carga o el grupo objetivo al que se adjunta la instancia y se verifica que la instancia esté en buen estado.
2. La instancia se elimina del equilibrador de carga o del grupo objetivo.
3. La automatización espera el período de tiempo especificado para el tiempo de drenaje de la conexión.
4. La RunPatchBaseline automatización de [AWS](#) se llama para parchear la instancia.
5. La instancia se vuelve a conectar al equilibrador de carga o al grupo objetivo.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Requisitos previos

- Compruebe que SSM Agent esté instalado en su instancia. Para obtener más información, consulte [Trabajar con el agente SSM en EC2 instancias para Windows Server](#).

Parámetros

- InstanceId

Tipo: cadena

Descripción: ID (obligatorio) de la instancia a la que se va a aplicar el parche y que está asociada a un equilibrador de cargas (clásico, ALB o NLB).

- ConnectionDrainTime

Tipo: cadena

Descripción: (opcional) el tiempo de drenaje de conexiones del equilibrador de carga, en minutos (1-59).

- S3BucketLog

Tipo: cadena

Descripción: (opcional) El nombre del bucket de Amazon S3 que se utilizará para almacenar las respuestas de salida de los comandos. Puede especificar un bucket que sea de su propiedad o uno que se comparta con usted. Si proporciona este parámetro, también debe proporcionar runCommandAssumeRole.

- runCommandAssumeRole

Tipo: cadena

Descripción: (opcional) El ARN del rol de IAM que se utilizará para ejecutar el comando en la instancia. El rol debe tener una relación de confianza con el principal del ssm.amazonaws.com servicio, debe tener la SSMManged InstanceCore política de Amazon adjunta y debe tener permisos de escritura para el bucket de Amazon S3 especificado para S3 BucketLog.

AWSEC2-SQLServerDBRestore

Descripción

El manual de procedimientos `AWSEC2-SQLServerDBRestore` restaura las copias de seguridad de bases de datos de Amazon S3 a Server 2017 en ejecución en una instancia Amazon Elastic Compute Cloud (EC2) de Linux. Puede proporcionar su propia instancia EC2 con SQL Server 2017 para Linux. Si no se proporciona ninguna instancia EC2, Automatización inicia y configura una nueva instancia EC2 de Ubuntu 16.04 con SQL Server 2017. Automation admite la restauración de copias de seguridad completas, diferenciales y de registros de transacciones. Automation acepta varios archivos de copia de seguridad de bases de datos y restaura automáticamente la copia de seguridad válida más reciente de cada base de datos de los archivos proporcionados.

Para automatizar la copia de seguridad y la restauración de una base de datos de SQL Server local en una instancia EC2 que ejecute SQL Server 2017 Linux, puede utilizar el script AWS PowerShell - signed. [MigrateSQLServerToEC2Linux](#)

Important

Este manual de procedimientos restablece la contraseña de usuario de administrador del servidor (SA) de SQL Server cada vez que se ejecuta la automatización. Una vez que finalice la automatización, debe establecer su propia contraseña de usuario de SA de nuevo antes de conectarse a la instancia de SQL Server.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Requisitos previos

Para ejecutar esta automatización, debe cumplir los siguientes requisitos previos:

- El usuario o rol de IAM que ejecute esta automatización debe tener una política integrada asociada con los permisos que se describen en. [Permisos de IAM necesarios](#)

- Si proporciona su propia instancia EC2, haga lo siguiente:
 - La instancia EC2 que proporcione debe ser una instancia de Linux que ejecute Microsoft SQL Server 2017.
 - La instancia EC2 debe ser configurada con un perfil de instancia de AWS Identity and Access Management (IAM) que tenga asociado la política administrada AmazonSSMManagedInstanceCore adjunta. Para obtener más información, consulte [Crear un perfil de instancias de IAM para Systems Manager](#).
 - El agente de SSM debe estar instalado en su instancia EC2. Para obtener más información, consulte [Installing and Configuring SSM Agent on EC2 Instances para Linux](#).
 - La instancia EC2 debe tener suficiente espacio libre en disco para descargar y restaurar las copias de seguridad de SQL Server.

Limitaciones

Automation no admite la restauración de SQL Server en ejecución en instancias EC2 para Windows Server. Automation solo restaura las copias de seguridad de bases de datos que sean compatibles con SQL Server 2017 para Linux. Para obtener más información, consulte la sección [Ediciones y características admitidas de SQL Server 2017 para Linux](#).

Parameters

Esta automatización tiene los siguientes parámetros:

- DatabaseNames

Tipo: cadena

Descripción: (opcional) la lista separada por comas de los nombres de las bases de datos que se restaurarán.

- DataDirectorySize

Tipo: cadena

Descripción: (opcional) el tamaño del volumen (GiB) deseado del directorio Data de SQL Server para la nueva instancia EC2.

Valor predeterminado: 100

- KeyPair

Tipo: cadena

Descripción: (opcional) el par de claves que se utilizará al crear la nueva instancia EC2.

- `IamInstanceProfileName`

Tipo: cadena

Descripción: (opcional) el perfil de instancia de IAM que se asociará a la nueva instancia EC2. El perfil de instancia de IAM debe tener la política administrada asociada de `AmazonSSMManagedInstanceCore`.

- `InstanceId`

Tipo: cadena

Descripción: (opcional) la instancia que ejecuta SQL Server 2017 en Linux. Si no `InstanceId` se proporciona, la automatización lanza una nueva instancia de EC2 con la `InstanceType` edición y proporcionada. `SQLServer`

- `InstanceType`

Tipo: cadena

Descripción: (opcional) el tipo de instancia EC2 que se va iniciar.

- `es S3 PresignedUrl`

Tipo: cadena

Descripción: (opcional) si `S3Input` es una URL de S3 prefirmada, indique yes.

Valor predeterminado: no

Valores válidos: yes | no

- `LogDirectorySize`

Tipo: cadena

Descripción: (opcional) el tamaño del volumen (GiB) deseado del directorio Log de SQL Server para la nueva instancia EC2.

Valor predeterminado: 100

- S3Input

Tipo: cadena

Descripción: (obligatorio) nombre del depósito de S3, lista separada por comas de claves de objetos de S3 o lista separada por comas de S3 prefirmados URLs que contiene los archivos de respaldo de SQL que se van a restaurar.

- SQLServerEdición

Tipo: cadena

Descripción: (opcional) la edición de SQL Server 2017 que se instalará en la instancia EC2 recién creada.

Valores permitidos: Standard | Enterprise | Web | Express

- SubnetId

Tipo: cadena

Descripción: (opcional) la subred en la que se iniciará la nueva instancia EC2. La subred debe tener conectividad saliente con los servicios. AWS Si no SubnetId se proporciona un valor para, la automatización utiliza la subred predeterminada.

- TempDbDirectorySize

Tipo: cadena

Descripción: (opcional) el tamaño del volumen (GiB) deseado del directorio TempDB de SQL Server para la nueva instancia EC2.

Valor predeterminado: 100

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar correctamente el manual de procedimientos.

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "ec2:CreateTags",
          "ec2:DescribeImages",
          "ec2:DescribeInstanceStatus",
          "ec2:DescribeInstances",
          "ec2:RebootInstances",
          "ec2:RunInstances",
          "ssm:DescribeInstanceInformation",
          "ssm:GetAutomationExecution",
          "ssm:ListCommandInvocations",
          "ssm:ListCommands",
          "ssm:SendCommand",
          "ssm:StartAutomationExecution"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::111122223333:role/ROLENAME"
      }
    ]
  }
}

```

Pasos de documentos

Para usar esta automatización, sigue los pasos que se aplican a tu tipo de instancia:

Para las nuevas instancias EC2:

1. `aws:executeAwsApi`: recupera el ID de AMI para SQL Server 2017 en Ubuntu 16.04.
2. `aws:runInstances`: lanza una nueva instancia EC2 para Linux.
3. `aws:waitForAwsResourceProperty`: espera a que la instancia EC2 recién creada esté lista.
4. `aws:executeAwsApi`: reinicia la instancia si no está lista.
5. `aws:assertAwsResourceProperty`: comprueba que el agente de SSM esté instalado.
6. `aws:runCommand`- Ejecute el script de restauración de SQL Server en PowerShell.

Para las instancias EC2 existentes:

1. `aws:waitForAwsResourceProperty`: verifica que la instancia EC2 está lista.
2. `aws:executeAwsApi`: reinicia la instancia si no está lista.
3. `aws:assertAwsResourceProperty`: comprueba que el agente de SSM esté instalado.
4. `aws:runCommand`- Ejecute el script de restauración de SQL Server en PowerShell.

Salidas

`GetInstance`. `InstanceId`

`restoreToNewInstancia`. `Salida`

`restoreToExistingInstancia`. `Salida`

AWSSupport-ActivateWindowsWithAmazonLicense

Descripción

El `AWSSupport-ActivateWindowsWithAmazonLicense` manual activa una instancia de Amazon Elastic Compute Cloud (Amazon EC2) para Windows Server con una licencia proporcionada por Amazon. La automatización verifica y configura los ajustes necesarios del sistema operativo del servicio de administración de claves e intenta realizar la activación. Esto incluye las rutas del sistema operativo a los servidores de administración de claves de Amazon y la configuración del sistema operativo del servicio de administración de claves. Si se configura el `AllowOffline` parámetro para `true` que la automatización se dirija correctamente a las instancias que no están gestionadas por la instancia AWS Systems Manager, pero que requieren una parada y un inicio de la instancia.

Note

Este manual no se puede usar en el modelo Bring Your Own License (BYOL) Windows Server instancias. Para obtener más información acerca del uso de su propia licencia, consulte [Licencias de Microsoft en AWS](#).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- AllowOffline

Tipo: cadena

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) establézcalo en `true` si permite una corrección de activación de Windows sin conexión en caso de que la solución de problemas en línea produzca un error o que la instancia proporcionada no sea una instancia administrada.

Important

El método offline requiere que la EC2 instancia proporcionada se detenga y, a continuación, se inicie. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ForceActivation

Tipo: cadena

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) establecerlo en true si desea continuar incluso si Windows ya está activado.

- InstanceId

Tipo: cadena

Descripción: ID (obligatorio) de la EC2 instancia gestionada para Windows Server.

- SubnetId

Tipo: cadena

Predeterminado: CreateNew VPC

Descripción: (opcional) Solo sin conexión: el ID de subred de la instancia de EC2 Rescue que se utiliza para solucionar los problemas sin conexión. Utilice SelectedInstanceSubnet para utilizar la misma subred que la instancia, o utilice CreateNewVPC para crear una nueva VPC. IMPORTANTE: La subred debe estar en la misma InstanceId zona de disponibilidad y debe permitir el acceso a los puntos finales de SSM.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Recomendamos que la EC2 instancia que recibe el comando tenga una función de IAM con la política gestionada por SSMManagedInstanceCoreAmazon adjunta. Debes tener al menos ssm: StartAutomationExecution y ssm: SendCommand para ejecutar la automatización y enviar el comando a la instancia, además de ssm: GetAutomationExecution para poder leer el resultado de la automatización. Para obtener información sobre la corrección sin conexión, consulte los permisos que necesita AWSSupport-StartEC2RescueWorkflow.

Pasos de documentos

1. aws:assertAwsResourceProperty: comprueba que la plataforma de la instancia proporcionada sea Windows.

2. `aws:assertAwsResourceProperty`: confirma que la instancia proporcionada es una instancia gestionada:
 - a. (Solución de activación en línea) Si la instancia de entrada es una instancia administrada, ejecute el PowerShell script `aws:runCommand` para intentar corregir la activación de Windows.
 - b. (Solución de activación sin conexión) Si la instancia de entrada no es una instancia administrada:
 - i. `aws:assertAwsResourceProperty`: verifica que el indicador `AllowOffline` esté establecido en `true`. En caso afirmativo, comienza la corrección sin conexión; de lo contrario, la automatización de trabajo finaliza.
 - ii. `aws:executeAutomation`: invoca `AWSSupport-StartEC2RescueWorkflow` con el script de corrección fuera de línea para la activación de Windows. El script usa `EC2 Config` o `EC2 Launch`, según la versión del sistema operativo.
 - iii. `aws:executeAwsApi`: lee el resultado de `AWSSupport-StartEC2RescueWorkflow`.

Salidas

`activateWindows.Output`

`getActivateWindowsOfflineResult.Salida`

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Descripción

El `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` manual analiza la conectividad desde una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o una interfaz de red elástica a un punto final. Servicio de AWS IPv6 no es compatible. El manual de procedimientos utiliza el valor que especifique para el parámetro `ServiceEndpoint` a fin de analizar la conectividad con un punto de conexión. Si no se encuentra un punto de conexión AWS PrivateLink en su VPC, el manual de procedimientos utiliza una dirección IP pública para el servicio en la Región de AWS actual. Esta automatización utiliza el Reachability Analyzer de la nube privada virtual de Amazon. Para obtener más información, consulte [What is Reachability Analyzer?](#) en el Reachability Analyzer.

Esta automatización comprueba lo siguiente:

- Compruebe si su nube privada virtual (VPC) está configurada para usar el servidor DNS proporcionado por Amazon.

- Comprueba si existe un AWS PrivateLink punto final en la VPC para el Servicio de AWS que especifique. Si se encuentra un punto de conexión, la automatización verifica que el atributo `privateDns` esté activado.
- Comprueba si el AWS PrivateLink punto final utiliza la política de puntos finales predeterminada.

Consideraciones

- Se le cobrará por cada análisis realizado entre un origen y un destino. Para obtener más información, consulte [Precios de Amazon VPC](#).
- Durante la automatización, se crea una ruta de información de la red y un análisis de la información de la red. Si la automatización se completa correctamente, el manual de procedimientos elimina estos recursos. Si se produce un error en el paso de limpieza, el manual de procedimientos no eliminará la ruta de información de la red y tendrá que eliminarla manualmente. Si no elimina la ruta de información de la red de forma manual, se seguirá teniendo en cuenta para la cuota de su Cuenta de AWS. Para obtener más información sobre las cuotas del Reachability Analyzer, consulte [Quotas for Reachability Analyzer](#) en Reachability Analyzer.
- Las configuraciones a nivel del sistema operativo, como el uso de un proxy, una resolución de DNS local o un archivo de hosts, pueden afectar a la conectividad incluso si el Reachability Analyzer muestra PASS.
- Revise la evaluación de todas las comprobaciones realizadas por el Reachability Analyzer. Si alguna de las comprobaciones regresa un estado de FAIL, esto podría afectar a la conectividad, incluso si la comprobación de accesibilidad general regresa un estado de PASS.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- origen

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia de Amazon EC2 o la interfaz de red desde la que desea analizar la accesibilidad.

- ServiceEndpoint

Tipo: cadena

Descripción: (obligatorio) el nombre de host del punto de conexión del servicio en el que desea analizar la accesibilidad.

- RetainVpcReachabilityAnalysis

Tipo: cadena

Predeterminado: false

Descripción: (opcional) determina si se retienen la ruta de conocimiento de la red y los análisis relacionados creados. De forma predeterminada, los recursos utilizados para analizar la accesibilidad se eliminan cuando el análisis se realiza correctamente. Si decide retener el análisis, el manual de procedimientos no lo elimina y puede visualizarlo en la consola de Amazon VPC. Hay un enlace a la consola disponible en el resultado de la automatización.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Pasos de documentos

1. `aws:executeScript`: valida el punto de conexión del servicio intentando resolver el nombre de host.
2. `aws:executeScript`: recopila detalles sobre la VPC y la subred.
3. `aws:executeScript`: evalúa la configuración de DNS de la VPC.
4. `aws:executeScript`: evalúa las comprobaciones de punto de conexión de VPC.
5. `aws:executeScript`: Localiza una puerta de enlace de Internet para conectarse al punto de conexión del servicio público.
6. `aws:executeScript`: determina el destino que se utilizará para el análisis de accesibilidad.
7. `aws:executeScript`: analiza la accesibilidad desde el origen hasta el punto de conexión mediante el Reachability Analyzer y limpia los recursos si el análisis se realiza correctamente.
8. `aws:executeScript`: genera un informe de evaluación de la accesibilidad.
9. `aws:executeScript`: genera el resultado en JSON.

Salidas

- `generateReport.EvalReport`: los resultados de las comprobaciones realizadas por la automatización en formato de texto.
- `generateJsonOutput.Output`: una versión mínima de los resultados en formato JSON.

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

Descripción

El manual de procedimientos `AWSPremiumSupport-ChangeInstanceTypeIntelToAMD` automatiza las migraciones desde instancias de Amazon Elastic Compute Cloud (Amazon EC2) con tecnología Intel a tipos de instancias equivalentes con tecnología AMD. Este manual de procedimientos admite instancias de uso general (M), de desempeño con ráfagas (T), optimizadas para cómputo (C) y optimizadas para memoria (R) creadas en el sistema Nitro. Este manual de procedimientos se puede usar en instancias que no estén administradas por Systems Manager.

Para reducir el posible riesgo de pérdida de datos y tiempo de inactividad, el manual de procedimientos comprueba el comportamiento de parada de la instancia, si la instancia está en un grupo de Amazon EC2 Auto Scaling, el estado de la instancia y si el tipo de instancia equivalente con tecnología AMD está disponible en la misma zona de disponibilidad. De forma predeterminada, este runbook no cambiará el tipo de instancia si hay volúmenes de almacenados de instancias adjuntos o si la instancia forma parte de una AWS CloudFormation pila. Si desea cambiar este comportamiento, especifique `yes` para cualquiera de los parámetros `AllowInstanceStoreInstances` y `AllowCloudFormationInstances`.

Important

El acceso a `AWSPremiumSupport-*` los manuales requiere una suscripción a Business + Support, Enterprise Support o Unified Operations. Para obtener más información, consulte [Comparar planes de AWS Support](#).

Consideraciones

- Recomendamos hacer una copia de seguridad de la instancia antes de usar este manual de procedimientos.
- Para cambiar el tipo de instancia, es necesario que el manual de procedimientos detenga su instancia. Cuando se detiene una instancia, se pierden todos los datos almacenados en la RAM o

en los volúmenes del almacén de instancias y se libera la IPv4 dirección pública automática. Para obtener más información, consulte [Detenimiento e inicio de la instancia](#).

- Si no especificas un valor para el `TargetInstanceType` parámetro, el manual intentará identificar la instancia AMD equivalente en términos de espacio virtual CPUs y memoria dentro de la misma familia de instancias. El manual de procedimientos finaliza si no es capaz de identificar un tipo de instancia AMD equivalente.
- Al usar la opción `DryRun`, puede capturar el tipo de instancia AMD equivalente y validar los requisitos sin cambiar realmente el tipo de instancia.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `Acknowledge`

Tipo: cadena

Descripción: (obligatorio) introduzca `yes` para confirmar que la instancia de destino se detendrá si se está ejecutando.

- `InstanceId`

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia de Amazon EC2 cuyo tipo desea cambiar.

- `TargetInstanceType`

Tipo: cadena

Predeterminado: `automatic`

Descripción: (opcional) el tipo de instancia AMD al que desea cambiar su instancia. El `automatic` valor predeterminado usa el tipo de instancia equivalente en términos de memoria CPUs y virtual. Por ejemplo, un `m5.large` se cambiaría a `m5a.large`.

- `AllowInstanceStoreInstances`

Tipo: cadena

Valores válidos: `no` | `yes`

Valor predeterminado: `no`

Descripción: (opcional) si especifica `yes`, el manual de procedimientos se ejecuta en instancias que tienen volúmenes de almacén de instancias adjuntos.

- `AllowCloudFormationInstances`

Tipo: cadena

Valores válidos: `no` | `yes`

Valor predeterminado: `no`

Descripción: (opcional) Si se establece en `yes`, el runbook se ejecuta en las instancias que forman parte de una CloudFormation pila.

- `AllowCrossGeneration`

Tipo: cadena

Valores válidos: `no` | `yes`

Descripción: (opcional) Si se establece en yes, el manual de procedimientos intenta encontrar el tipo de instancia AMD equivalente más reciente dentro de la misma familia de instancias.

- DryRun

Tipo: cadena

Valores válidos: no | yes

Valor predeterminado: no

Descripción: (opcional) si se establece en yes, el manual de procedimientos regresa el tipo de instancia AMD equivalente y valida los requisitos de migración sin realizar cambios en el tipo de instancia.

- SleepWait

Tipo: cadena

Predeterminado: S PT3

Descripción: (opcional) el tiempo que debe esperar el manual de procedimientos antes de iniciar una nueva automatización. El valor que proporcione para este parámetro debe coincidir con la norma ISO 8601. Para obtener más información sobre la creación de cadenas ISO 8601, consulte [Formatear cadenas de fecha y hora para Systems Manager](#).

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Pasos de documentos

1. `aws:assertAwsResourceProperty`: confirma que el estado de la instancia de Amazon EC2 de destino es `running`, `pending`, `stopped` o `stopping`. De lo contrario, la automatización finaliza.
2. `aws:executeAwsApi`: reúne las propiedades de la instancia de Amazon EC2 de destino.
3. `aws:branch`: ramifica la automatización en función del estado de la instancia de Amazon EC2.
 - a. En caso de `stopped` o `stopping`, la automatización ejecuta `aws:waitForAwsResourceProperty` hasta que la instancia de Amazon EC2 se detenga por completo.
 - b. En caso de `running` o `pending`, la automatización ejecuta `aws:waitForAwsResourceProperty` hasta que la instancia de Amazon EC2 supere las comprobaciones de estado.
4. `aws:assertAwsResourceProperty`: confirma que la instancia de Amazon EC2 no forma parte de un grupo de escalado automático comprobando si la etiqueta `aws:autoscaling:groupName` está aplicada.
5. `aws:executeAwsApi`: reúne las propiedades del tipo de instancia actual para buscar el tipo de instancia AMD equivalente.
6. `aws:assertAwsResourceProperty`: confirma que el código de AWS Marketplace producto no está asociado a la instancia Amazon EC2. Algunos productos no están disponibles en todos los tipos de instancias.
7. `aws:branch`: Ramifica la automatización en función de si desea que la automatización compruebe si la instancia de Amazon EC2 forma parte de una pila CloudFormation
 - a. Si la `aws:cloudformation:stack-name` etiqueta se aplica a la instancia, la automatización se ejecuta `aws:assertAwsResourceProperty` para confirmar que la instancia no forma parte de una CloudFormation pila.
8. `aws:branch`: ramifica la automatización en función de si el tipo de volumen raíz de la instancia es Amazon Elastic Block Store (Amazon EBS).

9. `aws:assertAwsResourceProperty`: confirma que el comportamiento de cierre de la instancia sea `stop` y no `terminate`.
10. `aws:executeScript`: confirma que solo hay una automatización de este manual de procedimientos dirigida a la instancia actual. Si ya hay otra automatización en curso dirigida a la misma instancia, regresa un error y finaliza.
11. `aws:executeAwsApi`: Devuelve una lista de los tipos de instancias de AMD con la misma cantidad de memoria y vCPUs.
12. `aws:executeScript`: comprueba si el tipo de instancia actual es compatible y regresa su tipo de instancia AMD equivalente. Si no hay un equivalente, la automatización finaliza.
13. `aws:executeScript`: confirma que el tipo de instancia AMD está disponible en la misma zona de disponibilidad y verifica los permisos de IAM proporcionados.
14. `aws:branch`: ramifica la automatización en función de si el valor del parámetro `DryRun` es `yes`.
15. `aws:branch`: comprueba si el tipo de instancia original y el de destino son iguales. Si son iguales, la automatización finaliza.
16. `aws:executeAwsApi`: obtiene el estado actual de la instancia.
17. `aws:changeInstanceState`: crea la instancia de Amazon EC2.
18. `aws:changeInstanceState`: obliga a la instancia a detenerse si está atascada en el estado de `parada`.
19. `aws:executeAwsApi`: cambia el tipo de instancia por el tipo de instancia AMD de destino.
20. `aws:sleep`: espera 3 segundos después de cambiar el tipo de instancia para lograr una coherencia definitiva.
21. `aws:branch`: ramifica la automatización en función del estado de la instancia anterior. Si se estaba `running`, se inicia la instancia.
 - a. `aws:changeInstanceState`: Inicia la instancia de Amazon EC2 si se estaba ejecutando antes de cambiar el tipo de instancia.
 - b. `aws:waitForAwsResourceProperty`: Espera a que la instancia de Amazon EC2 supere las comprobaciones de estado. Si la instancia no supera las comprobaciones de estado, la instancia cambia de regreso a su tipo de instancia original.
 - i. `aws:changeInstanceState`: detiene la instancia de Amazon EC2 antes de cambiarla a su tipo de instancia original.
 - ii. `aws:changeInstanceState`: obliga a la instancia de Amazon EC2 a detenerse antes de cambiarla a su tipo de instancia original en caso de que se quede atascada en un estado de `parada`.

- iii. `aws:executeAwsApi`: cambia la instancia de Amazon EC2 a su tipo original.
- iv. `aws:sleep`: espera 3 segundos después de cambiar el tipo de instancia para lograr una coherencia definitiva.
- v. `aws:changeInstanceState`: inicia la instancia de Amazon EC2 si se estaba ejecutando antes de cambiar el tipo de instancia.
- vi. `aws:waitForAwsResourceProperty`: espera a que la instancia de Amazon EC2 supere las comprobaciones de estado.

22`aws:sleep`: espera antes de finalizar el manual de procedimientos.

AWSSupport-CheckXenToNitroMigrationRequirements

Descripción

El `AWSSupport-CheckXenToNitroMigrationRequirements` runbook verifica que una instancia de Amazon Elastic Compute Cloud EC2 (Amazon) cumpla con los requisitos previos para cambiar correctamente el tipo de instancia de una instancia de tipo Xen a una instancia basada en Nitro. Esta automatización comprueba lo siguiente:

- El dispositivo raíz es un volumen Amazon Elastic Block Store (Amazon EBS).
- El atributo `enaSupport` está activado.
- El módulo ENA está instalado en la instancia.
- El NVMe módulo está instalado en la instancia. En caso afirmativo, el módulo está instalado y un script verifica que el módulo esté cargado en la imagen `initramfs`.
- Analiza `/etc/fstab` y busca los dispositivos de bloques que se están montando utilizando los nombres de los dispositivos.
- Determina si el sistema operativo (SO) utiliza de manera predeterminada nombres de interfaz de red predecibles.

Este manual de procedimientos admite los siguientes sistemas operativos:

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux

- Servidor Debian
- Servidor Ubuntu
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Predeterminado: false

Descripción: (Obligatorio) El ID de la EC2 instancia de Amazon cuyos requisitos previos quieres comprobar antes de migrar a un tipo de instancia basado en Nitro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeInstanceProperties`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:ListDocuments`
- `ssm:StartAutomationExecution`
- `ssm:SendCommand`
- `iam:ListRoles`
- `ec2:DescribeInstances`
- `ec2:DescribeInstancesTypes`

Pasos de documentos

- `aws:executeAwsApi`: recopila detalles sobre la instancia.
- `aws:executeAwsApi`: recopila información sobre el hipervisor de la instancia.
- `aws:branch`: se ramifica en función de si la instancia de destino ya ejecuta un tipo de instancia basado en Nitro.
- `aws:branch`: comprueba si el sistema operativo de la instancia es compatible con las instancias basadas en Nitro.
- `aws:assertAwsResourceProperty`: verifica que la instancia que especificó esté gestionada por Systems Manager y que su estado sea `Online`.
- `aws:branch`: se ramifica en función de si el dispositivo raíz de la instancia es un volumen de Amazon EBS.

- `aws:branch`: se ramifica en función de si el atributo ENA está o no habilitado para la instancia.
- `aws:runCommand`: comprueba si hay controladores ENA en la instancia.
- `aws:runCommand`- Comprueba si hay NVMe controladores en la instancia.
- `aws:runCommand`: comprueba si hay formatos no reconocidos en el archivo `fstab`.
- `aws:runCommand`: comprueba si hay una configuración predecible del nombre de la interfaz en la instancia.
- `aws:executeScript`: genera resultados en función de los pasos anteriores.

Salidas

`finalOutput.output`: los resultados de las comprobaciones realizadas por la automatización.

AWSSupport-CloneXenEC2InstanceAndMigrateToNitro

Descripción

[El AWSSupport-CloneXenEC2 InstanceAndMigrateToNitro runbook clona, prepara y migra la instancia Linux clonada de Amazon Elastic Compute Cloud \(Amazon EC2\) \(Amazon EC2\) Linux, que actualmente se ejecuta en la plataforma Amazon EC2 Xen, para que se ejecute en la plataforma Amazon EC2 Nitro.](#) Esta automatización se divide en tres ramas diferentes:

- Comprobaciones preliminares: evalúa todos los requisitos previos para continuar con la migración, incluida la comprobación de si la instancia Amazon EC2 de destino ya se está ejecutando en la plataforma Nitro, la determinación del estado del ciclo de vida, la validación del sistema operativo y la verificación de la conectividad de Systems Manager.
- Prueba: crea una prueba AMI a partir de la instancia Amazon EC2 de destino y lanza una instancia Amazon EC2 de prueba para validar el proceso de migración antes de continuar.
- CloneAndMigrate: crea un clon de la instancia Amazon EC2 de destino, instala los controladores necesarios, configura el sistema para la plataforma Nitro y cambia el tipo de instancia por el tipo Nitro deseado.

Important

Antes de conceder la aprobación para detener la instancia Amazon EC2 de destino, asegúrese de que todas las aplicaciones que se ejecutan en la instancia estén cerradas

correctamente. Si la instancia Amazon EC2 no tiene una dirección IP elástica asociada, la IPv4 dirección pública automática cambiará una vez que la instancia se detenga e inicie.

Important

Descargo de responsabilidad: la ejecución de este runbook puede implicar cargos adicionales en su cuenta para la instancia de Amazon EC2, Amazon EBS Volumes & s. AMI. Consulte los [precios de Amazon EC2](#) y [Amazon EBS](#) para obtener más información.

Important

Requisitos previos

La instancia Amazon EC2 de destino requiere acceso saliente a los repositorios para instalar controladores y dependencias como `kernel-devel`, `gcc`, `patch`, `rpm-build`, `wget`, `dracut`, `makelinux-headers`, y `unzip` usar un administrador de paquetes si es necesario.

Sistemas operativos compatibles

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

¿Cómo funciona?

El manual de instrucciones realiza los siguientes pasos de alto nivel:

- Valida los requisitos previos y comprueba si la instancia es adecuada para la migración.
- Crea y prueba una AMI para garantizar que la migración se realice correctamente.
- Activa el atributo de red mejorada (ENA) e instala los controladores ENA más recientes.
- Verifica y configura el NVMe módulo en `initramfs`.
- Analiza y modifica `/etc/fstab` para reemplazar los nombres de los dispositivos por. UUIDs

- Desactiva los nombres predecibles de las interfaces y elimina las reglas de red persistentes.
- Cambia el tipo de instancia clonada al tipo Nitro deseado.
- Crea una imagen final AMI que se puede usar como imagen dorada para lanzar instancias de Nitro.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `autoscaling:DescribeAutoScalingInstances`
- `ec2:CreateImage`
- `ec2:CreateTags`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeInstanceTypeOfferings`
- `ec2:DescribeInstanceTypes`
- `ec2:DeregisterImage`
- `ec2:ModifyInstanceAttribute`

- `ec2:RunInstances`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `ec2:TerminateInstances`
- `iam:PassRole`
- `sns:Publish`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`

Política de IAM de ejemplo:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingInstances",
        "ec2:CreateImage",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute:",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DeregisterImage",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "iam:PassRole",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:SendCommand"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    }
  ]
}
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-CloneXenEC2InstanceAndMigrateToNitro](#) Systems Manager, en Documentos.
2. Seleccione **Execute automation**.
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El ARN del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
 - Tipo: `AWS::IAM::Role::Arn`
 - TargetInstanceId (Obligatorio):
 - Descripción: (obligatorio) ID de instancia de la instancia Amazon EC2 de destino que desea migrar a la plataforma Nitro.
 - Tipo: `AWS::EC2::Instance::Id`
 - NitroInstanceType (Opcional):
 - Descripción: (opcional) Introduzca el tipo de instancia de Nitro de destino. Solo se admiten las instancias Nitro M5, M6, C5, R5, R6 y T3 (por ejemplo, t3.small). Predeterminado: m5.xlarge.
 - Tipo: `String`
 - Valor permitido: `^(m5a?z?d?n?|c5a?d?n?|r5a?d?n?b?|(c|m|r)6(a|i)?d?)\\.(2|4|8|12|16|24|32)?xlarge$|^t3a?\\.(x|2x)?large|nano|micro|small|medium)$`
 - Valor predeterminado: `m5.xlarge`
 - SNSTopicArn (obligatorio):
 - Descripción: (Obligatorio) Proporcione el ARN del tema de Amazon SNS para la notificación de aprobación. Este tema de Amazon SNS se utiliza para enviar notificaciones de aprobación durante la ejecución de la automatización.

- Tipo: String
- Valor permitido: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):sns:(us(-gov|-isob)?|ap|ca|af|me|cn|eu|sa)-(central|(north|south)?(east|west)?)-\\d:\\d{12}:[a-zA-Z0-9_.-]{1,256}$`
- ID de aprobación (obligatorio):
 - Descripción: (obligatorio) Proporcione una lista de los directores AWS autenticados que puedan aprobar o rechazar la acción. El número máximo de aprobadores es 10.
 - Tipo: StringList
 - Valor permitido: `^[a-zA-Z0-9_+=, .@\\-\\/] {1,128}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):(sts|iam)::[0-9]{12}:[a-zA-Z0-9_+=, .@\\-\\/] {1,256}$`
- MinimumRequiredApprovals (Opcional):
 - Descripción: (opcional) El número mínimo de aprobaciones necesarias para reanudar la automatización. Valor predeterminado: 1.
 - Tipo: entero
 - Valor predeterminado: 1
- DeleteResourcesOnFailure (Opcional):
 - Descripción: (opcional) Si se debe terminar la instancia de Amazon EC2 clonada AML y si se produce un error en la automatización.
 - Tipo: Boolean
 - Valores permitidos: `[true, false]`
 - Valor predeterminado: `true`
- Reconocimiento (obligatorio):
 - Descripción: (Obligatorio) Lee todos los detalles de las acciones que se llevan a cabo en este manual de automatización y escribe «Sí, entiendo y reconozco» si aceptas los pasos.
 - Tipo: String
 - Valor permitido: `^Yes, I understand and acknowledge$`
- AllowInstanceStoreInstances (Opcional):
 - Descripción: (opcional) si especifica yes, el manual de procedimientos se ejecuta en instancias que tienen volúmenes de almacén de instancias adjuntos. Advertencia: los datos de los volúmenes del almacén de instancias se pierden cuando la instancia se detiene. Este parámetro ayuda a evitar la pérdida accidental de datos.

- Tipo: Boolean
- Valores permitidos: [yes, no]
- Valor predeterminado: no

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **checkConcurrency:**

Garantiza que solo haya una ejecución de este runbook dirigida a la instancia actual de Amazon EC2.

- **getTargetInstanceProperties:**

Obtiene los detalles de la instancia Amazon EC2 de destino.

- **checkIfNitroInstanceTypeIsSupportedInAZ:**

Determina si el tipo de instancia de Nitro de destino se admite en la misma zona de disponibilidad que la instancia de Amazon EC2 de destino.

- **createTestImage:**

Crea una prueba a AML partir de la instancia proporcionada.

- **launchTestInstanceInSameSubnet:**

Lanza una instancia Amazon EC2 de prueba a partir de la prueba AML con la misma configuración que la instancia Amazon EC2 de destino.

- **approvalToStopTargetInstance:**

Espera la aprobación de los directores designados para detener la instancia de destino.

- **createBackupImage:**

Crea una copia AML de seguridad a partir de la instancia proporcionada.

- **launchInstanceInSameSubnet:**

Lanza una nueva instancia de Amazon EC2 desde la copia de seguridad AML con la misma configuración que la instancia Amazon EC2 de origen.

- **checkAndInstallENADrivers:**

Determina la disponibilidad de los controladores del adaptador de red mejorado (ENA) en la instancia de Amazon EC2 y los instala si faltan.

- **checkAndAddNVMEDrivers:**

Determina la disponibilidad de los controladores NVMe en la instancia de Amazon EC2 clonada y los instala, si faltan.

- **checkAndModifyFSTABEntries:**

Determina si el nombre del dispositivo se utiliza `/etc/fstab` y, si lo encuentra, lo reemplaza por el suyo UUIDs.

- **setNitroInstanceTypeForClonedInstance:**

Establece el tipo de instancia Amazon EC2 de destino proporcionado para la instancia de Amazon EC2 clonada.

- **approvalForCreatingImageAfterDriversInstallation:**

Espera la aprobación del usuario si la instancia clonada de Amazon EC2 se inicia correctamente en la plataforma Nitro.

- **createImageAfterDriversInstallation:**

Crea una imagen desde la nueva instancia de Amazon EC2 solo si la nueva instancia de Amazon EC2 se inicia correctamente en la plataforma Nitro.

7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

AWS Systems Manager Automation

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWSSupport-CollectSAPHANALogs

Descripción

El AWSSupport-CollectSAPHANALogs manual recopila los registros del sistema de SAP HANA en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que forma parte de un SAP en el momento de la implementación. AWS La instancia de Amazon EC2 debe gestionarla AWS Systems Manager (Systems Manager). El runbook comprueba los paquetes necesarios y los instala si faltan, ejecuta la herramienta de recopilación de registros adecuada para el sistema operativo detectado y, opcionalmente, carga los registros recopilados en un depósito de Amazon Simple Storage Service (Amazon S3).

Important

Este runbook requiere al menos 200 MB de espacio disponible en disco en la partición. / var/log Al ejecutar este runbook, es posible que se instalen paquetes adicionales en la instancia Amazon EC2 de destino. Debe reconocerlo configurando el Acknowledgement parámetro en. Yes El almacenamiento de registros en Amazon S3 conlleva cargos estándar de almacenamiento y solicitud de Amazon S3.

Sistemas operativos compatibles

- Red Hat Enterprise Linux8.4 y versiones posteriores
- SUSE Linux Enterprise Server SP5 12
- SUSE Linux Enterprise Server15 SP3 y versiones posteriores

Paquetes instalados si faltan

SUSE Linux Enterprise Server:

- supportutils
- yast2-support
- supportutils-plugin-suse-public-cloud
- supportutils-plugin-ha-sap
- crmsh
- unzip

- `curl`
- `aws-cli`(opcional, se instala si `InstallAWSCLI` está configurado en `Yes`)

Red Hat Enterprise Linux:

- `sos`
- `crm_report`
- `unzip`
- `curl`
- `aws-cli`(opcional, se instala si `InstallAWSCLI` está configurado en `Yes`)

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `InstanceId`

Escriba `AWS::EC2::Instance: :Id`

Descripción: (obligatorio) El ID de la instancia de Amazon EC2 que ejecuta la carga de trabajo de SAP desde la que se deben recopilar los registros.

- Reconocimiento

Tipo: cadena

Valores válidos: Yes

Descripción: (Obligatorio) Reconozco que este runbook puede instalar paquetes adicionales en la instancia Amazon EC2 de destino para la recopilación de registros.

- S3 LogDestination

Tipo: AWS::S3::Bucket :Nombre

Descripción: (opcional) El nombre del depósito de Amazon S3 en el que se cargan los registros. El bucket no debe ser público y debe pertenecer a la misma AWS cuenta. Si no se proporciona, los registros se almacenan en el almacenamiento local de la instancia.

- S3Prefix

Tipo: cadena

Predeterminado: AWSSupport-CollectSAPHANALogs

Patrón permitido: `^[a-zA-Z0-9][-. /a-zA-Z0-9]{0,255}$`

Descripción: (opcional) El prefijo del bucket de Amazon S3 donde se almacenan los registros. Si no se proporciona, el valor predeterminado es. AWSSupport-CollectSAPHANALogs

- Instalar AWSCLI

Tipo: cadena

Valores válidos: Yes | No

Valor predeterminado: No

Descripción: (opcional) Si se debe instalar la AWS CLI en la instancia. SiYes, el runbook instala la AWS CLI si aún no está presente.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketAcl`
- `s3:GetBucketLocation`
- `s3:GetBucketOwnershipControls`
- `s3:GetEncryptionConfiguration`
- `s3:PutObject`

Pasos de documentos

1. `AssertInstanceIsSSMManaged`- Verifica que la instancia Amazon EC2 de destino esté gestionada por Systems Manager y tenga un `PingStatus` de `Online`. El runbook se cancela si la instancia no está administrada.
2. `GetInstanceInformation`- Recupera información sobre la instancia Amazon EC2 especificada, incluido el nombre de la plataforma, que se utiliza para determinar el método de recopilación de registros adecuado.
3. `CollectLogs`- Ejecuta un script de shell en la instancia para recopilar los registros. Por SUSE Linux Enterprise Server ejemplo, el script `usasupportconfig`. Por Red Hat Enterprise Linux ejemplo, `usassos report`. En el caso de los clústeres de alta disponibilidad, el script también recopila registros de alta disponibilidad adicionales de los últimos 7 días mediante el `crm report` comando. Si faltan, se instalan los paquetes necesarios.
4. `BranchOnS3BucketProvided`- Ramifica la ejecución en función de si se ha incluido un bucket de Amazon S3 `S3LogDestination`. Si no se ha proporcionado ningún bucket, el manual pasa a `GenerateReport`. De lo contrario, pasa a `CheckS3BucketPublicStatus`.
5. `CheckS3BucketPublicStatus`- Comprueba si el bucket de Amazon S3 especificado `S3LogDestination` está configurado con cifrado del lado del servidor (SSE) y si permite permisos de acceso de lectura o escritura públicos o anónimos. También verifica que el propietario real del bucket sea el mismo que el propietario esperado del bucket. Si este paso no se realiza correctamente, el runbook seguirá `GenerateReport` sin cargarse.

6. `UploadLogsToS3`- Carga los registros recopilados en el bucket de Amazon S3 especificado. Si `InstallAWSCLI` está configurado en Yes y la AWS CLI no está instalada, el script instala la AWS CLI antes de cargarla.
7. `GenerateReport`- Genera un informe del proceso de recopilación de registros. Si se proporcionó un bucket de Amazon S3, este incluye el nombre y el prefijo del bucket de Amazon S3 donde se cargaron los registros. De lo contrario, indica que los registros se almacenaron localmente en la instancia. También indica por qué fallaron los pasos anteriores.

Salidas

`GenerateReport.Summary`- Un resumen del resultado de la recopilación de registros.

`GenerateReport.LogLocation`- La ubicación en la que se almacenaron los registros, ya sea una ruta local de la instancia o un URI de Amazon S3.

`GenerateReport.Status`- El estado general de la ejecución de la recopilación de registros.

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-CollectSAPHANALogs](#) Systems Manager en Documentos.
2. Elija `Execute automation` (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- `AutomationAssumeRole` (Opcional):

El ARN de la función de IAM que permite a Systems Manager Automation realizar acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- `InstanceId` (obligatorio):

El ID de la instancia de Amazon EC2 que ejecuta la carga de trabajo de SAP.

- `Reconocimiento` (obligatorio):

Introduzca Yes para confirmar que el runbook puede instalar paquetes adicionales en la instancia Amazon EC2 de destino.

- `S3 LogDestination` (opcional):

El nombre del bucket de Amazon S3 en el que se van a cargar los registros. Si no se proporcionan, los registros se almacenan localmente en la instancia.

- **Prefijo S3 (opcional):**

El prefijo de bucket de Amazon S3 para los registros almacenados. El valor predeterminado es `AWSSupport-CollectSAPHANALogs`.

- **Instalar AWSCLI (opcional):**

Seleccione esta opción Yes para instalar automáticamente la AWS CLI si no está presente en la instancia. El valor predeterminado es No.

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **AssertInstanceIsSSMManaged**

Verifica que la instancia Amazon EC2 de destino esté gestionada por Systems Manager y tenga un `PingStatus` de `Online`

- **GetInstanceInformation**

Recupera información sobre la instancia de Amazon EC2 especificada, incluido el nombre de la plataforma.

- **CollectLogs**

Ejecuta un script de shell para recopilar registros utilizando `supportconfig for SLES` o `supportconfig for RHEL`. En el caso de los clústeres de alta disponibilidad, también recopila los registros de alta disponibilidad de los últimos 7 días de `usocrm report`.

- **BranchOnS3BucketProvided**

Salta a `GenerateReport` si no se ha proporcionado ningún bucket de Amazon S3; de lo contrario, pasa a `CheckS3BucketPublicStatus`.

- **CheckS3BucketPublicStatus**

Verifica que el bucket de Amazon S3 tenga SSE habilitado, no permita el acceso público y sea propiedad de la misma AWS cuenta.

- **UploadLogsToS3**

Carga los registros recopilados en el bucket de Amazon S3 especificado. Instala la AWS CLI si `InstallAWSCLI` está Yes y no está ya presente.

- **GenerateReport**

Genera un resumen del resultado de la recopilación de registros, que incluye la ubicación del registro y cualquier error en los pasos.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSSupport-ConfigureEC2Metadata

Descripción

Este manual le ayuda a configurar las opciones del servicio de metadatos de instancias (IMDS) para las instancias de Amazon Elastic Compute Cloud EC2 (Amazon). Mediante este manual de procedimientos, puede realizar la configuración de:

- Imponga el uso de, IMDSv2 por ejemplo, metadatos.
- Configurar el valor `HttpPutResponseHopLimit`.
- Permitir o denegar el acceso a los metadatos de la instancia.

Para obtener más información sobre los metadatos de la instancia, consulte [Configuración del servicio de metadatos de la instancia](#) en la Guía del EC2 usuario de Amazon.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Hacer cumplir IMDSv2

Tipo: cadena

Valores válidos: obligatorio | opcional

Predeterminado: opcional

Descripción: (opcional) Hacer cumplir IMDSv2. Si lo desea `required`, solo se usará la EC2 instancia de Amazon IMDSv2. Si lo desea `optional`, puede elegir entre IMDSv1 y IMDSv2 para el acceso a los metadatos.

Important

Si lo hace cumplir IMDSv2, es IMDSv1 posible que las aplicaciones que utilice no funcionen correctamente. Antes de aplicarlo IMDSv2, asegúrese de que las aplicaciones que utilizan el IMDS estén actualizadas a una versión compatible. IMDSv2 Para obtener información sobre la versión 2 (IMDSv2) del servicio de metadatos de instancias, consulte [Configuración del servicio de metadatos de instancias](#) en la Guía del EC2 usuario de Amazon.

- **HttpPutResponseHopLimit**

Tipo: entero

Valores válidos: 0 - 64

Predeterminado: 0

Descripción: (opcional) el valor del límite de saltos de respuesta HTTP PUT deseado (1 - 64) para las solicitudes de metadatos de instancia. Este valor controla el número de saltos que puede recorrer la respuesta PUT. Para evitar que la respuesta viaje fuera de la instancia, especifique 1 para el valor del parámetro.

- **InstanceId**

Tipo: cadena

Descripción: (Obligatorio) El ID de la EC2 instancia de Amazon cuya configuración de metadatos quieres configurar.

- **MetadataAccess**

Tipo: cadena

Valores válidos: enabled | disabled

Valor predeterminado: habilitado

Descripción: (opcional) Permite o deniega el acceso a los metadatos de la EC2 instancia de Amazon. Si especifica disabled, se ignorarán todos los demás parámetros y se denegará el acceso a los metadatos de la instancia.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

1. `branchOnMetadataAcceso`: automatización de ramificaciones en función del valor del `MetadataAccess` parámetro.
2. `disableMetadataAccess` - Solicita a la `ModifyInstanceMetadataOptions` API una acción para deshabilitar el acceso al punto final de los metadatos.
3. `branchOnHttpPutResponseHopLimit` - La automatización de ramificaciones se basa en el valor del `HttpPutResponseHopLimit` parámetro.
4. `maintainHopLimitAndConfigureImdsVersion` - Si `HttpPutResponseHopLimit` es 0, mantiene el límite de saltos actual y cambia otras opciones de metadatos.
5. `waitBeforeAssertingIMDSv2Estado`: espera 30 segundos antes de confirmar el estado. `IMDSv2`
6. `setHopLimitAndConfigureImdsVersion` - Si `HttpPutResponseHopLimit` es mayor que 0, configura las opciones de metadatos utilizando los parámetros de entrada indicados.
7. `waitBeforeAssertingHopLimit` - Espera 30 segundos antes de activar las opciones de metadatos.
8. `assertHopLimit` - Afirma que la `HttpPutResponseHopLimit` propiedad está establecida en el valor que especificó.
9. `branchVerificationOnIMDSv2Opción`: la verificación de ramificaciones se basa en el valor del `EnforceIMDSv2` parámetro.
10. `afirmar IMDSv2IsOptional` : afirma el `HttpTokens` valor establecido en. `optional`
11. `afirmar IMDSv2IsEnforced` : afirma el `HttpTokens` valor establecido en. `required`
12. `waitBeforeAssertingMetadataState` - Espera 30 segundos antes de confirmar que el estado de los metadatos está desactivado.
13. `assertMetadataIsDesactivado`: afirma que los metadatos son. `disabled`
14. `describeMetadataOptions` - Obtiene las opciones de metadatos una vez aplicados los cambios que ha especificado.

Salidas

`describeMetadataOptions.Estado`

`describeMetadataOptions.MetadataAccess`

`describeMetadataOptions.IMDSv2`

`describeMetadataOptions.HttpPutResponseHopLimit`

AWSSupport-ContainEC2Instance

Descripción

El AWSSupport-ContainEC2Instance manual proporciona una solución automatizada para el procedimiento descrito en el artículo [¿Cómo puedo aislar la instancia Amazon EC2 ante una instancia potencialmente comprometida](#) o sospechosa? La automatización se ramifica en función de los valores que especifique.

¿Cómo funciona?

Este manual de automatización AWSSupport-ContainEC2Instance realiza la contención de red de una instancia de Amazon EC2 mediante una serie de pasos coordinados. Cuando se ejecuta en Contain modo, primero valida los parámetros de entrada y comprueba si la instancia no ha terminado. A continuación, realiza una copia de seguridad de la configuración actual del grupo de seguridad en un bucket de Amazon S3 para su posterior restauración. El manual crea dos grupos de seguridad: un grupo de seguridad temporal de «acceso total» y un grupo de seguridad final de «contención». De forma gradual, las interfaces de red de la instancia pasan de sus grupos de seguridad originales al grupo de seguridad de acceso total y, finalmente, al grupo de seguridad de contención. Si se especifica, crea AMI copias de seguridad cifradas y no cifradas de la instancia. En el caso de las instancias de un grupo de Auto Scaling, gestiona las modificaciones necesarias del grupo de Auto Scaling y pone la instancia en estado de espera. Cuando se ejecuta en Release modo, restaura la instancia a su configuración de red original mediante la configuración de copia de seguridad de Amazon S3. El runbook admite un DryRun parámetro para obtener una vista previa de las acciones sin realizar cambios reales, e incluye mecanismos integrales de gestión y notificación de errores en todos los flujos de trabajo de contención y publicación.

Important

- Este manual realiza varias operaciones que requieren privilegios elevados, como modificar grupos de seguridad, crear AMI grupos e interactuar con grupos de Auto Scaling. Estas acciones podrían provocar una escalada de privilegios o afectar a otras cargas de trabajo de su cuenta. Debes revisar los permisos otorgados al rol especificado por el AutomationAssumeRole parámetro y asegurarte de que son adecuados para el caso de uso previsto. Puede consultar la siguiente AWS documentación para obtener más información sobre los permisos de IAM: [AWS Identity and Access Management \(IAM\) PermissionsAWS Systems Manager Automation Permissions](#).

- Este manual realiza acciones mutativas que podrían provocar la falta de disponibilidad o la interrupción de sus cargas de trabajo. En concreto, modifica los grupos de seguridad asociados a la instancia Amazon EC2 de destino, lo que podría afectar a la conectividad de la red. Además, si la instancia forma parte de un grupo de Auto Scaling, el runbook puede modificar la configuración del grupo, lo que podría afectar a su comportamiento de escalado.
- Durante el proceso de contención, este manual crea recursos adicionales, como grupos de seguridad y grupos de seguridad. AMI Si bien estos recursos están etiquetados para su identificación, debe estar al tanto de su creación y garantizar una limpieza o administración adecuadas una vez finalizado el proceso de contención.
- Si el `Action` parámetro está establecido en `Release`, este runbook intenta restaurar la configuración de la instancia Amazon EC2 a su estado original. Sin embargo, existe el riesgo de que el proceso de restauración falle y deje la instancia en un estado incoherente. El manual proporciona instrucciones para la restauración manual en caso de que se produzcan estos errores, pero debes estar preparado para gestionar posibles problemas durante el proceso de restauración.

Se recomienda revisar el manual detenidamente, comprender sus posibles impactos y probarlo en un entorno que no sea de producción antes de ejecutarlo en su entorno de producción.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- escalado automático: `CreateOrUpdateTags`
- escalado automático: `DeleteTags`
- escalado automático: `DescribeAutoScalingGroups`
- escalado automático: `DescribeAutoScalingInstances`
- escalado automático: `DescribeTags`
- escalado automático: `EnterStandby`
- escalado automático: `ExitStandby`
- escalado automático: `UpdateAutoScalingGroup`
- ec2: `AuthorizeSecurityGroupEgress`
- ec2: `AuthorizeSecurityGroupIngress`
- ec2: `CopyImage`
- ec2: `CreateImage`
- ec2: `CreateSecurityGroup`
- ec2: `CreateSnapshot`
- ec2: `CreateTags`
- ec2: `DeleteSecurityGroup`
- ec2: `DeleteTags`
- ec2: `DescribeImages`
- ec2: `DescribeInstances`
- ec2: `DescribeSecurityGroups`
- ec2: `DescribeSnapshots`
- ec2: `DescribeTags`
- ec2: `ModifyNetworkInterfaceAttribute`
- ec2: `RevokeSecurityGroupEgress`
- km: `CreateGrant`
- km: `DescribeKey`
- km: `GenerateDataKeyWithoutPlaintext`
- km: `ReEncryptFrom`

- km: ReEncryptTo
- s3: CreateBucket
- s3: DeleteObjectTagging
- s3: GetAccountPublicAccessBlock
- s3: GetBucketAcl
- s3: GetBucketLocation
- s3: GetBucketOwnershipControls
- s3: GetBucketPolicy
- s3: GetBucketPolicyStatus
- s3: GetBucketPublicAccessBlock
- s3: GetObject
- s3: ListBucket
- s3: PutAccountPublicAccessBlock
- s3: PutBucketPolicy
- s3: PutBucketVersioning
- s3: PutObject
- s3: PutObjectTagging

Ejemplo de política:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOperations",
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
```

```

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

```

```
    "s3:PutBucketVersioning",
    "s3:PutObject",
    "s3:PutObjectTagging"
  ],
  "Resource": "*"
}
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-ContainEC2Instance](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.
 - Tipo: `AWS::IAM::Role::Arn`
 - Acción (obligatoria):
 - Descripción: (Obligatorio) Seleccione `Contain` esta opción para aislar la instancia de Amazon EC2 o `Restore` intentar restaurar la configuración original de la instancia de Amazon EC2 a partir de una copia de seguridad anterior.
 - Tipo: cadena
 - Valor permitido: `Contain|Restore`
 - DryRun (Opcional):
 - Descripción: (opcional) Si se configura en `true`, la automatización no ejecutará ninguno de los comandos, sino que informará sobre lo que habría intentado hacer y detallará cada paso. Valor predeterminado: `true`.
 - Tipo: Booleano
 - Valores permitidos: `true|false`

- Crear AMIBackup (opcional):
 - Descripción: (Opcional) Si se establece en `true`, se creará una AMI de las instancias de Amazon EC2 antes de realizar las acciones de contención.
 - Tipo: Booleano
 - Valores permitidos: `true` | `false`
- KmsKey (Opcional):
 - Descripción: (opcional) El ID de la AWS KMS clave que se utilizará para crear una instancia AMI de Amazon EC2 cifrada de destino. El valor predeterminado es. `alias/aws/ebs`
 - Tipo: cadena
 - Valor permitido: `^(((arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}:[0-9]{12}:key/)?([a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}|mrk-[a-f0-9]{32}))|(arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}:[0-9]{12}:)?alias/.{1,}))$`
- Copias de seguridad S3 BucketName (condicional):
 - Descripción: bucket de Amazon S3 (condicional) para cargar la configuración cuando Action esté Contain o para restaurarla cuando Action esté Release. Nota: Si el depósito proporcionado no existe en la cuenta, la automatización creará un depósito de Amazon S3 en tu nombre.
 - Tipo: `AWS::S3::Bucket::Name`
- TagIdentifier (Opcional):
 - Descripción: (opcional) Una etiqueta con el formato `Key=BatchId, Value=78925` que se añadirá a los AWS recursos creados o modificados por este manual durante el flujo de trabajo de contención. Esta etiqueta se puede usar para identificar y administrar los recursos asociados durante el proceso de contención. Durante el flujo de trabajo de restauración, la etiqueta especificada por este parámetro se eliminará de los recursos. Nota: Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
 - Tipo: cadena
 - Valor permitido: `^$|^([Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\/\\@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\/\\@a-zA-Z0-9]{0,128})$`
- Copias de seguridad 3 BucketAccess (condicionales):

- Descripción: (Condicional) El ARN de los usuarios o roles de IAM a los que se les permitirá acceder al bucket de respaldo de Amazon S3 después de ejecutar las acciones de contención. Este parámetro es obligatorio cuando lo es. Action Contain El usuario en cuyo contexto se ejecuta la automatización oAutomationAssumeRole, en su defecto, el usuario en cuyo contexto se ejecuta la automatización se añade automáticamente a la lista.
- Tipo: cadena
- Valor permitido: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:[0-9]{12}:(role|user)\\/[\\w+\\/=, .@-]+$`
- IngressTrafficRules (Opcional):
 - Descripción: (opcional) Un mapa separado por comas de las reglas de entrada de grupos de seguridad con Cidr FromPort y ToPort en el formato que se va a aplicar [{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}] a la instancia de Amazon EC2. IpProtocol Si no se proporciona ninguna regla, se adjuntará un grupo de seguridad sin reglas de entrada a la instancia de Amazon EC2, lo que la aislará eficazmente del tráfico entrante.
 - Tipo: MapList
 - Valor permitido: `^\\{\\}$|^\\{"Cidr\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"IpProtocol\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"FromPort\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"ToPort\\":\\"[\\x00-\\x7F+]{0,255}\\"}\\$`
- EgressTrafficRules (Opcional):
 - Descripción: (opcional) Un mapa separado por comas de las reglas de salida de los grupos de seguridad con Cidr FromPort y ToPort en el formato que se va a aplicar [{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}] a la instancia Amazon EC2 de Amazon. IpProtocol Si no se proporciona ninguna regla, se adjuntará un grupo de seguridad sin reglas de salida a la instancia de Amazon EC2, lo que impedirá de forma efectiva todo el tráfico saliente.
 - Tipo: MapList
 - Valor permitido: `^\\{\\}$|^\\{"Cidr\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"IpProtocol\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"FromPort\\":\\"[\\x00-\\x7F+]{1,128}\\",\\"ToPort\\":\\"[\\x00-\\x7F+]{0,255}\\"}\\$`
- BackupS3 KeyName (opcional):
 - Descripción: (Opcional) Si Action se establece enRestore, especifica la clave de Amazon S3 que la automatización utilizará para intentar restaurar la configuración de la instancia Amazon EC2 de destino. La clave de Amazon S3 suele seguir este formato:{year}/

`{month}/{day}/{hour}/{minute}/{automation_execution_id}.json`. La clave se puede obtener del resultado de una ejecución anterior de automatización de contención.

- Tipo: cadena
- Valor permitido: `^[a-zA-Z0-9\\.\\-\\_\\\\!*'()/{0,1024}$`

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `ValidateRequiredInputs`

Valida que se hayan proporcionado todas las entradas necesarias.

- `AssertInstanceIsNotTerminated`

Comprueba si la instancia Amazon EC2 de destino no está finalizada (eliminada).

- `GetAutoScalingInstanceInfo`

Obtiene el ciclo de vida de la instancia Amazon EC2 y el nombre del grupo si la instancia de Amazon EC2 de destino forma parte de un grupo de Auto Scaling.

- `CheckBackupS3BucketName`

Comprueba si el bucket de Amazon S3 de destino puede conceder acceso `write` público `read` o conceder acceso público a sus objetos. Se crea un nuevo bucket de Amazon S3 si el `BackupS3BucketName` bucket no existe.

- `BranchOnActionAndMode`

Ramifica la automatización en función de los parámetros de entrada `Action` y `DryRun`.

- `BranchOnAutoScalingGroupMembership`

Ramifica la automatización en función de si la instancia Amazon EC2 de destino forma parte del grupo Auto Scaling y del estado de su ciclo de vida.

- `DescribeAutoScalingGroups`

Obtiene y almacena la configuración del grupo Amazon EC2 Auto Scaling asociado.

- `ModifyAutoScalingGroup`

Modifica la configuración del grupo Amazon EC2 Auto Scaling asociado para las acciones de contención, establece el estado de la instancia de Amazon EC2 y ajusta Standby la capacidad del grupo de Auto Scaling. MinSize

- BackupInstanceSecurityGroups

Obtiene y almacena la configuración de los grupos de seguridad de las instancias Amazon EC2 de destino.

- CreateAllAccessSecurityGroup

Crea un grupo de seguridad temporal que permite todo el tráfico de entrada que sustituya a los grupos de seguridad de la instancia Amazon EC2 de destino.

- CreateContainmentSecurityGroup

Crea un grupo de seguridad de contención restrictivo con las reglas de entrada y salida especificadas y reemplaza el grupo temporal de acceso total por él.

- BranchOnCreateAMIBackup

Ramifica la automatización en función del parámetro de entrada. CreateAMIBackup

- AssertSourceInstanceRootVolumeIsEbs

Comprueba si el volumen raíz de la instancia Amazon EC2 de destino es Amazon EBS.

- CreateImage

Crea una AMI de las instancias Amazon EC2 de destino.

- RestoreInstanceConfiguration

Restaura la configuración de la instancia Amazon EC2 de destino a partir de la copia de seguridad.

- ReportContain

Muestra los detalles de ejecución en seco de las acciones de contención.

- ReportRestore

Muestra los detalles del ensayo en seco para las acciones de restauración.

- ReportRestoreFailure

Proporciona instrucciones para restaurar la configuración original de la instancia Amazon EC2 de destino durante un escenario de error en el flujo de trabajo de restauración.

- `ReportContainmentFailure`

Proporciona instrucciones para restaurar la configuración original de la instancia Amazon EC2 de destino durante un escenario de fallo en el flujo de trabajo de contención.

- `FinalOutput`

Muestra los detalles de las acciones de contención.

7. Una vez completada la ejecución, revise la sección de resultados para ver los resultados detallados de la ejecución:

- `FinalOutput.Salida`

Muestra los detalles de las acciones de contención realizadas por este manual cuando se establece en `DryRun False`.

- `RestoreInstanceConfiguration.Salida`

Muestra las acciones de restauración realizadas por este runbook cuando se establece en `DryRun False`.

- `ReportContain.Salida`

Muestra los detalles de las acciones de contención realizadas por este manual cuando `DryRun` se establece en `True`.

- `ReportRestore.Salida`

Muestra los detalles de las acciones de restauración realizadas por este runbook cuando `DryRun` se establece en `True`.

- `ReportContainmentFailure.Salida`

Proporciona instrucciones para restaurar la configuración original de la instancia Amazon EC2 de destino durante un escenario de fallo en el flujo de trabajo de contención.

- `ReportRestoreFailure.Salida`

Proporciona instrucciones para restaurar la configuración original de la instancia Amazon EC2 de destino durante un escenario de error en el flujo de trabajo de restauración.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización sencilla](#)
- [Configuración de la automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWSSupport-CopyEC2Instance

Descripción

El AWSSupport-CopyEC2Instance manual proporciona una solución automatizada para el procedimiento descrito en el artículo del Knowledge Center [¿Cómo muevo mi EC2 instancia a otra subred, zona de disponibilidad o VPC?](#) La automatización se ramifica en función de los valores que especifique para los parámetros Region y SubnetId.

Si especificas un valor para el SubnetId parámetro pero no un valor para el Region parámetro, la automatización crea un Amazon Machine Image (AMI) de la instancia de destino y lanza una nueva instancia desde AMI en la subred que especificó.

Si especifica un valor para el SubnetId parámetro y el Region parámetro, la automatización crea un AMI de la instancia de destino, copia el AMI a la Región de AWS que especificó y lanza una nueva instancia desde AMI en la subred que especificó.

Si especifica un valor para el Region parámetro pero no un valor para el SubnetId parámetro, la automatización crea un AMI de la instancia de destino, copia el AMI a la región que especificó y lanza una nueva instancia desde AMI en la subred predeterminada de su nube privada virtual (VPC) en la región de destino.

Si no se especifica ningún valor para los SubnetId parámetros Region o, la automatización crea un AMI de la instancia de destino y lanza una nueva instancia desde AMI en la subred predeterminada de la VPC.

Para copiar una AMI a una región diferente, debe proporcionar un valor para el AutomationAssumeRole parámetro. Si se agota el tiempo de espera de la automatización durante el waitForAvailableDestinationAmi paso, AMI puede que todavía esté copiando. En este caso puede esperar a que se complete la copia y lanzar la instancia manualmente.

Antes de ejecutar esta automatización, tenga en cuenta lo siguiente:

- AMIs se basan en instantáneas de Amazon Elastic Block Store (Amazon EBS). Para sistemas de archivos de gran tamaño sin una instantánea previa, AMI la creación puede tardar varias horas. Para disminuir el AMI hora de creación, cree una instantánea de Amazon EBS antes de crear el AMI.
- Creando un AMI no crea una instantánea, por ejemplo, almacena volúmenes en la instancia. Para obtener información sobre cómo hacer copias de seguridad de los volúmenes del almacén de instancias en Amazon EBS, consulte [¿Cómo hago una copia de seguridad de un volumen de almacén de instancias de mi EC2 instancia de Amazon en Amazon EBS?](#)
- La nueva EC2 instancia de Amazon tiene una dirección IPv6 IP pública IPv4 o privada diferente. Debe actualizar todas las referencias a las direcciones IP antiguas (por ejemplo, en las entradas de DNS) con las nuevas direcciones IP asignadas a la nueva instancia. Si utiliza una dirección IP elástica en la instancia de origen, asegúrese de adjuntarla a la nueva instancia.
- Se pueden producir problemas con el identificador de seguridad de dominio (SID) cuando la copia se lanza e intenta contactar con el dominio. Antes de capturar la AMI, utilice Sysprep o elimine la instancia unida al dominio del dominio para evitar problemas de conflicto. Para obtener más información, consulte [¿Cómo puedo usar Sysprep para crear e instalar Windows reutilizable personalizado? AMIs](#)

[Ejecuta esta automatización \(consola\)](#)

Important

No recomendamos usar este manual de procedimientos para copiar instancias del controlador de dominio de Microsoft Active Directory.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia de que desea reiniciar.

- KeyPair

Tipo: cadena

Descripción: (opcional) el par de claves que desea asociar con la nueva instancia copiada. Si va a copiar la instancia a una región diferente, asegúrese de que el par de claves existe en la región especificada.

- Región

Tipo: cadena

Descripción: (opcional) la región a la que quiere copiar la instancia. Si especifica un valor para este parámetro, pero no especifica valores para los parámetros SubnetId y SecurityGroupIds, la automatización intentará lanzar la instancia en la VPC predeterminada con el grupo de seguridad predeterminado. Si EC2 -Classic está activado en la región de destino, el lanzamiento fallará.

- SubnetId

Tipo: cadena

Descripción: (opcional) el ID de la subred en la que desea copiar la instancia. Si EC2 -Classic está activado en la región de destino, debe proporcionar un valor para este parámetro.

- InstanceType

Tipo: cadena

Descripción: (opcional) el tipo de instancia que se va iniciar como instancia copiada. Si no especifica un valor para este parámetro, se utiliza el tipo de instancia de origen. Si el tipo de instancia de origen no es compatible con la región en la que se está copiando la instancia, se produce un error en la automatización.

- `SecurityGroupIds`

Tipo: cadena

Descripción: (opcional) Una lista separada por comas del grupo de seguridad IDs que desea asociar a la instancia copiada. Si no especifica un valor para este parámetro y la instancia no se copia en una región diferente, se utilizan los grupos de seguridad asociados a la instancia de origen. Si va a copiar la instancia a una región diferente, se utiliza el grupo de seguridad predeterminado para la VPC predeterminada de la región de destino.

- `KeepImageSourceRegion`

Tipo: Booleano

Valores válidos: `true` | `false`

Predeterminado: `true`

Descripción: (opcional) Si especifica `true` este parámetro, la automatización no elimina el AMI de la instancia de origen. Si especifica `false` este parámetro, la automatización anula el registro del AMI y elimina las instantáneas asociadas.

- `KeepImageDestinationRegion`

Tipo: Booleano

Valores válidos: `true` | `false`

Predeterminado: `true`

Descripción: (opcional) Si especifica `true` este parámetro, la automatización no elimina el AMI que se copia en la región que especificó. Si especifica `false` este parámetro, la automatización anula el registro del AMI y elimina las instantáneas asociadas.

- `NoRebootInstanceBeforeTakingImage`

Tipo: Booleano

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) Si especifica `true` este parámetro, la instancia de origen no se reiniciará antes de crear el AMI. Cuando se utiliza esta opción, no se puede garantizar la integridad del sistema de archivos de la imagen creada.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

Si está copiando la instancia en una región diferente, también necesitará los siguientes permisos.

- `ec2:CopyImage`

Pasos de documentos

- `describeOriginalInstanceDetails`: recopila los detalles de la instancia que se va a copiar.
- `assertRootVolumeIsEbs` - Comprueba si el tipo de dispositivo del volumen raíz es el correcto y, de no ser así, finaliza la automatización.
- `evalInputParameters` - Evalúa los valores proporcionados para los parámetros de entrada.
- `createLocalAmi` - Crea un AMI de la instancia fuente.
- `tagLocalAmi` - Etiqueta el AMI creado en el paso anterior.

- `branchAssertRegionIsSame` - Se ramifica en función de si la instancia se está copiando dentro de la misma región o en una región diferente.
- `branchAssertSameRegionWithKeyPair` - Se ramifica en función de si se ha proporcionado un valor para el `KeyPair` parámetro de una instancia que se está copiando en la misma región.
- `sameRegionLaunchInstanceWithKeyPair` - Lanza una EC2 instancia de Amazon desde AMI de la instancia de origen en la misma subred o en la subred que especifique mediante el key pair que especificó.
- `sameRegionLaunchInstanceWithoutKeyPair` - Lanza una EC2 instancia de Amazon desde AMI de la instancia de origen en la misma subred o en la subred que especifique sin un key pair.
- `copyAmiToRegion`: copia el AMI a la región de destino.
- `waitForAvailableDestinationAmi` - Espera a que se copie AMI estado en el que se convertirá a `available`.
- `destinationRegionLaunchInstancia`: lanza una EC2 instancia de Amazon con la copia AMI.
- `branchAssertDestinationAmiToDelete` - Se ramifica en función del valor que proporcionó para el `KeepImageDestinationRegion` parámetro.
- `deregisterDestinationAmiAndDeleteSnapshots` - Anula el registro de lo copiado AMI y elimina las instantáneas asociadas.
- `branchAssertSourceAmiToDelete` - Se ramifica en función del valor que haya proporcionado para el `KeepImageSourceRegion` parámetro.
- `deregisterSourceAmiAndDeleteSnapshots` - Anula el registro del AMI se crea a partir de la instancia de origen y elimina las instantáneas asociadas.
- `sleep`: suspende la automatización durante 2 segundos. Se trata de un estado terminal.

Salidas

`sameRegionLaunchInstanceWithKeyPair.InstanceIds`

`sameRegionLaunchInstanceWithoutKeyPair.InstanceIds`

`destinationRegionLaunchInstancia.DestinationInstanceIds`

AWSPremiumSupport-DiagnoseDiskUsageOnLinux

Descripción

El `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` manual analiza los volúmenes de Amazon Elastic Block Store (Amazon EBS) de la instancia Amazon Elastic Compute Cloud (Amazon EC2) de destino para determinar si es necesario ampliarlos. Comprueba el uso, el tipo de sistema de archivos y el historial de expansión de cada volumen con respecto a los umbrales definidos en los parámetros de entrada del runbook. El script tiene en cuenta factores como las modificaciones recientes, los sistemas de archivos compatibles y los límites de AWS volumen. A continuación, muestra los volúmenes, si los hay, que son candidatos a ampliarse, junto con los detalles relevantes de cada volumen.

¿Cómo funciona?

Este manual realiza las siguientes operaciones:

- Comprueba que Systems Manager administra la instancia de destino y que no ejecuta Windows
- Recupera los detalles de la instancia, incluidos la plataforma y el tipo de dispositivo raíz
- Obtiene los volúmenes utilizados por la instancia de Amazon EC2
- Realiza comprobaciones previas en Linux para analizar el uso del disco y determinar los candidatos a la expansión
- Genera los volúmenes que son candidatos a la expansión con los detalles relevantes

Important

El acceso a `AWSPremiumSupport-*` los manuales requiere una suscripción a Business + Support, Enterprise Support o Unified Operations. Para obtener más información, consulte [Comparar planes de AWS Support](#).

[Ejecuta esta automatización \(consola\)](#)

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`
- `ec2:DescribeVolumes`

- ssm: SendCommand
- ssm: ListCommandInvocations

Ejemplo de política:

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

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSPremiumSupport-DiagnoseDiskUsageOnLinux](#) Systems Manager en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) de la función de IAM que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
 - Tipo: `AWS::IAM::Role::Arn`
 - InstanceId (Obligatorio):

- Descripción: (obligatorio) ID de la instancia Amazon EC2.
 - Tipo: `String`
 - Patrón de permiso: `^i-[0-9a-f]{8,17}$`
 - `VolumeExpansionUsageTrigger` (Obligatorio):
 - Descripción: (Obligatorio) Uso mínimo del espacio de partición necesario para activar la extensión (en porcentaje).
 - Tipo: `String`
 - Patrón de permiso: `^[0-9]{1,2}$`
 - `VolumeExpansionCapSize` (Obligatorio):
 - Descripción: (Obligatorio) Tamaño máximo al que se aumentará el volumen de Amazon EBS (en GiB).
 - Tipo: `String`
 - Patrón permitido: `^[0-9]{1,4}$`
 - `VolumeExpansionGibIncrease` (Obligatorio):
 - Descripción: (Obligatorio) Aumento del volumen en GiB. Se `VolumeExpansionPercentageIncrease` utilizará el mayor aumento neto entre `VolumeExpansionGibIncrease` y.
 - Tipo: `String`
 - Patrón de permiso: `^[0-9]{1,4}$`
 - `VolumeExpansionPercentageIncrease` (Obligatorio):
 - Descripción: (Obligatorio) Aumento porcentual del volumen. Se `VolumeExpansionPercentageIncrease` utilizará el mayor aumento neto entre `VolumeExpansionGibIncrease` y.
 - Tipo: `String`
 - Patrón de permiso: `^[0-9]{1,2}$`
4. Seleccione Ejecutar.
 5. Se inicia la automatización.
 6. Este documento realiza los siguientes pasos:
 - `AssertInstancelManagedInstance`:

Comprueba si la instancia de destino está gestionada por Systems Manager.

Describe la instancia Amazon EC2 de destino y recupera los detalles de la instancia, incluidos Platform y RootDeviceType

- BranchOnPlatform:

Se basa en el tipo de plataforma y continúa con la ejecución si es diferente de Windows.

- DescribeVolumes:

Obtiene los volúmenes utilizados por la instancia Amazon EC2.

- RunPreChecksOnLinux:

Realice las comprobaciones con los volúmenes recopilados en el paso anterior.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWSsupport-EnableWindowsEC2SerialConsole

Descripción

El manual le AWSsupport-EnableWindowsEC2SerialConsole ayuda a habilitar la consola serie Amazon EC2, la consola de administración especial (SAC) y el menú de arranque en su instancia Amazon EC2 de Windows. Con la función Amazon Elastic Compute Cloud (Amazon EC2) Serial Console, tiene acceso al puerto serie de su instancia Amazon EC2 para solucionar problemas de arranque, configuración de red y otros problemas. El manual automatiza los pasos necesarios para habilitar la función en las instancias en estado de ejecución y administradas por AWS Systems Manager, así como en las que están detenidas o no administradas por. AWS Systems Manager

¿Cómo funciona?

El manual de `AWSsupport-EnableWindowsEC2SerialConsole` automatización ayuda a habilitar el SAC y el menú de arranque en las instancias de Amazon EC2 que ejecutan Microsoft Windows Server. En el caso de las instancias en estado de ejecución y administradas por AWS Systems Manager, el runbook AWS Systems Manager ejecuta un PowerShell script Run Command para activar el SAC y el menú de arranque. En el caso de las instancias detenidas o no gestionadas por AWS Systems Manager, el runbook utiliza el [AWSsupport-StartEC2 RescueWorkflow](#) para crear una instancia temporal de Amazon EC2 a fin de realizar los cambios necesarios sin conexión.

Para obtener más información, consulte [Amazon EC2 Serial Console para instancias de Windows](#).

Important

- Si habilita SAC en una instancia, los servicios de Amazon EC2 que se basan en la recuperación de contraseñas no funcionarán desde la consola de Amazon EC2. Para obtener más información, consulte [Usar SAC para solucionar problemas de su instancia de Windows](#).
- Para configurar el acceso a la consola en serie, debe conceder el acceso a la consola en serie a nivel de cuenta y, a continuación, configurar las políticas AWS Identity and Access Management (IAM) para conceder el acceso a sus usuarios. También debe configurar un usuario basado en contraseña en cada instancia para que los usuarios puedan utilizar la consola serie para solucionar problemas. Para obtener más información, consulte [Configurar el acceso a la consola serie Amazon EC2](#).
- Para comprobar si la consola serie está habilitada en su cuenta, consulte [Ver el estado de acceso de la cuenta a la consola serie](#).
- El acceso a la consola en serie solo se admite en las instancias virtualizadas integradas en el sistema [Nitro](#).

[Para obtener más información, consulte los requisitos previos de la consola serie Amazon EC2.](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingInstances",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:Describe*",
        "ec2:createTags",
        "ec2:createImage",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "iam:GetInstanceProfile",
        "ssm:GetParameters",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ]
    }
  ]
}
```



```

    ],
    "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-02573cafcfEXAMPLE",
        "arn:aws:ec2:us-east-1:111122223333:volume/vol-049df61146EXAMPLE",
        "arn:aws:iam:111122223333:instance-profile/instance-profile-name",
        "arn:aws:ssm:us-east-1:111122223333:parameter/aws/service/*",
        "arn:aws:ssm:us-east-1:*:document/AWSSupport-StartEC2RescueWorkflow",
        "arn:aws:ssm:us-east-1:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:us-east-1:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:us-east-1:111122223333:automation-execution/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/Name": "AWSSupport-EC2Rescue: *"
        },
        "ForAllValues:StringEquals": {
            "aws:TagKeys": [
                "AWSSupport-EC2Rescue-AutomationExecution",
                "Name"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:RebootInstances",

```

```

        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ssm:SendCommand"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/Name": "AWSSupport-EC2Rescue: *"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateLaunchTemplate",
        "ec2>DeleteLaunchTemplate",
        "ec2:RunInstances"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": [
                "cloudformation.amazonaws.com"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "ssm.amazonaws.com",
                "ec2.amazonaws.com"
            ]
        }
    }
}
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta `AWSSupport-EnableWindowsEC2SerialConsole` la AWS Systems Manager consola.
2. Elija `Execute automation` (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- `Instanceld`: (Obligatorio)

El ID de la instancia de Amazon EC2 en la que desea habilitar la consola serie (SAC) y el menú de arranque de Amazon EC2.

- `AutomationAssumeRole`: (Opcional)

El nombre del recurso de Amazon (ARN) de la función de IAM que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- `HelperInstanceType`: (Condicional)

El tipo de instancia de Amazon EC2 que el runbook proporciona para configurar la consola serie Amazon EC2 para una instancia fuera de línea.

- `HelperInstanceProfileName`: (Condicional)

El nombre de un perfil de instancia de IAM existente para la instancia auxiliar. Si habilitas el SAC y el menú de arranque en una instancia que está detenida o no está gestionada por ella AWS Systems Manager, es obligatorio. Si no se especifica un perfil de instancia de IAM, la automatización crea uno en tu nombre.

- `SubnetId`: (Condicional)

El ID de subred de una instancia auxiliar. De forma predeterminada, usa la misma subred en la que reside la instancia proporcionada.

Important

Si proporciona una subred personalizada, debe estar en la misma `Instanceld` zona de disponibilidad y debe permitir el acceso a los puntos finales de Systems Manager. Esto

solo es necesario si la instancia de destino está detenida o no está gestionada por ella.
AWS Systems Manager

- `CreateInstanceBackupBeforeScriptExecution`: (Opcional)

Especifique `True` para crear una copia de seguridad de Amazon Machine Images (AMI) de la instancia Amazon EC2 antes de activar SAC y el menú de arranque. La AMI se conservará una vez terminada la automatización. Es su responsabilidad proteger el acceso a la AMI o eliminarla.

- `BackupAmazonMachineImagePrefix`: (Condicional)

Un prefijo para la Amazon Machine Image (AMI) que se crea si el `CreateInstanceBackupBeforeScriptExecution` parámetro está establecido en `True`.

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `CheckIfEc2: SerialConsoleAccessEnabled`

Comprueba si el acceso a la consola serie Amazon EC2 está habilitado a nivel de cuenta. Nota: El acceso a la consola serie no está disponible de forma predeterminada. Para obtener más información, consulte [Configurar el acceso a la consola serie Amazon EC2](#).

- `CheckIfEc2: InstanceIsWindows`

Afirma si la plataforma de la instancia de destino es Windows.

- `GetInstanceType`:

Recupera el tipo de instancia de la instancia de destino.

- `CheckIfInstanceTypeIsNitro`:

Comprueba si el hipervisor del tipo de instancia está basado en Nitro. El acceso a la consola en serie solo se admite en instancias virtualizadas creadas en el sistema Nitro.

- `CheckIfInstanceIsInAutoScalingGroup`:

Comprueba si la instancia de Amazon EC2 forma parte de un grupo de Amazon EC2 Auto Scaling mediante una llamada a la API `DescribeAutoScalingInstances`. Si la instancia forma parte de un grupo de Amazon EC2 Auto Scaling, se asegura de que la instancia de Porting Assistant para .NET esté en estado de ciclo de vida en espera.

Espera a que la instancia esté en estado de ejecución o parada.

- `GetEc2: InstanceState`

Obtiene el estado actual de la instancia.

- `BranchOnEc2InstanceState:`

Se ramifica en función del estado de la instancia recuperado en el paso anterior. Si ese estado de instancia se está ejecutando, pasa al `CheckIfEc2InstanceIsManagedBySSM` paso y, si no, va al `CheckIfHelperInstanceProfileIsProvided` paso.

- `CheckIfEc2 InstanceIsManagedBy SSM:`

Comprueba si la instancia está gestionada por AWS Systems Manager. Si se administra, el runbook habilita el SAC y el menú de arranque mediante un comando de PowerShell ejecución.

- `BranchOnPreEC2RescueBackup:`

Se ramifica según el parámetro `CreateInstanceBackupBeforeScriptExecution` de entrada.

- `CreateAmazonMachineImageBackup:`

Crea una copia de seguridad AMI de la instancia.

- `Habilita SACAndBootMenu:`

Activa el SAC y el menú de arranque mediante la ejecución de un script de PowerShell ejecución de comandos.

- `RebootInstance:`

Reinicia la instancia Amazon EC2 para aplicar la configuración. Este es el último paso si la instancia está en línea y la administra. AWS Systems Manager

- `CheckIfHelperInstanceProfileIsProvided:`

Comprueba si el `HelperInstanceProfileName` especificado existe antes de habilitar el SAC y el menú de arranque sin conexión mediante una instancia temporal de Amazon EC2.

- `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu:`

Ejecuta el menú `AWSSupport-StartEC2RescueWorkflow` para habilitar el SAC y el menú de arranque cuando la instancia está detenida o no está gestionada por AWS Systems Manager.

- `GetExecutionDetails:`

Recupera el identificador de imagen de la copia de seguridad y la salida del script sin conexión.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución:

- Habilitar SACAnd BootMenu .Salida:

Resultado de la ejecución del comando en el EnableSACAndBootMenu paso.

- GetExecutionDetails.OfflineScriptOutput:

Resultado del script fuera de línea ejecutado en el RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu paso.

- GetExecutionDetails.BackupBeforeScriptExecution:

ID de imagen de la copia de seguridad de la AMI tomada si el parámetro CreateInstanceBackupBeforeScriptExecution de entrada es True.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSPremiumSupport-ExtendVolumesOnWindows

Descripción

El AWSPremiumSupport-ExtendVolumesOnWindows manual amplía los volúmenes de Amazon Elastic Block Store (Amazon EBS), sus particiones y sistemas de archivos en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) de destino.

Consideraciones importantes

- Impacto de la operación y estados del volumen: las modificaciones del volumen de Amazon EBS se producen en tres fases: modifyingoptimizing, ycompleted. Esta automatización continúa con la extensión del sistema de archivos cuando el volumen

alcanza ese estado. **optimizing** Durante este **optimizing** estado, es posible que experimente un impacto temporal en el rendimiento y posibles interrupciones a nivel del sistema de archivos durante el cambio de tamaño de la partición. Puede [supervisar el progreso de las modificaciones de los volúmenes de Amazon EBS](#).

- **Coste y limitaciones:** aumentar el tamaño del volumen de Amazon EBS se traducirá en un aumento de los costes mensuales de almacenamiento. Para obtener más información, consulte los [precios de Amazon EBS](#). La AMI de respaldo y las instantáneas asociadas creadas por este manual incurrirán en cargos adicionales en función de su tamaño y del tiempo que las guarde. Para algunos tipos de volúmenes, si necesita mantener la misma proporción de IOPS por GB después de la expansión, es posible que tenga que modificar las IOPS aprovisionadas.
- **Backup y recuperación:** el runbook crea una AMI de respaldo antes de realizar cualquier cambio en los volúmenes. La AMI y las instantáneas asociadas no se eliminan automáticamente de su cuenta. Debe eliminar estas copias de seguridad manualmente si ya no las necesita. En caso de error, los volúmenes se pueden recuperar de las instantáneas de la AMI asociada, tal y como se describe en [Sustituir un volumen de Amazon EBS por una instantánea](#).

¿Cómo funciona?

Este manual de ejecución realiza las siguientes operaciones:

- Comprueba que la instancia de destino esté gestionada por Systems Manager y que ejecute Windows Server
- Garantiza que solo haya una ejecución de este runbook dirigida a la instancia Amazon EC2 actual
- Crea una copia de seguridad de Amazon Machine Image (AMI) desde la instancia de destino
- Amplía los volúmenes de Amazon EBS que se especificaron para la expansión
- Amplía los sistemas de archivos de la instancia de destino mediante comandos PowerShell

Important

El acceso a `AWSPremiumSupport-*` los manuales requiere una suscripción a Business + Support, Enterprise Support o Unified Operations. Para obtener más información, consulte [Comparar planes de AWS Support](#).

[Ejecuta esta automatización \(consola\)](#)

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Política de IAM de ejemplo:

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


Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSPremiumSupport-ExtendVolumesOnWindows](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) de la función de IAM que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
 - Tipo: `AWS::IAM::Role::Arn`
 - InstanceId (Obligatorio):
 - Descripción: (Obligatorio) ID de la instancia Amazon EC2.
 - Tipo: `String`
 - Patrón de permiso: `^i-[0-9a-f]{8,17}$`
 - VolumeExpansionCapSize (Obligatorio):
 - Descripción: (Obligatorio) Tamaño máximo (en GiB) en el que se aumentarán los volúmenes de Amazon EBS.
 - Tipo: `String`
 - Patrón de permisos: `^[0-9]{1,4}$`
 - DiagnosticResults (Obligatorio):
 - Descripción: (Obligatorio) Los resultados del script de comprobaciones previas del DiagnoseDiskUsage documento, con el formato de CSV de una línea. La cadena comienza con la información del EXTEND; volumen separada por comas para cada volumen, con los volúmenes separados por punto y coma. La información de cada volumen incluye: el identificador del volumen, la letra de unidad, el indicador de extensión (1 para ampliar y 0 para omitir), el nuevo tamaño en GB, la AWS región y el motivo o la acción.
 - Tipo: `String`
 - Patrón de permisos: `^EXTEND;[0-9a-zA-Z\\\.;_%:\-\/,\\s]{7,5400}$`

4. Seleccione Ejecutar

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `AssertInstanceIsManagedInstance`:

Verifica que la instancia de destino esté gestionada por Systems Manager.

- `DescribeInstance`:

Recupera la información de la plataforma de la instancia Amazon EC2 de destino.

- `BranchOnPlatform`:

Confirma que la plataforma de instancias Amazon EC2 de destino es Windows Server.

- `CheckConcurrency`:

Garantiza que solo haya una ejecución de este runbook dirigida a la instancia actual de Amazon EC2.

- `CreateImage`:

Crea una copia de seguridad de Amazon Machine Image (AMI) a partir de la instancia de destino.

- `WaitUntillImageReady`:

Espera a que la Amazon Machine Image (AMI) complete su creación y alcance el `available` estado.

- `ExtiendaEBSVolume`:

Amplía los volúmenes de Amazon EBS de la instancia de destino que se especificaron para la expansión.

- `DescribeVolumes`:

Describe los volúmenes de Amazon EBS de la instancia de destino que se especificaron para la expansión.

- `ExtendFilesystem`:

Amplía los sistemas de archivos de la instancia de destino mediante comandos PowerShell.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)
- [Solicitar modificaciones de volumen de Amazon EBS](#)

AWSSupport - ExecuteEC2Rescue

Descripción

En este manual se utiliza el EC2Rescue herramienta para solucionar problemas y, cuando sea posible, reparar problemas de conectividad comunes con la instancia de Amazon Elastic Compute Cloud (Amazon EC2) especificada para Linux o Windows Server. No se admiten instancias con volúmenes raíz cifrados.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **EC2RescueInstanceType**

Tipo: cadena

Valores permitidos: `t2.small` | `t2.medium` | `t2.large`

Valor predeterminado: `t2.small`

Descripción: (obligatorio) El tipo de EC2 instancia de EC2Rescue instancia. Tamaño recomendado: `t2.small`

- **LogDestination**

Tipo: cadena

Descripción: (opcional) nombre del bucket de Amazon S3 en la cuenta donde desea cargar los registros de solución de problemas. Asegúrese de que la política de bucket no concede permisos de lectura y escritura innecesarios a las partes que no necesitan tener acceso a los registros recopilados.

- **SubnetId**

Tipo: cadena

Predeterminado: `CreateNew VPC`

Descripción: (opcional) El ID de subred del EC2Rescue instancia. De forma predeterminada, AWS Systems Manager Automation crea una nueva VPC. De forma alternativa, utilice `SelectedInstanceSubnet` para usar la misma subred que la instancia o especifique un ID de subred personalizado.

 Important

La subred debe estar en la misma zona de disponibilidad que `UnreachableInstanceId` y debe permitir el acceso a puntos de conexión de SSM.

- **UnreachableInstanceId**

Tipo: cadena

Descripción: ID (obligatorio) de la instancia a la que no EC2 se puede acceder.

 Important

Systems Manager Automation detiene esta instancia y crea una AMI antes de intentar realizar cualquier operación. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Debe tener al menos `ssm:StartAutomationExecution` y `ssm:GetAutomationExecution` para poder leer el resultado de la automatización.

Para obtener más información sobre los permisos necesarios, consulte [AWS Support - StartEC2RescueWorkflow](#).

Pasos de documentos

1. `aws:assertAwsResourceProperty`- Afirma si la instancia proporcionada es Windows Server:
 - a. (EC2Rescue for Windows Server) Si la instancia proporcionada es una Windows Server instancia:
 - i. `aws:executeAutomation`- Invoca `AWS Support - StartEC2RescueWorkflow` con The EC2 Rescue para Windows Server guión fuera de línea.
 - ii. `aws:executeAwsApi`: recuperar el ID de AMI de copia de seguridad de la automatización anidada.
 - iii. `aws:executeAwsApi`- Recupera el resumen de EC2 Rescue de la automatización anidada.
 - b. (EC2Rescue (para Linux) Si la instancia proporcionada es una instancia de Linux:
 - i. `aws:executeAutomation`- Se invoca `AWS Support - StartEC2RescueWorkflow` con los scripts offline de EC2 Rescue for Linux
 - ii. `aws:executeAwsApi`: recuperar el ID de AMI de copia de seguridad de la automatización anidada.
 - iii. `aws:executeAwsApi`- Recupera el resumen de EC2 Rescue de la automatización anidada.

Salidas

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

Descripción

El `AWSSupport-ListEC2Resources` runbook devuelve información sobre las EC2 instancias de Amazon y los recursos relacionados, como los volúmenes de Amazon Elastic Block Store (Amazon EBS), las direcciones IP elásticas y los grupos de Amazon EC2 Auto Scaling, de los que especifique. Regiones de AWS De forma predeterminada, la información se recopila de todas las regiones y se muestra en el resultado de la automatización. Si lo desea, puede especificar un bucket de Amazon Simple Storage Service (Amazon S3) donde se cargue la información como un archivo de valores separados por comas (.csv).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

Tipo: cadena

Descripción: (opcional) el nombre del bucket de S3 donde se carga la información recopilada.

- DisplayResourceDeletionDocumentation

Tipo: cadena

Predeterminado: true

Descripción: (opcional) si se establece en true, la automatización crea enlaces en el resultado a la documentación relacionada con la eliminación de los recursos.

- RegionsToQuery

Tipo: cadena

Valor predeterminado: All

Descripción: (opcional) Las regiones de las que quieres recopilar información EC2 relacionada con Amazon.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- autoscaling:DescribeAutoScalingGroups
- ec2:DescribeAddresses
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRegions

- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

Además, para cargar correctamente la información recopilada en el bucket de S3 que especifique, el `AutomationAssumeRole` necesita realizar las siguientes acciones:

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

Pasos de documentos

- `aws:executeAwsApi`: recopila las regiones habilitadas para la cuenta.
- `aws:executeScript`: confirma que las regiones habilitadas para la cuenta admiten las regiones especificadas en el parámetro `RegionsToQuery`.
- `aws:branch`: si no hay ninguna región habilitada para la cuenta, la automatización finaliza.
- `aws:executeScript`- Muestra todas las EC2 instancias de la cuenta y las regiones que especifique.
- `aws:executeScript`: muestra todas las imágenes de máquinas de Amazon (AMI) de la cuenta y las regiones que especifique.
- `aws:executeScript`: muestra todos los volúmenes de EBS de la cuenta y las regiones que especifique.
- `aws:executeScript`: muestra todas las direcciones IP elásticas de la cuenta y las regiones que especifique.
- `aws:executeScript`: muestra todas las interfaces de red elásticas de la cuenta y las regiones que especifique.
- `aws:executeScript`: muestra todos los grupos de escalado automático de la cuenta y las regiones que especifique.
- `aws:executeScript`: muestra todos los balanceadores de carga de la cuenta y las regiones que especifique.
- `aws:executeScript`: carga la información recopilada en el bucket de S3 especificado si se proporciona un valor para el parámetro `Bucket`.

AWSSupport-ManageRDPSettings

Descripción

El manual de procedimientos de AWSSupport-ManageRDPSettings permite al usuario administrar la configuración común del protocolo de escritorio remoto (RDP), como, por ejemplo, la configuración del puerto RDP y la autenticación en el nivel de red (NLA). De forma predeterminada, el manual de procedimientos lee los valores de estos ajustes y los incluye en la salida.

Important

Los cambios en la configuración de RDP deben revisarse detenidamente antes de ejecutar este manual de procedimientos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia administrada para administrar la configuración de RDP.

- Acción de NLASetting

Tipo: cadena

Valores válidos: Check | Enable | Disable

Valor predeterminado: Check

Descripción: (obligatorio) una acción para realizar en la configuración de NLA: comprobar, habilitar, deshabilitar.

- RDPPort

Tipo: cadena

Valor predeterminado: 3389

Descripción: (opcional) especifique el nuevo puerto RDP. Solo se utiliza cuando la acción se establece en Modify. El número de puerto debe estar comprendido entre 1025 y 65535. Nota: Después de que se cambia el puerto, se reinicia el servicio de RDP.

- Acción de RDPPort

Tipo: cadena

Valores válidos: Check | Modify

Valor predeterminado: Check

Descripción: (obligatorio) una acción que aplicar al puerto RDP.

- RemoteConnections

Tipo: cadena

Valores válidos: Check | Enable | Disable

Valor predeterminado: Check

Descripción: (Obligatoria) Una acción que se debe realizar en la TSConnections configuración Denegar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

La EC2 instancia que recibe el comando debe tener una función de IAM con la política gestionada por `SSMManagedInstanceCoreAmazon` adjunta. El usuario debe tener al menos `ssm:SendCommand` para enviar el comando a la instancia, más `ssm:GetCommandInvocation` para poder leer el resultado del comando.

Pasos de documentos

`aws:runCommand`- Ejecute el PowerShell script para cambiar o comprobar la configuración de RDP en la instancia de destino.

Salidas

administrar .Output RDPSettings

AWSSupport-ManageWindowsService

Descripción

El manual de procedimientos `AWSSupport-ManageWindowsService` permite detener, iniciar, reiniciar, pausar o deshabilitar cualquier servicio de Windows en la instancia de destino.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia administrada para administrar los servicios de.

- ServiceAction

Tipo: cadena

Valores permitidos: Check | Restart | Force-Restart | Start | Stop | Force-Stop | Pause

Valor predeterminado: Check

Descripción: (obligatorio) una acción para aplicarla al servicio de Windows. Tenga en cuenta que Force-Restart y Force-Stop se pueden utilizar para reiniciar y detener un servicio que tiene servicios dependientes.

- StartupType

Tipo: cadena

Valores válidos: Comprobar | Automático | Demanda | Desactivado | DelayedAutoStart

Valor predeterminado: Check

Descripción: (obligatorio) un tipo de inicio para aplicarlo al servicio de Windows.

- WindowsServiceName

Tipo: cadena

Descripción: (obligatorio) un nombre de servicio de Windows válido.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que la EC2 instancia que recibe el comando tenga una función de IAM con la política gestionada por `SSMManagedInstanceCoreAmazon` adjunta. El usuario debe tener al menos `ssm: StartAutomationExecution` y `ssm: SendCommand` para ejecutar la automatización y enviar el comando a la instancia, además de `ssm: GetAutomationExecution` para poder leer el resultado de la automatización.

Pasos de documentos

`aws:runCommand`- Ejecute el PowerShell script para aplicar la configuración deseada al servicio de Windows en la instancia de destino.

Salidas

`manageWindowsService.Salida`

AWSSupport-MigrateEC2ClassicToVPC

Descripción

El `AWSSupport-MigrateEC2ClassicToVPC` manual migra una instancia de Amazon Elastic Compute Cloud EC2 (Amazon) de EC2 -Classic a una nube privada virtual (VPC). Este runbook admite la migración de EC2 instancias de Amazon del tipo de virtualización de máquinas virtuales de hardware (HVM) con volúmenes raíz de Amazon Elastic Block Store (Amazon EBS).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- ApproverIAM

Tipo: StringList

Descripción: (opcional) Los nombres de los recursos de Amazon (ARNs) de los usuarios de IAM que pueden aprobar o denegar la acción. Este parámetro solo se aplica si especifica un valor CutOver para el parámetro MigrationType.

- DestinationSecurityGroupId

Tipo: StringList

Descripción: (opcional) El ID del grupo de seguridad que quieres asociar a la EC2 instancia de Amazon que se lanza en tu VPC. Si no especificas un valor para este parámetro, la automatización crea un grupo de seguridad en la VPC y copia las reglas del grupo de seguridad en EC2 -Classic. Si las reglas no se copian en el nuevo grupo de seguridad, el grupo de seguridad predeterminado de la VPC se asocia a la instancia de Amazon EC2 .

- DestinationSubnetId

Tipo: cadena

Descripción: (opcional) El ID de la subred a la que quieres migrar tu EC2 instancia de Amazon. Si no especifica un valor para este parámetro, la automatización elige de forma aleatoria una subred de la VPC.

- InstanceId

Tipo: cadena

Descripción: (Obligatorio) El ID de la EC2 instancia de Amazon que quieres migrar.

- MigrationType

Tipo: cadena

Valores válidos: CutOver | Prueba

Descripción: (obligatorio) el tipo de migración que desea realizar.

La `CutOver` opción requiere aprobación para detener la EC2 instancia de Amazon que se ejecuta en EC2 -Classic. Una vez aprobada esta acción, la EC2 instancia de Amazon se detiene y la automatización crea un Amazon Machine Image (AMI). Cuando el AMI el estado es `available` que se lanza una nueva EC2 instancia de Amazon desde este AMI en el `DestinationSubnetId` que especifique en su VPC. Si la EC2 instancia de Amazon que se ejecuta en EC2 -Classic tiene una dirección IP elástica adjunta, la instancia se moverá a la EC2 instancia de Amazon recién creada en la VPC. Si la EC2 instancia de Amazon que se está lanzando en su VPC no se crea por algún motivo, se cancelará y se solicitará la aprobación para iniciar la EC2 instancia de Amazon en EC2 -Classic.

La `Test` opción crea un AMI de tu EC2 instancia de Amazon que se ejecuta en EC2 -Classic sin reiniciarse. Como la EC2 instancia de Amazon no se reinicia, no podemos garantizar la integridad del sistema de archivos de la imagen creada. Cuando el AMI el estado es `available` que se lanza una nueva EC2 instancia de Amazon desde este AMI en el `DestinationSubnetId` que especifique en su VPC. Si tu EC2 instancia de Amazon que se ejecuta en EC2 -Classic tiene una dirección IP elástica adjunta, la automatización verifica que la que `DestinationSubnetId` especifiques sea pública. Si la EC2 instancia de Amazon que se está lanzando en tu VPC no se crea por algún motivo, se cancela y finaliza la automatización.

- `SNSNotificationARNforAprobación`

Tipo: cadena

Descripción: (opcional) se establece el ARN del tema de Amazon Simple Notification Service (Amazon SNS) al que desea enviar las solicitudes de aprobación. Este parámetro solo se aplica si especifica un valor `CutOver` para el parámetro `MigrationType`.

- `TargetInstanceType`

Tipo: cadena

Predeterminado: `t2.2xlarge`

Descripción: (opcional) El tipo de EC2 instancia de Amazon que quieres lanzar en tu VPC. Solo se admiten los tipos de instancias basados en Xen, como T2, M4 o C4.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeAwsApi`- Recopila detalles sobre la EC2 instancia de Amazon que especificas en el `InstanceId` parámetro.
- `aws:assertAwsResourceProperty`: confirma que el tipo de instancia que especifica en el parámetro `TargetInstanceType` está basado en Xen.
- `aws:assertAwsResourceProperty`- Confirma que la EC2 instancia de Amazon que especificó en el `InstanceId` parámetro es del tipo de virtualización HVM.
- `aws:assertAwsResourceProperty`- Confirma que la EC2 instancia de Amazon que especificó en el `InstanceId` parámetro tiene un volumen raíz de Amazon EBS.
- `aws:executeScript`: crea un grupo de seguridad según sea necesario en función del valor que especifique para el parámetro `DestinationSecurityGroupId`.
- `aws:branch`: se ramifica en función del valor que especifique en el parámetro `DestinationSubnetId`.
- `aws:executeAwsApi`: identifica la VPC predeterminada en la Región de AWS donde se ejecuta esta automatización.
- `aws:executeAwsApi`: elige aleatoriamente el ID de una subred ubicada en la VPC predeterminada.
- `aws:createImage`- Crea un AMI sin reiniciar la instancia de Amazon EC2.
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `MigrationType`.
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `DestinationSubnetId`.
- `aws:runInstances`- Lanza una nueva instancia desde AMI creado sin reiniciar la EC2 instancia de Amazon en EC2 -Classic.
- `aws:changeInstanceState`- Termina la EC2 instancia de Amazon recién lanzada si el paso anterior falla por cualquier motivo.
- `aws:runInstances`- Lanza una nueva instancia desde AMI creado sin reiniciar la EC2 instancia de Amazon en EC2 -Classic en el `DestinationSubnetId` si se proporciona.

- `aws:changeInstanceState`- Termina la EC2 instancia de Amazon recién lanzada si el paso anterior falla por cualquier motivo.
- `aws:assertAwsResourceProperty`- Confirma el comportamiento de parada de la EC2 instancia de Amazon que se ejecuta en EC2 -Classic.
- `aws:approve`- Espera la aprobación para detener la EC2 instancia de Amazon.
- `aws:changeInstanceState`- Detiene la ejecución de la EC2 instancia de Amazon en EC2 -Classic.
- `aws:changeInstanceState`- Force detiene la EC2 instancia de Amazon que se ejecuta en EC2 -Classic si es necesario.
- `aws:createImage`- Crea un AMI de la EC2 instancia de Amazon después de que se haya detenido.
- `aws:branch`: se ramifica en función del valor especificado para el parámetro `DestinationSubnetId`.
- `aws:runInstances`- Lanza una nueva instancia desde AMI creado a partir de la EC2 instancia de Amazon detenida en EC2 -Classic.
- `aws:approve`- Espera la aprobación para finalizar la instancia recién lanzada e inicia la instancia de Amazon EC2 en EC2 -Classic si el paso anterior falla por algún motivo.
- `aws:changeInstanceState`- Termina la EC2 instancia de Amazon recién lanzada.
- `aws:runInstances`- Lanza una nueva instancia desde AMI creado a partir de la EC2 instancia de Amazon detenida en EC2 -Classic a partir del `DestinationSubnetId` parámetro.
- `aws:approve`- Espera la aprobación para finalizar la instancia recién lanzada e inicia la instancia de Amazon EC2 en EC2 -Classic si el paso anterior falla por algún motivo.
- `aws:changeInstanceState`- Termina la EC2 instancia de Amazon recién lanzada.
- `aws:changeInstanceState`- Inicia la EC2 instancia de Amazon que se detuvo en EC2 -Classic.
- `aws:branch`- Se ramifica en función de si la EC2 instancia de Amazon tiene una dirección IP pública.
- `aws:executeAwsApi`: verifica si la dirección IP pública es una dirección IP elástica.
- `aws:branch`: se ramifica en función del valor que especifique en el parámetro `MigrationType`.
- `aws:executeAwsApi`: mueve la dirección IP elástica a la VPC.
- `aws:executeAwsApi`: recopila el ID de asignación de la dirección IP elástica que se trasladó a la VPC.

- `aws:branch`- Se ramifica en función de la subred en la que se lanzó la EC2 instancia de Amazon que se ejecuta en la VPC.
- `aws:executeAwsApi`: adjunta la dirección IP elástica a la instancia recién lanzada en la VPC.
- `aws:executeScript`- Confirma que la subred que acaba de lanzar su EC2 instancia de Amazon y que se ejecuta en su VPC es pública.

Salidas

`getInstanceProperties.virtualizationType`: el tipo de virtualización de la EC2 instancia de Amazon que se ejecuta en EC2 -Classic.

`getInstanceProperties.rootDeviceType`- El tipo de dispositivo raíz de la EC2 instancia de Amazon que se ejecuta en EC2 -Classic.

`createAMIWithoutReboot.ImageId`- El ID del AMI creado sin reiniciar la EC2 instancia de Amazon que se ejecuta en EC2 -Classic.

`getDefaultVPC.VpcId`- El ID de la VPC predeterminada en la que se lanza la nueva EC2 instancia de Amazon si no se proporciona un valor para el `DestinationSubnetId` parámetro.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`- El ID de la subred de la VPC predeterminada en la que se lanza la nueva instancia de EC2 Amazon si no se proporciona un valor para `DestinationSubnetId` el parámetro.

`launchTestInstanceDefaultVPC.InstanceIds`- El ID de la EC2 instancia de Amazon recién lanzada en tu VPC predeterminada durante el tipo de Test migración.

`launchTestInstanceProvidedSubnet.InstanceIds`- El ID de la EC2 instancia de Amazon recién lanzada `DestinationSubnetId` que especificó durante el tipo de Test migración.

`createAMIAfterStoppingInstance.ImageId`- El ID de la AMI creado después de detener la ejecución de la EC2 instancia de Amazon en EC2 -Classic.

`launchCutOverInstanceProvidedSubnet.InstanceIds`- El ID de la EC2 instancia de Amazon recién lanzada `DestinationSubnetId` que especificó durante el tipo de CutOver migración.

`launchCutOverInstanceDefaultVPC.InstanceIds`- El ID de la EC2 instancia de Amazon recién lanzada en tu VPC predeterminada durante el tipo de CutOver migración.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`: si la subred elegida por la automatización en tu VPC predeterminada es pública.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`: si la subred que especificó en `DestinationSubnetId` es pública.

AWSSupport-MigrateXenToNitroLinux

Descripción

El `AWSSupport-MigrateXenToNitroLinux` runbook clona, prepara y migra una instancia de Amazon Elastic Compute Cloud EC2 (Amazon) Linux Xen a una [Nitro tipo de instancia](#). Este manual de procedimientos ofrece dos opciones para los tipos de operaciones:

- **Clone&Migrate**— El flujo de trabajo de esta opción consiste en las comprobaciones preliminares, las pruebas y `Clone&Migrate` fases. El flujo de trabajo se ejecuta mediante el manual de procedimientos `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro`.
- **FullMigration**: esta opción ejecuta el flujo de trabajo de `Clone&Migrate` y, a continuación, realiza el paso adicional de reemplazar los volúmenes raíz de Amazon EBS.

Important

El uso de este runbook supone costes para su cuenta por el tiempo de ejecución de las EC2 instancias de Amazon, la creación de volúmenes de Amazon Elastic Block Store (Amazon EBS) y AMLs. Para obtener más información, consulte [Amazon EC2 Pricing](#) y [Amazon EBS Pricing](#).

Controles preliminares

La automatización realiza las siguientes comprobaciones preliminares antes de continuar con la migración. Si alguna de las comprobaciones falla, la automatización finaliza. Esta fase es solo una parte del flujo de trabajo de `Clone&Migrate`.

- Comprueba si la instancia de destino ya es una Nitro tipo de instancia.
- Comprueba si se utilizó la opción de compra de instancias de spot para la instancia de destino.
- Comprueba si los volúmenes del almacén de instancias están adjuntos a la instancia de destino.
- Comprueba si el sistema operativo (SO) de la instancia de destino es Linux.

- Comprueba si la instancia de destino forma parte de un grupo de Amazon EC2 Auto Scaling. Si forma parte de un grupo de escalado automático, la automatización verifica si la instancia se encuentra en el estado `standby`.
- Verifica que la instancia esté gestionada por AWS Systems Manager.

Pruebas

La automatización crea un Amazon Machine Image (AMI) desde la instancia de destino y lanza una instancia de prueba a partir de la recién creada AMI. Esta fase forma parte únicamente del `Clone&Migrate` flujo de trabajo.

Si la instancia de prueba supera todas las comprobaciones de estado, la automatización se detiene y se solicita la aprobación de los directores designados mediante una notificación de Amazon Simple Notification Service (Amazon SNS). Si se aprueba, la automatización finaliza la instancia de prueba, detiene la instancia de destino y continúa con la migración, mientras se crea la nueva AMI se anula del registro al final del flujo de trabajo. `Clone&Migrate`

Note

Antes de conceder la aprobación, recomendamos comprobar que todas las aplicaciones que se ejecutan en la instancia de destino se hayan cerrado correctamente.

Clonar y migrar

La automatización crea otra AMI desde la instancia de destino y lanza una nueva instancia para cambiarla a una Nitro tipo de instancia. La automatización cumple los siguientes requisitos previos antes de continuar con la migración. Si alguna de las comprobaciones falla, la automatización finaliza. Esta fase también es solo una parte del flujo de trabajo de `Clone&Migrate`.

- Activa el atributo de red mejorada (ENA).
- Instala la versión más reciente de los controladores ENA si aún no están instalados, o actualiza la versión de los controladores ENA a la versión más reciente. Para garantizar el máximo rendimiento de la red, es necesario actualizar a la última versión del controlador ENA si Nitro el tipo de instancia es de sexta generación.
- Verifica que el NVMe módulo esté instalado. Si el módulo está instalado, la automatización verifica si el módulo está cargado en `initramfs`.

- Analiza `/etc/fstab` y reemplaza las entradas con los nombres de los dispositivos de bloques (`/dev/sd*o/dev/xvd*`) con sus respectivos UUIDs nombres. Antes de modificar la configuración, la automatización crea una copia de seguridad del archivo en la ruta `/etc/fstab*`.
- Desactiva la nomenclatura predecible de la interfaz añadiendo la opción `net.ifnames=0` a la línea `GRUB_CMDLINE_LINUX` del archivo `/etc/default/grub`, si existe, o al núcleo en `/boot/grub/menu.lst`.
- Elimina el archivo `/etc/udev/rules.d/70-persistent-net.rules` si existe. Antes de eliminar el archivo, la automatización crea una copia de seguridad del archivo en la ruta `/etc/udev/rules.d/`.

Después de verificar todos los requisitos, el tipo de instancia se cambia a Nitro tipo de instancia que especifique. La automatización espera a que la instancia recién creada pase todas las comprobaciones de estado después de empezar como Nitro tipo de instancia. A continuación, la automatización espera la aprobación de los directores designados para crear un AMI de los lanzados con éxito Nitro instancia. Si se deniega la aprobación, la automatización finaliza, dejando la instancia recién creada en ejecución y la instancia de destino permanece detenida.

Reemplazar un volumen de Amazon EBS

Si eliges `FullMigration` como `OperationType`, la automatización migra la EC2 instancia de Amazon de destino a la Nitro tipo de instancia que especifiques. La automatización solicita la aprobación de los directores designados para reemplazar el volumen raíz de Amazon EBS de la EC2 instancia de Amazon de destino por el volumen raíz de la instancia de EC2 Amazon clonada. Cuando la migración se haya realizado correctamente, la EC2 instancia de Amazon clonada finalizará. Si la automatización falla, el volumen raíz original de Amazon EBS se adjunta a la EC2 instancia de Amazon de destino. Si el volumen raíz de Amazon EBS adjunto a la EC2 instancia de Amazon de destino tiene etiquetas con el `aws:` prefijo aplicado, no se admite la `FullMigration` operación.

Antes de empezar

La instancia de destino debe tener acceso saliente a Internet. Esto sirve para acceder a los repositorios de controladores y dependencias, como `kernel-devel`, `gcc`, `patch`, `rpm-build`, `wget`, `dracut`, `make`, `linux-headers`, y `unzip`. Si es necesario, se usa el administrador de paquetes.

Se requiere un tema de Amazon SNS para enviar notificaciones de aprobaciones y actualizaciones. Para obtener más información acerca de la creación de un tema Amazon SNS, consulte [Creating an Amazon SNS topic](#) (Creación de un tema de Amazon SNS) en la Guía para desarrolladores de Amazon Simple Notification Service.

Este manual de procedimientos admite los siguientes sistemas operativos:

- RHEL 7.x - 8.5
- Amazon Linux (2018.03), Amazon Linux 2
- Servidor Debian
- Ubuntu Server 18.04 LTS, 20.04 LTS, and 20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5, SUSE15SP2)

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Reconocimiento

Tipo: cadena

Descripción: (obligatorio) lea los detalles completos de las acciones realizadas por este manual de procedimientos e introduzca **Yes, I understand and acknowledge** para continuar con el uso del manual.

- ApproverIAM

Tipo: cadena

Descripción: (Obligatorio) Los roles, usuarios o nombres ARNs de usuario de IAM que pueden aprobar la automatización. Puede especificar un máximo de 10 aprobadores.

- DeleteResourcesOnFailure

Tipo: Booleano

Descripción: (opcional) Determina si la instancia recién creada y AMI para la migración se eliminan si se produce un error en la automatización.

Valores válidos: True | False

Valor predeterminado: True

- MinimumRequiredApprovals

Tipo: cadena

Descripción: (opcional) el número mínimo de aprobaciones necesario para seguir ejecutando la automatización cuando se solicitan aprobaciones.

Valores válidos: 1-10

Valor predeterminado: 1

- NitroInstanceType

Tipo: cadena

Descripción: (Obligatorio) El Nitro tipo de instancia al que desea cambiar la instancia. Los tipos de instancias compatibles incluyen M5, M6, C5, C6, R5, R6 y T3.

Predeterminado: m5.xlarge

- OperationType

Tipo: cadena

Descripción: (obligatorio) la operación que desea realizar. La opción FullMigration realiza las mismas tareas que Clone&Migrate y reemplaza el volumen raíz de la instancia de destino. Tras el proceso de migración, el volumen raíz de la instancia de destino se sustituye por el volumen

raíz de la instancia recién creada. La operación `FullMigration` no admite los volúmenes raíz definidos por Logical Volume Manager (LVM).

Valores válidos: `Clone&Migrate` | `FullMigration`

- `SNSTopicArn`

Tipo: cadena

Descripción: (obligatorio) el ARN del tema de SNS para que se notifique la aprobación. El tema Amazon SNS se utiliza para enviar las notificaciones de aprobación obligatorias durante la automatización.

- `TargetInstanceIds`

Tipo: cadena

Descripción: (Obligatorio) El ID de las EC2 instancias de Amazon que se van a migrar.

Clone&Migrate flujo de trabajo

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `startOfPreliminaryChecksBranch`: se ramifica al flujo de trabajo de las comprobaciones preliminares.
- `getTargetInstanceProperties`: recopila detalles de la instancia de destino.
- `checkIfNitroInstanceTypeIsSupportedInAZ`- Determina si el tipo de EC2 instancia de Amazon de destino se admite en la misma zona de disponibilidad que la instancia de destino.
- `getXenInstanceTypeDetails`: recopila detalles sobre el tipo de instancia de origen.
- `checkIfInstanceHypervisorIsNitroAlready`- Comprueba si la instancia de destino ya se está ejecutando como Nitro tipo de instancia.
- `checkIfTargetInstanceLifecycleIsSpot`: comprueba si la opción de compra de la instancia de destino es Spot.
- `checkIfOperatingSystemIsLinux`: comprueba si el sistema operativo de la instancia de destino es Linux.
- `verifySSMConnectivityForTargetInstance`: verifica que la instancia de destino esté gestionada por Systems Manager.

- `checkIfEphemeralVolumeAreSupported`: comprueba si el tipo de instancia actual de la instancia de destino admite los volúmenes de almacén de instancias.
- `verifyIfTargetInstanceHasEphemeralVolumesAttached`: comprueba si la instancia de destino tiene volúmenes de almacenamiento de instancias adjuntos.
- `checkIfRootVolumeIsEBS`: comprueba si el tipo de volumen raíz de la instancia de destino es EBS.
- `checkIfTargetInstanceIsInASG`: comprueba si la instancia de destino forma parte de un grupo de escalado automático.
- `endOfPreliminaryChecksBranch`: fin de la rama de comprobaciones preliminares.
- `startOfTestBranch`: se ramifica en el flujo de trabajo de las pruebas.
- `createTestImage`- Crea una prueba AMI de la instancia de destino.
- `launchTestInstanceInSameSubnet`- Lanza una instancia de prueba a partir de la prueba AMI utilizando la misma configuración que la instancia de destino.
- `cleanupTestInstance`: termina la instancia de prueba.
- `endOfTestBranch`: fin de la rama de pruebas.
- `checkIfTestingBranchSucceeded`: comprueba el estado de la rama de pruebas.
- `approvalToStopTargetInstance`: espera la aprobación de los directores designados para detener la instancia de destino.
- `stopTargetEC2Instance`: detiene la instancia de destino.
- `forceStopTargetEC2Instance`: la fuerza detiene la instancia de destino solo si el paso anterior no logra detenerla.
- `startOfCloneAndMigrateBranch`- Se ramifica al Clone&Migrate flujo de trabajo.
- `createBackupImage`- Crea un AMI de la instancia de destino para que sirva de respaldo.
- `launchInstanceInSameSubnet`- Lanza una nueva instancia desde la copia de seguridad AMI utilizando la misma configuración que la instancia de origen.
- `waitForClonedInstanceToPassStatusChecks`: espera a que la instancia recién creada pase todas las comprobaciones de estado.
- `verifySSMConnectivityForClonedInstance`: verifica que la instancia recién creada esté gestionada por Systems Manager.
- `checkAndInstallENADrivers`: comprueba si los controladores ENA están instalados en la instancia recién creada e instala los controladores si es necesario.

- `checkAndAddNVMEDrivers`- Comprueba si NVMe los controladores están instalados en la instancia recién creada e instala los controladores si es necesario.
- `checkAndModifyFSTABEntries`- Comprueba si se utilizan nombres de dispositivos `/etc/fstab` y los sustituye por otros UUIDs si es necesario.
- `stopClonedInstance`: detiene la instancia recién creada.
- `forceStopClonedInstance`: fuerza la detención de la instancia recién creada solo si el paso anterior no logra detenerla.
- `checkENAAtributeForClonedInstance`: comprueba si el atributo de red mejorado está activado en la instancia recién creada.
- `setNitroInstanceTypeForClonedInstance`- Cambia el tipo de instancia de la instancia recién creada a Nitro tipo de instancia que especifique.
- `startClonedInstance`: inicia la instancia recién creada cuyo tipo de instancia ha cambiado.
- `approvalForCreatingImageAfterDriversInstallation`- Si la instancia se inicia correctamente como Nitro en el tipo de instancia, la automatización espera la aprobación de los directores necesarios. Si se proporciona la aprobación, un AMI está creado para ser utilizado como Golden AMI.
- `createImageAfterDriversInstallation`- Crea un AMI para ser usado como dorado AMI.
- `endOfCloneAndMigrateBranch`- Fin de Clone&Migrate sucursal.
- `cleanupTestImage`- Anula el registro del AMI creado para pruebas.
- `failureHandling`: comprueba si ha optado por cancelar los recursos en caso de fallo.
- `onFailureTerminateClonedInstance`: termina la instancia recién creada si se produce un error en la automatización.
- `onFailurecleanupTestImage`- Anula el registro del AMI creado para pruebas.
- `onFailureApprovalToStartTargetInstance`: si la automatización falla, espera la aprobación de los directores designados para iniciar la instancia de destino.
- `onFailureStartTargetInstance`: si la automatización falla, inicia la instancia de destino.

FullMigration flujo de trabajo

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

El flujo de trabajo de `FullMigration` ejecuta los mismos pasos que el flujo de trabajo de `Clone&Migrate` y, además, realiza los siguientes pasos:

- `checkConcurrency`- Verifica que solo haya una automatización de este runbook dirigida a la EC2 instancia de Amazon que especifiques. Si el manual de procedimientos encuentra otra automatización en curso dirigida a la misma instancia, la automatización finaliza.
- `getTargetInstanceProperties`: recopila detalles de la instancia de destino.
- `checkRootVolumeTags`- Determina si el volumen raíz de la EC2 instancia de Amazon de destino contiene etiquetas AWS reservadas.
- `cloneTargetInstanceAndMigrateToNitro`: inicia una automatización secundaria utilizando el manual de procedimientos `AWS-CloneXenInstanceToNitro`.
- `branchOnTheOperationType`: se ramifica según el valor que especifique para el parámetro `OperationType`.
- `getClonedInstanceId`: recupera el ID de la instancia recién lanzada de la automatización secundaria.
- `checkIfRootVolumeIsBasedOnLVM`: determina si la partición raíz está gestionada por LVM.
- `branchOnTheRootVolumeLVMStatus`: si se reciben las aprobaciones mínimas requeridas por parte de los directores, la automatización continúa con la sustitución del volumen raíz.
- `manualInstructionsInCaseOfLVM`: si LVM administra el volumen raíz, la automatización envía un resultado que contiene instrucciones sobre cómo reemplazar manualmente los volúmenes raíz.
- `startOfReplaceRootEBSVolumeBranch`: inicia el flujo de trabajo de la rama Reemplazar el volumen raíz de EBS.
- `checkIfTargetInstanceIsManagedByCFN`- Determina si la instancia de destino está gestionada por una AWS CloudFormation pila.
- `branchOnCFNStackStatus`- Se ramifica en función del estado de la CloudFormation pila.
- `approvalForRootVolumesReplacement(WithCFN)`- Si la instancia de destino fue lanzada por CloudFormation, la automatización espera su aprobación después de que la instancia recién lanzada se inicie correctamente como Nitro tipo de instancia. Cuando se proporcionan las aprobaciones, los volúmenes de Amazon EBS de la instancia de destino se sustituyen por los volúmenes raíz de la instancia recién lanzada.
- `approvalForRootVolumesReplacement`- Espera la aprobación después de que la instancia recién lanzada se inicie correctamente como Nitro tipo de instancia. Cuando se proporcionan las

aprobaciones, los volúmenes de Amazon EBS de la instancia de destino se sustituyen por los volúmenes raíz de la instancia recién lanzada.

- `assertIfTargetEC2InstanceIsStillStopped`: verifica que la instancia de destino esté en estado `stopped` antes de reemplazar el volumen raíz.
- `stopTargetInstanceForRootVolumeReplacement`: si la instancia de destino está en ejecución, la automatización detiene la instancia antes de reemplazar el volumen raíz.
- `forceStopTargetInstanceForRootVolumeReplacement`: la instancia de destino se detiene por la fuerza si se produce un error en el paso anterior.
- `stopClonedInstanceForRootVolumeReplacement`: detiene la instancia recién creada antes de sustituir los volúmenes de Amazon EBS.
- `forceStopClonedInstanceForRootVolumeReplacement`: fuerza la detención de la instancia recién creada si se produce un error en el paso anterior.
- `getBlockDeviceMappings`: recupera las asignaciones de dispositivos de bloques tanto para las instancias de destino como para las recién creadas.
- `replaceRootEbsVolumes`: sustituye el volumen raíz de la instancia de destino por el volumen raíz de la instancia recién creada.
- `EndOfReplaceRootEBSVolumeBranch`: finalización del flujo de trabajo de la rama `Replace Root EBS Volume`.
- `checkENAAttributeForTargetInstance`- Comprueba si el atributo de red mejorada (ENA) está activado para la EC2 instancia de Amazon de destino.
- `enableENAAttributeForTargetInstance`- Activa el atributo ENA para la EC2 instancia de Amazon de destino si es necesario.
- `setNitroInstanceTypeForTargetInstance`- Cambia la instancia de destino a Nitro tipo de instancia que especifique.
- `replicateRootVolumeTags`- Replica las etiquetas del volumen raíz de Amazon EBS de la instancia de Amazon EC2 de destino.
- `startTargetInstance`- Inicia la EC2 instancia de Amazon de destino tras cambiar el tipo de instancia.
- `onFailureStopTargetEC2Instance`- Detiene la EC2 instancia de Amazon de destino si no se inicia como Nitro tipo de instancia.
- `onFailureForceStopTargetEC2Instance`- Force detiene la EC2 instancia de Amazon de destino si se produce un error en el paso anterior.

- `OnFailureRevertOriginalInstanceType`- Revierte la EC2 instancia de Amazon de destino al tipo de instancia original si la instancia de destino no se inicia como Nitro tipo de instancia.
- `onFailureRollbackRootVolumeReplacement`: si es necesario, revierte todos los cambios realizados por el paso `replaceRootEbsVolumes`.
- `onFailureApprovalToStartTargetInstance`- Espera la aprobación del director designado para iniciar la EC2 instancia de Amazon de destino tras anular los cambios anteriores.
- `onFailureStartTargetInstance`- Inicia la EC2 instancia de Amazon de destino.
- `terminateClonedEC2Instance`- Finaliza la EC2 instancia de Amazon clonada tras sustituir el volumen raíz de Amazon EBS.

AWSSupport-ResetAccess

Descripción

Este runbook utilizará la herramienta EC2 Rescue en la EC2 instancia especificada para volver a habilitar el descifrado de contraseñas mediante la EC2 consola (Windows) o para generar y añadir un nuevo key pair de claves SSH (Linux). Si ha perdido el par de claves, esta automatización creará una AMI con contraseña que podrá utilizar para lanzar una EC2 nueva instancia con un par de claves de su propiedad (Windows).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- EC2RescueInstanceType

Tipo: cadena

Valores permitidos: t2.small | t2.medium | t2.large

Valor predeterminado: t2.small

Descripción: (obligatorio) El tipo de EC2 instancia de la instancia de EC2 Rescue. Tamaño recomendado: t2.small.

- InstanceId

Tipo: cadena

Descripción: ID (obligatorio) de la EC2 instancia a la que quieres restablecer el acceso.

 Important

Systems Manager Automation detiene esta instancia y crea una AMI antes de intentar realizar cualquier operación. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.

- SubnetId

Tipo: cadena

Predeterminado: CreateNew VPC

Descripción: (opcional) El ID de subred de la instancia de EC2 Rescue. De forma predeterminada, Systems Manager Automation crea una nueva VPC. También puedes SelectedInstanceSubnet usar la misma subred que la instancia o especificar un ID de subred personalizado.

 Important

La subred debe estar en la misma InstanciaId zona de disponibilidad y debe permitir el acceso a los puntos finales del SSM.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Debe tener al menos `ssm:StartAutomationExecution`, `ssm: GetParameter` (para recuperar el nombre del parámetro clave SSH) y `ssm: GetAutomationExecution` para poder leer el resultado de la automatización. Para obtener más información sobre los permisos necesarios, consulte [AWSSupport-StartEC2RescueWorkflow](#).

Pasos de documentos

1. `aws:assertAwsResourceProperty`: afirma si la instancia proporcionada es Windows.
 - a. (EC2Rescue para Windows) Si la instancia proporcionada es Windows:
 - i. `aws:executeAutomation`- Invoque `AWSSupport-StartEC2RescueWorkflow` con el script de restablecimiento de contraseña sin conexión de EC2 Rescue for Windows
 - ii. `aws:executeAwsApi`: recupera el ID de AMI de copia de seguridad de la automatización anidada.
 - iii. `aws:executeAwsApi`: recuperar el ID de AMI habilitada para contraseña de la automatización anidada.
 - iv. `aws:executeAwsApi`- Recupera el resumen de EC2 Rescue de la automatización anidada
 - b. (EC2Rescue para Linux) Si la instancia proporcionada es Linux:
 - i. `aws:executeAutomation`- Invoque `AWSSupport-StartEC2RescueWorkflow` con el script de inyección de claves SSH fuera de línea de EC2 Rescue for Linux
 - ii. `aws:executeAwsApi`: recupera el ID de AMI de copia de seguridad de la automatización anidada.
 - iii. `aws:executeAwsApi`: recupera el nombre de parámetro de SSM para la clave SSH inyectada.
 - iv. `aws:executeAwsApi`- Recupera el resumen de EC2 Rescue de la automatización anidada

Salidas

obtener .Output EC2 RescueForWindowsResult

getWindowsBackupAmi. ImageId

getWindowsPasswordEnabledAmi.ImageId

obtener EC2 RescueForLinuxResult .Output

getLinuxBackupAmi. ImageId

GetLinux Parameter.Name SSHKey

AWSsupport-ResetLinuxUserPassword

Descripción

El manual de procedimientos AWSsupport-ResetLinuxUserPassword le ayuda a restablecer la contraseña de un usuario del sistema operativo (SO) local. Este manual de procedimientos es especialmente útil para los usuarios que necesitan acceder a sus instancias de Amazon Elastic Compute Cloud (Amazon EC2) mediante la consola de serie. El runbook crea una instancia temporal de Amazon EC2 en Cuenta de AWS usted con un rol AWS Identity and Access Management generado automáticamente (IAM) o un perfil de instancia de IAM personalizado que especifique. El perfil de instancia personalizado (IAM) debe tener permisos para recuperar el valor AWS Secrets Manager secreto que contiene la contraseña.

El manual de procedimientos detiene la instancia de Amazon EC2 de destino, separa el volumen raíz de Amazon Elastic Block Store (Amazon EBS) y lo conecta a la instancia de Amazon EC2 temporal. Con Run Command, se ejecuta un script en la instancia temporal para establecer la contraseña del usuario del sistema operativo que especifique. A continuación, el volumen raíz de Amazon EBS se vuelve a adjuntar a la instancia de destino. El manual de procedimientos también ofrece una opción para crear una instantánea del volumen raíz al comienzo de la automatización.

Antes de empezar

Cree un secreto de Secrets Manager con el valor de la contraseña que desee asignar al usuario de su sistema operativo. El valor debe estar en texto sin formato. Para obtener más información, consulte [Crear un secreto de AWS Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager .

Consideraciones

- Recomendamos hacer una copia de seguridad de la instancia antes de usar este manual de procedimientos. Considere la posibilidad de establecer el valor del parámetro `CreateSnapshot` como **Yes**.
- Para cambiar la contraseña del usuario local, es necesario que el manual de procedimientos detenga la instancia. Los datos guardados en la memoria o en el almacén de instancias se perderán cuando se detenga una instancia. Además, se liberarán todas IPv4 las direcciones públicas que se asignen automáticamente. Para obtener más información sobre lo que ocurre cuando detiene una instancia, consulte [Detener e iniciar la instancia](#) en la Guía del usuario de Amazon EC2.
- Si los volúmenes de Amazon EBS adjuntos a su instancia Amazon EC2 de destino están cifrados con una clave AWS Key Management Service gestionada por el cliente AWS KMS(), asegúrese de que AWS KMS la clave `deleted` no lo esté `disabled` o la instancia no podrá iniciarse.
- El uso de un perfil de instancia de IAM personalizado requiere `AutomationAssumeRole` tener `GetInstanceProfile` permiso de IAM para la validación, y el propio perfil de instancia personalizado debe incluir los permisos de acceso a Systems Manager y Secrets Manager. El manual valida la existencia del perfil de instancia por adelantado, pero fallará durante las operaciones de la instancia auxiliar si el perfil de la instancia no tiene el acceso necesario.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia Linux Amazon EC2 que contiene la contraseña de usuario del sistema operativo que desea restablecer.

- LinuxUserName

Tipo: cadena

Predeterminado: ec2-user

Descripción: (opcional) la cuenta de usuario del sistema operativo cuya contraseña desea restablecer.

- SecretArn

Tipo: cadena

Descripción: (obligatorio) el ARN del secreto de Secrets Manager que contiene la nueva contraseña.

- SecurityGroupId

Tipo: cadena

Descripción: (opcional) el ID del grupo de seguridad que se va a asociar a la instancia de Amazon EC2 temporal. Si no proporciona un valor para este parámetro, se usa el grupo de seguridad Amazon Virtual Private Cloud (Amazon VPC) predeterminado.

- SubnetId

Tipo: cadena

Descripción: (opcional) el ID de la subred en la que desea lanzar la instancia temporal de Amazon EC2. De forma predeterminada, la automatización elige la misma subred que la instancia de destino. Si elige proporcionar una subred diferente, debe estar en la misma zona de disponibilidad que la instancia de destino y tener acceso a los puntos de enlace de Systems Manager.

- CreateSnapshot

Tipo: cadena

Valores válidos: Yes | No

Valor predeterminado: Yes

Descripción: (opcional) determina si se crea una instantánea del volumen raíz de la instancia Amazon EC2 de destino antes de que se ejecute la automatización.

- StopConsent

Tipo: cadena

Valores válidos: Yes | No

Valor predeterminado: No

Descripción: introduzca **Yes** para confirmar que su instancia Amazon EC2 de destino se detendrá durante esta automatización. Cuando se detiene la instancia Amazon EC2, se pierden todos los datos almacenados en la memoria o en los volúmenes del almacén de instancias y se libera la IPv4 dirección pública automática. Para obtener más información, consulte [Detener e iniciar la instancia](#) en la Guía del usuario de Amazon EC2.

- InstanceProfileName

Tipo: cadena

Descripción: (opcional) El nombre del perfil de instancia de IAM que se va a adjuntar a la instancia auxiliar de Amazon EC2. Si no se proporciona, se creará automáticamente un perfil de instancia temporal con los permisos necesarios. El perfil de instancia personalizado debe tener permisos para acceder al secreto de Secrets Manager y a Systems Manager especificados.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:DescribeInstanceInformation
- ssm:ListTagsForResource
- ssm:SendCommand

- `ec2:AttachVolume`
- `ec2:CreateSnapshot`
- `ec2:CreateSnapshots`
- `ec2:CreateVolume`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeSnapshotAttribute`
- `ec2:DescribeSnapshots`
- `ec2:DescribeSnapshotTierStatus`
- `ec2:DescribeVolumes`
- `ec2:DescribeVolumeStatus`
- `ec2:DetachVolume`
- `ec2:RunInstances`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `ec2:TerminateInstances`
- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:ListStacks`
- `logs:CreateLogDelivery`
- `logs:CreateLogGroup`
- `logs>DeleteLogDelivery`
- `logs>DeleteLogGroup`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:PutLogEvents`
- `iam:GetInstanceProfile`

Pasos de documentos

1. `aws:branch`: se ramifica en función de si ha dado su consentimiento para detener la instancia Amazon EC2 de destino.
2. `aws:assertAwsResourceProperty`— Garantiza que el estado de la instancia Amazon EC2 esté en estado `running` o `stopped`. De lo contrario, la automatización finaliza.
3. `aws:executeAwsApi`— Obtiene las propiedades de la instancia Amazon EC2.
4. `aws:executeAwsApi`— Obtiene las propiedades del volumen raíz.
5. `aws:branch`— Ramifica la automatización en función de si se proporcionó un ID de subred para la instancia temporal de Amazon EC2.
6. `aws:assertAwsResourceProperty`— Garantiza que la subred que especifique en el `SubnetId` parámetro esté en la misma zona de disponibilidad que la instancia Amazon EC2 de destino.
7. `aws:assertAwsResourceProperty`— Garantiza que el volumen raíz de la instancia Amazon EC2 de destino sea un volumen de Amazon EBS.
8. `aws:assertAwsResourceProperty`— Garantiza que la arquitectura de la instancia Amazon EC2 sea `arm64` o `x86_64`.
9. `aws:assertAwsResourceProperty`— Garantiza que el comportamiento de cierre de la instancia de Amazon EC2 sea `stop` o no. `terminate`.
10. `aws:branch`— Garantiza que la instancia Amazon EC2 no sea una instancia puntual. De lo contrario, la automatización finaliza.
11. `aws:executeScript`— Garantiza que la instancia de Amazon EC2 no forme parte de un grupo de autoescalado. Si la instancia forma parte de un grupo de escalado automático, la automatización confirma que la instancia de Amazon EC2 se encuentra en un estado `Standby` de ciclo de vida.
12. `aws:branch`— Ramifica la automatización en función de si se proporcionó o no un nombre de perfil de instancia de IAM personalizado.
13. `aws:assertAwsResourceProperty`— Garantiza la existencia del perfil de instancia de IAM personalizado y valida que su nombre coincida con el parámetro de entrada.
14. `aws:createStack`— Crea una instancia Amazon EC2 temporal que se utiliza para restablecer la contraseña del usuario del sistema operativo que especifique.
15. `aws:waitForAwsResourceProperty`— Espera a que se ejecute la instancia temporal de Amazon EC2 recién lanzada.

- 16 `aws:executeAwsApi`— Obtiene el ID de la instancia temporal de Amazon EC2.
- 17 `aws:waitForAwsResourceProperty`— Espera a que la instancia temporal de Amazon EC2 muestre que está gestionada por Systems Manager.
- 18 `aws:changeInstanceState`— Detiene la instancia Amazon EC2 de destino.
- 19 `aws:changeInstanceState`— Obliga a la instancia Amazon EC2 de destino a detenerse en caso de que se quede atascada en un estado de parada.
- 20 `aws:branch`— Ramifica la automatización en función de si se solicitó una instantánea del volumen raíz de la instancia Amazon EC2 de destino.
- 21 `aws:executeAwsApi`— Crea una instantánea del volumen raíz de Amazon EBS de la instancia Amazon EC2 de destino.
- 22 `aws:waitForAwsResourceProperty`— Espera a que la instantánea esté en un estado `completed`.
- 23 `aws:executeAwsApi`— Separa el volumen raíz de Amazon EBS de la instancia Amazon EC2 de destino.
- 24 `aws:waitForAwsResourceProperty`— Espera a que el volumen raíz de Amazon EBS se separe de la instancia Amazon EC2 de destino.
- 25 `aws:executeAwsApi`— Adjunta el volumen raíz de Amazon EBS a la instancia temporal de Amazon EC2.
- 26 `aws:waitForAwsResourceProperty`— Espera a que el volumen raíz de Amazon EBS se adjunte a la instancia temporal de Amazon EC2.
- 27 `aws:runCommand`— Restablece la contraseña del usuario de destino mediante la ejecución de un script de shell mediante Run Command en la instancia temporal de Amazon EC2.
- 28 `aws:executeAwsApi`— Separa el volumen raíz de Amazon EBS de la instancia temporal de Amazon EC2.
- 29 `aws:waitForAwsResourceProperty`— Espera a que el volumen raíz de Amazon EBS se separe de la instancia temporal de Amazon EC2.
- 30 `aws:executeAwsApi`— Separa el volumen raíz de Amazon EBS de la instancia temporal de Amazon EC2 tras un error.
- 31 `aws:waitForAwsResourceProperty`— Espera a que el volumen raíz de Amazon EBS se separe de la instancia temporal de Amazon EC2 tras un error.
- 32 `aws:branch`— Ramifica la automatización en función de si se ha solicitado una instantánea del volumen raíz para determinar la ruta de recuperación en caso de error.

- 33 `aws:executeAwsApi`— Vuelve a conectar el volumen raíz de Amazon EBS a la instancia Amazon EC2 de destino.
- 34 `aws:waitForAwsResourceProperty`— Espera a que el volumen raíz de Amazon EBS se adjunte a la instancia de Amazon EC2.
- 35 `aws:executeAwsApi`— Crea un nuevo volumen de Amazon EBS a partir de la instantánea del volumen raíz de la instancia Amazon EC2 de destino.
- 36 `aws:waitForAwsResourceProperty`— Espera hasta que el nuevo volumen de Amazon EBS esté en un `available` estado.
- 37 `aws:executeAwsApi`— Adjunta el nuevo volumen de Amazon EBS a la instancia de destino como volumen raíz.
- 38 `aws:waitForAwsResourceProperty`— Espera a que el volumen de Amazon EBS esté en un `attached` estado.
- 39 `aws:executeAwsApi`— Describe los eventos de la CloudFormation pila si los runbooks no pueden crear o actualizar la pila. CloudFormation
- 40 `aws:branch`— Ramifica la automatización en función del estado anterior de la instancia de Amazon EC2. Si el estado era `running`, se inicia la instancia. Si estaba en un estado `stopped`, la automatización continúa.
- 41 `aws:changeInstanceState`— Inicia la instancia Amazon EC2 si es necesario.
- 42 `aws:waitForAwsResourceProperty`— Espera a que la CloudFormation pila esté en estado `terminal` antes de eliminarla.
- 43 `aws:executeAwsApi`— Elimina la CloudFormation pila, incluida la instancia temporal de Amazon EC2.

AWSSupport-RunEC2RescueForWindowsTool

Descripción

El `RescueForWindowsTool` manual `AWSSupport-RunEC2` ejecuta la herramienta de solución de problemas Amazon EC2 Rescue for Windows Server en la instancia gestionada por Windows de Amazon Elastic Compute Cloud (Amazon EC2) de destino para ayudar a solucionar problemas comunes. Este manual admite tres acciones principales:

- `ResetAccess`: restablece la contraseña del administrador local. La contraseña se genera aleatoriamente y se almacena de forma segura en el almacén de AWS Systems Manager parámetros como `/EC2Rescue/Password/<instance_id>`. Si no proporciona ningún

parámetro, la contraseña se cifra con la clave predeterminada AWS Key Management Service (AWS KMS) `alias/aws/ssm`. Si lo desea, puede especificar un identificador de AWS KMS clave para cifrar la contraseña con su propia clave.

- **CollectLogs:** recopila registros y archivos de configuración del sistema operativo y los carga en un bucket de Amazon Simple Storage Service (Amazon S3) de su cuenta ejecutando Amazon EC2 Rescue con la opción `/collect:all`
- **FixAll:** intenta detectar y solucionar problemas en un volumen raíz de Windows sin conexión adjunto a la instancia actual mediante la ejecución de Amazon EC2 Rescue con la `/rescue:all` opción.

Important

Este manual requiere que la instancia de destino sea una instancia administrada por Windows con las AWS herramientas para Windows PowerShell instaladas. El manual instala la herramienta Amazon EC2 Rescue for Windows Server mediante el paquete Systems Manager Distributor. `AWSSupport-EC2Rescue`

¿Cómo funciona?

El manual de ejecución realiza los siguientes pasos:

- Instala la herramienta de solución de problemas Amazon EC2 Rescue para Windows Server mediante el paquete Systems Manager Distributor.
- Ejecuta la acción especificada (`ResetAccessCollectLogs`, o `FixAll`) con los parámetros proporcionados.
- **ParaResetAccess:** genera una contraseña segura y la almacena en el almacén de parámetros.
- **ParaCollectLogs:** Recopila los registros del sistema y los carga en el bucket de Amazon S3 especificado.
- **ParaFixAll:** intenta solucionar problemas en el volumen sin conexión especificado.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:DescribeInstanceInformation`
- `ssm:GetCommandInvocation`
- `ssm:PutParameter`(para `ResetAccess` tomar medidas)
- `kms:Encrypt`(para `ResetAccess` actuar con AWS KMS clave personalizada)
- `s3:PutObject`(para `CollectLogs` actuar)
- `s3:GetBucketAcl`(para `CollectLogs` tomar medidas)
- `s3:GetBucketPolicy`(para `CollectLogs` tomar medidas)
- `s3:GetBucketPolicyStatus`(para `CollectLogs` tomar medidas)

Ejemplo de política:

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

```

        "ssm:GetCommandInvocation",
        "ssm:PutParameter",
        "kms:Encrypt",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus"
    ],
    "Resource": "*"
}
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-RunEC2RescueForWindowsTool](#) Systems Manager en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - Comando (obligatorio):
 - Descripción: (Obligatoria) La acción a realizar.
 - Tipo: String
 - Permitir valores: [ResetAccess, CollectLogs, FixAll]
 - Valor predeterminado: ResetAccess
 - Parámetros (obligatorios):
 - Descripción: (Obligatorio) Parámetros del comando:
 - ParaResetAccess: el identificador de AWS AWS KMS clave o el alias (predeterminado:alias/aws/ssm)
 - ParaCollectLogs: el nombre del bucket de Amazon S3 en el que se van a cargar los registros
 - ParaFixAll: el nombre del dispositivo para la corrección sin conexión (por ejemplo,xvdf)
 - Tipo: String
 - Permitir patrón: `^[0-9a-z][a-z0-9-.]{3,63}$|^(dev\[a-z0-9]{2,10}|xv[a-z0-9]{1,10})$|^(alias\\aws\\ssm[a-zA-Z0-9-/_]{1,32})$`

4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:

- instala EC2 Rescue:

Instala la herramienta de solución de problemas Amazon EC2 Rescue para Windows Server mediante el paquete Systems Manager Distributor. `AWSSupport-EC2Rescue`

- ejecute: `EC2 RescueForWindows`

Ejecuta el PowerShell script con la acción especificada en el parámetro `Command` para realizar la operación solicitada.

7. Una vez finalizada, consulte la sección de resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)
- [Utilice Amazon EC2 Rescue para Windows Server con el comando Run de Systems Manager](#)

AWSPremiumSupport-ResizeNitroInstance

Descripción

El manual de procedimientos `AWSPremiumSupport-ResizeNitroInstance` proporciona una solución automatizada para cambiar el tamaño de las instancias de Amazon Elastic Compute Cloud (Amazon EC2) creadas en el sistema Nitro.

Para reducir el riesgo potencial de pérdida de datos y tiempo de inactividad, el manual de procedimientos verifica lo siguiente:

- El comportamiento de detención de instancias.
- Si la instancia forma parte de un grupo de Amazon EC2 Auto Scaling y está en modo `standby`.
- El estado y tenencia de la instancia.

- El tipo de instancia al que quiere cambiar es compatible con la cantidad de interfaces de red actualmente conectadas a su instancia.
- La arquitectura del procesador y el tipo de virtualización tanto para el tipo de instancia actual como para el de destino son los mismos.
- Si la instancia está en ejecución, supera todas las comprobaciones de estado.
- El tipo de instancia que ha seleccionado está disponible en la misma zona de disponibilidad elegida.

Si Amazon EC2 no supera las comprobaciones de estado después de cambiar el tipo de instancia, el manual de procedimientos regresa automáticamente al tipo de instancia anterior.

De forma predeterminada, este manual de procedimientos no cambiará el tipo de instancia si está en ejecución y hay volúmenes de almacén de instancias adjuntos. El runbook tampoco cambiará el tipo de instancia si la instancia forma parte de una AWS CloudFormation pila. Si quiere cambiar alguno de estos comportamientos, especifique yes para los parámetros `AllowInstanceStoreInstances` y `AllowCloudFormationInstances`.

El manual de procedimientos proporciona dos formas diferentes de especificar el tipo de instancia al que quiere cambiar:

- Para las automatizaciones simples dirigidas a una sola instancia, especifique el tipo de instancia al que quiere cambiar mediante el parámetro `TargetInstanceTypeFromParameter`.
- Para ejecutar automatizaciones a escala y cambiar el tipo de instancia de varias instancias, especifique el tipo de instancia mediante el parámetro `TargetInstanceTypeFromTagValue`. Para obtener información sobre la ejecución de automatizaciones a escala, consulte [Ejecutar automatizaciones a escala](#).

Si no especifica un valor para ninguno de los parámetros, la automatización falla.

Important

El acceso a `AWSPremiumSupport-*` los manuales requiere una suscripción a Business + Support, Enterprise Support o Unified Operations. Para obtener más información, consulte [Comparar planes de AWS Support](#).

Consideraciones

- Recomendamos hacer una copia de seguridad de la instancia antes de usar este manual de procedimientos.
- Para obtener información sobre la compatibilidad para cambiar los tipos de instancia, consulte [Compatibilidad para cambiar el tipo de instancia](#).
- Si la automatización falla y regresa al tipo de instancia original, consulte [Cómo solucionar problemas al cambiar el tipo de instancia](#).
- Para cambiar el tipo de instancia, es necesario que el manual de procedimientos detenga su instancia. Los datos guardados en la memoria o en el almacén de instancias se perderán cuando se detenga una instancia. Además, se publican todas IPv4 las direcciones públicas que se asignen automáticamente. Para obtener información sobre lo que ocurre cuando detiene una instancia, consulte [Detener y terminar una instancia](#).
- Con el parámetro `SkipInstancesWithTagKey`, puede omitir las instancias a las que se haya aplicado una clave de etiqueta específica de Amazon EC2.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Acknowledge

Tipo: cadena

Descripción: (obligatorio) introduzca **yes** para confirmar que su instancia se detendrá si se está ejecutando actualmente.

- AllowInstanceStoreInstances

Tipo: cadena

Valores válidos: no | yes

Valor predeterminado: no

Descripción: (opcional) si especifica yes, permite que el manual de procedimientos se ejecute en instancias que tengan volúmenes de almacén de instancias adjuntos.

- AllowCloudFormationInstances

Tipo: cadena

Valores válidos: no | yes

Valor predeterminado: no

Descripción: (opcional) Si lo especifica yes, el runbook se ejecuta en instancias que forman parte de una CloudFormation pila.

- DryRun

Tipo: cadena

Valores válidos: no | yes

Valor predeterminado: no

Descripción: (opcional) si especifica yes, el manual de procedimientos valida los requisitos de cambio de tamaño sin realizar cambios en el tipo de instancia.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia Amazon EC2 de la que quiera cambiar el tipo.

- `SkipInstancesWithTagKey`

Tipo: cadena

Descripción: (opcional) la automatización omite una instancia de destino si la clave de etiqueta que especifique se aplica a la instancia.

- `SleepTime`

Tipo: cadena

Predeterminado: 3

Descripción: (opcional) el número de segundos que debe permanecer inactivo este manual de procedimientos una vez finalizado.

- `TagInstance`

Tipo: cadena

Descripción: (Opcional) Etiqueta las instancias con la clave y el valor que prefiera utilizando el siguiente formato: *Key=ChangingType, Value=True*. Esta opción le permite realizar un seguimiento de las instancias a las que se ha dirigido este manual de procedimientos. Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.

- `TargetInstanceTypeFromParameter`

Tipo: cadena

Descripción: (opcional) el tipo de instancia al que quiere cambiar su instancia. Deje este parámetro en blanco si quiere usar el valor de la clave de etiqueta proporcionada en el parámetro `TargetInstanceTypeFromTagValue`.

- `TargetInstanceTypeFromTagValue`

Tipo: cadena

Descripción: (opcional) la clave de etiqueta que se aplica a las instancias de destino cuyo valor contiene el tipo de instancia al que desea cambiar. Si no especifica un valor para el parámetro `TargetInstanceTypeFromParameter`, anula cualquier valor que especifique para este parámetro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

1. `aws:assertAwsResourceProperty`: garantiza que la instancia de Amazon EC2 no esté etiquetada con la clave de etiqueta de recurso especificada en el parámetro `SkipInstancesWithTagKey`. Si se encuentra la clave de etiqueta aplicada a la instancia, se produce un error en el paso y finaliza la automatización.
2. `aws:assertAwsResourceProperty`: confirma que el estado de la instancia de Amazon EC2 de destino es `running`, `pending`, `stopped` o `stopping`. De lo contrario, la automatización finaliza.
3. `aws:executeAwsApi`: recopila las propiedades de la instancia de Amazon EC2.
4. `aws:executeAwsApi`: recopila detalles sobre el tipo de instancia de Amazon EC2 actual.
5. `aws:branch`: comprueba si el tipo de instancia actual y el tipo de instancia especificado en el parámetro `TargetInstanceTypeFromParameter` son iguales. Si lo son, la automatización finaliza.
6. `aws:assertAwsResourceProperty`: garantiza que la instancia se ejecute en el sistema Nitro.
7. `aws:branch`: garantiza que el tipo de volumen raíz de la instancia de Amazon EC2 sea un volumen de Amazon Elastic Block Store (Amazon EBS).

8. `aws:assertAwsResourceProperty`: confirma que el comportamiento de cierre de la instancia sea `stop` y no `terminate`.
9. `aws:branch`: garantiza que la instancia de Amazon EC2 no sea una instancia de `spot`.
10. `aws:branch`: garantiza que la tenencia de la instancia de Amazon EC2 sea la predeterminada y no el `host` dedicado o la instancia dedicada.
11. `aws:executeScript`: confirma que solo hay una automatización de este manual de procedimientos dirigida al ID de la instancia actual. Si ya hay otra automatización en curso dirigida a la misma instancia, la automatización regresa un error y finaliza.
12. `aws:branch`: ramifica la automatización en función del estado de la instancia de Amazon EC2.
 - a. En caso de `stopped` o `stopping`, la automatización ejecuta `aws:waitForAwsResourceProperty` hasta que la instancia de Amazon EC2 se detenga por completo.
 - b. En caso de `running` o `pending`, la automatización ejecuta `aws:waitForAwsResourceProperty` hasta que la instancia de Amazon EC2 supere las comprobaciones de estado.
13. `aws:assertAwsResourceProperty`: confirma que la instancia de Amazon EC2 no forma parte de un grupo de escalado automático mediante una llamada a la operación API de `DescribeAutoScalingInstances`. Si la instancia forma parte de un grupo de escalado automático, asegúrese de que la instancia de Amazon EC2 esté en modo `standby`.
14. `aws:branch`: Ramifica la automatización en función de si desea que la automatización compruebe si la instancia de Amazon EC2 forma parte de una CloudFormation pila:
 - a. `aws:executeScript` Garantiza que la instancia de Amazon EC2 no forme parte de una CloudFormation pila mediante una llamada a la operación de `DescribeStackResources` API.
15. `aws:executeAwsApi`: regresa una lista de tipos de instancias con el mismo tipo de arquitectura de procesador y tipo de virtualización y que admite el número de interfaces de red actualmente conectadas a la instancia de destino.
16. `aws:executeAwsApi`: obtiene el valor del tipo de instancia de destino a partir de la clave de etiqueta especificada en el parámetro `TargetInstanceTypeFromTagValue`.
17. `aws:executeScript`: confirma que los tipos de instancia actual y de destino son compatibles. Garantiza que el tipo de instancia de destino esté disponible en la misma subred. Comprueba que la entidad principal que inició el manual de procedimientos tiene permisos para cambiar el tipo de instancia y detener e iniciar la instancia si se estaba ejecutando.

18. `aws:branch`: ramifica la automatización en función de si el valor del parámetro `DryRun` está establecido en `yes`. Si `yes`, la automatización finaliza.
19. `aws:branch`: comprueba si el tipo de instancia original y el de destino son iguales. Si son iguales, la automatización finaliza.
20. `aws:executeAwsApi`: obtiene el estado actual de la instancia.
21. `aws:changeInstanceState`: crea la instancia de Amazon EC2.
22. `aws:changeInstanceState`: obliga a la instancia a detenerse si está atascada en el estado `stopping`.
23. `aws:executeAwsApi`: cambia el tipo de instancia por el tipo de instancia de destino.
24. `aws:sleep`: espera 3 segundos después de cambiar el tipo de instancia para lograr una coherencia definitiva.
25. `aws:branch`: ramifica la automatización en función del estado de la instancia anterior. Si se estaba `running`, se inicia la instancia.
- a. `aws:changeInstanceState`: Inicia la instancia de Amazon EC2 si se estaba ejecutando antes de cambiar el tipo de instancia.
 - b. `aws:waitForAwsResourceProperty`: Espera a que la instancia de Amazon EC2 supere las comprobaciones de estado. Si la instancia no supera las comprobaciones de estado, la instancia cambia de regreso a su tipo de instancia original.
 - i. `aws:changeInstanceState`: detiene la instancia de Amazon EC2 antes de cambiarla a su tipo de instancia original.
 - ii. `aws:changeInstanceState`: obliga a la instancia de Amazon EC2 a detenerse antes de cambiarla a su tipo de instancia original en caso de que se quede atascada en un estado de parada.
 - iii. `aws:executeAwsApi`: cambia la instancia de Amazon EC2 a su tipo original.
 - iv. `aws:sleep`: espera 3 segundos después de cambiar el tipo de instancia para lograr una coherencia definitiva.
 - v. `aws:changeInstanceState`: inicia la instancia de Amazon EC2 si se estaba ejecutando antes de cambiar el tipo de instancia.
 - vi. `aws:waitForAwsResourceProperty`: espera a que la instancia de Amazon EC2 supere las comprobaciones de estado.
26. `aws:sleep`: espera antes de finalizar el manual de procedimientos.

AWSSupport-ShareEncryptedAMIorEBSSnapshot

Descripción

Este manual automatiza el proceso de compartir instantáneas cifradas Amazon Machine Image o de Amazon Elastic Block Store con otras cuentas de Amazon Web Services. Este manual aborda los complejos requisitos para compartir recursos cifrados entre cuentas, incluidas las modificaciones AWS Key Management Service clave de las políticas y las actualizaciones de los permisos de los recursos.

Esta automatización lleva a cabo los pasos descritos en el artículo del blog de AWS seguridad [Cómo compartir AMI s cifrados entre cuentas para lanzar instancias cifradas de Amazon Elastic Compute Cloud](#).

Consideraciones importantes

- Este manual modificará sus recursos: añadirá permisos multicuenta a su política de claves gestionadas por el AWS KMS cliente (CMK) y concederá permisos de lanzamiento o AMI permisos de creación de volúmenes de creación de instantáneas de Amazon EBS a la cuenta de destino.
- Pueden aplicarse costes adicionales: al copiar recursos (cifrado de clave AWS gestionada o de región diferente), se incurrirá en costes adicionales por la instantánea nueva AMI o de Amazon EBS y por cualquier transferencia de datos entre regiones.
- Compruebe el ID de la cuenta de destino: vuelva a comprobar el ID de la cuenta de destino, ya que este manual no puede validar la existencia de la cuenta.
- Reversión automática con verificación manual: este manual intenta revertir automáticamente los cambios si fallan. Sin embargo, si la reversión en sí misma no funciona, compruebe que no hayan quedado copias adicionales de AMI /Snapshot en su cuenta, que LaunchPermission/CreateVolumePermission los atributos de los recursos no incluyan las cuentas no deseadas y que la política AWS KMS clave esté en su estado original.

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos de alto nivel:

- Valida la existencia, el estado y la configuración de cifrado de los recursos de entrada

- Comprueba los permisos actuales para compartir recursos con la cuenta de destino
- Analiza AWS KMS la política clave y crea una vista previa completa de todos los cambios necesarios
- Solicita la aprobación de los directores designados antes de realizar cualquier cambio
- Ejecuta los cambios aprobados, incluida la copia de recursos (si es necesario), las actualizaciones de permisos y las modificaciones AWS KMS clave de las políticas
- Proporciona un informe de ejecución completo con información sobre la reversión si es necesario

[Ejecuta esta automatización \(consola\)](#)

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

El `AutomationAssumeRole` parámetro requiere las siguientes acciones:

- `ec2: DescribeImages`
- `ec2: DescribeSnapshots`
- `ec2: DescribeImageAttribute`
- `ec2: DescribeSnapshotAttribute`
- `ec2: ModifyImageAttribute`
- `ec2: ModifySnapshotAttribute`
- `ec2: CopyImage`
- `ec2: CopySnapshot`
- `ec2: DeregisterImage`
- `ec2: DeleteSnapshot`
- `km: DescribeKey`
- `km: GetKeyPolicy`
- `km: PutKeyPolicy`
- `km: CreateGrant`
- `km: GenerateDataKey *`
- `km: ReEncrypt *`

- kms:Decrypt
- analizador de acceso: CheckAccessNotGranted

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-ShareEncryptedAMIOrEBSSnapshot](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon del AWS AWS Identity and Access Management rol que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Aprobadores (obligatorio):

La lista de directores AWS autenticados que pueden aprobar o rechazar la acción. El número máximo de aprobadores es 10. Puede especificar los principales mediante cualquiera de los siguientes formatos: nombre de usuario, ARN de usuario, ARN del rol de IAM o ARN de asumir rol de IAM.

- ResourceId (Obligatorio):

AMIo ID de instantánea de Amazon EBS para compartir (por ejemplo, ami-123456789012 o snap-123456789012).

- DestinationAccountId (Obligatorio):

El ID de AWS cuenta de 12 dígitos en el que se compartirá el recurso.

- CustomerManagedKeyId (Opcional):

AWS KMS ID de CMK para volver a cifrar el recurso. Es obligatorio si el recurso está cifrado con una clave AWS gestionada o si DestinationRegion se especifica para la copia entre regiones. Para copiar entre regiones, esta clave debe estar en la región de destino.

- DestinationRegion (Opcional):

La AWS región en la que se copiará el recurso. El valor predeterminado es la región actual. Si se especifica una región diferente, el recurso se copiará en la región de destino mediante la AWS KMS CMK especificada en el `CustomerManagedKeyId` parámetro.

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **ValidateResources:**

Valida la existencia, el estado y la configuración de cifrado de los recursos de entrada y determina los cambios necesarios para compartirlos.

- **BranchOnResourcePermission:**

Ramifica el flujo de trabajo en función de si es necesario comprobar el permiso para compartir recursos.

- **CheckResourcePermission:**

Comprueba si la cuenta de destino requiere el permiso para compartir el recurso.

- **AnalyzeChanges:**

Analiza AWS KMS la política clave y crea una vista previa completa de todos los cambios necesarios.

- **BranchOnChanges:**

Ramifica el flujo de trabajo en función de si los cambios requieren aprobación.

- **GetApproval:**

Espera la aprobación de los directores de AWS IAM designados para proceder con los cambios necesarios.

- **ExecuteChanges:**

Ejecuta los cambios aprobados y los revierte en caso de error.

- **Results:**

Genera un informe de ejecución completo que resume todas las acciones realizadas durante el proceso de cifrado AMI o de intercambio de instantáneas.

7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.

AWS AWS Identity and Access Management Política requerida para la cuenta de destino

El rol o usuario de IAM de la cuenta de destino debe configurar los siguientes permisos de IAM para lanzar instancias de Amazon EC2 cifradas a partir de la instantánea de Amazon EBS AMI cifrada compartida o para crear volúmenes a partir de la instantánea de Amazon EBS cifrada compartida:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:<region>:<account-id>:key/<key-id>"
      ]
    }
  ]
}
```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)
- [Comparta una AWS KMS clave](#)

AWSSupport-RestoreEC2InstanceFromSnapshot

Descripción

El AWSSupport-RestoreEC2InstanceFromSnapshot manual le ayuda a identificar y restaurar una instancia de Amazon Elastic Compute Cloud (Amazon EC2) a partir de una instantánea activa del volumen raíz de Amazon Elastic Block Store (Amazon EBS).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- EndDate

Tipo: cadena

Descripción: (opcional) la última fecha en la que quiere que la automatización busque una instantánea.

- InplaceSwap

Tipo: Booleano

Valores válidos: true | false

Descripción: (opcional) si el valor de este parámetro se establece en `true`, el volumen recién creado a partir de la instantánea sustituirá al volumen raíz existente adjunto a su instancia.

- `Instanceld`

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia de base de datos de que desea restaurar de una instantánea.

- `LookForInstanceStatusCheck`

Tipo: Booleano

Valores válidos: `true` | `false`

Predeterminado: `true`

Descripción: (opcional) si el valor de este parámetro se establece en `true`, la automatización comprueba si las comprobaciones de estado de las instancias fallan en las instancias de prueba lanzadas desde las instantáneas.

- `SkipSnapshotsBy`

Tipo: cadena

Descripción: (opcional) el intervalo en el que se omiten las instantáneas al buscar instantáneas para restaurar su instancia. Por ejemplo, si hay 100 instantáneas disponibles y especifica un valor de 2 para este parámetro, se revisará una de cada tres instantáneas.

Predeterminado: 0

- `SnapshotId`

Tipo: cadena

Descripción: (opcional) el ID de la instantánea desde la que quiere restaurar la instancia.

- `StartDate`

Tipo: cadena

Descripción: (opcional) la primera fecha en la que quiere que la automatización busque una instantánea.

- TotalSnapshotsToLook

Tipo: cadena

Descripción: (opcional) el número de instantáneas que revisa la automatización.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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

Pasos de documentos

1. `aws:executeAwsApi`: recopila detalles sobre la instancia de destino.
2. `aws:assertAwsResourceProperty`: verifica la existencia de la instancia de destino.
3. `aws:assertAwsResourceProperty`: verifica que el volumen raíz sea un volumen de Amazon EBS.
4. `aws:assertAwsResourceProperty`: verifica que no se esté ejecutando otra automatización dirigida a esta instancia.
5. `aws:executeAwsApi`: etiqueta la instancia de destino.
6. `aws:executeAwsApi`- Crea un AMI de la instancia.
7. `aws:executeAwsApi`- Recopila detalles sobre el AMI creado en el paso anterior.
8. `aws:waitForAwsResourceProperty`- Espera a que AMI estado en el que se convertirá available antes de continuar.
9. `aws:executeScript`- Lanza una nueva instancia a partir de la recién creada AMI.
10. `aws:assertAwsResourceProperty`: comprueba que el estado de la instancia sea available.
11. `aws:executeAwsApi`: recopila detalles sobre la instancia recién lanzada.
12. `aws:branch`: se ramifica en función de si ha proporcionado un valor para el parámetro `SnapshotId`.
13. `aws:executeScript`: regresa una lista de instantáneas dentro del período de tiempo especificado.
14. `aws:executeAwsApi`: detiene la instancia.
15. `aws:waitForAwsResourceProperty`: espera a que el estado del volumen sea available.
16. `aws:waitForAwsResourceProperty`: espera a que el estado de la instancia sea stopped.
17. `aws:executeAwsApi`: separa el volumen raíz.
18. `aws:waitForAwsResourceProperty`: espera a que se separe el volumen raíz.
19. `aws:executeAwsApi`: fija el nuevo volumen raíz.
20. `aws:waitForAwsResourceProperty`: espera a que se adjunte el nuevo volumen.
21. `aws:executeAwsApi`: inicie la instancia.
22. `aws:waitForAwsResourceProperty`: espera a que el estado de la instancia sea available.
23. `aws:waitForAwsResourceProperty`: espera a que las comprobaciones de estado del sistema y de la instancia sean superadas por la instancia.
24. `aws:executeScript`: ejecuta un script para encontrar una instantánea que pueda usarse para crear correctamente un volumen.

25.aws:executeScript: ejecuta un script para recuperar la instancia utilizando el volumen recién creado a partir de la instantánea identificada por la automatización, o utilizando el volumen creado a partir de la instantánea que especificó en el parámetro SnapshotId.

26.aws:executeScript: elimina los recursos creados por la automatización.

Salidas

launchCloneInstance.InstanceIds

ListSnapshotByDate.FinalSnapshots

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.Instantánea de trabajo

InstanceRecovery.resultado

AWSSupport-SendLogBundleToS3Bucket

Descripción

El AWSSupport-SendLogBundleToS3Bucket runbook carga un paquete de registros generado por la herramienta EC2 Rescue desde la instancia de destino al depósito de S3 especificado. El runbook instala la versión de EC2 Rescue específica de la plataforma en función de la plataforma de la instancia de destino. EC2A continuación, Rescue se utiliza para recopilar todos los registros del sistema operativo (SO) disponibles.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia administrada de Windows o Linux de la que desea recopilar los registros.

- S3 BucketName

Tipo: cadena

Descripción: (obligatorio) bucket de S3 en el que cargar los registros.

- S3Path

Tipo: cadena

Valor predeterminado: `AWSSupport-SendLogBundleToS3Bucket/`

Descripción: (opcional) ruta de S3 para los registros recopilados.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que la EC2 instancia que recibe el comando tenga una función de IAM con la política gestionada por `SSMManagedInstanceCoreAmazon` adjunta. El usuario debe tener al menos `ssm: StartAutomationExecution` y `ssm: SendCommand` para ejecutar la automatización y enviar el comando a la instancia, además de `ssm: GetAutomationExecution` para poder leer el resultado de la automatización.

Pasos de documentos

1. `aws:runCommand`- Instale Rescue mediante EC2. `AWS-ConfigureAWSPackage`
2. `aws:runCommand`- Ejecute el PowerShell script para recopilar los registros de solución de problemas de Windows con EC2 Rescue.
3. `aws:runCommand`- Ejecute el script bash para recopilar los registros de solución de problemas de Linux con EC2 Rescue.

Salidas

`collectAndUploadWindowsLogBundle`.Salida

`collectAndUploadLinuxLogBundle`.Salida

AWSSupport-StartEC2RescueWorkflow

Descripción

El manual de procedimientos `AWSSupport-StartEC2RescueWorkflow` ejecuta el script codificado en base64 (Bash o PowerShell) en una instancia auxiliar creada para rescatar la instancia. El volumen raíz de la instancia se adjunta y se monta en la instancia auxiliar, también conocida como instancia de EC2 rescate. Si la instancia es Windows, proporcione un script de PowerShell. De lo contrario, utilice Bash. El manual de procedimientos establece algunas variables de entorno que se puede utilizar en su script. Las variables de entorno contienen información sobre la entrada que ha facilitado, así como información sobre el volumen raíz sin conexión. El volumen sin conexión ya está montado y listo para su uso. Por ejemplo, puede guardar un archivo de configuración de estado deseado en un volumen raíz de Windows sin conexión o usar chroot en un volumen raíz de Linux sin conexión y realizar una corrección sin conexión.

[Ejecuta esta automatización \(consola\)](#)

Important

Esta automatización no admite las instancias de Amazon EC2 creadas a partir de Amazon Machine Images (AMIs) de Marketplace.

Información adicional

Para codificar un script en base64, puede utilizar PowerShell o Bash. Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

Bash:

```
base64 PATH_TO_FILE
```

A continuación se muestra una lista de variables de entorno que puede utilizar en sus scripts sin conexión, en función del sistema operativo de destino.

Windows:

Variable	Description (Descripción)	Ejemplo de valor
\$env: RESCUE_ACCOUNT_ID EC2	{{ global:ACCOUNT_ID }}	123456789012
\$env: FECHA DE EC2 RESCATE	{{ global:DATE }}	07/09/2018
\$env: EC2 FECHA Y HORA DE RESCATE	*{{ global:DATE_TIME }}	2018-09-07_18.09.59
\$env: EC2 RESCUE_RW_DIR EC2	EC2Ruta de instalación de Rescue para Windows	C:\Program Files\ Amazon\ EC2 Rescue
\$env: EC2 RESCUE_RW_DIR EC2	EC2Ruta de instalación de Rescue para Windows	C:\Program Files\ Amazon\ EC2 Rescue
\$env: RESCUE_EXECUTION_ID EC2	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
\$env: EC2 RESCUE_OF_FLINE_CURRENT_CONTROL_SET	Ruta del conjunto de control actual de Windows sin conexión	HKLM:\AWSTempSystem\ControlSet001
\$env: EC2 RESCUE_OF_FLINE_DRIVE	Letra de unidad de Windows sin conexión	D:\

Variable	Description (Descripción)	Ejemplo de valor
\$env: EC2 RESCUE_OF FLINE_EBS_DEVICE	Dispositivo de EBS de volumen raíz sin conexión	xvdf
\$env: EC2 RESCUE_OF FLINE_KERNEL_VER	Versión del kernel de Windows sin conexión	6.1.7601.24214
\$env: EC2 RESCUE_OF FLINE_OS_ARCHITECTURE	Arquitectura de Windows sin conexión	AMD64
\$env: EC2 RESCUE_OF FLINE_OS_CAPTION	Título de Windows sin conexión	Windows Server 2008 R2 Datacenter
\$env: EC2 RESCUE_OF FLINE_OS_TYPE	Tipo del sistema operativo Windows sin conexión	Server
\$env: EC2 RESCUE_OF FLINE_PROGRAM_FILE S_DIR	Ruta del directorio Program Files de Windows sin conexión	D:\Program Files
\$env: EC2 RESCUE_OF FLINE_PROGRAM_FILE S_X86_DIR	Ruta del directorio Program Files x86 de Windows sin conexión	D:\Program Files (x86)
\$env: EC2 RESCUE_OF FLINE_REGISTRY_DIR	Ruta del directorio del Registro de Windows sin conexión	D:\Windows\System32\config
\$env: EC2 RESCUE_OF FLINE_SYSTEM_ROOT	Ruta del directorio raíz del sistema de Windows sin conexión	D:\Windows
\$env: REGIÓN DE EC2 RESCATE	{{ global:REGION }}	us-west-1
\$env: EC2 RESCUE_S3 _BUCKET	{{S3}} BucketName	balde de demostración aman- S3

Variable	Description (Descripción)	Ejemplo de valor
\$env: RESCUE_S3_PREFIX EC2	{{ S3Prefix }}	myprefix/
\$env: EC2 RESCUE_SO URCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
\$script: EC2 RESCUE_OF FLINE_WINDOWS_INSTALL	Metadatos de la instalación de Windows sin conexión	Objeto de Powershell del cliente

Linux:

Variable	Description (Descripción)	Ejemplo de valor
EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
EC2FECHA DE RESCATE	{{ global:DATE }}	07/09/2018
EC2FECHA Y HORA DE RESCATE	*{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_RL_DIR EC2	EC2Ruta de instalación de Rescue para Linux	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTIO N_ID	{{ automation:EXECUTI ON_ID }}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_ DEVICE	Nombre del dispositivo sin conexión	/dev/xvdf1
EC2RESCUE_OFFLINE_ EBS_DEVICE	Dispositivo de EBS de volumen raíz sin conexión	/dev/sdf
EC2RESCUE_OFFLINE_ SYSTEM_ROOT	Punto de montaje del volumen raíz sin conexión	/mnt/mount
EC2RESCATE_PYTHON	Versión de Python	python2.7

Variable	Description (Descripción)	Ejemplo de valor
EC2REGIÓN DE RESCATE	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{S3}} BucketName	balde de demostración aman-S3
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AMIPrefix

Tipo: cadena

Valor predeterminado: `AWSSupport-EC2Rescue`

Descripción: (opcional) prefijo para el nombre de la AMI de copia de seguridad.

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **CreatePostEC2RescueBackup**

Tipo: cadena

Valores válidos: true | false

Predeterminado: false

Descripción: (Opcional) Configúrelo `true` para crear una AMI `InstanceId` después de ejecutar el script, antes de iniciarlo. La AMI se conservará una vez terminada la automatización. Es su responsabilidad proteger el acceso a la AMI o eliminarla.

- **CreatePreEC2RescueBackup**

Tipo: cadena

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) Configúrelo `true` para crear una AMI `InstanceId` antes de ejecutar el script. La AMI se conservará una vez terminada la automatización. Es su responsabilidad proteger el acceso a la AMI o eliminarla.

- **EC2RescueInstanceType**

Tipo: cadena

Valores válidos: `t2.small` | `t2.medium` | `t2.large` | `t3.small` | `t3.medium` | `t3.large` | `i3.large`

Valor predeterminado: `t3.medium`

Descripción: (opcional) El tipo de instancia EC2 de la instancia de Rescue. EC2

- **InstanceId**

Tipo: cadena

Descripción: (obligatorio) ID de la instancia EC2. **IMPORTANTE:** AWS Systems Manager La automatización detiene esta instancia. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.

- **OfflineScript**

Tipo: cadena

Descripción: (obligatorio) el script con codificación base64 que se ejecuta en la instancia auxiliar. Usa Bash si la instancia de origen es Linux y PowerShell si es Windows.

- S3BucketName

Tipo: cadena

Descripción: (opcional) nombre del bucket de S3 en la cuenta donde desea cargar los registros de solución de problemas. Asegúrese de que la política de depósitos no conceda read/write permisos innecesarios a las partes que no necesitan acceder a los registros recopilados.

- S3Prefix

Tipo: cadena

Valor predeterminado: `AWSSupport-EC2Rescue`

Descripción: (opcional) prefijo para los registros de S3.

- SubnetId

Tipo: cadena

Predeterminado: `SelectedInstanceSubnet`

Descripción: (opcional) El ID de subred de la instancia de EC2 Rescue. De forma predeterminada, se utiliza la misma subred en la que reside instancia proporcionada. IMPORTANTE: Si proporciona una subred personalizada, debe estar en la misma InstanceId zona de disponibilidad y debe permitir el acceso a los puntos finales de SSM.

- UniqueId

Tipo: cadena

Valor predeterminado: `{{ automation:EXECUTION_ID }}`

Descripción: (opcional) un identificador único para la automatización.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que el usuario que ejecuta la automatización tenga adjunta la política gestionada por Amazon SSMAutomation Role IAM. Además de dicha política, el usuario debe tener:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:*:111122223333:function:AWSSupport-
EC2Rescue-*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::awssupport-ssm.*/*.template",
        "arn:aws:s3:::awssupport-ssm.*/*.zip"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:PutRolePolicy",
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
```



```

        "iam:DeleteInstanceProfile"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/AWSSupport-EC2Rescue-*",
        "arn:aws:iam::111122223333:instance-profile/AWSSupport-EC2Rescue-
*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "lambda:CreateFunction",
        "ec2:CreateVpc",
        "ec2:ModifyVpcAttribute",
        "ec2:DeleteVpc",
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2:DeleteInternetGateway",
        "ec2:CreateSubnet",
        "ec2:DeleteSubnet",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:CreateRouteTable",
        "ec2:AssociateRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteRouteTable",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:Describe*"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

Pasos de documentos

1. `aws:executeAwsApi`: describe la instancia proporcionada
2. `aws:executeAwsApi`: describe el volumen raíz de la instancia proporcionada.

3. `aws:assertAwsResourceProperty`: comprueba que el tipo de dispositivo del volumen raíz sea EBS
4. `aws:assertAwsResourceProperty`: comprueba que el volumen raíz no esté cifrado
5. `aws:assertAwsResourceProperty`: comprueba el ID de subred proporcionado
 - a. (Usa la subred de la instancia actual): Si `* SubnetId = SelectedInstanceSubnet *`, ejecuta `aws:createStack` para implementar la EC2 pila de Rescue CloudFormation
 - b. (Crear una nueva VPC): si `* SubnetId = CreateNew VPC*`, ejecute `aws:createStack` para implementar la pila Rescue EC2 CloudFormation
 - c. (Usar subred personalizada): en el resto de casos:

`aws:assertAwsResourceProperty`: comprueba que la subred proporcionada está en la misma zona de disponibilidad que la instancia proporcionada.

`aws:createStack`- Despliega la pila Rescue EC2 CloudFormation
6. `aws:invokeLambdaFunction`: realiza una validación de entrada adicional
7. `aws:executeAwsApi`- Actualiza la CloudFormation pila de EC2 Rescue para crear la instancia auxiliar de EC2 Rescue
8. `aws:waitForAwsResourceProperty`- Espera a que se complete la actualización de la CloudFormation pila de EC2 Rescue
9. `aws:executeAwsApi`- Describe el resultado de la CloudFormation pila de EC2 Rescue para obtener el ID de la instancia auxiliar de EC2 Rescue
10. `aws:waitForAwsResourceProperty`- Espere a que la instancia auxiliar de EC2 Rescue se convierta en una instancia gestionada
11. `aws:changeInstanceState`: detiene la instancia proporcionada
12. `aws:changeInstanceState`: detiene la instancia proporcionada
13. `aws:changeInstanceState`: fuerza la detención de la instancia proporcionada
14. `aws:assertAwsResourceProperty`- Compruebe el valor de CreatePre EC2 RescueBackup entrada
 - a. (Crear una copia de seguridad previa EC2 al rescate) - Si `* CreatePre EC2 RescueBackup = verdadero*`
 - b. `aws:executeAwsApi`: crea una copia de seguridad de AMI de la instancia proporcionada.
 - c. `aws:createTags`: etiqueta la copia de seguridad de la AMI
15. `aws:runCommand`- Instale EC2 Rescue en la instancia auxiliar de EC2 Rescue

16 `aws:executeAwsApi`: desconecta el volumen raíz de la instancia

17 `aws:assertAwsResourceProperty`: comprueba la plataforma de instancia proporcionada

a. (La instancia es Windows):

`aws:executeAwsApi`- Adjunte el volumen raíz a la instancia auxiliar de EC2 Rescue como `*xvdf*`

`aws:sleep`: en espera 10 segundos

`aws:runCommand`: ejecuta el script sin conexión proporcionado en PowerShell.

b. (Instancia es Linux):

`aws:executeAwsApi`- Adjunte el volumen raíz a la instancia auxiliar de Rescue como EC2 `*/dev/sdf*`

`aws:sleep`: en espera 10 segundos

`aws:runCommand`: ejecuta el script sin conexión proporcionado en Bash

18 `aws:changeInstanceState`- EC2 Detenga la instancia auxiliar de Rescue

19 `aws:changeInstanceState`- Detenga por la fuerza la instancia auxiliar de EC2 Rescue

20 `aws:executeAwsApi`- Separe el volumen raíz de la instancia auxiliar de EC2 Rescue

21 `aws:executeAwsApi`: vuelve a asociar el volumen raíz a la instancia proporcionada.

22 `aws:assertAwsResourceProperty`- Compruebe el valor de entrada `CreatePost EC2 RescueBackup`

a. (Crear una copia de seguridad posterior EC2 al rescate) - Si `* CreatePost EC2 RescueBackup = verdadero*`

b. `aws:executeAwsApi`: crea una copia de seguridad de AMI de la instancia proporcionada.

c. `aws:createTags`: etiqueta la copia de seguridad de la AMI

23 `aws:executeAwsApi`: restaura la eliminación inicial en estado de terminación para el volumen raíz de la instancia proporcionada.

24 `aws:changeInstanceState`: restaura el estado inicial de la instancia proporcionada (en ejecución/detenida).

25 `aws:deleteStack`- Elimine la pila de EC2 Rescue CloudFormation

Salidas

runScriptForLinux. Salida

runScriptForSalida de Windows

preScriptBackup.Imageld

postScriptBackup.Imageld

AWSSupport-TroubleshootActiveDirectoryReplication

Descripción

El AWSSupport-TroubleshootActiveDirectoryReplicationmanual ayuda a solucionar los errores de replicación del controlador de dominio de Microsoft Active Directory (AD) al comprobar la configuración común de una instancia de controlador de dominio de destino. Este manual ejecuta una serie de PowerShell comandos en la instancia de controlador de dominio proporcionada para comprobar el estado actual de la replicación e informar de los errores que pueden provocar problemas de replicación del dominio. De forma opcional, el runbook puede iniciar los servicios críticos de replicación (NetlogonRPCSS,W32Time, yKDC) si están parados y sincronizar la hora del sistema ejecutándolos w32tm /resync /force en la instancia de destino.

Important

AWS Managed Microsoft AD no está en el ámbito de este manual.

Important

Mientras la automatización ejecuta comandos en la instancia de destino, se realizan cambios en el sistema de archivos de la instancia de destino. Estos cambios incluyen la creación del directorio de registro (\$env:ProgramData \TroubleshootActiveDirectoryReplication) y los archivos de informe.

¿Cómo funciona?

El manual de ejecución realiza las siguientes comprobaciones y acciones:

- Verifica que la instancia de destino ejecute Windows y que la administre Systems Manager.

- Ejecuta PowerShell scripts para comprobar la configuración y el estado de la replicación de Active Directory.
- Comprueba la configuración de las ACL de los grupos de seguridad y de la red para comprobar la conectividad del socio de replicación.
- Soluciona problemas de sincronización horaria y estado de los servicios críticos.
- Carga los archivos de registro en el bucket de Amazon S3 especificado para su análisis.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:DescribeInstances`
- `secretsmanager:GetSecretValue`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicy`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutObject`

Ejemplo de política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "secretsmanager:GetSecretValue",
        "ssm:DescribeInstanceInformation",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Secrets Manager configuración

El PowerShell script de replicación de comprobaciones se conecta al controlador de dominio de Microsoft Active Directory de destino recuperando el nombre de usuario y la contraseña con una llamada en tiempo de ejecución a AWS Secrets Manager. Siga los pasos de [Crear un AWS Secrets Manager secreto](#) para crear un AWS Secrets Manager secreto nuevo. Asegúrese de que el nombre de usuario y la contraseña estén guardados mediante un key/value par en el formato{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}. Tras crear el AWS Secrets Manager secreto, asegúrate de conceder el `secretsmanager:GetSecretValue` permiso sobre el ARN secreto a la función de perfil de instancia de IAM del controlador de dominio de destino.

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootActiveDirectoryReplication](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
 - Tipo: `AWS::IAM::Role::Arn`
 - InstanceId (Obligatorio):
 - Descripción: (obligatorio) El ID de la instancia del controlador de dominio de Amazon EC2 que desea solucionar los problemas de replicación de Active Directory. Tenga en cuenta que la instancia proporcionada debe ser un controlador de dominio.
 - Tipo: `AWS::EC2::Instance::Id`
 - SecretsManagerArn (Obligatorio):
 - Descripción: (Obligatorio) El ARN de su AWS Secrets Manager secreto que contiene un nombre de usuario y una contraseña de Active Directory con permisos de administrador empresarial o equivalentes para acceder a la configuración de dominio y bosque de Active Directory. Asegúrese de que el nombre de usuario y la contraseña se almacenen mediante un key/value par en ese formato `{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}`. Asegúrese de adjuntar el `secretsmanager:GetSecretValue` permiso del ARN secreto a la función de perfil de instancia de IAM del controlador de dominio de destino.
 - Tipo: `String`
 - Valor permitido: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z0-9-]{2,20}:[0-9]{12}:secret:[a-zA-Z0-9]{1}[a-zA-Z0-9\\/_+=.@-]{1,256}$`
 - TimeSync (Opcional):
 - Descripción: (opcional) Seleccione Check o Sync. Si lo selecciona Check, el manual imprimirá el estado actual de la sincronización horaria del sistema. Si Sync se selecciona, el runbook intentará forzar la resincronización temporal ejecutándose `w32tm /resync /force` en la instancia de destino.
 - Tipo: `String`

- Valores permitidos: [Check, Sync]
- Valor predeterminado: Check
- ServiceAction (Opcional):
 - Descripción: (opcional) Seleccione Check o Fix. Si selecciona Check, el manual imprimirá el estado actual de los Key Distribution Center (KDC) servicios NetlogonWindows Time service (W32Time), Remote Procedure Call (RPC) Service, y. Si Fix se selecciona, el runbook intentará iniciar estos servicios si alguno está detenido.
 - Tipo: String
 - Valores permitidos: [Check, Fix]
 - Valor predeterminado: Check
- LogDestination (Obligatorio):
 - Descripción: (Obligatorio) El bucket de Amazon S3 de su AWS cuenta para cargar los resultados de los comandos.
 - Tipo: String

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- assertIfOperatingSystemIsWindows:

Comprueba si el sistema operativo de la instancia Amazon EC2 de destino proporcionada es Windows.

- assertIfInstanceIsSsmManaged:

Garantiza que Systems Manager administre la instancia de Amazon EC2; de lo contrario, la automatización finaliza.

- Compruebe la replicación:

Ejecuta un PowerShell script en la instancia del controlador de dominio especificada para obtener la configuración y el estado de la replicación del dominio de Active Directory.

- checkInstanceSgAndNACL:

Comprueba si el grupo de seguridad y la ACL de red asociadas a la instancia del controlador de dominio de destino permiten el tráfico a los socios de replicación.

Ejecuta un PowerShell script para solucionar los problemas de sincronización horaria y del estado de los servicios críticos.

- Verifica S3 BucketPublicStatus:

Comprueba si el bucket de Amazon S3 especificado en LogDestination permite permisos de acceso de lectura o escritura públicos o anónimos.

- **runUploadScript:**

Ejecuta un PowerShell script para cargar el archivo de registro en el bucket de AAmazon S3 especificado en el LogDestination parámetro y elimina el archivo de registro archivado del sistema operativo. Los archivos de registro se pueden usar para solucionar problemas o se pueden compartir con AWS Support al solucionar problemas de replicación.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWSPremiumSupport-TroubleshootEC2DiskUsage

Descripción

El manual de procedimientos AWSPremiumSupport-TroubleshootEC2DiskUsage le ayuda a investigar y, si es posible, solucionar problemas relacionados con el uso de discos raíz y no raíz de instancias de Amazon Elastic Compute Cloud (Amazon EC2). Si es posible, el manual de procedimientos intenta solucionar los problemas ampliando el volumen y su sistema de archivos. Para realizar estas tareas, este manual de procedimientos orquesta la ejecución de varios manuales de procedimientos en función del sistema operativo de la instancia afectada.

El primer manual de procedimientos, `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` o `AWSPremiumSupport-DiagnoseDiskUsageOnLinux`, determina si los problemas del disco se pueden mitigar expandiendo el volumen.

El segundo manual de procedimientos, `AWSPremiumSupport-ExtendVolumesOnWindows` o `AWSPremiumSupport-ExtendVolumesOnLinux`, utiliza la salida del primer manual de procedimientos para ejecutar el código de Python que modifica el volumen. Una vez modificado el volumen, el manual de procedimientos amplía la partición y el sistema de archivos de los volúmenes afectados.

 Important

El acceso a `AWSPremiumSupport-*` los manuales requiere una suscripción a Business + Support, Enterprise Support o Unified Operations. Para obtener más información, consulte [Comparar planes de AWS Support](#).

Este documento se creó en colaboración con AWS Managed Services (AMS). AMS le ayuda a gestionar su AWS infraestructura de forma más eficiente y segura. AMS también proporciona flexibilidad operativa, seguridad y cumplimiento mejorados, optimización de la capacidad e identificación del ahorro de costos. Para obtener más información, consulte [AWS Managed Services](#).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, Windows

Parámetros

- `InstanceId`

Tipo: cadena

Valores permitidos: `^[a-z0-9]{8,17}$`

Descripción: (obligatorio) ID de la instancia Amazon EC2.

- `VolumeExpansionEnabled`

Tipo: Booleano

Descripción: (opcional) indicador para controlar si el documento ampliará los volúmenes y las particiones afectados.

Predeterminado: `true`

- `VolumeExpansionUsageTrigger`

Tipo: cadena

Descripción: (opcional) uso mínimo del espacio de partición necesario para activar la extensión (en porcentaje).

Valores permitidos: `^[0-9]{1,2}$`

Predeterminado: `85`

- `VolumeExpansionCapSize`

Tipo: cadena

Descripción: (opcional) el volumen máximo de Amazon Elastic Block Store (Amazon EBS) se incrementará a (en GiB).

Valores permitidos: `^[0-9]{1,4}$`

Predeterminado: `2048`

- `VolumeExpansionGibIncrease`

Tipo: cadena

Descripción: (opcional) aumento en GiB del volumen. Se `VolumeExpansionPercentageIncrease` utilizará el mayor aumento neto entre `VolumeExpansionGibIncrease` y

Valores permitidos: `^[0-9]{1,4}$`

Predeterminado: 20

- VolumeExpansionPercentageIncrease

Tipo: cadena

Descripción: (opcional) aumento en el porcentaje del volumen. Se VolumeExpansionPercentageIncrease utilizará el mayor aumento neto entre VolumeExpansionGibIncrease y.

Valores permitidos: `^[0-9]{1,2}$`

Predeterminado: 20

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Pasos de documentos

1. `aws:assertAwsResourceProperty`: comprueba si la instancia está gestionada por Systems Manager.
2. `aws:executeAwsApi`: describe la instancia para obtener la plataforma.
3. `aws:branch`: ramifica la automatización en función de la plataforma de la instancia.
 - a. Si la instancia es Windows:
 - i. `aws:executeAutomation`: ejecuta el manual de procedimientos `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` para diagnosticar los problemas de uso del disco en la instancia.
 - ii. `aws:executeAwsApi`: obtiene el resultado de la automatización anterior.
 - iii. `aws:branch`: se ramifica en función del resultado de los diagnósticos y de si hay volúmenes que se puedan ampliar para mitigar la alerta.
 - A. No hay volúmenes que deban ampliarse: finalizar la automatización.
 - B. Hay volúmenes que deben ampliarse:
 - I. `aws:executeAwsApi`: crea una Amazon Machine Image (AMI) de la instancia.
 - II. `aws:waitForAwsResourceProperty`: espera a que el estado de AMI sea `available`.
 - III. `aws:executeAutomation`: ejecuta el manual de procedimientos `AWSPremiumSupport-ExtendVolumesOnWindows` para realizar la modificación del volumen y también los pasos necesarios en el sistema operativo (SO) para disponer del nuevo espacio.
 - b. (La plataforma no es Windows) Si la instancia de entrada no es Windows:

- i. `aws:executeAutomation`: ejecuta el manual de procedimientos `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` para diagnosticar los problemas de uso del disco en la instancia.
- ii. `aws:executeAwsApi`: obtiene el resultado de la automatización anterior.
- iii. `aws:branch`: se ramifica en función del resultado de los diagnósticos y de si hay volúmenes que se puedan ampliar para mitigar la alerta.
 - A. No hay volúmenes que deban ampliarse: finalizar la automatización.
 - B. Hay volúmenes que deben ampliarse:
 - I. `aws:executeAwsApi`: crea una AMI de la instancia.
 - II. `aws:waitForAwsResourceProperty`: espera a que el estado de AMI sea `available`.
 - III. `aws:executeAutomation`: ejecuta el manual de procedimientos `AWSPremiumSupport-ExtendVolumesOnLinux` para realizar la modificación del volumen y también los pasos necesarios en el sistema operativo para disponer del nuevo espacio.

Salidas

`diagnoseDiskUsageAlertOnWindows.Producción`

`extendVolumesOnWindows. Salida`

`diagnoseDiskUsageAlertOnLinux.Salida`

`extendVolumesOnLinux. Salida`

`BackupAMILinux. Imaged`

`BackupAMIWindows. Imaged`

AWSSupport-TroubleshootEC2InstanceConnect

Descripción

`AWSSupport-TroubleshootEC2InstanceConnect` la automatización ayuda a analizar y detectar los errores que impiden la conexión a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) mediante Amazon EC2 [Instance Connect](#). Identifica los problemas causados por una imagen

de máquina de Amazon (AMI) no compatible, la falta de instalación o configuración del paquete a nivel del sistema operativo, la falta de permisos AWS Identity and Access Management (IAM) o problemas de configuración de la red.

¿Cómo funciona?

El runbook incluye el ID de instancia de Amazon EC2, el nombre de usuario, el modo de conexión, el CIDR de IP de origen, el puerto SSH y el nombre de recurso de Amazon (ARN) del rol o usuario de IAM que tenga problemas con Amazon EC2 Instance Connect. A continuación, comprueba los [requisitos previos](#) para conectarse a una instancia de Amazon EC2 mediante Amazon EC2 Instance Connect:

- La instancia está en ejecución y en buen estado.
- La instancia está ubicada en una AWS región compatible con Amazon EC2 Instance Connect.
- Amazon EC2 Instance Connect admite la AMI de la instancia.
- La instancia puede acceder al servicio de metadatos de la instancia (IMDSv2).
- El paquete Amazon EC2 Instance Connect está correctamente instalado y configurado a nivel del sistema operativo.
- La configuración de red (grupos de seguridad, ACL de red y reglas de tabla de enrutamiento) permite la conexión a la instancia a través de Amazon EC2 Instance Connect.
- El rol o usuario de IAM que se utiliza para aprovechar Amazon EC2 Instance Connect tiene acceso a las teclas push de la instancia de Amazon EC2.

Important

- Para comprobar la AMI de la instancia, la accesibilidad de IMDSv2 y la instalación del paquete Instance Connect de Amazon EC2, la instancia debe estar gestionada por SSM. De lo contrario, omite esos pasos. Para obtener más información, consulte [¿Por qué mi instancia de Amazon EC2 no se muestra como un nodo gestionado?](#)
- La comprobación de red solo detectará si el grupo de seguridad y las reglas de ACL de la red bloquean el tráfico cuando se proporciona el SourceIP CIDR como parámetro de entrada. De lo contrario, solo mostrará las reglas relacionadas con SSH.
- Las conexiones que utilizan [Amazon EC2 Instance Connect Endpoint](#) no se validan en este manual de ejecución.

- En el caso de las conexiones privadas, la automatización no comprueba si el cliente SSH está instalado en la máquina de origen ni si puede acceder a la dirección IP privada de la instancia.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`
- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSsupport-TroubleshootEC2InstanceConnect](#) la AWS Systems Manager consola.

2. Elija Execute automation (Ejecutar automatización).

3. Para los parámetros de entrada, introduzca lo siguiente:

- InstanceId (Obligatorio):

El ID de la instancia de Amazon EC2 de destino a la que no se pudo conectar mediante Amazon EC2 Instance Connect.

- AutomationAssumeRole (Opcional):

El ARN de la función de IAM que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- Nombre de usuario (obligatorio):

El nombre de usuario utilizado para conectarse a la instancia de Amazon EC2 mediante Amazon EC2 Instance Connect. Se utiliza para evaluar si se concede el acceso de IAM a este usuario en particular.

- EC2InstanceConnectRoleOrUser(Obligatorio):

El ARN del rol o usuario de IAM que utiliza Amazon EC2 Instance Connect para introducir las teclas de la instancia.

- SSHPort (Opcional):

El puerto SSH configurado en la instancia de Amazon EC2. El valor predeterminado es 22. El número de puerto debe estar intermedio. 1-65535

- SourceNetworkType (Opcional):

El método de acceso de red a la instancia de Amazon EC2:

- Navegador: se conecta desde la consola AWS de administración.
- Pública: se conecta a la instancia ubicada en una subred pública a través de Internet (por ejemplo, su ordenador local).
- Privado: te conectas a través de la dirección IP privada de la instancia.
- SourceIpCIDR (opcional):

El CIDR de origen que incluye la dirección IP del dispositivo (por ejemplo, su ordenador local) desde el que iniciará sesión mediante Amazon EC2 Instance Connect. Ejemplo: 172.31.48.6/32. Si no se proporciona ningún valor con el modo de acceso público o privado, el runbook no evaluará si el grupo de seguridad de la instancia Amazon EC2 y las reglas de ACL de la red permiten el tráfico SSH. En su lugar, mostrará las reglas relacionadas con SSH.

Input parameters	
InstanceId (Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect. ☒ Show interactive instance picker	
AWS::EC2::instance::id	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.	Username (Required) The username used to connect to the EC2 instance using EC2 Instance Connect. It is used to evaluate if IAM access is granted for this particular user.
String	String
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.	SSHPort (Optional) The SSH port configured on the EC2 instance. Default value is '22'. The port number must be between '1-65535'.
String	22
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.	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.
Browser	None

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **AssertInitialState:**

Garantiza que el estado de la instancia de Amazon EC2 se esté ejecutando. De lo contrario, la automatización finaliza.

- **GetInstanceProperties:**

Obtiene las propiedades actuales de la instancia Amazon EC2 (PlatformDetails, PublicIpAddress VpcId, SubnetId y MetadataHttpEndpoint).

- **GatherInstanceInformationFromSSM:**

Obtiene el estado de ping de la instancia de Systems Manager y los detalles del sistema operativo si la instancia está gestionada por SSM.

- **CheckIfAWSRegionCompatible:**

Comprueba si la instancia de Amazon EC2 se encuentra en una región compatible con Amazon EC2 Instance Connect AWS .

- **BranchOnIfAWSRegionCompatible:**

Continúa la ejecución si Amazon EC2 Instance Connect admite la AWS región. De lo contrario, crea la salida y sale de la automatización.

- `CheckIfInstanceAMIsCompatible`:

Comprueba si la AMI asociada a la instancia es compatible con Amazon EC2 Instance Connect.

- `BranchOnIfInstanceAMIsCompatible`:

Si la AMI de la instancia es compatible, realiza las comprobaciones a nivel del sistema operativo, como la accesibilidad de los metadatos y la instalación y configuración del paquete Amazon EC2 Instance Connect. De lo contrario, comprueba si los metadatos HTTP están habilitados mediante la AWS API y, a continuación, pasa al paso de comprobación de la red.

- `Comprobar IMDSReachabilityFromOs`:

Ejecuta un script Bash en la instancia de Amazon EC2 Linux de destino para comprobar si es capaz de acceder a. IMDSv2

- `Compruebe la instalaciónEICPackage`:

Ejecuta un script Bash en la instancia de Amazon EC2 Linux de destino para comprobar si el paquete Amazon EC2 Instance Connect está correctamente instalado y configurado.

- `Compruebe: SSHConfig FromOs`

Ejecuta un script Bash en la instancia Linux Amazon EC2 de destino para comprobar si el puerto SSH configurado coincide con el parámetro de entrada ``SSHPort``

- `CheckMetadataHTTPEndpointIsEnabled`:

Comprueba si el punto final HTTP del servicio de metadatos de la instancia está activado.

- `Compruebe el EICNetwork acceso`:

Comprueba si la configuración de la red (grupos de seguridad, ACL de red y reglas de la tabla de enrutamiento) permite la conexión a la instancia a través de Amazon EC2 Instance Connect.

- `Compruebe IAMRoleOrUserPermissions`:

Comprueba si el rol o usuario de IAM utilizado para aprovechar Amazon EC2 Instance Connect tiene acceso a las teclas push de la instancia de Amazon EC2 mediante el nombre de usuario proporcionado.

- `MakeFinalOutput`:

Consolida el resultado de todos los pasos anteriores.

7. Una vez finalizado, revise la sección de resultados para ver los resultados detallados de la ejecución:

Ejecución en la que la instancia de destino cumple todos los requisitos previos necesarios:

```
▼ 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 '██████████' 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
```

Ejecución en la que no se admite la AMI de la instancia de destino:

```
▼ 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:
```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS documentación de servicio

- [¿Cómo soluciono los problemas de conexión a mi instancia de Amazon EC2 mediante Amazon EC2 Instance Connect?](#)

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

Descripción

AWSSupport-TroubleshootLinuxMGNDRSAgentLogsEl manual de automatización se utiliza para detectar errores comunes al instalar los agentes de replicación AWS Application Migration Service (AWS MGN) y AWS Elastic Disaster Recovery (AWS DRS) en servidores Linux para migrar los servidores de origen a la nube. AWS

¿Cómo funciona?

El runbook AWSSupport-TroubleshootLinuxMGNDRSAgentLogs toma la ruta Amazon Simple Storage Service (Amazon S3) en la que se carga como parámetro AWS el `aws_replication_agent_installer.log` registro de instalación de MGN AWS o DRS. A continuación, realiza las siguientes tareas:

- Validación: comprueba si el archivo de registro proporcionado es válido y si contiene al menos una instalación de agente.
- Análisis: analiza minuciosamente la última instalación del agente en el archivo de registro para detectar errores conocidos de AWS MGN o AWS DRS.
- Detección y resolución de errores: en función del análisis, detecta y enumera cualquier error o problema durante el proceso de instalación del agente. Para cada error detectado, el manual proporciona pasos detallados para ayudar a resolver o mitigar el problema.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `s3:GetObject`
- `s3:ListBucket`

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootLinuxMGNDRAgentLogs](#) Systems Manager, en Documentos.
2. Elija `Execute automation` (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - `AutomationAssumeRole` (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- `BucketName` (Obligatorio):

El nombre del depósito de Amazon S3 en el que se almacena el registro del agente de replicación.

- `S3 ObjectKey` (obligatorio):

La clave del objeto de Amazon S3 en el que se almacena el archivo de registro del instalador del agente de replicación. Ejemplo: Si el URI de Amazon S3 lo es `s3://bucket_name/path/to/file/aws_replication_agent_installer.log`, debe introducirlo `path/to/file/aws_replication_agent_installer.log`.

- `ServiceName` (Obligatorio):

El nombre del servicio para el que está instalado el agente de replicación. Valores permitidos: `AWS_MGN` o `AWS_DRS`

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.	BucketName (Required) The name of the Amazon S3 bucket where the replication agent log is stored. s3bucket-name
S3ObjectKey (Required) The key of S3 object where the replication agent installer log file is stored. Example: if S3 URI is `s3://bucket_name/path/to/file/aws_replication_agent_installer.log` then you should provide `path/to/file/aws_replication_agent_installer.log` as input. aws_replication_agent_installer.log	ServiceName (Required) The name of the service for which the Replication agent is done: **AWS MGN**: AWS Application Migration Service. **AWS DRS**: AWS Elastic Disaster Recovery. AWS MGN

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **ValidateInput**

Garantiza que el archivo de registro del agente de replicación sea válido y accesible mediante el nombre del bucket de Amazon S3 y la ruta al objeto proporcionados y, a continuación, devuelve el número de bytes de la última instalación del agente.

- **CheckReplicationAgentLogErrors**

Lee el archivo de registro del agente de replicación empezando por el último byte de instalación y busca los errores AWS MGN o AWS DRS conocidos.

- **MakeFinalOutput**

Crea el resultado de las comprobaciones anteriores, que incluye información sobre los errores encontrados y recomendaciones para la solución de problemas.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución:

▼ Outputs

MakeFinalOutput.Output

Input Validation Step

✓ The replication agent log file is valid and accessible using the provided S3 path.

Log file error checking results

✗ Detected error: Kernel development package for [REDACTED] are missing from repositories

✓ Recommendations and troubleshooting steps:

During agent installation, the installer downloads a matching "kernel-devel/linux-headers" package from the repository configured in your Linux operating system. This error occurs when the agent installation workflow can't install the matching "kernel-devel/linux-headers" package to the Linux OS current running kernel.

1. Check the current kernel version on the source server:

```
$ sudo uname -r
```

2. Make sure to install the version that corresponds exactly to the current kernel version that you are running (displayed in the output of "sudo uname -r" command).

Use the following commands to install "kernel-devel/linux-headers" package for the running kernel:

+ For all Red Hat and CentOS source servers:

```
$ sudo yum install kernel-devel-`uname -r`
```

+ For all Ubuntu/Debian source servers:

```
$ sudo apt-get install linux-headers-`uname -r`
```

+ For all SUSE source servers:

```
$ sudo zypper install kernel-default-devel-`uname -r`
```

Note: When the "kernel-devel/linux-headers" packages are installed for both the running kernel and other installed kernels, you will find the following directories generated for each installed kernel. They are located under "/usr/src/kernels" for all Red Hat-based operating systems and under "/usr/src" for Ubuntu and Debian-based operating systems:

```
$ sudo ls -la /usr/src/kernels
```

```
$ sudo ls -la /usr/src
```

3. Sometimes, you will find that the "kernel-devel/linux-headers" package for the running kernel is not available in your server repositories. In that case, you have three options:

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSSupport-TroubleshootRDP

Descripción

El manual de procedimientos AWSSupport-TroubleshootRDP permite al usuario comprobar o modificar los ajustes comunes de la instancia de destino que podrían afectar a las conexiones del Protocolo de escritorio remoto (RDP), tales como los perfiles de puerto RDP, Autenticación en el nivel de red (NLA) y Firewall de Windows. Opcionalmente, los cambios se pueden aplicar sin conexión parando e iniciando la instancia, si el usuario permite explícitamente la corrección sin conexión. De forma predeterminada, el manual de procedimientos lee los valores de estos ajustes y los incluye en la salida.

⚠ Important

Los cambios realizados a los perfiles de configuración de RDP, el servicio RDP y el Firewall de Windows deben revisarse detenidamente antes de ejecutar este manual de procedimientos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- Acción

Tipo: cadena

Valores válidos: CheckAll | FixAll | Personalizado

Valor predeterminado: Custom

Descripción: (Opcional) [Personalizado] Utilice los valores de Firewall RDPSERVICEStartupType, RDPSERVICE Action, RDPPort Action, NLASetting Action y RemoteConnections para gestionar la configuración. [CheckAll] Lea los valores de la configuración sin cambiarlos. [FixAll] Restaure la configuración predeterminada de RDP y desactive el Firewall de Windows.

- AllowOffline

Tipo: cadena

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) solo corregir: establecer en True si permite una corrección de RDP sin conexión en caso de que falle la solución de problemas online o que la instancia proporcionada no sea una instancia administrada. Nota: Para la corrección sin conexión, SSM Automation detiene la instancia y crea una AMI antes de intentar realizar ninguna operación.

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Firewall

Tipo: cadena

Valores válidos: Check | Disable

Valor predeterminado: Check

Descripción: (opcional) comprobar o deshabilitar el Firewall de Windows (todos los perfiles).

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia para solucionar problemas de la configuración de RDP.

- Acción de NLASetting

Tipo: cadena

Valores válidos: Check | Disable

Valor predeterminado: Check

Descripción: (opcional) comprobar o deshabilitar la Autenticación en el nivel de red (NLA).

- Acción de RDPPort

Tipo: cadena

Valores válidos: Check | Modify

Valor predeterminado: Check

Descripción: (opcional) comprobar el puerto utilizado actualmente para las conexiones RDP o modificar el puerto RDP y volver a establecerlo en 3389 y reiniciar el servicio.

- Acción de RDPSERVICE

Tipo: cadena

Valores permitidos: Check | Start | Restart | Force-Restart

Valor predeterminado: Check

Descripción: (Opcional) Compruebe, inicie, reinicie o fuerce el reinicio del servicio RDP ().
TermService

- RDPServiceStartupType

Tipo: cadena

Valores válidos: Check | Auto

Valor predeterminado: Check

Descripción: (opcional) comprobar o establecer el servicio RDP para que se comience automáticamente cuando se inicia Windows.

- RemoteConnections

Tipo: cadena

Valores válidos: Check | Enable

Valor predeterminado: Check

Descripción: (opcional) Acción que se debe realizar en la TSConnections configuración Denegar: activar o activar.

- S3 BucketName

Tipo: cadena

Descripción: (opcional) solo sin conexión: nombre del bucket de S3 en la cuenta donde desea cargar los registros de solución de problemas. Asegúrese de que la política de bucket no concede permisos de lectura y escritura innecesarios a las partes que no necesitan tener acceso a los registros recopilados.

- SubnetId

Tipo: cadena

Predeterminado: SelectedInstanceSubnet

Descripción: (opcional) Solo sin conexión: el ID de subred de la instancia de EC2 Rescue utilizada para solucionar problemas sin conexión. Si no se especifica ningún ID de subred, AWS Systems Manager Automation creará una nueva VPC. IMPORTANTE: La subred debe estar en la misma InstanceId zona de disponibilidad y debe permitir el acceso a los puntos finales de SSM.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que la EC2 instancia que recibe el comando tenga una función de IAM con la política gestionada por SSMMangedInstanceCoreAmazon adjunta. Para la corrección en línea, el usuario debe tener al menos ssm:DescribeInstanceInformation, ssm: StartAutomationExecution y ssm: SendCommand para ejecutar la automatización y enviar el comando a la instancia, además de ssm: GetAutomationExecution para poder leer el resultado de la automatización. Para la corrección sin conexión, el usuario debe tener al menos ssm:DescribeInstanceInformation, ssm:, ec2:DescribeInstances, más ssm: StartAutomationExecution para poder leer el resultado de la automatización. GetAutomationExecution AWSSupport-TroubleshootRDP llamadas AWSSupport-ExecuteEC2Rescue para realizar la corrección sin conexión: revise los permisos para asegurarse de que puede ejecutar la AWSSupport-ExecuteEC2Rescue automatización correctamente.

Pasos de documentos

1. aws:assertAwsResourceProperty- Compruebe si la instancia es Windows Server instancia
2. aws:assertAwsResourceProperty: comprueba si la instancia es una instancia gestionada
3. (Solución de problemas online) Si la instancia es una instancia administrada, entonces:

- a. `aws:assertAwsResourceProperty`: comprueba el valor de acción proporcionado
- b. (Comprobación en línea) Si la acción = `CheckAll`, entonces:

`aws:runPowerShellScript`- Ejecuta el PowerShell script para obtener el estado de los perfiles del Firewall de Windows.

`aws:executeAutomation`: llama a `AWSSupport-ManageWindowsService` para obtener el estado del servicio RDP.

`aws:executeAutomation`: llama a `AWSSupport-ManageRDPSettings` para obtener la configuración del RDP.

- c. (Solución en línea) Si la acción = `FixAll`, entonces:

`aws:runPowerShellScript`- Ejecuta el PowerShell script para deshabilitar todos los perfiles de Firewall de Windows.

`aws:executeAutomation`: llama a `AWSSupport-ManageWindowsService` para iniciar el servicio RDP.

`aws:executeAutomation`: llama a `AWSSupport-ManageRDPSettings` para habilitar las conexiones remotas y deshabilitar el NLA.

- d. (Administración online) Si `Action` = `Custom`, entonces:

`aws:runPowerShellScript`- Ejecuta el PowerShell script para administrar los perfiles del Firewall de Windows.

`aws:executeAutomation`: llama a `AWSSupport-ManageWindowsService` para gestionar el servicio RDP.

`aws:executeAutomation`: llama a `AWSSupport-ManageRDPSettings` para gestionar la configuración del RDP.

- 4. (Corrección sin conexión) Si la instancia de entrada no es una instancia administrada, entonces:

- a. `aws:assertAwsResourceProperty`- `Assert AllowOffline` = verdadero
- b. `aws:assertAwsResourceProperty`- Afirmar una acción = `FixAll`
- c. `aws:assertAwsResourceProperty`- Afirma el valor de `SubnetId`

(Utilice la subred de la instancia proporcionada) Si `SubnetId` es

`SELECTED_INSTANCE_SUBNET`

`aws:executeAwsApi`: recupera la subred de la instancia actual.

`aws:executeAutomation`: ejecuta `AWSSupport-ExecuteEC2Rescue` con la subred de la instancia proporcionada.

- d. (Usa la subred personalizada proporcionada) Si no es `SELECTED_INSTANCE_SUBNET SubnetId`

`aws:executeAutomation- AWSSupport-ExecuteEC2Rescue SubnetId` Ejecute con el valor proporcionado.

Salidas

`manageFirewallProfiles`.Salida

administrar `RDPService` la configuración.Salida

gestionar `RDPSettings` .Output

`checkFirewallProfiles`.Salida

compruebe la configuración. Salida `RDPService`

`RDPSettings`compruebe .Salida

`disableFirewallProfiles`.Salida

Restaurar `RDPService` la configuración predeterminada. Salida

Restaurar el valor predeterminado. `RDPSettings` Salida

solucionar problemas. `RDPOffline` Salida

solucionar problemas .Salida `RDPOffline WithSubnetId`

AWSSupport-TroubleshootSSH

Descripción

El `AWSSupport-TroubleshootSSH` runbook instala la herramienta Amazon EC2 Rescue para Linux y, a continuación, utiliza la herramienta EC2 Rescue para comprobar o intentar solucionar problemas comunes que impiden la conexión remota a la máquina Linux mediante SSH. Opcionalmente, los cambios se pueden aplicar sin conexión parando e iniciando la instancia, si el

usuario permite explícitamente la corrección sin conexión. De forma predeterminada, el manual de procedimientos opera en modo de solo lectura.

[Ejecuta esta automatización \(consola\)](#)

Para obtener información sobre cómo trabajar con el manual de procedimientos AWSSupport-TroubleshootSSH, consulte este [tema sobre la solución de problemas de AWSSupport-TroubleshootSSH](#) de Premium Support de AWS .

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- Acción

Tipo: cadena

Valores válidos: | CheckAll FixAll

Predeterminado: CheckAll

Descripción: (obligatorio) especificar si buscar errores sin corregirlos o buscar y corregir automáticamente cualquier problema descubierto.

- AllowOffline

Tipo: cadena

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) solo corregir: establecer en True si permite una corrección de SSH sin conexión en caso de que falle la solución de problemas online o que la instancia proporcionada no

sea una instancia administrada. Nota: Para la corrección sin conexión, SSM Automation detiene la instancia y crea una AMI antes de intentar realizar ninguna operación.

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: ID (obligatorio) de tu EC2 instancia para Linux.

- S3 BucketName

Tipo: cadena

Descripción: (opcional) solo sin conexión: nombre del bucket de S3 en la cuenta donde desea cargar los registros de solución de problemas. Asegúrese de que la política de bucket no concede permisos de lectura y escritura innecesarios a las partes que no necesitan tener acceso a los registros recopilados.

- SubnetId

Tipo: cadena

Predeterminado: SelectedInstanceSubnet

Descripción: (opcional) Solo sin conexión: el ID de subred de la instancia de EC2 Rescue utilizada para solucionar problemas sin conexión. Si no se especifica ningún ID de subred, AWS Systems Manager Automation creará una nueva VPC.

 Important

La subred debe estar en la misma InstanceId zona de disponibilidad y debe permitir el acceso a los puntos finales de SSM.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que la EC2 instancia que recibe el comando tenga una función de IAM con la política gestionada por `SSMManagedInstanceCoreAmazon` adjunta. Para la corrección en línea, el usuario debe tener al menos `ssm:DescribeInstanceInformation`, `ssm:StartAutomationExecution` y `ssm:SendCommand` para ejecutar la automatización y enviar el comando a la instancia, además de `ssm:GetAutomationExecution` para poder leer el resultado de la automatización. Para la corrección sin conexión, el usuario debe tener al menos `ssm:DescribeInstanceInformation`, `ssm:`, `ec2:DescribeInstances`, más `ssm:StartAutomationExecution` para poder leer el resultado de la automatización. `GetAutomationExecution` `AWSSupport-TroubleshootSSH` llamadas `AWSSupport-ExecuteEC2Rescue` para realizar la corrección sin conexión: revise los permisos para asegurarse de que puede ejecutar la `AWSSupport-ExecuteEC2Rescue` automatización correctamente.

Pasos de documentos

1. `aws:assertAwsResourceProperty`: comprueba si la instancia es una instancia gestionada
 - a. (Corrección online) Si la instancia de entrada no es una instancia administrada, entonces:
 - i. `aws:configurePackage`- Instale EC2 Rescue para Linux mediante `AWS-ConfigureAWSPackage`.
 - ii. `aws:runCommand`- Ejecute el script bash para ejecutar EC2 Rescue para Linux.
 - b. (Corrección sin conexión) Si la instancia de entrada no es una instancia administrada, entonces:
 - i. `aws:assertAwsResourceProperty`- Assert AllowOffline = verdadero
 - ii. `aws:assertAwsResourceProperty`- Afirmar una acción = FixAll
 - iii. `aws:assertAwsResourceProperty`- Afirma el valor de SubnetId
 - iv. (Usa la subred de la instancia proporcionada) Si `SelectedInstanceSubnet` vamos `SubnetId` `aws:executeAutomation` a ejecutar `AWSSupport-ExecuteEC2Rescue` con la subred de la instancia proporcionada.
 - v. (Usa la subred personalizada proporcionada) Si no `SubnetId` se `SelectedInstanceSubnet` usa `aws:executeAutomation` para ejecutar `AWSSupport-ExecuteEC2Rescue` con el valor proporcionado. `SubnetId`

Salidas

troubleshootSSH.Output

solucionar problemasSSHOOffline. Salida

solucionar problemas .Salida SSHOOffline WithSubnetId

AWSSupport-TroubleshootSUSERegistration

Descripción

El AWSSupport-TroubleshootSUSERegistration manual le ayuda a identificar por qué se registra una Amazon Elastic Compute Cloud (Amazon EC2) SUSE Linux Enterprise Server se produjo un error en una instancia con SUSE Update Infrastructure. El resultado de la automatización proporciona los pasos para resolver el problema o le ayuda a solucionar el problema. Si la instancia supera todas las comprobaciones durante la automatización, la instancia se registra en SUSE Update Infrastructure.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `Instanceld`

Tipo: cadena

Descripción: (Obligatorio) El ID de la EC2 instancia de Amazon que quieres solucionar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:ListCommands`

Pasos de documentos

- `aws:assertAwsResourceProperty`- Comprueba si la EC2 instancia de Amazon está gestionada por AWS Systems Manager.
- `aws:runCommand`- Comprueba si la plataforma de EC2 instancias de Amazon es SLES.
- `aws:runCommand`: comprueba si la versión del paquete `cloud-regionsrv-client` es superior o igual a la versión 9.0.10 requerida.
- `aws:runCommand`: comprueba si el enlace simbólico del producto base está roto y corrige el enlace si está roto.
- `aws:runCommand`: comprueba si el archivo de hosts (`/etc/hosts`) contiene registros para `smt-ec2-suscloud.net`. La automatización elimina cualquier entrada duplicada.
- `aws:runCommand`: comprueba si el comando `curl` está instalado.
- `aws:runCommand`- Comprueba si la EC2 instancia de Amazon puede acceder a la dirección 169.254.169.254 del Instance Metadata Service (IMDS).

- `aws:runCommand`- Comprueba si la EC2 instancia de Amazon tiene un código de facturación o un código de AWS Marketplace producto.
- `aws:runCommand`- Comprueba si la EC2 instancia de Amazon puede llegar al menos a un servidor regional a través de HTTPS.
- `aws:runCommand`- Comprueba si la EC2 instancia de Amazon puede acceder a los servidores de la herramienta de gestión de suscripciones (SMT) a través de HTTP.
- `aws:runCommand`- Comprueba si la EC2 instancia de Amazon puede acceder a los servidores de la herramienta de gestión de suscripciones (SMT) a través de HTTPS.
- `aws:runCommand`- Comprueba si la EC2 instancia de Amazon puede acceder a la `smt-ec2.susecloud.net` dirección a través de HTTPS.
- `aws:runCommand`- Registra la EC2 instancia de Amazon en SUSE Update Infrastructure.
- `aws:executeScript`: recopila y genera el resultado de todos los pasos anteriores.

AWSSupport-TroubleshootWindowsPerformance

Descripción

El manual `AWSSupport-TroubleshootWindowsPerformance` ayuda a solucionar problemas de rendimiento continuos en la instancia de Windows de Amazon Elastic Compute Cloud (Amazon EC2). El manual captura los registros de la instancia de destino y analiza las métricas de rendimiento de la CPU, la memoria, el disco y la red. Opcionalmente, la automatización puede capturar un volcado de procesos para ayudarte a determinar la posible causa de la degradación del rendimiento. La automatización también captura los registros de eventos y del sistema con la [EC2Rescue](#) herramienta más reciente, si permite que este manual la instale.

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Comprueba los requisitos previos de la instancia Amazon EC2.
- Genera registros de rendimiento en el disco raíz de la instancia Amazon EC2 de Windows
- Almacena los registros capturados en una carpeta `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Si se proporciona un bucket de Amazon Simple Storage Service (Amazon S3) y el rol de responsable de automatización tiene los permisos necesarios, los registros capturados se cargan en el bucket de Amazon S3.

- Instala la EC2Rescue herramienta más reciente en la instancia Amazon EC2 de Windows para capturar eventos y registros del sistema si decide instalarla, pero no analiza el volcado de procesos ni los registros capturados por ella. EC2Rescue

Important

- Para ejecutar este runbook, la instancia de Windows de Amazon EC2 debe estar gestionada por AWS Systems Manager. Para obtener más información, consulte [¿Por qué mi instancia de Amazon EC2 no se muestra como un nodo gestionado?](#)
- Para ejecutar este runbook, la instancia de Windows de Amazon EC2 debe ejecutarse en las versiones Windows 8.1/Windows Server 2012 R2 (6.3) o posterior PowerShell con 4.0 o superior. Para obtener más información, consulte la versión [del sistema operativo Windows](#).
- Para generar los registros de rendimiento, se requieren al menos 10 GB de espacio libre en el dispositivo raíz. Si el disco raíz tiene más de 100 GB, el espacio libre debe ser superior al 10% del tamaño del disco. Si descarga un proceso durante la ejecución, el espacio libre debe ser superior a 10 GB más el tamaño total de memoria consumido por el proceso cuando el proceso consume más de 10 GB de memoria.
- Los registros generados en el dispositivo raíz no se eliminan automáticamente.
- El runbook no desinstala la EC2Rescue herramienta. Para obtener más información, consulte [Uso EC2Rescue para Windows Server](#).
- Se recomienda ejecutar esta automatización durante un período en el que el rendimiento se vea afectado. También puede ejecutarla periódicamente mediante una asociación de AWS Systems Manager administradores estatales o programando Windows AWS Systems Manager de mantenimiento.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

(Opcional) La función de IAM asociada al perfil de la instancia o al usuario de IAM configurado en la instancia requiere las siguientes acciones para cargar los registros en el bucket de Amazon S3 especificado para el parámetro: *LogUploadBucketName*

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSsupport-TroubleshootWindowsPerformance](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS IAM Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- InstanceId (Obligatorio):

El ID de la instancia Amazon EC2 de Windows de destino en la que desea ejecutar la automatización. La instancia debe estar gestionada por Systems Manager para ejecutar la automatización.

- CaptureProcessDump (Opcional):

El tipo de volcado del proceso que se va a capturar. La automatización puede capturar un volcado de proceso para el proceso que podría estar causando un impacto en el rendimiento al principio de la automatización. El volumen raíz de la instancia requiere al menos 10 GB de espacio libre (más del 10% del tamaño del disco cuando el tamaño del volumen raíz es superior a 100 GB y 10 GB más el tamaño total de memoria que consume el proceso cuando el proceso consume más de 10 GB de memoria).

- LogCaptureDuration (Opcional):

El número de minutos transcurridos entre 1 y 15 durante los que esta automatización capturará los registros mientras el problema esté presente. El valor predeterminado es 5.

- LogUploadBucketName (Opcional):

El depósito de Amazon S3 de su cuenta en el que desea cargar los registros. El depósito debe configurarse con el cifrado del lado del servidor (SSE) y la política del depósito no debe conceder read/write permisos innecesarios a partes que no necesiten acceder a los registros capturados. La instancia Amazon EC2 para Windows debe tener acceso al bucket de Amazon S3.

- Instalación EC2 RescueTool (opcional):

YesConfigúrelo para permitir que el runbook instale la última versión de la EC2Rescue herramienta para capturar los eventos de Windows y los registros del sistema. El valor predeterminado es No.

- Reconocimiento (obligatorio):

Lea los detalles completos de las acciones realizadas por este manual de automatización y, si está de acuerdo, escriba. 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. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **CheckConcurrency:**

Garantiza que solo haya una ejecución de este manual dirigida a la instancia. Si el runbook encuentra otra ejecución dirigida a la misma instancia, devuelve un error y finaliza.

- **AssertInstanceIsWindows:**

Afirma que la instancia Amazon EC2 se ejecuta en el sistema operativo Windows. De lo contrario, la automatización finaliza.

- **AssertInstanceIsManagedInstance:**

Afirma que la instancia de Amazon EC2 está gestionada por. AWS Systems Manager De lo contrario, la automatización finaliza.

- **VerifyPrerequisites:**

Verifica la PowerShell versión en el sistema operativo de la instancia y se asegura de que la instancia se pueda conectar a través de Systems Manager para ejecutar PowerShell comandos. Esta automatización es compatible con la versión PowerShell 4.0 y superior que se ejecuta en las versiones Windows 8.1/Server 2012 R2 (6.3) o posteriores. Si la versión es anterior, se produce un error en la automatización. Cuando decide cargar los registros al bucket de Amazon S3, esta automatización comprueba que el PowerShell módulo AWS Tools for esté disponible. Si no, la automatización finaliza.

- **BranchOnProcessDump:**

Se ramifica en función de si lo configuró para capturar el cúmulo de procesos que afectaron al rendimiento.

- **CaptureProcessDump:**

Comprueba si la instancia tiene suficiente espacio para ejecutar esta automatización (si eliges la CPU o memoria más altas).

- **CapturePerformanceLogs:**

Comprueba de nuevo el espacio en disco y ejecuta el PowerShell script en la instancia para crear contadores perfectos e iniciar el registro de Performance Monitor y Windows Performance Recorder. El script se detiene cuando LogCaptureDuration se cumple lo definido.

- **SummarizePerformanceLogs:**

Resume el informe XML generado en el paso anterior para encontrar el proceso responsable que consume más el WorkingSet 64 (memoria) y el% de tiempo de procesador (CPU) mostrado como resultado de la automatización. CapturePerformanceLogs Genera información similar sobre el uso de la interfaz de red LogicalDisk TCPv4 IPv4, la memoria UDPv4 y la guarda analysis_output.log en la carpeta de salida.

- **BranchOnInstallEC2Rescue:**

Se ramifica si lo configuró para instalar la EC2Rescue herramienta más reciente en la instancia de Amazon EC2.

- **InstallEC2RescueTool:**

Instala la EC2Rescue herramienta en el sistema operativo de la instancia para capturar los EC2Rescue registros que utiliza. AWS-ConfigureAWSPackage

- **RunEC2RescueTool:**

Ejecuta la EC2Rescue herramienta en el sistema operativo de la instancia para capturar todos los registros necesarios. EC2Rescue captura solo los registros necesarios para ahorrar espacio.

- **BranchOnIfS3BucketProvided:**

Se divide en función de los datos introducidos por el usuario LogUploadBucketName para comprobar si hay un nombre de depósito disponible para cargar los registros.

- **GetS3BucketPublicStatus:**

Determina si se proporciona un bucket de Amazon S3 y, de ser así, confirma que el bucket de Amazon S3 no es público y está configurado con SSE.

- **UploadLogResult:**

Carga los registros en el bucket de Amazon S3 proporcionado. Si la PowerShell versión es 5.0 o superior, comprime los registros en un archivo ZIP y los carga. Elimina el archivo ZIP una vez finalizada la carga. Si la PowerShell versión es inferior a la 5.0, carga los archivos directamente a una carpeta.

- **CleanUpLogsOnFailure:**

Limpia todos los registros generados por el CapturePerformanceLogs paso cuando se produce un error. El CleanUpLogsOnFailure paso puede fallar o agotarse el tiempo de espera si el agente SSM no funciona correctamente o si el sistema Windows no responde.

7. Una vez finalizado, consulte la sección de resultados para ver los resultados detallados de la ejecución:

Ejecución en la que la instancia de destino reúne todos los requisitos previos necesarios.

▼ Outputs

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

CapturePerformanceLogs.Output

The instance has enough space to capture performance logs.
WPR capture process is in 'Stopped' state.
Data Collector Set TroubleshootWindowsPerformance-... was not found.
Attempting to create Performance monitor Data Collector Set TroubleshootWindowsPerformance-...
Data Collector Set TroubleshootWindowsPerformance-... created successfully.
Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance-...
Data Collector Set TroubleshootWindowsPerformance-... started successfully.
Current CPU usage is '54.73%' and Memory usage is '17.15%'
Not both CPU and Memory usage are over 95% at this moment hence continue to capture WPR log.
Starting Windows Performance Recording (WPR) capture process.
Stopping WPR capture process.
WPR capture process is in 'Stopped' state.
The Data Collector Set TroubleshootWindowsPerformance-... is currently generating logs.
The Data Collector Set TroubleshootWindowsPerformance-... has finished generating logs and is currently in 'Stopped' state.
Attempting to delete Data Collector Set TroubleshootWindowsPerformance-...
Data Collector Set TroubleshootWindowsPerformance-... deleted successfully.

[PASSED] Performance logs are captured successfully inside the folder: C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance-...
The captured log files will not be deleted by this automation, please manually delete it after analysis.

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

RunEC2RescueTool.Output

[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance-..._EC2Rescue_23-05-48.zip'. The latest EC2Rescue tool is installed by this automation and please manually remove it if you don't need it. Its installed path is C:\Program Files\Amazon\EC2Rescue\EC2RescueCmd.exe.

SummarizePerformanceLogs.Output

Top 5 Processes which consumed most CPU in percentage as below. If you see a percentage higher than 100 that means the process is using more than one CPU core.

Process	Counter	Min %	Max %	Avg %
sppsv	Processor	0.00	106.00	9.00
WmiPrvSE#2	Processor	0.00	90.00	2.00
MsMpEng	Processor	0.00	38.00	0.75
GenValObj	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

Ejecución en la que la instancia de destino está en una plataforma Linux y la ejecución ha fallado. Debe seleccionar el ID del paso para ver los detalles del error.

▼ Outputs

CapturePerformanceLogs.Output

No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

SummarizePerformanceLogs.Output

No output available yet because the step is not successfully executed

VerifyPrerequisites.Output

No output available yet because the step is not successfully executed

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

RunEC2RescueTool.Output

No output available yet because the step is not successfully executed

UploadLogResult.Output

No output available yet because the step is not successfully executed

Execution status

Overall status

⛔ Failed

Executed steps

2

Succeeded

1

Failed

1

Cancelled

0

TimedOut

0

Executed steps (2)

Find Steps

Step ID	Step #	Step name	Action	Status	Start time	End time
...	1	CheckConcurrency	aws:executeScript	✔ Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT
...0a3a9	2	AssertInstanceIsWindows	aws:assertAwsResourceProperty	⛔ Failed	Tue, 19 Mar 2024 16:15:00 GMT	Tue, 19 Mar 2024 16:15:01 GMT

Los detalles de error del pasoAssertInstanceIsWindows.

Failure details


Failure message
 Step fails when it is Execute/Cancelling 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'].	

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSSupport-TroubleshootWindowsUpdate

Descripción

El `AWSSupport-TroubleshootWindowsUpdate` manual se utiliza para identificar los problemas que podrían fallar en las actualizaciones de Windows para las instancias de Windows de Amazon Elastic Compute Cloud (Amazon EC2).

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Comprueba si la instancia Amazon EC2 de destino está gestionada por. AWS Systems Manager
- Comprueba si las versiones AWS Systems Manager Agent (SSM Agent) y Windows Server son compatibles con las operaciones de aplicación de parches de Systems Manager.
- Comprueba el espacio en disco disponible recomendado para las actualizaciones de Windows y si hay un reinicio pendiente. Un reinicio pendiente normalmente indica que hay actualizaciones pendientes y es necesario reiniciarlo antes de realizar actualizaciones adicionales.
- Configura los ajustes del proxy a nivel del sistema operativo, lo que puede ayudar a solucionar problemas de conectividad.

- Realiza una prueba de conectividad de puntos finales del Amazon Simple Storage Service (Amazon S3) y llama a la operación de [GetDeployablePatchSnapshotForInstance](#) la API para recuperar la instantánea actual de la línea base del parche que utiliza el nodo gestionado.
- Si se produce un error en la conexión, ofrece la opción de ejecutar el `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook para analizar la conectividad de la instancia con los puntos de enlace de Amazon S3.
- Valida la configuración de actualizaciones de Windows y prueba Windows Server Update Services (WSUS) (si corresponde).

Important

- No se admiten los controladores de dominio de Active Directory.
- La versión 2008 R2 o las versiones anteriores de Windows Server no son compatibles.
- No se admiten SSM Agent 1.2.371 ni las versiones anteriores.
- El `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` manual se utiliza [VPC Reachability Analyzer](#) para analizar la conectividad de red entre una fuente y un punto final del servicio. Se le cobrará por cada análisis realizado entre un origen y un destino. Para obtener más información, consulte [Precios de Amazon EFS](#).
- El `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` manual no está disponible en todas las regiones en las que se admite Systems Manager.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

Note

Para ejecutar el manual secundario `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`, añada los permisos que se indican en [este](#) documento.

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootWindowsUpdate](#) Systems Manager, en Documentos.
2. Elija `Execute automation` (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- `AutomationAssumeRole` (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- `InstanceId` (Obligatorio):

Introduzca el ID de la instancia de Amazon EC2 en la que se produjo un error en la actualización de Windows.

- **RunVpcReachabilityAnalyzer(Opcional):**

Especifique `true` que se ejecute la `AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2` automatización si las comprobaciones ampliadas determinan un problema de red o si el ID de instancia especificado no es una instancia administrada. Para obtener más información sobre esta automatización secundaria, consulta la [documentación](#). El valor predeterminado es `false`.

- **RetainVpcReachabilityAnalysis(Opcional):**

Solo relevante si lo `RunVpcReachabilityAnalyzer` es `true`. Especifique `true` conservar la ruta de conocimiento de la red y los análisis relacionados creados por `ReachabilityAnalyzer`. De forma predeterminada, esos recursos se eliminan tras un análisis correcto. Si decide conservar el análisis, el manual secundario no elimina el análisis y puede visualizarlo en la consola de Amazon VPC. El enlace a la consola estará disponible en la salida de automatización secundaria. El valor predeterminado es `false`.

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 instance.

☒ Show interactive instance picker

AWS::EC2::Instance::Id

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

RunVpcReachabilityAnalyzer
(Optional) Specify 'true' to run the 'AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2' automation if a network issue is determined by the extended checks, or if the instance ID specified is not a managed instance. For more information on this child automation, please refer to the documentation above. This parameter defaults to 'false'.

false

RetainVpcReachabilityAnalysis
(Optional) Only relevant if 'RunVpcReachabilityAnalyzer' is true. Specify 'true' to retain the network insight path and related analyses created by VPC Reachability Analyzer. By default, those resources are deleted after successful analysis. If you choose to retain the analysis, the child runbook does not delete the analysis and you can visualize it in the VPC console. The console link will be available in the child automation output. This parameter defaults to 'false'.

false

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **getWindowsServerAndSSMAgentVersion:**

Comprueba que la instancia de destino esté gestionada por la versión del agente SSM AWS Systems Manager y la versión de Windows y obtiene detalles sobre ellas.

- **assertIfInstanceIsSsmManaged:**

Garantiza que la instancia de Amazon EC2 esté gestionada por AWS Systems Manager (SSM); de lo contrario, la automatización finaliza.

- **CheckProxy:**

Comprueba todos los tipos de proxy de la instancia de Windows.

- **CheckPrerequisites:**

Obtiene la versión del agente SSM y la versión de Windows y determina si se trata de un controlador de dominio (DC) de Active Directory. Si la instancia es una versión DC o no se admite la versión del agente SSM o Windows, el runbook se detiene.

- **CheckDiskSpace:**

Obtiene y valida el espacio en disco disponible en la instancia de Windows si es suficiente para realizar la actualización de Windows.

- **CheckPendingReboot:**

Comprueba si hay algún reinicio pendiente en la instancia de Windows.

- **CheckS3Connectivity:**

Comprueba si la instancia puede llegar a los puntos de enlace de Amazon S3 paraPatchbaseline.

- **branchOnRunVpcReachabilityAnalyzer:**

Si RunVpcReachabilityAnalyzer es cierto, entonces ramifica la automatización para ejecutar un análisis más profundo de la depuración de la conectividad de Amazon S3.

- **GenerateEndpoints:**

Genera un punto final para realizar una comprobación de conectividad ampliada para el punto final Amazon S3.

- **analyzeAwsEndpointReachabilityFromEC2:**

Llama al manual de automatización,AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2. para comprobar si la instancia seleccionada es accesible a los puntos de enlace necesarios.

- **CheckWindowsUpdateServices:**

Comprueba el estado del servicio Windows Update y el tipo de inicio.

- **CheckWindowsUpdateSettings:**

Comprueba las políticas de Windows Update configuradas en la instancia de Windows.

- **CheckWSUSSettings:**

Comprueba si la actualización de Windows está configurada con WSUS o el catálogo de Microsoft Update y comprueba la conectividad.

- **CheckWUGlobalSettings:**

Comprueba la configuración global de Windows Update configurada en la instancia de Windows.

- **GenerateLogs:**

Descarga los registros de Windows Update y CBS en el escritorio de la instancia y comprueba si hay errores en los registros de eventos de Windows.

- **FinalReport:**

Genera un informe completo de todos los pasos.

7. Una vez finalizado, revise la sección de resultados para ver los resultados detallados de la ejecución:

```

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
"

```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)

- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

Documentación relacionada con el AWS servicio

- Consulte el artículo [Troubleshoot Windows Update](#) para obtener más información.

AWSSupport-UpgradeWindowsAWSDrivers

Descripción

El `AWSSupport-UpgradeWindowsAWSDrivers` manual actualiza o repara los AWS controladores de almacenamiento y red de la instancia EC2 especificada. El manual intenta instalar las versiones más recientes de los AWS controladores en línea llamando a SSM Agent. Si no se puede contactar con el agente SSM, el manual puede realizar una instalación sin conexión de los AWS controladores si se solicita explícitamente.

Este manual de procedimientos admite los siguientes sistemas operativos:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Note

Tanto la actualización online como la actualización sin conexión crearán una AMI antes de intentar realizar ninguna operación, que se conservará incluso después de que se complete la automatización. Es su responsabilidad proteger el acceso a la AMI o eliminarla. El método en línea reinicia la instancia como parte del proceso de actualización, mientras que el método sin conexión requiere detener y reiniciar la instancia EC2 proporcionada.

Important

Si tus instancias se conectan AWS Systems Manager mediante puntos de enlace de VPC, este manual fallará a menos que se utilice en la región us-east-1. Este manual de

procedimientos también producirá un error en un controlador de dominio. Para actualizar los controladores AWS PV en un controlador de dominio, consulta [Actualizar un controlador de dominio \(PV Upgrade\)](#).AWS

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- AllowOffline

Tipo: cadena

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) establecer en true si se permite una actualización de los controladores sin conexión en caso de que no se puede llevar a cabo la instalación online. Nota: El método sin conexión requiere detener y volver a iniciar la instancia EC2 proporcionada. Se perderán los datos almacenados en los volúmenes de almacén de instancias. La dirección IP pública cambiará si no se utiliza una dirección IP elástica.

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ForceUpgrade

Tipo: cadena

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) solo sin conexión: establecer en true si se permite la actualización de los controladores sin conexión para continuar incluso aunque la instancia ya tenga instalada la versión más reciente de los controladores.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia EC2 para Windows Server.

- SubnetId

Tipo: cadena

Predeterminado: SelectedInstanceSubnet

Descripción: (opcional) Solo sin conexión: el ID de subred de la instancia de EC2 Rescue utilizada para realizar la actualización de los controladores sin conexión. Si no se especifica el ID de subred, Systems Manager Automation creará una nueva VPC.

 Important

La subred debe estar en la misma InstanceId zona de disponibilidad y debe permitir el acceso a los puntos finales del SSM.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

La instancia EC2 que reciba el comando debe tener, como mínimo, una función de IAM que incluya permisos para que ssm: StartAutomationExecution y ssm: execute la automatización y envíe el comando SendCommand a la instancia, además de ssm: GetAutomationExecution para

poder leer el resultado de la automatización. Puede adjuntar la política administrada por AmazonSSMManagedInstanceCore a su rol de IAM para proporcionar estos permisos. Sin embargo, recomendamos utilizar el rol de IAM de Automatización de AmazonSSMAutomationRole para este propósito. Para obtener más información, consulte [Uso de IAM para configurar roles para Automatización](#).

Si está realizando una actualización sin conexión, consulte los permisos que requiere [AWSSupport-StartEC2RescueWorkflow](#).

Pasos de documentos

1. `aws:assertAwsResourceProperty`: comprueba que la instancia de entrada sea Windows.
2. `aws:assertAwsResourceProperty`: verifica que la instancia de entrada sea una instancia gestionada. En caso afirmativo, comienza la actualización online, de lo contrario, se evalúa la actualización sin conexión.
 - a. (Actualización online) Si la instancia de entrada es una instancia administrada:
 - i. `aws:createImage`: crea una copia de seguridad de AMI.
 - ii. `aws:createTags`: etiqueta la copia de seguridad de AMI.
 - iii. `aws:runCommand`- Instala el controlador de red ENA.
 - iv. `aws:runCommand`- Instala el controlador NVMe .
 - v. `aws:runCommand`- Instala un controlador AWS fotovoltaico.
 - b. (Actualización sin conexión) Si la instancia de entrada no es una instancia administrada:
 - i. `aws:assertAwsResourceProperty`: verifica que el indicador AllowOffline esté establecido en true. En caso afirmativo, comienza la actualización sin conexión; de lo contrario, la automatización finaliza.
 - ii. `aws:changeInstanceState`: fuerza la detención de la instancia.
 - iii. `aws:changeInstanceState`: fuerza la detención de la instancia de origen.
 - iv. `aws:createImage`: crear una copia de seguridad de AMI de la instancia de origen.
 - v. `aws:createTags`: etiqueta la copia de seguridad de AMI de la instancia de origen.
 - vi. `aws:executeAwsApi`: habilita ENA para la instancia
 - vii. `aws:assertAwsResourceProperty`- Haz valer la ForceUpgrade bandera.
 - viii. Si ForceUpgrade = true (forzar la actualización sin conexión), ejecútelo `aws:executeAutomation` para invocarlo `AWSSupport-StartEC2RescueWorkflow`

con el script Drivers Force Upgrade. Esto instala los controladores independientemente de la versión actual instalada.

- ix. (Actualización sin conexión) Si ForceUpgrade = false, ejecútelo `aws:executeAutomation` para invocarlo `AWSSupport-StartEC2RescueWorkflow` con el script de actualización de controladores.

Salidas

`preUpgradeBackup.ImageId`

`preOfflineUpgradeBackup. ImageId`

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

`upgradeDriversOffline.Salida`

`forceUpgradeDriversSalida` fuera de línea

Amazon ECS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic Container Service. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-CollectECSInstanceLogs](#)
- [AWS-InstallAmazonECSAgent](#)
- [AWS-ECSRunTask](#)
- [AWSSupport-TroubleshootECSContainerInstance](#)
- [AWSSupport-TroubleshootECSTaskFailedToStart](#)
- [AWS-UpdateAmazonECSAgent](#)

AWSSupport-CollectECSInstanceLogs

Descripción

El manual de procedimientos AWSSupport-CollectECSInstanceLogs recopila archivos de registro relacionados con el sistema operativo y Amazon Elastic Container Service (Amazon ECS) de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) para ayudarle a solucionar problemas comunes de Amazon ECS. Mientras la automatización recopila los archivos de registro asociados, se realizan cambios en el sistema de archivos. Estos cambios incluyen la creación de directorios temporales y un directorio de registro, la copia de los archivos de registro a estos directorios y la compresión de los archivos de registro en un archivo.

Si especificas un valor para el `LogDestination` parámetro, la instancia de destino debe tener instalada la interfaz de línea de AWS comandos (AWS CLI) para las instancias de Linux o AWS las herramientas para Windows PowerShell para las instancias de Windows. La automatización evalúa el estado de la política del bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Para mejorar la seguridad de los registros recopilados de su instancia de Amazon EC2, si el estado de la política `isPublic` está establecido en `true` o si la lista de control de acceso (ACL) concede permisos de `READ|WRITE` al grupo predefinido de `All Users Amazon S3`, los registros no se cargan. Además, si el bucket proporcionado no está disponible en su cuenta, los registros no se cargarán. Para obtener más información sobre los grupos g predefinidos de Amazon S3, consulte los [grupos predefinidos de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `ECSInstanceID`

Tipo: cadena

Descripción: (obligatorio) ID de la instancia de la que desea recopilar los registros. La instancia que especifique debe ser administrada por Systems Manager.

- `LogDestination`

Tipo: cadena

Descripción: (opcional) El depósito de Amazon S3 en el Cuenta de AWS que debe cargar los registros archivados.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`

Recomendamos que la instancia Amazon EC2 que recibe el comando `ECSInstanceId` tenga un rol de IAM con la política administrada Amazon de `AmazonSSMManagedInstanceCore` asociada. Para cargar el archivo de registro en el bucket de Amazon S3 que especifique en el parámetro `LogDestination`, debe añadir los siguientes permisos:

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

Pasos de documentos

- `assertInstanceIsManaged`: verifica si la instancia que especifique en el parámetro `ECSInstanceId` está gestionada por Systems Manager.
- `getInstancePlatform`: obtiene información acerca de la plataforma del sistema operativo (SO) de la instancia especificada en el parámetro `ECSInstanceId`.
- `verifyInstancePlatform`: ramifica la automatización en función de la plataforma del sistema operativo.
- `runLogCollectionScriptOnLinux`: recopila los archivos de registro relacionados con el sistema operativo y Amazon ECS en las instancias de Linux y crea un archivo de almacenamiento en el directorio `/var/log/collectECSlogs`.
- `runLogCollectionScriptOnWindows`: recopila los archivos de registro relacionados con el sistema operativo y Amazon ECS en las instancias de Windows y crea un archivo de almacenamiento en el directorio `C:\ProgramData\collectECSlogs`.
- `verifyIfS3BucketProvided`: verifica si se especificó un valor para el parámetro `LogDestination`.
- `runUploadScript`: ramifica el paso de automatización en función de la plataforma del sistema operativo.
- `runUploadScriptOnLinux`: carga el archivo de registro en el bucket de Amazon S3 especificado en el parámetro `LogDestination` y elimina el archivo de registro archivado del sistema operativo.
- `runUploadScriptOnWindows`: carga el archivo de registro en el bucket de Amazon S3 especificado en el parámetro `LogDestination` y elimina el archivo de registro archivado del sistema operativo.

AWS-InstallAmazonECSAgent

Descripción

El manual de procedimientos `AWS-InstallAmazonECSAgent` instala el agente de Amazon Elastic Container Service (Amazon ECS) en la instancia de Amazon Elastic Compute Cloud (Amazon EC2) que especifique. Este manual de procedimientos solo es compatible con instancias de Amazon Linux y Amazon Linux 2.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceIds

Tipo: StringList

Descripción: (obligatorio) los ID de las instancias de Amazon EC2 en las que desea instalar el agente de Amazon ECS.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances

Pasos de documentos

`aws:executeScript`: instala el agente de Amazon ECS en las instancias de Amazon EC2 que especifique en el parámetro `InstanceIds`.

Salidas

`InstallAmazonECSAgent.SuccessfullInstances` - El ID de la instancia en la que se ha realizado correctamente la instalación del agente de Amazon ECS.

`InstallAmazonECSAgent.FailedInstances` - El ID de la instancia en la que se produjo un error en la instalación del agente de Amazon ECS.

`InstallAmazonECSAgent.InProgressInstances` - El ID de la instancia en la que se está instalando el agente Amazon ECS.

AWS-ECSRunTask

Descripción

El `AWS-ECSRunTask` manual ejecuta la tarea de Amazon Elastic Container Service (Amazon ECS) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `capacityProviderStrategy`

Tipo: cadena

Descripción: (opcional) La estrategia del proveedor de capacidad que se utilizará para la tarea.

- `clúster`

Tipo: cadena

Descripción: (opcional) El nombre abreviado o el ARN del clúster en el que se ejecutará la tarea. Si no especifica un clúster, se utiliza el clúster predeterminado.

- `count`

Tipo: cadena

Descripción: (opcional) El número de instancias de la tarea especificada que se van a colocar en el clúster. Puedes especificar hasta 10 tareas para cada solicitud.

- `habilitar ECSManaged etiquetas`

Tipo: Booleano

Descripción: (opcional) Especifica si se van a utilizar etiquetas gestionadas de Amazon ECS para la tarea. Para obtener más información, consulte [Etiquetado de los recursos de Amazon ECS](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

- `enableExecuteCommand`

Tipo: Booleano

Descripción: (opcional) Determina si se debe activar la funcionalidad de ejecución de comandos para los contenedores de esta tarea. Si es cierto, se activa la función de ejecución de comandos en todos los contenedores de la tarea.

- `grupo`

Tipo: cadena

Descripción: (opcional) El nombre del grupo de tareas que se va a asociar a la tarea. El valor predeterminado es el apellido de la definición de la tarea. Por ejemplo, `family:my-family-name`.

- Tipo de lanzamiento

Tipo: cadena

Valores válidos: EC2 | FARGATE | EXTERNAL

Descripción: (opcional) La infraestructura en la que ejecutar la tarea independiente.

- networkConfiguration

Tipo: cadena

Descripción: (opcional) La configuración de red de la tarea. Este parámetro es necesario para las definiciones de tareas que utilizan el modo de `aws-ec2` red para recibir su propia interfaz de red elástica y no se admite en otros modos de red.

- anulaciones

Tipo: cadena

Descripción: (opcional) Una lista de anulaciones de contenedores en formato JSON que especifica el nombre de un contenedor en la definición de tarea especificada y las anulaciones que debe recibir. Puedes anular el comando predeterminado de un contenedor especificado en la definición de la tarea o en la imagen de Docker con una sobrescritura de comandos. También puedes anular las variables de entorno existentes que se especifican en la definición de la tarea o en la imagen de Docker de un contenedor. Además, puedes añadir nuevas variables de entorno con una anulación de entorno.

- placementConstraints

Tipo: cadena

Descripción: (opcional) Una matriz de objetos de restricción de ubicación para utilizarlos en la tarea. Puede especificar hasta 10 restricciones para cada tarea, incluidas las restricciones en la definición de la tarea y las especificadas en tiempo de ejecución.

- placementStrategy

Tipo: cadena

Descripción: (opcional) Los objetos de la estrategia de colocación que se van a utilizar en la tarea. Puede especificar un máximo de 5 reglas de estrategia para cada tarea.

- platformVersion

Tipo: cadena

Descripción: (opcional) La versión de plataforma que utiliza la tarea. Solo se especifica una versión de plataforma para las tareas alojadas en Fargate. Si no se especifica una versión de la plataforma, se utilizará la versión LATEST.

- propagateTags

Tipo: cadena

Descripción: (opcional) Determina si las etiquetas se propagan de la definición de la tarea a la tarea. Si no se especifica ningún valor, las etiquetas no se propagan. Las etiquetas solo se pueden propagar a la tarea durante la creación de tareas.

- referenceId

Tipo: cadena

Descripción: (opcional) El identificador de referencia que se utilizará para la tarea. El identificador de referencia puede tener una longitud máxima de 1024 caracteres.

- Empezado por

Tipo: cadena

Descripción: (opcional) Una etiqueta opcional que se especifica cuando se inicia una tarea. Esto le ayuda a identificar qué tareas pertenecen a un trabajo específico al filtrar los resultados de una operación de ListTasks API. Se permiten hasta 36 letras (mayúsculas y minúsculas), números, guiones (-) y guiones bajos (_).

- etiquetas

Tipo: cadena

Descripción: (opcional) Metadatos que desea aplicar a la tarea para ayudarlo a categorizar y organizar las tareas. Cada etiqueta consta de una clave y un valor definidos por el usuario.

- Definición de tarea

Tipo: cadena

Descripción: (opcional) El `family` y `revision` (`family:revision`) o el ARN completo de la definición de tarea que se va a ejecutar. Si no se especifica una revisión, se utiliza la última `ACTIVE`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ecs:RunTask`

Pasos de documentos

`aws:executeScript`- Ejecuta la tarea Amazon ECS en función de los valores que especifique para los parámetros de entrada del runbook.

AWSSupport-TroubleshootECSTaskInstance

Descripción

El manual de procedimientos `AWSSupport-TroubleshootECSTaskInstance` le ayuda a solucionar problemas de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que no se registra con un clúster de Amazon ECS. Esta automatización comprueba si los datos de usuario de la instancia contienen la información de clúster correcta, si el perfil de instancia contiene los permisos necesarios y si hay problemas de configuración de la red.

Important

Para ejecutar correctamente esta automatización, el estado de su instancia de Amazon EC2 debe ser `running` y el estado del clúster de Amazon ECS debe ser `ACTIVE`.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ClusterName

Tipo: cadena

Descripción: (obligatorio) el nombre del clúster de Amazon ECS en el que no se pudo registrar la instancia.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia Amazon EC2 que quiere resolver.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Pasos de documentos

`aws:executeScript`: comprueba si la instancia de Amazon EC2 cumple los requisitos previos necesarios para registrarse en un clúster de Amazon ECS.

AWSSupport-TroubleshootECSTaskFailedToStart

Descripción

El manual de procedimientos `AWSSupport-TroubleshootECSTaskFailedToStart` le ayuda a resolver por qué no se pudo iniciar una tarea de Amazon Elastic Container Service (Amazon ECS) en un clúster de Amazon ECS. Debe ejecutar este manual de ejecución Región de AWS igual que la tarea que no se pudo iniciar. El manual de procedimientos analiza los siguientes problemas comunes que pueden impedir el inicio de una tarea:

- Conectividad de red con el registro de contenedores configurado
- Faltan los permisos de IAM necesarios para la función de ejecución de la tarea
- Conectividad del punto de conexión de VPC
- Configuración de regla de grupo de seguridad
- AWS Secrets Manager secretos, referencias
- Configuración de registro

Note

Si el análisis determina que es necesario probar la conectividad de la red, se crean en su cuenta una función de Lambda y el rol de IAM necesario. Estos recursos se utilizan para

simular la conectividad de red de su tarea fallida. La automatización elimina estos recursos cuando ya no son necesarios. Sin embargo, si la automatización no elimina los recursos, debe hacerlo manualmente.

Cuando se proporciona una función de IAM de Lambda, la automatización la utilizará en lugar de crear una nueva. La función de IAM de Lambda proporcionada debe incluir la política AWS administrada `AWSLambdaVPCLambdaAccessExecutionRole` y tener una política de confianza que permita que el director del servicio de Lambda la asuma.

`lambda.amazonaws.com`

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LambdaRoleArn

Tipo: cadena

Descripción: (opcional) El ARN del rol de IAM que permite a la AWS Lambda función acceder a los AWS servicios y recursos necesarios. Si no se especifica ningún rol, System Manager Automation creará un rol de IAM para Lambda en su cuenta con el

`NetworkToolSSMRunbookExecution<ExecutionId>` nombre que incluye la política administrada: `AWSLambdaVPCLambdaAccessExecutionRole`

- `ClusterName`

Tipo: cadena

Descripción: (obligatorio) el nombre del clúster de Amazon ECS donde no se pudo iniciar la tarea.

- `CloudwatchRetentionPeriod`

Tipo: entero

Descripción: (opcional) El período de retención, en días, para que los registros de la función Lambda se almacenen en Amazon CloudWatch Logs. Esto solo es necesario si el análisis determina que es necesario probar la conectividad de la red.

Valores válidos: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

Valor predeterminado: 30

- `TaskId`

Tipo: cadena

Descripción: (obligatorio) ID de la tarea fallida. Use la tarea fallida más reciente.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudtrail:LookupEvents`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeDhcpOptions`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpcAttribute`
- `elasticfilesystem:DescribeFileSystems`
- `elasticfilesystem:DescribeMountTargets`
- `elasticfilesystem:DescribeMountTargetSecurityGroups`
- `elasticfilesystem:DescribeFileSystemPolicy`
- `ecr:DescribeImages`
- `ecr:GetRepositoryPolicy`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeServices`
- `ecs:DescribeTaskDefinition`
- `ecs:DescribeTasks`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListRoles`
- `iam:ListUsers`
- `iam:PassRole`
- `iam:SimulateCustomPolicy`
- `iam:SimulatePrincipalPolicy`
- `kms:DescribeKey`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`

- `lambda:GetFunctionConfiguration`
- `lambda:InvokeFunction`
- `lambda:TagResource`
- `logs:DescribeLogGroups`
- `logs:PutRetentionPolicy`
- `secretsmanager:DescribeSecret`
- `ssm:DescribeParameters`
- `sts:GetCallerIdentity`

Cuando `LambdaRoleArn` se proporciona, no es necesario que la automatización cree el rol y se pueden excluir los siguientes permisos:

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

Pasos de documentos

- `aws:executeScript`: comprueba que el usuario o rol que inició la automatización tiene los permisos de IAM necesarios. Si no tiene los permisos suficientes para usar este manual de procedimientos, los permisos necesarios que faltan se incluyen en el resultado de la automatización.
- `aws:branch`: se ramifica en función de si tiene permisos para todas las acciones necesarias para el manual de procedimientos.
- `aws:executeScript`: crea una función de Lambda en su VPC si el análisis determina que es necesario probar la conectividad de la red.
- `aws:branch`: se ramifica en función de los resultados del paso anterior.
- `aws:executeScript`: analiza las posibles causas del error al iniciar la tarea.
- `aws:executeScript`: elimina los recursos creados por esta automatización.
- `aws:executeScript`: formatea la salida de la automatización para regresar los resultados del análisis a la consola. Puede revisar el análisis después de este paso antes de que se complete la automatización.

- `aws:branch`: se ramifica en función de si la función de Lambda y los recursos asociados se crearon y si es necesario eliminarlos.
- `aws:sleep`: permanece en reposo durante 30 minutos para poder eliminar la interfaz de red elástica de la función de Lambda.
- `aws:executeScript`: elimina la interfaz de red de la función de Lambda.
- `aws:executeScript`: formatea la salida del paso de eliminación de la interfaz de red de la función de Lambda.

AWS-UpdateAmazonECSAgent

Descripción

El manual de procedimientos AWS-UpdateAmazonECSAgent actualiza el agente de Amazon Elastic Container Service (Amazon ECS) en la instancia de Amazon Elastic Compute Cloud (Amazon EC2) que especifique. Este manual de procedimientos solo es compatible con instancias de Amazon Linux y Amazon Linux 2.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **ClusterARN**

Tipo: `StringList`

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del clúster de Amazon ECS con el que están registradas las instancias de contenedor.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeImage`
- `ec2:DescribeInstance`
- `ec2:DescribeInstanceAttribute`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

Pasos de documentos

`aws:executeScript`: actualiza el agente de Amazon ECS en el clúster de Amazon ECS que especifique en los parámetros `ClusterARN`.

Salidas

`UpdateAmazonECSAgent`. `UpdatedContainers` - El ID de la instancia en la que se realizó correctamente la actualización del agente de Amazon ECS.

`UpdateAmazonECSAgent`. `FailedContainers` - El ID de la instancia en la que se produjo un error en la actualización del agente de Amazon ECS.

UpdateAmazonECSAgent. InProgressContainers - El ID de la instancia en la que se está realizando la actualización del agente de Amazon ECS.

Amazon EFS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic File System. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-CheckAndMountEFS](#)

AWSSupport-CheckAndMountEFS

Descripción

El manual de procedimientos AWSSupport-CheckAndMountEFS verifica los requisitos previos para montar su sistema de archivos Amazon Elastic File System (Amazon EFS) y lo monta en la instancia de Amazon Elastic Compute Cloud (Amazon EC2) que especifique. Este manual de procedimientos admite el montaje del sistema de archivos Amazon EFS con el nombre DNS o con la dirección IP del destino del montaje.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Action

Tipo: cadena

Valores válidos: Check | CheckAndMount

Descripción: (obligatorio) determina si el manual de procedimientos verifica los requisitos previos o si verifica los requisitos previos y monta el sistema de archivos.

- EfsId

Tipo: cadena

Descripción: (obligatorio) el ID del sistema de archivos que desea montar.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia de Amazon EC2 en la que desea montar el sistema de archivos.

- MountOptions

Tipo: cadena

Descripción: (opcional) las opciones compatibles con el asistente de montaje de Amazon EFS que desea utilizar al montar el sistema de archivos. Si especifica la opción `tls`, verifique que `stunnel` se haya actualizado en la instancia de destino.

- MountPoint

Tipo: cadena

Descripción: (opcional) el directorio en el que desea montar el sistema de archivos. Si especifica el valor `Check` del parámetro `Action`, no debe especificarse este parámetro.

- MountTargetIP

Tipo: cadena

Descripción: (opcional) la dirección IP del objetivo de montaje. El montaje por dirección IP funciona en entornos en los que el DNS está desactivado, como las nubes privadas virtuales (VPCs) con los nombres de host DNS desactivados. Además, puede utilizar esta opción si su entorno utiliza un proveedor de DNS distinto de Amazon Route 53 (Route 53).

- Region

Tipo: cadena

Descripción: (Obligatorio) El Región de AWS lugar donde se encuentran la instancia y el sistema de archivos de Amazon EC2.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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:*`

Pasos de documentos

- `aws:executeScript`: recopila detalles sobre la instancia de Amazon EC2 que especifique en el parámetro `InstanceId`.
- `aws:executeScript`: recopila detalles sobre el sistema de archivos que especifique en el parámetro `EfsId`.
- `aws:executeScript`: verifica que el grupo de seguridad asociado al sistema de archivos permita el tráfico en el puerto 2049 desde la instancia de Amazon EC2 que especifique en el parámetro `InstanceId`.
- `aws:assertAwsResourceProperty`: verifica que la instancia de Amazon EC2 que especifique en el parámetro `InstanceId` esté gestionada por Systems Manager y que su estado sea `Online`.
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Action`.
- `aws:runCommand`: verifica los requisitos previos para montar el sistema de archivos que especifique en el parámetro `EfsId`.
- `aws:runCommand`: verifica los requisitos previos para montar el sistema de archivos que especifique en el parámetro `EfsId` y monta el sistema de archivos en la instancia de Amazon EC2 que especifique en el parámetro `InstanceId`.

Amazon EKS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Elastic Kubernetes Service. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-CreateEKSClusterWithFargateProfile](#)
- [AWS-CreateEKSClusterWithNodegroup](#)

- [AWS-DeleteEKSCluster](#)
- [AWS-MigrateToNewEKSSelfManagedNodeGroup](#)
- [AWSPremiumSupport-TroubleshootEKSCluster](#)
- [AWSSupport-TroubleshootEKSWorkerNode](#)
- [AWS-UpdateEKSCluster](#)
- [AWS-UpdateEKSMangedNodeGroup](#)
- [AWS-UpdateEKSSelfManagedLinuxNodeGroups](#)
- [AWSSupport-CollectEKSLinuxNodeStatistics](#)
- [AWSSupport-CollectEKSInstanceLogs](#)
- [AWSSupport-SetupK8sApiProxyForEKS](#)
- [AWSSupport-TroubleshootEbsCsiDriversForEks](#)
- [AWSSupport-TroubleshootEKSSALBControllerIssues](#)
- [AWSSupport-TroubleshootEKSDNSFailure](#)

AWS-CreateEKSClusterWithFargateProfile

Descripción

El AWS-CreateEKSClusterWithFargateProfile manual crea un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) mediante un. AWS Fargate

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ClusterName

Tipo: cadena

Descripción: (obligatorio) Un nombre único para el clúster.

- ClusterRoleArn

Tipo: cadena

Descripción: (obligatorio) El ARN de la función de IAM que proporciona permisos para que el plano de control de Kubernetes realice llamadas a AWS las operaciones de la API en su nombre.

- FargateProfileName

Tipo: cadena

Descripción: (Obligatorio) El nombre del perfil de Fargate.

- FargateProfileRoleArn

Tipo: cadena

Descripción: (obligatorio) El ARN de la función de IAM de ejecución del Amazon EKS Pod.

- FargateProfileSelectors

Tipo: cadena

Descripción: (Obligatorio) Los selectores hacen coincidir las cápsulas con el perfil de Fargate.

- SubnetIds

Tipo: StringList

Descripción: (Obligatoria) Las IDs subredes que quiere usar para su clúster de Amazon EKS. Amazon EKS crea interfaces de red elásticas en estas subredes para la comunicación entre los nodos y el plano de control de Kubernetes. Debe especificar al menos dos subredes. IDs

- `EKSEndpointPrivateAccess`

Tipo: Booleano

Valor predeterminado: `True`

Descripción: (opcional) Defina este valor para permitir el acceso privado `True` al punto final del servidor de la API de Kubernetes de su clúster. Si habilita el acceso privado, las solicitudes de la API de Kubernetes desde la VPC del clúster utilizan el punto de conexión de VPC privada. Si deshabilita el acceso privado y tiene nodos o AWS Fargate pods en el clúster, asegúrese de `publicAccessCidrs` incluir los bloques CIDR necesarios para la comunicación con los nodos o los pods de Fargate.

- `EKSEndpointPublicAccess`

Tipo: Booleano

Valor predeterminado: `False`

Descripción: (opcional) Defina este valor para deshabilitar el acceso público `False` al punto final del servidor de la API de Kubernetes de su clúster. Si inhabilitas el acceso público, el servidor de API de Kubernetes de tu clúster solo podrá recibir solicitudes desde la VPC en la que se lanzó.

- `PublicAccessCIDRs`

Tipo: `StringList`

Descripción: (opcional) El CIDR bloquea el acceso al punto final del servidor de API de Kubernetes público de tu clúster. Se deniega la comunicación al punto de conexión desde direcciones fuera de los bloques de CIDR que se especifiquen. Si ha desactivado el acceso a los terminales privados y tiene nodos o pods de Fargate en el clúster, asegúrese de especificar los bloques CIDR necesarios.

- `SecurityGroupIds`

Tipo: `StringList`

Descripción: (opcional) Especifique uno o más grupos de seguridad para asociarlos a las interfaces de red elásticas creadas en su cuenta por Amazon EKS.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `Create EKSCluster (aws:executeAwsApi)`: crea un clúster de Amazon EKS.
- `Verify EKSCluster IsActive (aws: waitForAwsResourceProperty)` - Comprueba que el estado del clúster es `ACTIVE`.
- `CreateFargateProfile (aws:executeAwsApi)` - Crea un Fargate para el clúster.
- `VerifyFargateProfileIsActive (aws: waitForAwsResourceProperty)` - Verifica el estado del perfil de Fargate. `ACTIVE`

Salidas

`CreateEKSCluster.CreateClusterResponse`

Descripción: Respuesta recibida de la llamada a la `CreateCluster` API.

`CreateFargateProfile.CreateFargateProfileResponse`

Descripción: Respuesta recibida de la llamada a la `CreateFargateProfile` API.

AWS-CreateEKSClusterWithNodegroup

Descripción

El AWS-CreateEKSClusterWithNodegroup manual crea un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) utilizando un grupo de nodos para aumentar la capacidad.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ClusterName

Tipo: cadena

Descripción: (obligatorio) Nombre exclusivo para el clúster.

- ClusterRoleArn

Tipo: cadena

Descripción: (obligatorio) El ARN de la función de IAM que proporciona permisos para que el plano de control de Kubernetes realice llamadas a AWS las operaciones de la API en su nombre.

- **NodegroupName**

Tipo: cadena

Descripción: (obligatorio) Un nombre único para el grupo de nodos.

- **NodegroupRoleArn**

Tipo: cadena

Descripción: (obligatorio) El ARN del rol de IAM que se va a asociar al grupo de nodos. El daemon kubelet del nodo de trabajo de Amazon EKS realiza llamadas AWS APIs en su nombre. Los nodos reciben permisos de dichas llamadas de API a través de políticas asociadas y de un perfil de instancias de IAM. Antes de poder lanzar nodos y registrarlos en un clúster, debe crear un rol de IAM para dichos nodos, para utilizarlo cuando se lancen.

- **SubnetIds**

Tipo: StringList

Descripción: (Obligatoria) Las IDs subredes que quiere usar para su clúster de Amazon EKS. Amazon EKS crea interfaces de red elásticas en estas subredes para la comunicación entre los nodos y el plano de control de Kubernetes. Debe especificar al menos dos subredes. IDs

- **EKSEndpointPrivateAccess**

Tipo: Booleano

Valor predeterminado: True

Descripción: (opcional) Defina este valor para permitir el acceso privado True al punto final del servidor de la API de Kubernetes de su clúster. Si habilita el acceso privado, las solicitudes de la API de Kubernetes desde la VPC del clúster utilizan el punto de conexión de VPC privada. Si deshabilita el acceso privado y tiene nodos o AWS Fargate pods en el clúster, asegúrese de `publicAccessCidrs` incluir los bloques CIDR necesarios para la comunicación con los nodos o los pods de Fargate.

- **EKSEndpointPublicAccess**

Tipo: Booleano

Valor predeterminado: False

Descripción: (opcional) Defina este valor para deshabilitar el acceso público `False` al punto final del servidor de la API de Kubernetes de su clúster. Si inhabilitas el acceso público, el servidor de API de Kubernetes de tu clúster solo podrá recibir solicitudes desde la VPC en la que se lanzó.

- `PublicAccessCIDRs`

Tipo: `StringList`

Descripción: (opcional) El CIDR bloquea el acceso al punto final del servidor de API de Kubernetes público de tu clúster. Se deniega la comunicación al punto de conexión desde direcciones fuera de los bloques de CIDR que se especifiquen. Si ha desactivado el acceso a los terminales privados y tiene nodos o pods de Fargate en el clúster, asegúrese de especificar los bloques CIDR necesarios.

- `SecurityGroupIds`

Tipo: `StringList`

Descripción: (opcional) Especifique uno o más grupos de seguridad para asociarlos a las interfaces de red elásticas creadas en su cuenta por Amazon EKS.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

Pasos de documentos

- `CreateEKSCluster` (aws:executeAwsApi): crea un clúster de Amazon EKS.
- `VerifyEKSClusterIsActive` (aws: waitForAwsResourceProperty) - Comprueba que el estado del clúster es `ACTIVE`.
- `CreateNodegroup` (aws:executeAwsApi) - Crea un grupo de nodos para el clúster.
- `VerifyNodegroupIsActive` (aws: waitForAwsResourceProperty) - Verifica el estado del grupo de nodos. `ACTIVE`

Salidas

- `CreateEKSCluster.CreateClusterResponse`: Respuesta recibida de la llamada a la `CreateCluster` API.
- `CreateNodegroup.CreateNodegroupResponse`: Respuesta recibida de la llamada a la `CreateNodegroup` API.

AWS-DeleteEKSCluster

Descripción

Este manual de procedimientos elimina los recursos asociados a un clúster de Amazon EKS, incluyendo los grupos de nodos y los perfiles de Fargate. Si lo desea, puede optar por eliminar todos los nodos autogestionados, las CloudFormation pilas utilizadas para crear los nodos y la CloudFormation pila de VPC de su clúster. Para obtener más información sobre cómo eliminar un clúster, consulte [Eliminación de un clúster](#) en la Guía del usuario de Amazon EKS.

Note

Si tiene en el clúster servicios activos asociados a un equilibrador de carga, deberá eliminar los servicios antes de eliminar el clúster. Si no lo hace, el sistema no podrá eliminar los equilibradores de carga. Utilice el siguiente procedimiento para buscar y eliminar servicios antes de ejecutar el manual de procedimientos `AWS-DeleteEKSCluster`.

Cómo localizar y eliminar los servicios del clúster

1. Instale la utilidad de línea de comandos de Kubernetes, `kubectl`. Para obtener más información, consulte [Instalación del kubectl](#) en la Guía del usuario de Amazon EKS.
2. Ejecute el siguiente comando para enumerar todos los servicios que se ejecutan en su clúster.

```
kubectl get svc --all-namespaces
```

3. Ejecute el siguiente comando para eliminar cualquier servicio que tenga un valor de IP EXTERNO asociado. Estos servicios se presentan por medio de un equilibrador de carga de y debe eliminarlos en Kubernetes para que el equilibrador y los recursos asociados se liberen correctamente.

```
kubectl delete svc  
service-name
```

Ahora puede ejecutar el manual de procedimientos `AWS-DeleteEKSCluster`.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **EKSClusterNombre**

Tipo: cadena

Descripción: (obligatorio) el nombre del clúster de Amazon EKS que se va a eliminar.

- **VPCCloudFormationStack**

Tipo: cadena

Descripción: nombre de CloudFormation pila (opcional) para la VPC del clúster de EKS que se va a eliminar. Esto elimina la CloudFormation pila de la VPC y todos los recursos creados por la pila.

- **VPCCloudFormationStackRole**

Tipo: cadena

Descripción: (opcional) El ARN de una función de IAM que CloudFormation supone eliminar la pila de VPC. CloudFormation CloudFormation utiliza las credenciales del rol para realizar llamadas en tu nombre.

- **SelfManagedNodeStacks**

Tipo: cadena

Descripción: (opcional) Lista de nombres de CloudFormation pila separados por comas para los nodos autogestionados. Esto eliminará las CloudFormation pilas de los nodos autogestionados.

- **SelfManagedNodeStacksRole**

Tipo: cadena

Descripción: (opcional) El ARN de una función de IAM que CloudFormation asume la eliminación de las pilas de nodos autogestionadas. CloudFormation utiliza las credenciales del rol para realizar llamadas en tu nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `sts:AssumeRole`
- `eks:ListNodegroups`
- `eks:DeleteNodegroup`
- `eks:ListFargateProfiles`
- `eks:DeleteFargateProfile`
- `eks:DeleteCluster`
- `cfn:DescribeStacks`
- `cfn>DeleteStack`

Pasos de documentos

- `aws:executeScript- DeleteNodeGroups`: Busque y elimine todos los grupos de nodos del clúster de EKS.
- `aws:executeScript- DeleteFargateProfiles`: Busque y elimine todos los perfiles de Fargate en el clúster EKS.
- `aws:executeScript- DeleteSelfManagedNodes`: Elimine todos los nodos autogestionados y las CloudFormation pilas utilizadas para crear los nodos.
- `aws:executeScript- EliminarEKSCluster`: elimine el clúster EKS.
- `aws:executeScript- Eliminar VPCCloudFormationStack`: elimina la pila de VPC. CloudFormation

AWS-MigrateToNewEKSSelfManagedNodeGroup

Descripción

El AWS-MigrateToNewEKSSelfManagedNodeGroup manual le ayuda a crear un nuevo grupo de nodos de Linux de Amazon Elastic Kubernetes Service (Amazon EKS) al que migrar la aplicación existente. Para obtener más información, consulte [Migración a un nuevo grupo de nodos](#) en la Guía del usuario de Amazon EKS.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- OldStackName

Tipo: cadena

Descripción: (obligatorio) El nombre o el ID de pila de su CloudFormation pila existente.

- NewStackName

Tipo: cadena

Descripción: (opcional) El nombre de la nueva CloudFormation pila que se crea para el nuevo grupo de nodos. Si no especificas un valor para este parámetro, el nombre de la pila se crea con el formato: `NewNodeGroup-ClusterName-AutomationExecutionID`.

- ClusterControlPlaneSecurityGroup

Tipo: cadena

Descripción: (opcional) El ID del grupo de seguridad que desea que usen los nodos para comunicarse con el plano de control de Amazon EKS. Si no especifica un valor para este parámetro, se utilizará el grupo de seguridad especificado en la CloudFormation pila existente.

- NodeInstanceType

Tipo: cadena

Descripción: (opcional) El tipo de instancia que quieres usar para el nuevo grupo de nodos. Si no especificas un valor para este parámetro, se usará el tipo de instancia especificado en tu CloudFormation pila existente.

- NodeGroupName

Tipo: cadena

Descripción: (opcional) El nombre del nuevo grupo de nodos. Si no especificas un valor para este parámetro, se utilizará el nombre del grupo de nodos especificado en la CloudFormation pila existente.

- NodeAutoScalingGroupDesiredCapacity

Tipo: cadena

Descripción: (opcional) La cantidad de nodos a los que se debe escalar cuando se cree la nueva pila. Este número debe ser mayor o igual que el NodeAutoScalingGroupMinSize valor y menor o igual que NodeAutoScalingGroupMaxSize. Si no especificas un valor para este parámetro, se utilizará la capacidad deseada del grupo de nodos especificada en la CloudFormation pila existente.

- NodeAutoScalingGroupMaxSize

Tipo: cadena

Descripción: (opcional) El número máximo de nodos al que puede ampliarse tu grupo de nodos. Si no especificas un valor para este parámetro, se utilizará el tamaño máximo del grupo de nodos especificado en la CloudFormation pila existente.

- NodeAutoScalingGroupMinSize

Tipo: cadena

Descripción: (opcional) La cantidad mínima de nodos a la que puede ampliarse tu grupo de nodos. Si no especificas un valor para este parámetro, se utilizará el tamaño mínimo del grupo de nodos especificado en la CloudFormation pila existente.

- NodeImageId

Tipo: cadena

Descripción: (opcional) el ID del Amazon Machine Image (AMI) que desea que utilice el grupo de nodos.

- `NodeImageIdSSMParam`

Tipo: cadena

Descripción: (opcional) el parámetro público de Systems Manager para la AMI que desea que utilice el grupo de nodos.

- `NodeVolumeSize`

Tipo: cadena

Descripción: (opcional) El tamaño del volumen raíz de los nodos en GiB. Si no especificas un valor para este parámetro, se utilizará el tamaño del volumen de nodo especificado en la CloudFormation pila existente.

- `NodeVolumeType`

Tipo: cadena

Descripción: (opcional) El tipo de volumen de Amazon EBS que desea utilizar para el volumen raíz de sus nodos. Si no especifica un valor para este parámetro, se utilizará el tipo de volumen especificado en la CloudFormation pila existente.

- `KeyName`

Tipo: cadena

Descripción: (opcional) El key pair que quieres asignar a tus nodos. Si no especificas un valor para este parámetro, se utilizará el par de claves especificado en la CloudFormation pila existente.

- `Subredes`

Tipo: `StringList`

Descripción: (opcional) Una lista separada por comas de la subred IDs que quieres usar para tu nuevo grupo de nodos. Si no especificas un valor para este parámetro, se utilizarán las subredes especificadas en la pila existente CloudFormation .

- `Desactivar IMDSv1`

Tipo: Booleano

Descripción: (opcional) Especifique si `true` desea deshabilitar la versión 1 del servicio de metadatos de instancia (IMDSv1). De forma predeterminada, los nodos admiten IMDSv1 y IMDSv2.

- `BootstrapArguments`

Tipo: cadena

Descripción: (opcional) Argumentos adicionales que desea pasar al script de arranque del nodo.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `DetermineParameterValuesForNewNodeGroup` (AWS:ExecuteScript): recopila los valores de los parámetros que se utilizarán en el nuevo grupo de nodos.
- `CreateStack` (aws:CreateStack): crea la pila para el nuevo grupo de nodos. CloudFormation
- `GetNewStackNodeInstanceRole` (aws:executeAwsApi) - Obtiene la función de instancia del nodo.
- `GetNewStackSecurityGroup` (aws:executeAwsApi) - El paso obtiene el grupo de seguridad del nodo.
- `AddIngressRulesToNewNodeSecurityGroup` (aws:executeAwsApi) - Añade reglas de entrada al grupo de seguridad recién creado para que pueda aceptar el tráfico del grupo de nodos anterior asignado al grupo de nodos anterior.
- `AddIngressRulesToOldNodeSecurityGroup` (aws:executeAwsApi) - Añade reglas de entrada al grupo de seguridad anterior para que pueda aceptar el tráfico del grupo asignado al grupo de nodos recién creado.
- `VerifyStackComplete` (aws: assertAwsResource Property): verifica que el estado de la nueva pila sea. `CREATE_COMPLETE`

Salidas

`DetermineParameterValuesForNewNodeGroup`. `NewStackParameters` - Los parámetros utilizados para crear la nueva pila.

`GetNewStackNodeInstanceRole`. `NewNodeInstanceRole` - La función de instancia de nodo para el nuevo grupo de nodos.

`GetNewStackSecurityGroup`. `NewNodeSecurityGroup` - El ID del grupo de seguridad del nuevo grupo de nodos.

`DetermineParameterValuesForNewNodeGroup`. `NewStackName` - El nombre de la CloudFormation pila del nuevo grupo de nodos.

`CreateStack`. `StackId` - El ID de CloudFormation pila del nuevo grupo de nodos.

AWSPremiumSupport-TroubleshootEKSCluster

Descripción

El manual de procedimientos `AWSPremiumSupport-TroubleshootEKSCluster` diagnostica problemas comunes con un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) y la infraestructura subyacente y proporciona las medidas de corrección recomendadas.

⚠ Important

El acceso a `AWSPremiumSupport` - * los manuales requiere una suscripción a Business + Support, Enterprise Support o Unified Operations. Para obtener más información, consulte [Comparar planes de AWS Support](#).

Si especifica un valor para el parámetro `S3BucketName`, la automatización evalúa el estado de la política del bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Para mejorar la seguridad de los registros recopilados de su instancia EC2, si el estado de la política `isPublic` está establecido en `true` o si la lista de control de acceso (ACL) concede permisos de `READ|WRITE` al grupo predefinido de `All Users Amazon S3`, los registros no se cargan. Para obtener más información acerca de los grupos predefinidos de Amazon S3, consulte los [Grupos predefinidos de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `ClusterName`

Tipo: cadena

Descripción: (obligatorio) el nombre del clúster de Amazon EKS del que desea solucionar problemas.

- S3 BucketName

Tipo: cadena

Descripción: (Obligatorio) El nombre del depósito privado de Amazon S3 en el que se debe cargar el informe generado por el runbook.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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

Además, la política AWS Identity and Access Management (IAM) asociada al usuario o rol que inicia la automatización debe permitir la `ssm:GetParameter` operación con los siguientes AWS Systems Manager parámetros públicos para obtener la última versión recomendada de Amazon EKS Amazon Machine Image (AMI) para los nodos de trabajo.

- `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`

Para cargar el informe generado por el manual de procedimientos en un bucket de Amazon S3, se requieren los siguientes permisos para el bucket específico de Amazon S3 que especifique.

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

Pasos de documentos

- `aws:executeAwsApi`: recopila detalles para el clúster de Amazon EKS especificado.
- `aws:executeScript`: recopila detalles de las instancias de Amazon Elastic Compute Cloud (Amazon EC2), los grupos de escalado automático, AMI y los tipos de instancias gráficas de GPU de Amazon EC2.
- `aws:executeScript`- Recopila detalles de la nube privada virtual (VPC), las subredes, las pasarelas de traducción de direcciones de red (NAT), las rutas de subred, los grupos de seguridad y las listas de control de acceso a la red (ACLs) del clúster de Amazon EKS.
- `aws:executeScript`: recopila detalles de los perfiles de instancias y políticas de funciones de IAM adjuntos.

- `aws:executeScript`: recopila detalles del bucket de Amazon S3 que especifique en el parámetro `S3BucketName`.
- `aws:executeScript`: clasifica las subredes de Amazon VPC como públicas o privadas.
- `aws:executeScript`: comprueba las subredes de Amazon VPC en busca de las etiquetas que se requieren como parte de un clúster de Amazon EKS.
- `aws:executeScript`: comprueba las subredes de Amazon VPC en busca de las etiquetas necesarias para las subredes de Elastic Load Balancing.
- `aws:executeScript`: comprueba si las instancias de Amazon EC2 del nodo de trabajo utilizan la última versión optimizada de Amazon EKS AMI.
- `aws:executeScript`: comprueba si los grupos de seguridad de Amazon VPC conectados a los nodos de trabajo tienen las etiquetas necesarias.
- `aws:executeScript`: comprueba las reglas del grupo de seguridad del clúster de Amazon EKS y del nodo de trabajo de Amazon VPC para las reglas de entrada recomendadas para el clúster de Amazon EKS.
- `aws:executeScript`: comprueba las reglas del grupo de seguridad del clúster de Amazon EKS y del nodo de trabajo de Amazon VPC para las reglas de salida recomendadas desde el clúster de Amazon EKS.
- `aws:executeScript`: comprueba la configuración de ACL de red de las subredes de Amazon VPC.
- `aws:executeScript`: comprueba si las instancias Amazon EC2 del nodo de trabajo tienen las políticas gestionadas requeridas.
- `aws:executeScript`: comprueba si los grupos de escalado automático tienen las etiquetas necesarias para el escalado automático del clúster.
- `aws:executeScript`: comprueba si las instancias Amazon EC2 del nodo de trabajo están conectadas a Internet.
- `aws:executeScript`: genera un informe basado en los resultados de los pasos anteriores. Si se especifica un valor para el parámetro `S3BucketName`, el informe generado se carga en el bucket de Amazon S3.

AWSSupport-TroubleshootEKSTaskWorkerNode

Descripción

El manual de procedimientos `AWSsupport-TroubleshootEKSWorkerNode` analiza un nodo de trabajo de Amazon Elastic Compute Cloud (Amazon EC2) y un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) para ayudarle a identificar y solucionar las causas comunes que impiden que los nodos de trabajo se unan a un clúster. El manual de procedimientos contiene una guía que le ayudará a resolver cualquier problema que identifique.

 Important

Para ejecutar correctamente esta automatización, el estado del nodo de trabajo de Amazon EC2 debe ser `running`, y el estado del clúster de Amazon EKS debe ser `ACTIVE`.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `ClusterName`

Tipo: cadena

Descripción: (obligatorio) el nombre del clúster de Amazon EKS.

- WorkerID

Tipo: cadena

Descripción: (obligatorio) el ID del nodo de trabajo de Amazon EC2 que no pudo unirse al clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el clúster de Amazon EKS que especifique en el parámetro `ClusterName` existe y se encuentra en un estado `ACTIVE`.
- `aws:assertAwsResourceProperty`: confirma que el nodo de trabajo de Amazon EC2 que especifique en el parámetro `WorkerID` existe y se encuentra en un estado `running`.
- `aws:executeScript`: ejecuta un script de Python que ayuda a identificar las posibles causas por las que el nodo de trabajo no se une al clúster.

AWS-UpdateEKSCluster

Descripción

El `AWS-UpdateEKSCluster` manual le ayuda a actualizar el clúster de Amazon Elastic Kubernetes Service (Amazon EKS) a la versión de Kubernetes que desee utilizar.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `ClusterName`

Tipo: cadena

Descripción: (obligatorio) El nombre del clúster de Amazon EKS.

- Versión

Tipo: cadena

Descripción: (Obligatoria) La versión de Kubernetes a la que desea actualizar el clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `eks:DescribeUpdate`
- `eks:UpdateClusterVersion`

Pasos de documentos

- `aws:executeAwsApi`- Actualiza la versión de Kubernetes que utiliza su clúster de Amazon EKS.
- `aws:waitForAwsResourceProperty`- Espera a que aparezca el estado de la actualización.
`Successful`

AWS-UpdateEKSMangedNodeGroup

Descripción

El manual de procedimientos `AWS-UpdateEKSMangedNodeGroup` le ayuda a actualizar un grupo de nodos administrado de Amazon Elastic Kubernetes Service (Amazon EKS). Puede elegir entre una actualización de `Version` o `Configuration`.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ClusterName

Tipo: cadena

Descripción: (obligatorio) el nombre del clúster cuyo grupo de nodos desea actualizar.

- NodeGroupName

Tipo: cadena

Descripción: (obligatorio) el nombre del grupo de nodos para actualizar.

- UpdateType

Tipo: cadena

Valores válidos: Update Node Group Version | Update Node Group Configurations

Predeterminado: actualizar la versión del grupo de nodos

Descripción: (obligatorio) el tipo de actualización que desea realizar en el grupo de nodos.

Los siguientes parámetros solo se aplican al tipo de actualización `Version`:

- AMIReleaseVersion

Tipo: cadena

Descripción: (opcional) la versión optimizada de Amazon EKS AML que desea utilizar. Por defecto, se utiliza la última versión.

- ForceUpgrade

Tipo: Booleano

Descripción: (opcional) si es cierto, la actualización no fallará en respuesta a una infracción del presupuesto por interrupción del pod.

- KubernetesVersion

Tipo: cadena

Descripción: (opcional) la versión de Kubernetes a la que actualizar el grupo de nodos.

- LaunchTemplateId

Tipo: cadena

Descripción: (opcional) el ID de la plantilla de lanzamiento.

- LaunchTemplateName

Tipo: cadena

Descripción: (opcional) el nombre de la plantilla de lanzamiento.

- LaunchTemplateVersion

Tipo: cadena

Descripción: (opcional) la versión de la plantilla de lanzamiento de Amazon Elastic Compute Cloud (Amazon EC2). Este parámetro solo es válido si se creó un grupo de nodos a partir de una plantilla de lanzamiento.

Los siguientes parámetros solo se aplican al tipo de actualización Configuration:

- AddOrUpdateNodeGroupLabels

Tipo: StringMap

Descripción: (opcional) etiquetas de Kubernetes que desea añadir o actualizar.

- AddOrUpdateKubernetesTaintsEffect

Tipo: StringList

Descripción: (opcional) las taints de Kubernetes que desea añadir o actualizar.

- MaxUnavailableNodeGroups

Tipo: entero

Predeterminado: 0

Descripción: (opcional) número máximo de nodos no disponibles a la vez durante una actualización de versión.

- MaxUnavailablePercentageNodeGroup

Tipo: entero

Predeterminado: 0

Descripción: (opcional) el porcentaje de nodos que no están disponibles durante una actualización de versión.

- NodeGroupDesiredSize

Tipo: entero

Predeterminado: 0

Descripción: (opcional) cantidad actual de nodos que debería conservar el grupo de nodos administrados.

- NodeGroupMaxSize

Tipo: entero

Predeterminado: 0

Descripción: (opcional) cantidad máxima de nodos a los que puede escalar horizontalmente el grupo de nodos administrados.

- NodeGroupMinSize

Tipo: entero

Predeterminado: 0

Descripción: (opcional) cantidad mínima de nodos a los que puede reducir horizontalmente el grupo de nodos administrados.

- `RemoveKubernetesTaintsEffect`

Tipo: `StringList`

Descripción: (opcional) las taints de Kubernetes que desea eliminar.

- `RemoveNodeGroupLabels`

Tipo: `StringList`

Descripción: (opcional) una lista separada por comas de etiquetas que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

Pasos de documentos

- `aws:executeScript`: actualiza un grupo de nodos de un clúster de Amazon EKS según los valores que especifique para los parámetros de entrada del manual de procedimientos.
- `aws:waitForAwsResourceProperty`: espera a que el estado de actualización del clúster sea `Successful`.

AWS-UpdateEKSSelfManagedLinuxNodeGroups

Descripción

El manual de procedimientos `AWS-UpdateEKSSelfManagedLinuxNodeGroups` actualiza los grupos de nodos autogestionados del clúster de Amazon Elastic Kubernetes Service (Amazon EKS) mediante una pila `AWS CloudFormation`.

Si su clúster usa el escalado automático, le recomendamos que escale la implementación a dos réplicas antes de usar este manual de procedimientos.

Cómo escalar una implementación a dos réplicas

1. Instale la utilidad de línea de comandos de Kubernetes, `kubectl`. Para obtener más información, consulte [Instalación del kubectl](#) en la Guía del usuario de Amazon EKS.
2. Ejecute el comando siguiente.

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. Ejecute el manual de procedimientos `AWS-UpdateEKSSelfManagedLinuxNodeGroups`.
4. Escale la implementación de regreso al número deseado de réplicas ejecutando el siguiente comando.

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **ClusterName**

Tipo: cadena

Descripción: (obligatorio) el nombre del clúster de Amazon EKS.

- **NodeGroupName**

Tipo: cadena

Descripción: (obligatorio) el nombre del grupo de nodos administrados.

- **ClusterControlPlaneSecurityGroup**

Tipo: cadena

Descripción: (obligatorio) el ID del grupo de seguridad del plano de control.

- **Desactivar IMDSv1**

Tipo: Booleano

Descripción: (opcional) Determina si desea permitir las versiones 1 (IMDSv1) y IMDSv2.

- **KeyName**

Tipo: cadena

Descripción: (opcional) nombre de la clave para las instancias.

- **NodeAutoScalingGroupDesiredCapacity**

Tipo: cadena

Descripción: (opcional) el número de nodos que debe conservar el grupo de nodos.

- **NodeAutoScalingGroupMaxSize**

Tipo: cadena

Descripción: (opcional) cantidad máxima de nodos a los que puede escalar horizontalmente el grupo de nodos.

- **NodeAutoScalingGroupMinSize**

Tipo: cadena

Descripción: (opcional) cantidad mínima de nodos a los que puede reducir horizontalmente el grupo de nodos.

- **NodeInstanceType**

Tipo: cadena

Valor predeterminado: t3.large

Descripción: (opcional) el tipo de instancia que desea usar para el grupo de nodos.

- **NodeImageId**

Tipo: cadena

Descripción: (opcional) el ID del Amazon Machine Image (AMI) que desea que utilice el grupo de nodos.

- **NodeImageIdSSMParam**

Tipo: cadena

Predeterminado:/aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

Descripción: (opcional) el parámetro público de Systems Manager para la AMI que desea que utilice el grupo de nodos.

- **StackName**

Tipo: cadena

Descripción: (obligatorio) El nombre de la CloudFormation pila utilizada para actualizar el grupo de nodos.

- **Subredes**

Tipo: cadena

Descripción: (Obligatorio) Una lista separada IDs por comas de las subredes que desea que utilice su clúster.

- **VpcId**

Tipo: cadena

Valor predeterminado: Default

Descripción: (obligatorio) la nube privada virtual (VPC) donde se implementa el clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks>DeleteNodegroup`
- `eks>DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

Pasos de documentos

- `aws:executeScript`: actualiza un grupo de nodos de un clúster de Amazon EKS según los valores que especifique para los parámetros de entrada del manual de procedimientos.
- `aws:waitForAwsResourceProperty`- Espera a que se devuelva el estado de actualización de la CloudFormation pila.

AWSSupport-CollectEKSLinuxNodeStatistics

Descripción

El `AWSSupport-CollectEKSLinuxNodeStatistics` runbook recopila estadísticas de Linux de una instancia de Amazon EC2 que forma parte de un clúster de Amazon EKS y de un contenedor que se ejecuta en la instancia si se especifica `containerid` un ID de contenedor. La instancia de Amazon EC2 debe gestionarla. AWS Systems Manager

Las estadísticas de Linux a nivel de host recopiladas incluyen:

- Información del sistema operativo.
- Estadísticas de la interfaz de red: desde `ethtool` y `/sys/class/net/interface/statistics` directorio.
- Recuentos de descriptores de archivos.
- Los puertos efímeros cuentan.
- Un basurero de reglas. `iptables`
- Comprueba si hay una tabla de conexiones completa.

Las estadísticas de Linux a nivel de contenedor incluyen:

- Información sobre el identificador: URI de la imagen y etiquetas.
- Estadísticas de la interfaz de red: desde `ethtool` y `/sys/class/net/interface/statistics` directorio.
- Si se rellena el `NetworkTargets` parámetro, se obtienen los resultados de Traceroute y DNS.
- El análisis de captura de paquetes cuenta: retransmisiones TCP, paquetes fuera de servicio, etc.

El runbook recopila datos de varias distribuciones de Linux, incluidas Amazon Linux 2, Amazon Linux 2023 y Debian/Ubuntu. Utiliza las versiones más recientes de las siguientes imágenes de la galería pública de Amazon ECR:

- `amazon-ecs-network-sidecar` imagen para acceder a las herramientas de solución de problemas.
- `aws-cli` imagen para cargar el archivo JSON y los archivos de captura de paquetes del informe de estadísticas en el bucket de Amazon S3 especificado.

Important

Este manual no es compatible con las instancias de Fargate. Este runbook puede fallar si la instancia se apaga o se desconecta durante la ejecución.

¿Cómo funciona?

El manual de ejecución realiza las siguientes acciones:

- Verifica que el bucket de Amazon S3 de destino no conceda acceso público de lectura o escritura.
- Garantiza que la instancia Amazon EC2 de destino esté gestionada por Systems Manager y se encuentre en estado de ejecución.
- Verifica que la instancia ejecute un sistema operativo Linux.
- Recopila estadísticas completas de Linux de la instancia Amazon EC2 y, opcionalmente, de un contenedor específico.
- Carga las estadísticas recopiladas en el bucket de Amazon S3 especificado.

[Ejecuta esta automatización \(consola\)](#)

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

El `AutomationAssumeRole` parámetro requiere las siguientes acciones:

- `s3:GetAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketLocation`
- `s3:GetEncryptionConfiguration`
- `s3:PutObject`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `ec2:DescribeInstances`

Política de IAM de ejemplo:

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

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetAccountPublicAccessBlock"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketPublicAccessBlock",
      "s3:GetBucketAcl",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketLocation",
      "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::S3_BUCKET_NAME"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::S3_BUCKET_NAME/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:DescribeInstanceInformation"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:SendCommand"
    ],
    "Resource": [
      "arn:aws:ssm:*:*:document/AWS-RunShellScript",
      "arn:aws:ec2:*:111122223333:instance/*"
    ]
  },
  {

```



```

        "Effect": "Allow",
        "Action": [
            "ssm:GetCommandInvocation"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances"
        ],
        "Resource": "*"
    }
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-CollectEKSLinuxNodeStatistics](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) de la función de IAM que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId (Obligatorio):

El ID de la instancia Amazon EC2 para recopilar estadísticas.

- S3 BucketName (obligatorio):

Nombre del bucket de Amazon S3 para exportar la salida JSON de la instancia de Amazon EC2 como un archivo.

- S3 KeyPrefix (opcional):

El prefijo clave de Amazon S3 (subcarpeta) para exportar la salida JSON de la instancia de Amazon EC2 como un archivo. Predeterminado: `AWSSupport-CollectEKSLinuxNodeStatistics`.

- `S3 BucketOwnerRoleArn` (opcional):

El ARN de la función de IAM con permisos para obtener la configuración de acceso público del bucket y el bloqueo de cuentas de Amazon S3, la configuración de cifrado del bucket, el bucket ACLs, el estado de la política del bucket y cargar objetos al bucket. Si no se especifica este parámetro, el runbook utiliza el runbook `AutomationAssumeRole` (si se especifica) o el usuario que inicia este runbook (si no `AutomationAssumeRole` se especifica).

- `S3 BucketOwnerAccount` (opcional):

La AWS cuenta propietaria del bucket de Amazon S3. Si no especifica este parámetro, el runbook asume que el bucket está en esta cuenta.

- `ContainerId` (Opcional):

El ID de un contenedor que se ejecuta en la instancia de Amazon EC2 especificada.

- `NetworkTargets` (Opcional):

Una lista de IPv4 direcciones, nombres de and/or DNS separados por comas para probar la resolución del DNS y la conectividad mediante traceroute.

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **CheckBucketAccess:**

Comprueba si el bucket de Amazon S3 de destino puede conceder acceso público de lectura y and/or escritura a sus objetos.

- **AssertInstanceIsSSMManaged:**

Garantiza que Systems Manager administre la instancia Amazon EC2 de destino; de lo contrario, la automatización finaliza.

- **VerifyInstanceState:**

Comprueba que la instancia de Amazon EC2 esté en ejecución antes de intentar recopilar estadísticas.

- **BranchOnVerifyLinuxInstance:**

Comprueba que la instancia es una instancia de Linux antes de continuar.

- **BranchOnVerifyInstanceRunning:**

Comprueba que la instancia esté en ejecución antes de continuar.

- **CollectEKSLinuxNodeStatistics:**

Recopila estadísticas completas de Linux de la instancia Amazon EC2, que incluyen información del sistema operativo, estadísticas de la interfaz de red, descriptores de archivos, puertos efímeros, reglas de firewall y, opcionalmente, estadísticas a nivel de contenedor.

- **GenerateStatisticsOutputS3Uri:**

Genera el URI completo de Amazon S3 para los archivos de estadísticas de Linux que se utilizarán como salida del documento de automatización.

7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWSsupport-CollectEKSIInstanceLogs

Descripción

El manual de procedimientos AWSsupport-CollectEKSIInstanceLogs recopila los archivos de registro relacionados con el sistema operativo y Amazon Elastic Kubernetes Service (Amazon EKS) de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) para ayudarle a solucionar problemas comunes. Mientras la automatización recopila los archivos de registro asociados, se realizan cambios en la estructura del sistema de archivos, incluyendo la creación de directorios temporales, la copia de los archivos de registro en los directorios temporales y la compresión de los

archivos de registro en un archivo. Esta actividad puede provocar un aumento de `CPUUtilization` en la instancia de Amazon EC2. Para obtener más información `CPUUtilization`, consulta [las métricas de instancias](#) en la Guía del CloudWatch usuario de Amazon.

Si especifica un valor para el parámetro `LogDestination`, la automatización evalúa el estado de la política del bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Para mejorar la seguridad de los registros recopilados de su instancia de Amazon EC2, si el estado de la política `isPublic` está establecido en `true` o si la lista de control de acceso (ACL) concede permisos de `READ|WRITE` al grupo predefinido de `All Users` Amazon S3, los registros no se cargan. Para obtener más información acerca de los grupos predefinidos de Amazon S3, consulte los [Grupos predefinidos de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

 Note

Esta automatización requiere al menos el 10 por ciento del espacio en disco disponible en el volumen raíz de Amazon Elastic Block Store (Amazon EBS) adjunto a la instancia de Amazon EC2. Si no hay suficiente espacio en disco disponible en el volumen raíz, la automatización se detiene.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `EKSInstanceID`

Tipo: cadena

Descripción: (obligatorio) ID de la instancia Amazon EC2 de Amazon EKS de la que desea recopilar los registros.

- `LogDestination`

Tipo: cadena

Descripción: (Opcional) El depósito de Amazon Simple Storage Service (Amazon S3) de su cuenta en el que cargar los registros archivados.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Permisos de IAM necesarios para el perfil de instancia de Amazon EC2

El perfil de instancia utilizado por el `EKSInstanceId` debe tener adjunta la política gestionada por `SSMManagedInstanceCoreAmazon`.

También debe poder acceder al bucket de `LogDestination` Amazon S3 para poder cargar los registros recopilados. A continuación, se muestra un ejemplo de una política de IAM que podría adjuntarse a ese perfil de instancia:

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

```

    "Action": [
      "s3:PutObject",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketAcl"
    ],
    "Resource": [
      "arn:aws:s3:::LogDestination/*",
      "arn:aws:s3:::LogDestination"
    ]
  }
]
}

```

Si LogDestination utiliza el AWS KMS cifrado, se debe añadir una declaración adicional a la política de IAM que conceda acceso a la AWS KMS clave utilizada en el cifrado:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::LogDestination/*",
        "arn:aws:s3:::LogDestination"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:REGION:ACCOUNT:key/KMS-KEY-ID"
    }
  ]
}

```

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el sistema operativo del valor especificado en el parámetro `EKSInstanceId` es Linux.
- `aws:runCommand`: recopila los archivos de registro relacionados con el sistema operativo y Amazon EKS y los comprime en un archivo del directorio `/var/log`.
- `aws:branch`: confirma si se especificó un valor para el parámetro `LogDestination`.
- `aws:runCommand`: Carga el archivo de registro en el depósito de Amazon S3 que especifique en el `LogDestination` parámetro.

AWSSupport-SetupK8sApiProxyForEKS

Descripción

El manual de automatización de `AWSSupport-SetupK8sApiProxyForeKS` proporciona una forma de crear una AWS Lambda función que actúa como proxy para realizar llamadas a la API del plano de control al punto final del clúster de Amazon Elastic Kubernetes Service. Sirve como base para los runbooks que requieren realizar llamadas a la API del plano de control para automatizar tareas y solucionar problemas con un clúster de Amazon EKS.

Important

Todos los recursos creados por esta automatización están etiquetados para que se puedan encontrar fácilmente. Las etiquetas utilizadas son:

- `AWSSupport-SetupK8sApiProxyForEKS: true`

Note

- La automatización es un manual auxiliar y no se puede ejecutar como un manual independiente. Se invoca como una automatización secundaria para los runbooks que requieren llamadas a la API del plano de control al clúster Amazon EKS.
- Asegúrese de ejecutar la `Cleanup` operación después del uso para evitar incurrir en costos no deseados.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ClusterName

Tipo: cadena

Descripción: (obligatorio) El nombre del clúster de Amazon Elastic Kubernetes Service.

- Operación

Tipo: cadena

Descripción: (Obligatoria) Operación a realizar: Setup aprovisiona la función Lambda en la cuenta y desaprovisiona Cleanup los recursos creados como parte de la fase de configuración.

Valores permitidos: | Setup Cleanup

Predeterminado: Configuración

- LambdaRoleArn

Tipo: cadena

Descripción: (opcional) El ARN del rol de IAM que permite a la AWS Lambda función acceder a los AWS servicios y recursos necesarios. Si no se especifica ningún rol, Systems Manager Automation creará un rol de IAM para Lambda en su cuenta con el Automation-K8sProxy-

Role- <ExecutionId> nombre que incluye las políticas AWSLambdaBasicExecutionRole administradas: y. AWSLambdaVPCAccessExecutionRole

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Valida que la automatización se esté ejecutando como una ejecución secundaria. El manual de ejecución no funcionará cuando se invoque como un manual independiente, ya que no realiza ningún trabajo significativo por sí solo.
- Comprueba la CloudFormation pila existente de la función Lambda proxy para el clúster especificado.
 - Si la pila existe, la infraestructura existente se reutiliza en lugar de volver a crearla.
 - Se mantiene un contador de referencias mediante etiquetas para garantizar que un runbook no elimine la infraestructura si otro runbook la reutiliza para el mismo clúster.
- Realice el tipo de operación (Setup/Cleanup) especificado para la invocación:
 - Configuración: crea o describe los recursos existentes.

Limpieza: elimina los recursos aprovisionados si la infraestructura no está siendo utilizada por ningún otro manual.

Permisos de IAM necesarios

El AutomationAssumeRole parámetro requiere que no se pasen los siguientes permisos LambdaRoleArn:

- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation>DeleteStack
- cloudformation:UpdateStack
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets

- `ec2:DescribeVpcs`
- `ec2:DeleteNetworkInterface`
- `eks:DescribeCluster`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:ListTags`
- `lambda:GetFunction`
- `lambda:ListTags`
- `lambda:TagResource`
- `lambda:UntagResource`
- `lambda:UpdateFunctionCode`
- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:TagResource`
- `logs:UntagResource`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:ListTagsForResource`
- `iam:CreateRole`
- `iam:AttachRolePolicy`
- `iam:DetachRolePolicy`
- `iam:PassRole`
- `iam:GetRole`
- `iam>DeleteRole`
- `iam:TagRole`
- `iam:UntagRole`
- `tag:GetResources`
- `tag:TagResources`

Cuando `LambdaRoleArn` se proporciona, la automatización no necesita crear el rol y se pueden excluir los siguientes permisos:

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

A continuación, se muestra un ejemplo de política que demuestra los permisos necesarios AutomationAssumeRole cuando no LambdaRoleArn se aprueban:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "eks:DescribeCluster",
        "iam:GetRole",
        "cloudformation:DescribeStacks",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "lambda:GetFunction",
        "lambda:ListTags",
        "logs:ListTagsForResource"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowActionsWithoutConditions"
    },
    {
```

```

    "Condition": {
      "StringEquals": {
        "aws:RequestTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
      }
    },
    "Action": "iam:CreateRole",
    "Resource": [
      "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "AllowCreateRoleWithRequiredTag"
  },
  {
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
      }
    },
    "Action": [
      "iam:DeleteRole",
      "iam:TagRole",
      "iam:UntagRole"
    ],
    "Resource": [
      "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "IAMActions"
  },
  {
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
      },
      "StringLike": {
        "iam:PolicyARN": [
          "arn:aws:iam::111122223333:policy/service-role/
AWSLambdaBasicExecutionRole",
          "arn:aws:iam::111122223333:policy/service-role/
AWSLambdaVPCLambdaAccessExecutionRole"
        ]
      }
    },
    "Action": [

```

```

        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "AttachRolePolicy"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode"
    ],
    "Resource": "arn:aws:lambda:us-east-1:111122223333:function:Automation-K8sProxy*",
    "Effect": "Allow",
    "Sid": "LambdaActions"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
    ],
    "Resource": "arn:aws:cloudformation:us-east-1:111122223333:stack/AWSSupport-SetupK8sApiProxyForEKS*",
    "Effect": "Allow",
    "Sid": "CloudFormationActions"
},
{

```

```

        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
            }
        },
        "Action": [
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:PutLogEvents",
            "logs:PutRetentionPolicy",
            "logs:TagResource",
            "logs:UntagResource"
        ],
        "Resource": [
            "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/Automation-K8sProxy*",
            "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/Automation-K8sProxy*:*"
        ],
        "Effect": "Allow",
        "Sid": "LogsActions"
    },
    {
        "Condition": {
            "StringLikeIfExists": {
                "iam:PassedToService": "lambda.amazonaws.com"
            }
        },
        "Action": [
            "iam:PassRole"
        ],
        "Resource": [
            "arn:aws:iam::111122223333:role/Automation-K8sProxy-Role*"
        ],
        "Effect": "Allow",
        "Sid": "PassRoleToLambda"
    }
]
}

```

En caso de que `LambdaRoleArn` se apruebe, asegúrese de que tenga una [AWSLambdaBasicExecutionRole](#) política adjunta para los clústeres públicos y, además, [AWSLambdaVPCLambdaAccessExecutionRole](#) para los clústeres privados.

Recursos creados

Los siguientes recursos se crean durante la `Setup` operación:

1. AWS Lambda función
2. Función de IAM: función de ejecución de Lambda, si no se proporciona.
3. CloudWatch Grupo de registros (registros Lambda)

La función Lambda y el rol de ejecución se conservan hasta que se ejecute `Cleanup` la operación. El grupo de registros Lambda se conservará durante 30 días o hasta que se elimine manualmente.

Instrucciones

El runbook es una utilidad auxiliar diseñada para ejecutarse desde otros runbooks como una automatización secundaria. Facilita la creación de una infraestructura que permite al runbook principal realizar llamadas a la API del plano de control de Amazon EKS K8. Para utilizar el manual, puede seguir los pasos que se indican a continuación desde el contexto de la automatización principal.

1. Fase de configuración: invoque la automatización mediante una operación de `aws:executeAutomation` acción del manual que desee realizar llamadas a la API del plano de control de Amazon EKS K8 con la operación establecida en. `Setup`

Ejemplo de parámetros de entrada:

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Setup"
}
```

El resultado del `aws:executeAutomation` paso contendrá el ARN de la función Lambda proxy.

2. Uso del proxy Lambda: invoca la función Lambda dentro de la `aws:executeScript` acción que utiliza `Lambda.Client.invoke(...)` con una lista de rutas `boto3` de llamadas a la API y

un token de portador. La función Lambda realizará GET llamadas HTTP a la ruta especificada pasando el token portador como parte del encabezado de autorización.

Ejemplo de evento de invocación de Lambda:

```
{
  "ApiCalls": ["/api/v1/pods/", ...],
  "BearerToken": "..."
```

Note

El token portador debe generarse como parte del script de automatización principal. Debe asegurarse de que la persona principal que ejecuta el runbook principal tenga permiso de solo lectura para el clúster de Amazon EKS especificado.

3. Fase de limpieza: invoque la automatización mediante una operación de `aws:executeAutomation` acción del manual que desee realizar llamadas a la API del plano de control de Amazon EKS K8 con la operación configurada en `Cleanup`

Ejemplo de parámetros de entrada:

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Cleanup"
}
```

Pasos de automatización

1. ValidateExecution

- Verifica que la automatización no se ejecute como una ejecución independiente.

2. CheckForExistingStack

- Comprueba si ya se ha aprovisionado una CloudFormation pila para el nombre del clúster especificado.
- Devuelve el estado de existencia de la pila y si es seguro eliminarla.

3. BranchOnIsStackExists

- Paso de decisión que se ramifica en función de la existencia de la pila.
- Rutas para actualizar el nombre de la pila existente o continuar con la ramificación de la operación.

4. UpdateStackName

- Actualiza la `StackName` variable con el nombre de la pila existente.
- Solo se ejecuta si la pila ya existe.

5. BranchOnOperation

- Enruta la automatización en función del `Operation` parámetro (Setup/Cleanup).
- `ParaSetup`: Rutas para crear una nueva pila o describir los recursos existentes.
- `ParaCleanup`: Procede a eliminar la pila si es seguro eliminarla.

6. GetClusterNetworkConfig

- Describe el clúster de Amazon EKS para obtener la configuración de VPC.
- Recupera datos de punto final, ID de VPC, IDs subred, ID de grupo de seguridad y CA.

7. ProvisionResources

- Crea una CloudFormation pila con los recursos necesarios.
- Aprovisiona la función Lambda con la configuración de red necesaria.
- Etiqueta todos los recursos para su seguimiento y administración.

8. DescribeStackResources

- Recupera información sobre la `created/existing` pila.
- Obtiene el ARN de la función Lambda aprovisionada.

9. BranchOnIsLambdaDeploymentRequired

- Determina si es necesario implementar código Lambda.
- Solo se procede al despliegue de las pilas recién creadas.

10DeployLambdaFunctionCode

- Implementa el código de la función Lambda mediante el paquete de despliegue.
- Actualiza la función con la implementación del proxy.

11AssertLambdaAvailable

- Comprueba que la actualización del código de la función Lambda se ha realizado correctamente.
- Espera a que la función esté en estado. `Successful`

12PerformStackCleanup

- Elimina la CloudFormation pila y los recursos asociados.
- Se ejecuta durante la Cleanup operación o en caso de fallo de la Setup operación.

Salidas

LambdaFunctionArn: ARN de la función Lambda proxy

Referencias

Automatización de Systems Manager

- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWSSupport-TroubleshootEbsCsiDriversForEks

Descripción

El AWSSupport-TroubleshootEbsCsiDriversForEks manual ayuda a solucionar problemas relacionados con los montajes de volumen de Amazon Elastic Block Store en Amazon Elastic Kubernetes Service (Amazon EKS) y problemas con los controladores de la interfaz de almacenamiento de contenedores (CSI) de Amazon EBS

Important

Actualmente, no se admite el controlador CSI de Amazon EBS que se AWS Fargate está ejecutando.

¿Cómo funciona?

El manual de ejecución AWSSupport-TroubleshootEbsCsiDriversForEks lleva a cabo los siguientes pasos de alto nivel:

- Comprueba si el clúster Amazon EKS de destino existe y se encuentra en estado activo.
- Implementa los recursos de autenticación necesarios para realizar llamadas a la API de Kubernetes en función de si el complemento está gestionado por Amazon EKS o autogestionado.

- Realiza comprobaciones de estado y diagnósticos del controlador CSI de Amazon EBS.
- Realiza comprobaciones de permisos de IAM en las funciones de los nodos y las funciones de las cuentas de servicio.
- Diagnostica los problemas persistentes de creación de volúmenes para el pod de aplicaciones especificado.
- Comprueba node-to-pod la programación y examina los eventos del pod.
- Recopila los registros de Kubernetes y aplicaciones relevantes y los carga en el bucket de Amazon S3 especificado.
- Realiza comprobaciones de estado de los nodos y verifica la conectividad con los puntos de enlace de Amazon EC2.
- Revisa los archivos adjuntos de los dispositivos de bloqueo de volumen persistente y el estado de montaje.
- Limpia la infraestructura de autenticación creada durante la resolución de problemas.
- Genera un informe completo de solución de problemas que combina todos los resultados del diagnóstico.

Note

- El modo de autenticación del clúster de Amazon EKS debe estar configurado en API o API_AND_CONFIG_MAP. Recomendamos utilizar la entrada Amazon EKS Access. El manual requiere permisos de control de acceso basado en roles (RBAC) de Kubernetes para realizar las llamadas a la API necesarias.
- Si no especificas un rol de IAM para la función Lambda `LambdaRoleArn` (parámetro), la automatización crea un rol con el `Automation-K8sProxy-Role-<ExecutionId>` nombre de tu cuenta. Esta función incluye las políticas `AWSLambdaBasicExecutionRole` gestionadas y `AWSLambdaVPCLambdaAccessExecutionRole`.
- Algunos pasos de diagnóstico requieren que los nodos de trabajo de Amazon EKS sean instancias administradas por Systems Manager. Si los nodos no son instancias administradas por Systems Manager, se omiten los pasos que requieren acceso a Systems Manager, pero las demás comprobaciones continúan.
- La automatización incluye un paso de limpieza que elimina los recursos de la infraestructura de autenticación. Este paso de limpieza se ejecuta incluso cuando los

pasos anteriores fallan, lo que ayuda a evitar que los recursos de la cuenta queden huérfanos. AWS

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeInstanceStatus`
- `ec2:GetEbsEncryptionByDefault`
- `eks:DescribeAddon`
- `eks:DescribeAddonVersions`
- `eks:DescribeCluster`
- `iam:GetInstanceProfile`
- `iam:GetOpenIDConnectProvider`
- `iam:GetRole`
- `iam:ListOpenIDConnectProviders`
- `iam:SimulatePrincipalPolicy`
- `s3:GetBucketLocation`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketVersioning`

- `s3:ListBucket`
- `s3:ListBucketVersions`
- `ssm:DescribeInstanceInformation`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`

Instrucciones

Siga estos pasos para configurar la automatización:

1. Crea un rol de automatización de SSM `TroubleshootEbsCsiDriversForEks-SSM-Role` en tu cuenta. Verifique que la relación de confianza contiene la siguiente política.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Adjunta la siguiente política a la función de IAM para conceder los permisos necesarios para realizar las acciones especificadas en los recursos especificados.
 - Si espera cargar los registros de ejecución y recursos al bucket de Amazon S3 de la misma AWS región, sustitúyalos por `arn:{partition}:s3::BUCKET_NAME/*` los suyos `enOptionalRestrictPutObjects`.

- El bucket de Amazon S3 debe apuntar al bucket de Amazon S3 correcto si lo selecciona S3BucketName en la ejecución de SSM.
- Este permiso es opcional si no lo especificas S3BucketName
- El bucket de Amazon S3 debe ser privado y estar en la misma AWS región en la que se ejecuta la automatización de SSM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OptionalRestrictPutObjects",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstanceStatus",
        "ec2:GetEbsEncryptionByDefault",
        "eks:DescribeAddon",
        "eks:DescribeAddonVersions",
        "eks:DescribeCluster",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "iam:ListOpenIDConnectProviders",
        "iam:SimulatePrincipalPolicy",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "ssm:DescribeInstanceInformation",
```

```

        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
    ],
    "Resource": "*"
},
{
    "Sid": "SetupK8sApiProxyForEKSActions",
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:TagRole",
        "iam:UntagRole",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource",
        "logs:PutLogEvents",
    ]
}

```

```

        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource",
        "ssm:DescribeAutomationExecutions",
        "tag:GetResources",
        "tag:TagResources"
    ],
    "Resource": "*"
},
{
    "Sid": "PassRoleToAutomation",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
        "arn:aws:iam::*:role/TroubleshootEbsCsiDriversForEks-SSM-Role",
        "arn:aws:iam::*:role/Automation-K8sProxy-Role-*"
    ],
    "Condition": {
        "StringLikeIfExists": {
            "iam:PassedToService": [
                "lambda.amazonaws.com",
                "ssm.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "AttachRolePolicy",
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
    ],
    "Resource": "*",
    "Condition": {
        "StringLikeIfExists": {
            "iam:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    }
}
]
}

```


- Otorgue los permisos necesarios para el clúster RBAC (control de acceso basado en roles) de Amazon EKS. El enfoque recomendado consiste en crear una entrada de acceso en el clúster de Amazon EKS.

En la consola de Amazon EKS, navegue hasta el clúster. Para las entradas de acceso de Amazon EKS, compruebe que la configuración de acceso esté establecida en `API_AND_CONFIG_MAP` o `API`. Para ver los pasos para configurar el modo de autenticación de las entradas de acceso, consulte [Configuración de entradas de acceso](#).

Elija Crear entrada de acceso.

- Para el ARN principal de IAM, seleccione el rol de IAM que creó para la automatización de SSM en el paso anterior.
- En Tipo, seleccione Standard.

- Agregue una política de acceso:

- En Alcance de acceso, seleccione `Cluster`.
- En Nombre de la política, seleccione `AmazonEKSAAdminViewPolicy`.

Elija Add Policy (Agregar política).

Si no utilizas las entradas de acceso para gestionar los permisos de la API de Kubernetes, debes actualizar `aws-auth ConfigMap` y crear un enlace de roles entre tu usuario o rol de IAM. Asegúrese de que su entidad de IAM tenga los siguientes permisos de API de Kubernetes de solo lectura:

- GET `/apis/apps/v1/namespaces/{namespace}/deployments/{name}`
- GET `/apis/apps/v1/namespaces/{namespace}/replicasets/{name}`
- GET `/apis/apps/v1/namespaces/{namespace}/daemonsets/{name}`
- GET `/api/v1/nodes/{name}`
- GET `/api/v1/namespaces/{namespace}/serviceaccounts/{name}`
- GET `/api/v1/namespaces/{namespace}/persistentvolumeclaims/{name}`
- GET `/api/v1/persistentvolumes/{name}`
- GET `/apis/storage.k8s.io/v1/storageclasses/{name}`
- GET `/api/v1/namespaces/{namespace}/pods/{name}`
- GET `/api/v1/namespaces/{namespace}/pods`
- GET `/api/v1/namespaces/{namespace}/pods/{name}/log`

- GET /api/v1/events

5. [Ejecute la automatización \(consola\) AWSSupport-TroubleshootEbsCsiDriversForEks](#)

6. Elija Execute automation (Ejecutar automatización).

7. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a SSM Automation realizar las acciones en su nombre. El rol debe añadirse a la entrada de acceso al clúster de Amazon EKS o al permiso RBAC para permitir las llamadas a la API de Kubernetes.
 - Tipo: `AWS::IAM::Role::Arn`
 - Ejemplo: `TroubleshootEbsCsiDriversForEks-SSM-Role`
- EksClusterName:
 - Descripción: nombre del clúster de Amazon Elastic Kubernetes Service (Amazon EKS) de destino.
 - Tipo: `String`
- ApplicationPodName:
 - Descripción: El nombre del pod de aplicaciones de Kubernetes que tiene problemas con el controlador CSI de Amazon EBS.
 - Tipo: `String`
- ApplicationNamespace:
 - Descripción: El espacio de nombres de Kubernetes para el pod de la aplicación tiene problemas con el controlador CSI de Amazon EBS.
 - Tipo: `String`
- EbsCsiControllerDeploymentName(Opcional):
 - Descripción: (opcional) El nombre de la implementación del pod de controladores CSI de Amazon EBS.
 - Tipo: `String`
 - Valor predeterminado: `ebs-csi-controller`
- EbsCsiControllerNamespace(Opcional):
 - Descripción: (opcional) El espacio de nombres de Kubernetes para el pod de controladores CSI de Amazon EBS.
 - Tipo: `String`

- Valor predeterminado: kube-system
- S3 (opcional)BucketName :
 - Descripción: (opcional) El nombre del bucket de Amazon S3 de destino donde se cargarán los registros de solución de problemas.
 - Tipo: AWS::S3::Bucket::Name
- LambdaRoleArn (Opcional):
 - Descripción: (opcional) El ARN del rol de IAM que permite a la AWS Lambda función acceder a los AWS servicios y recursos necesarios.
 - Tipo: AWS::IAM::Role::Arn

Seleccione Ejecutar.

8. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

Para obtener más información sobre el controlador CSI de Amazon EBS, consulte el controlador CSI de [Amazon EBS](#).

AWSSupport-TroubleshootEKSALBControllerIssues

Descripción

El manual de AWSSupport-TroubleshootEKSALBControllerIssues automatización ayuda a diagnosticar problemas comunes que impiden que el AWS Load Balancer Controller aprovisiona y gestione correctamente el Application Load Balancer (ALB) y el Network Load Balancer (NLB) para las entradas y los servicios de Kubernetes.

Este manual end-to-end valida los componentes esenciales, como la configuración del proveedor de identidad del OIDC, la configuración del IRSA, los requisitos previos de red, la configuración

y las cuotas de recursos. `ingress/service` También recopila los registros de los controladores y las configuraciones de recursos de Kubernetes relevantes para ayudar a identificar errores de configuración o problemas operativos.

 Important

Este manual de automatización está diseñado para clústeres de Amazon EKS que utilizan grupos de nodos de Amazon Elastic Compute Cloud (Amazon EC2) (Amazon EC2) y actualmente no admite clústeres en ejecución. AWS Fargate

¿Cómo funciona?

El manual de ejecución `AWSSupport-TroubleshootEKSALBControllerIssues` lleva a cabo los siguientes pasos de alto nivel:

- Valida el estado del clúster de Amazon EKS, la configuración de entrada de acceso y la configuración del proveedor de OIDC.
- Crea un proxy Lambda temporal para la comunicación de la API de Kubernetes.
- Comprueba la implementación del AWS Load Balancer Controller y la configuración de la cuenta de servicio.
- Verifica la identidad del pod, el webhook y la inyección de roles de IAM.
- Valida la configuración y el etiquetado de subredes para el aprovisionamiento de Application Load Balancer y Network Load Balancer.
- Compara las cuotas de las cuentas de Application Load Balancer y Network Load Balancer con el uso actual.
- Valida las anotaciones de los recursos de entrada y servicio.
- Comprueba el etiquetado de los grupos de seguridad del nodo de trabajo para la integración del balanceador de carga.
- Recopila los registros de los módulos del controlador para realizar diagnósticos.
- Limpia los recursos de autenticación temporales.
- Genera un informe de diagnóstico con los hallazgos y los pasos de remediación.

 Note

- El clúster de Amazon EKS debe tener una entrada de acceso configurada para la entidad de IAM que ejecuta esta automatización. El modo de autenticación del clúster debe estar configurado en API o API_AND_CONFIG_MAP. Sin una configuración de entrada de acceso adecuada, la automatización finalizará durante la validación inicial.
- El LambdaRoleArn parámetro es obligatorio y debe tener las políticas AWS administradas AWSLambdaBasicExecutionRole y AWSLambdaVPCAccessExecutionRole adjuntadas para permitir que la función de proxy se comuniquen con la API de Kubernetes.
- El controlador AWS Load Balancer debe ser de una versión v2.1.1 o posterior.
- La automatización incluye un paso de limpieza que elimina los recursos temporales de la infraestructura de autenticación. Este paso de limpieza se ejecuta incluso cuando los pasos anteriores fallan, lo que garantiza que no queden recursos huérfanos en su cuenta. AWS

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- `ec2:CreateNetworkInterface`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `eks:DescribeCluster`
- `eks:ListAssociatedAccessPolicies`
- `elasticloadbalancing:DescribeAccountLimits`
- `elasticloadbalancing:DescribeLoadBalancers`
- `iam:GetRole`
- `iam:ListOpenIDConnectProviders`
- `iam:PassRole`
- `lambda:CreateFunction`
- `lambda:DeleteFunction`
- `lambda:GetFunction`
- `lambda:InvokeFunction`
- `lambda:ListTags`
- `lambda:TagResource`
- `lambda:UntagResource`
- `lambda:UpdateFunctionCode`
- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:ListTagsForResource`
- `logs:PutLogEvents`
- `logs:PutRetentionPolicy`

- logs:TagResource
- logs:UntagResource
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- tag:GetResources
- tag:TagResources

Instrucciones

Siga estos pasos para configurar y ejecutar la automatización:

Note

Antes de ejecutar la automatización, siga estos pasos para configurar las funciones de IAM necesarias: una para que Systems Manager Automation ejecute el runbook y otra para que Lambda se comuniquen con la API de Kubernetes:

1. Cree un rol de automatización de SSM en su cuenta.

TroubleshootEKSALBController-SSM-Role Verifique que la relación de confianza contiene la siguiente política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Adjunta la siguiente política de IAM para conceder los permisos necesarios:

```
{
```

```

"Version": "2012-10-17",
"Statement": [{
  "Sid": "TroubleshootEKSSALBControllerIssuesActions",
  "Effect": "Allow",
  "Action": [
    "eks:DescribeCluster",
    "eks:ListAssociatedAccessPolicies",
    "iam:GetRole",
    "iam:ListOpenIDConnectProviders",
    "ssm:StartAutomationExecution",
    "ssm:GetAutomationExecution",
    "ssm:DescribeAutomationExecutions",
    "ec2:DescribeSubnets",
    "ec2:DescribeRouteTables",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeAccountLimits",
    "ec2:DescribeInstances",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups"
  ],
  "Resource": "*"
},
{
  "Sid": "SetupK8sApiProxyForEKSACTIONS",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeStacks",
    "cloudformation:UpdateStack",
    "ec2:CreateNetworkInterface",
    "ec2>DeleteNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "eks:DescribeCluster",
    "iam:GetRole",
    "lambda:CreateFunction",
    "lambda>DeleteFunction",
    "lambda:GetFunction",
    "lambda:InvokeFunction",
    "lambda:ListTags",

```



```

        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource",
        "ssm:DescribeAutomationExecutions",
        "tag:GetResources",
        "tag:TagResources"
    ],
    "Resource": "*"
  },
  {
    "Sid": "PassRoleToAutomation",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
      "StringLikeIfExists": {
        "iam:PassedToService": [
          "lambda.amazonaws.com",
          "ssm.amazonaws.com"
        ]
      }
    }
  }
]
}

```

3. Configure la entrada de acceso para su clúster de Amazon EKS. Este es un requisito obligatorio para la automatización. Para ver los pasos para configurar el modo de autenticación de las entradas de acceso, consulte [Configurar las entradas de acceso](#).

En la consola de Amazon EKS, navegue hasta el clúster y siga estos pasos:

- En la sección Acceso, compruebe que la configuración de autenticación esté establecida en API oAPI_AND_CONFIG_MAP.
- Seleccione Crear entrada de acceso y configure:

- Para el ARN principal de IAM, seleccione el rol de IAM que creó ().
TroubleshootEKSALBController-SSM-Role
 - En Tipo, seleccione Standard.
 - Agregue una política de acceso:
 - En el nombre de la política, seleccione AmazonEKSAdminViewPolicy.
 - En Alcance de acceso, seleccione Cluster.
 - Elija Add Policy (Agregar política).
 - Compruebe los detalles y seleccione Crear.
4. Cree una función de IAM para la función Lambda (referenciada LambdaRoleArn como en los parámetros de entrada):
- Cree un nuevo rol de IAM con la siguiente política de confianza:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Adjunte las siguientes políticas AWS gestionadas a este rol:
 - AWSLambdaBasicExecutionRole
 - AWSLambdaVPCLAccessExecutionRole
- Anote el ARN de este rol, ya que lo necesitará para el parámetro de LambdaRoleArn entrada.

1. Navegue hasta [AWSSupport-TroubleshootEKSALBControllerIssues](#) en la consola de AWS Systems Manager.

2. Elija Ejecutar automatización.

3. Para los parámetros de entrada, introduzca lo siguiente:

AWSSupport-TroubleshootEKSALBControllerIssues

- AutomationAssumeRole (Opcional):

Tipo AWS::IAM::Role: :Arn

Descripción: (opcional) El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

Patrón permitido: ^arn :(? :aws|aws-cn|aws-us-gov) :iam::\ d {12} :role/? [A-Za-Z_0-9+=, .@\ - _/]+ \$

- EksClusterName (Obligatorio):

Tipo: cadena

Descripción: (obligatorio) Nombre del clúster de Amazon Elastic Kubernetes Service (Amazon EKS).

Patrón permitido: ^ [0-9a-za-Z] [a-zA-Z0-9-_] {0,99} \$

- ALBControllerDeploymentName (Opcional):

Tipo: cadena

Descripción: (opcional) El nombre de la implementación del AWS Load Balancer Controller en el clúster de Amazon EKS. Por lo general, es «aws-load-balancer-controller», a menos que lo haya personalizado durante la instalación.

Patrón permitido: ^ [a-z0-9] ([-a-z0-9] {0,251} [a-z0-9])? \$

Predeterminado: aws-load-balancer-controller

- ALBControllerEspacio de nombres (opcional):

Tipo: cadena

Descripción: (opcional) El espacio de nombres de Kubernetes donde se implementa el Load Balancer Controller AWS . De forma predeterminada, es «kube-system», pero puede ser diferente si has instalado el controlador en un espacio de nombres personalizado.

Patrón permitido: ^ [a-z0-9] ([-a-z0-9] {0,61} [a-z0-9])? \$

Predeterminado: kube-system

- ServiceAccountName (Opcional):

Tipo: cadena

Descripción: (opcional) El nombre de la cuenta de servicio de Kubernetes asociada al controlador del Load Balancer AWS . Suele ser «aws-load-balancer-controller», a menos que se personalice durante la instalación.

Patrón permitido: ^ [a-z0-9] ([-a-z0-9] {0,251} [a-z0-9])? \$

Predeterminado: aws-load-balancer-controller

- ServiceAccountNamespace (Opcional):

Tipo: cadena

Descripción: (opcional) El espacio de nombres de Kubernetes donde se encuentra la cuenta de servicio del Load Balancer Controller AWS . Suele ser el «sistema kube», pero puede variar si has utilizado un espacio de nombres personalizado.

Patrón permitido: ^ [a-z0-9] ([-a-z0-9] {0,61} [a-z0-9])? \$

Predeterminado: kube-system

- IngressName (Opcional):

Tipo: cadena

Descripción: (opcional) Nombre del recurso de ingreso que se va a validar (Application Load Balancer). Si no se especifica, se omitirá la validación de ingreso.

Patrón permitido: ^\$|^ [a-z0-9] [a-z0-9.-] {0,251} [a-z0-9] \$

Predeterminado: «» (cadena vacía)

- IngressNamespace (Opcional):

Tipo: cadena

Descripción: (opcional) Espacio de nombres del recurso de Ingress. Es obligatorio si se ha especificado IngressName.

Patrón permitido: `^$|^ [a-z0-9] [a-z0-9-] {0,61} [a-z0-9] $`

Predeterminado: «» (cadena vacía)

- **ServiceName (Opcional):**

Tipo: cadena

Descripción: (opcional) Nombre de un recurso de servicio específico para validar las anotaciones del Network Load Balancer (Network Load Balancer). Si no se especifica, se omitirá la validación de los recursos de servicio.

Patrón permitido: `^$|^ [a-z0-9] [a-z0-9-] {0,251} [a-z0-9] $`

Predeterminado: «» (cadena vacía)

- **ServiceNamespace (Opcional):**

Tipo: cadena

Descripción: (opcional) Espacio de nombres del recurso de servicio. Es obligatorio si se ha especificado `ServiceName`.

Patrón permitido: `^$|^ [a-z0-9] [a-z0-9-] {0,61} [a-z0-9] $`

Predeterminado: «» (cadena vacía)

- **LambdaRoleArn (Obligatorio):**

Tipo `AWS::IAM::Role` : `Arn`

Descripción: (obligatorio) El ARN de la función de IAM que permite a la función (AWS Lambda Lambda) acceder a los servicios y recursos necesarios. AWS Asocie las políticas AWS gestionadas `AWSLambdaBasicExecutionRole` y `AWSLambdaVPCLAccessExecutionRole` a su función de IAM de ejecución de funciones lambda.

Patrón permitido: `^arn :(? :aws|aws-cn|aws-us-gov) :iam::\ d {12} :role/? [A-Za-Z_0-9+=, .@\ -_ /] +$`

4. Elija Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

a. `ValidateAccessEntryAndOIDCProvider`:

Valida la configuración de IAM del clúster de Amazon EKS comprobando los permisos de entrada de acceso y la configuración del proveedor de OIDC.

b. Configuración K8: `sAuthenticationClient`

Ejecute el documento `SAW AWSSupport-SetupK8 sApiProxy FoREKs` para configurar una función lambda que ejecute llamadas a la API de Amazon EKS en el clúster.

c. Verifique `ALBController` y: `IRSASetup`

Comprueba si la cuenta de servicio y el controlador `Application Load Balancer` determinados existen en sus respectivos espacios de nombres. Comprueba también la política de confianza y anotación de roles de cuentas de servicio del controlador `Application Load Balancer`.

d. `VerifyPodIdentityWebhookAndEnv`:

Comprueba si `pod-identity-webhook` está ejecutando. También comprueba si el `IRSA` se inyecta en las variables `ENV` del módulo.

e. `ValidateSubnetRequirements`:

Compruebe al menos dos subredes en dos zonas de disponibilidad con 8 IP disponibles. Los balanceadores de carga cuentan con el etiquetado de subredes adecuado. `public/private`

f. `CheckLoadBalancerLimitsAndUsage`:

Compare el límite de la cuenta con el número de `Application Load Balancer` y `Network Load Balancer`.

g. `CheckIngressOrServiceAnnotations`:

Comprueba las anotaciones y especificaciones correctas en los recursos de `Ingress` y `Service` para garantizar que estén configurados correctamente para el uso de `Application Load Balancer` y `Network Load Balancer`.

h. `CheckWorkerNodeSecurityGroupTags`:

Compruebe que exactamente un grupo de seguridad adjunto a los nodos de trabajo tenga la etiqueta de clúster requerida.

i. `ALBController` Registros de captura:

Recupera los registros de diagnóstico más recientes de los pods del controlador `AWS Load Balancer` que se ejecutan en el clúster de Amazon EKS.

j. Limpiar K8: sAuthenticationClient

Ejecuta el documento SAW «AWSSupport-SetupK8 sApiProxy FoReks» mediante la operación de «Limpieza» para limpiar los recursos creados como parte de la automatización.

k. GenerateReport:

Genera el informe de automatización.

7. Una vez finalizada la ejecución, revise la sección de resultados para ver los resultados detallados de la ejecución:

a. Informe:

Proporciona un resumen completo de todas las comprobaciones realizadas, incluido el estado del clúster de Amazon EKS, la configuración de Application Load Balancer Controller, la configuración de IRSA, los requisitos de subred, los límites del balanceador de carga, ingress/service las anotaciones, las etiquetas de los grupos de seguridad del nodo de trabajo y los registros del Application Load Balancer Controller. También incluye los problemas identificados y las medidas de corrección recomendadas.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de la automatización](#)
- [Flujos de trabajo de automatización de Support](#)

Documentación relacionada con el controlador AWS Load Balancer

- [AWS Controlador Load Balancer](#)
- [Configuración de entradas de acceso](#)

AWSSupport-TroubleshootEKSDNSFailure

Descripción

El `AWSsupport-TroubleshootEKSDNSFailure` manual ayuda a solucionar problemas con los pods de CoreDNS y la configuración en Amazon Elastic Kubernetes Service (Amazon EKS) cuando las aplicaciones o los pods encuentran errores en la resolución de DNS. El manual valida la configuración de DNS de la VPC, inspecciona la implementación de CoreDNS y comprueba la configuración del escalador automático de pods horizontales (HPA) ConfigMap, recopila los registros de CoreDNS y realiza comprobaciones de resolución de DNS en los nodos de trabajo. Opcionalmente, se puede crear una instancia de Amazon Elastic Compute Cloud de sondeo en la misma subred que el nodo de trabajo problemático para realizar comprobaciones de resolución de DNS sin necesidad de acceso directo al nodo.

 Important

El modo de autenticación del clúster de Amazon EKS debe estar establecido en `API` o `API_AND_CONFIG_MAP`. Este manual implementa una función (AWS Lambda) como proxy para realizar llamadas autenticadas a la API de Kubernetes y limpia todos los recursos creados al final de la ejecución.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Escriba: `:Arn AWS::IAM::Role`

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- EKSClusterName

Tipo: cadena

Descripción: (obligatorio) El nombre del clúster Amazon EKS de destino.

- DnsName

Tipo: cadena

Predeterminado: amazon.com

Descripción: (opcional) El sufijo de dominio auxiliar del nombre de dominio que la aplicación o el pod no pueden resolver.

- ProblematicNodeInstanceId

Escriba: :Id AWS::EC2::Instance

Descripción: (opcional) El ID de instancia del nodo de trabajo en el que se ejecuta la aplicación que experimenta errores de resolución de DNS. Cuando se proporciona, el runbook crea una instancia Amazon EC2 de sondeo en la misma subred para realizar comprobaciones de resolución de DNS. Utilice este parámetro si el nodo de trabajo no está en una subred pública o si no está permitida la instalación `bind-utils` en el nodo de trabajo.

- CoreDnsNamespace

Tipo: cadena

Predeterminado: kube-system

Descripción: (opcional) El espacio de nombres de Kubernetes para los pods de CoreDNS.

- S3 BucketName

Tipo: AWS::S3::Bucket :Nombre

Descripción: (opcional) El nombre del depósito de Amazon Simple Storage Service donde se cargan los registros de solución de problemas de CoreDNS.

- LambdaRoleArn

Escriba: :Arn AWS::IAM::Role

Descripción: (opcional) El ARN del rol de IAM para la función de proxy Lambda. Si no se proporciona, el manual de instrucciones crea un rol `Automation-K8sProxy-Role-
<ExecutionId>` con el nombre de las `AWSLambdaBasicExecutionRole` políticas administradas. `AWSLambdaVPCLambdaAccessExecutionRole` Se recomienda proporcionar su propia función.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `eks:DescribeCluster`
- `ec2:DescribeVpcs`
- `ec2:DescribeInstances`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `cloudformation:CreateStack`
- `cloudformation:DescribeStacks`
- `cloudformation>DeleteStack`
- `lambda:InvokeFunction`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketAcl`
- `s3:PutObject`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Pasos de documentos

1. `AssertIfTargetClusterExists`- Comprueba que el clúster de Amazon EKS especificado en `EksClusterName` existe y se encuentra en ese `ACTIVE` estado. Si el clúster no se encuentra o no está activo, el runbook pasa a `GenerateReport`
2. `UpdateEksClusterExists`- Establece la `eksClusterExists` variable interna `true` para utilizarla en la generación de informes.
3. `GetVpcDnsSettings`- Recupera la `enableDnsHostnames` configuración `enableDnsSupport` y la configuración de Amazon Virtual Private Cloud asociada al clúster Amazon EKS.
4. `BranchOnVpcDnsSettings`- Comprueba si ambas configuraciones de DNS de la VPC están habilitadas. Si alguna de ellas está deshabilitada, el runbook pasa a `GenerateReport`. De lo contrario, continúa con `DeployK8sAuthApisResources`
5. `DeployK8sAuthApisResources`- Se ejecuta `AWSSupport-SetupK8sApiProxyForEKS` para implementar una función Lambda como proxy para realizar llamadas autenticadas a la API de Kubernetes al clúster de Amazon EKS.
6. `RetrieveCoreDNSDeployment`- Recupera información sobre la implementación de CoreDNS, incluida la preparación del pod, el estado del contenedor y la preparación de los nodos que alojan los pods de CoreDNS. También recupera la IP del clúster de CoreDNS.
7. `RetrieveAndInspectCoreDNSConfigMap`- Recupera los `ConfigMap` CoreDNS del clúster de Amazon EKS y comprueba si hay problemas de configuración, incluida la configuración del dominio `stub` del dominio especificado en `DnsName`
8. `ValidateHpaConfiguration`- Comprueba si hay un escalador automático de pod horizontal (HPA) configurado para la implementación de CoreDNS en el espacio de nombres especificado.
9. `CheckS3BucketPublicStatus`- Valida que el bucket de Amazon S3 especificado en `S3BucketName` no permite el acceso de lectura o escritura público o anónimo.
10. `CollectLogToS3`- Recopila los registros de los pods de CoreDNS y los carga en el bucket de Amazon S3 especificado.
11. `BranchOnProblematicNodeInstanceId`- Comprueba si `ProblematicNodeInstanceId` se proporciona y si existen nodos host de CoreDNS. Si se cumplen ambas condiciones, continúa con `VerifyThatProblematicNodeInstanceBelongsToCluster`. De lo contrario, se ramifica a `BranchOnCoreDnsDeployment`.
12. `VerifyThatProblematicNodeInstanceBelongsToCluster`- Confirma que la instancia especificada en `ProblematicNodeInstanceId` es un nodo de trabajo del clúster de Amazon EKS.
13. `UpdateProblematicNodeInstanceStanding`- Establece la `problematicNodeInstanceStanding` variable interna en `true`.

- 14.`GetProblematicInstanceDetails`- Recupera el ID de AMI, el tipo de instancia, el ID de subred y los ID del grupo de seguridad del nodo de trabajo problemático para usarlos al crear la instancia de Amazon EC2 de sondeo.
- 15.`CreateProbingInfrastructure`- Crea un perfil de instancia y explora la instancia de Amazon EC2 a través de AWS CloudFormation una pila en la misma subred que el nodo de trabajo problemático. La pila recibe un nombre. `AWSSupport-TroubleshootEKSDNSFailure-<ExecutionId>`
- 16.`GetProbingInstanceId`- Recupera el ID de la instancia Amazon EC2 de sondeo de las salidas de CloudFormation la pila.
- 17.`WaitForProbingInstanceSSMAgentStateToBeOnline`- Espera a que el agente Amazon EC2 Systems Manager de la instancia de Amazon EC2 que está sondeando informe de un estado antes de continuarOnline.
- 18.`RetrieveCoreDNSPodsIPFromProblematicNode`- Recupera las direcciones IP del pod de CoreDNS vistas desde el nodo de trabajo problemático.
- 19.`PerformDNSResolutionOnProbingEC2Instance`- Ejecuta comprobaciones de resolución de DNS en la instancia de Amazon EC2 que está sondeando mediante la IP del clúster y la IP del pod de CoreDNS.
- 20.`DeleteCloudFormationStack`- Elimina la CloudFormation pila que creó la instancia y el perfil de instancia de Amazon EC2 de sondeo.
- 21.`UpdateCfnStackDeleted`- Establece la variable interna `cfnStackDeleted` en. `true`
- 22.`BranchOnCoreDnsDeployment`- Comprueba si no `ProblematicNodeInstanceId` se proporcionó y si existen nodos host de CoreDNS. Si se cumplen ambas condiciones, continúa con. `PerformDNSResolutionOnCoreDnsWorkerNodes` De lo contrario, procede a `CleanupK8sAuthenticationInfrastructure`.
- 23.`BranchOnCoreDnsNodesExistForRunCommandSteps`- Comprueba si existen nodos host de CoreDNS antes de ejecutar los pasos. `aws:runCommand` Si no existe ningún nodo (por ejemplo, cuando CoreDNS no tiene réplicas), salta a. `CleanupK8sAuthenticationInfrastructure`
- 24.`PerformDNSResolutionOnCoreDnsWorkerNodes`- Ejecuta comprobaciones de resolución de DNS directamente en los nodos de trabajo de CoreDNS mediante la IP del clúster y la IP del pod de CoreDNS.
- 25.`VerifyNameserverMatchAndKubeProxyLogsAndIPTableEntries`- Comprueba que la IP del servidor de nombres coincide con la IP del clúster, comprueba el acceso del pod kube-proxy al servidor API y valida las entradas iptables de kube-dns en los nodos de trabajo de CoreDNS.

26. `VerifyPPSThrottlingOnENIs`- Comprueba el límite de DNS packets-per-second (PPS) por interfaz de red elástica (ENI) en los nodos de trabajo de CoreDNS para identificar posibles limitaciones.
27. `UpdateChecksOnNodes`- Establece la `checksOnNodes` variable interna para indicar que se realizaron comprobaciones `true` a nivel de nodo.
28. `CleanupK8sAuthenticationInfrastructure`- Se ejecuta `AWSsupport-SetupK8sApiProxyForEKS` con la `Cleanup` operación para eliminar la función proxy de Lambda y los recursos asociados creados durante la automatización.
29. `UpdateK8sInfrastructureDeleted`- Establece la `K8sInfrastructureDeleted` variable interna en `true`.
30. `CleanUpAllResources`- Realiza una limpieza exhaustiva de los recursos restantes, incluida la CloudFormation pila y la función de proxy Lambda, en caso de que los pasos de limpieza anteriores no se hayan completado correctamente.
31. `CollectOutputFromAllRunCommandSteps`- Recopila y consolida el resultado de todos los `aws:runCommand` pasos que se ejecutaron durante la automatización.
32. `GenerateReport`- Recopila los resultados de todos los pasos anteriores en un informe de evaluación exhaustivo que abarca la configuración de DNS de la VPC, el estado de la implementación de CoreDNS, la configuración, la configuración de HPA ConfigMap, el estado de la recopilación de registros y los resultados de las comprobaciones de resolución del DNS.

Salidas

`GenerateReport.EvalReport`- Un informe completo de todas las comprobaciones de solución de problemas de DNS realizadas, incluidas las conclusiones y las medidas de corrección recomendadas.

Elastic Beanstalk

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Elastic Beanstalk Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSsupport-CollectElasticBeanstalkLogs](#)

- [AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming](#)
- [AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications](#)
- [AWSSupport-TroubleshootElasticBeanstalk](#)

AWSSupport-CollectElasticBeanstalkLogs

Descripción

El manual de procedimientos AWSSupport-CollectElasticBeanstalkLogs recopila archivos de registro AWS Elastic Beanstalk relacionados de una instancia de Amazon Elastic Compute Cloud (Amazon EC2) Windows Server lanzada por Elastic Beanstalk para ayudarle a solucionar problemas comunes. Mientras la automatización recopila los archivos de registro asociados, se realizan cambios en la estructura del sistema de archivos, incluyendo la creación de directorios temporales, la copia de los archivos de registro en los directorios temporales y la compresión de los archivos de registro en un archivo. Esta actividad puede provocar un aumento de CPUUtilization en la instancia de Amazon EC2. Para obtener más información CPUUtilization, consulta [las métricas de instancias](#) en la Guía del CloudWatch usuario de Amazon.

Si especifica un valor para el parámetro S3BucketName, la automatización evalúa el estado de la política del bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Para mejorar la seguridad de los registros recopilados de su instancia de Amazon EC2, si el estado de la política isPublic está establecido en true o si la lista de control de acceso (ACL) concede permisos de READ|WRITE al grupo predefinido de All Users Amazon S3, los registros no se cargan. Para obtener más información acerca de los grupos predefinidos de Amazon S3, consulte los [Grupos predefinidos de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

Si no especifica un valor para el parámetro S3BucketName, la automatización carga el paquete de registros en el bucket predeterminado Amazon S3 de Elastic Beanstalk, en la Región de AWS en la que ejecuta la automatización. El nombre del directorio se basa en la siguiente estructura, elasticbeanstalk- *region* - *accountID* . *accountID* Los valores *region* y *accountID* variarán en función de la región en la Cuenta de AWS que ejecute la automatización. El paquete de registros se guardará en el directorio resources/environments/logs/bundle/ *environmentID* / *instanceID* . *instanceID* Los valores *environmentID* y *instanceID* diferirán en función del entorno de Elastic Beanstalk y de la instancia de Amazon EC2 de la que esté recopilando los registros.

De forma predeterminada, el perfil de instancia AWS Identity and Access Management (IAM) adjunto a las instancias de Amazon EC2 del entorno de Elastic Beanstalk tiene los permisos necesarios

para cargar el paquete en el bucket Amazon S3 de Elastic Beanstalk predeterminado de su entorno. Si especifica un valor para el parámetro `S3BucketName`, el perfil de instancia adjunto a la instancia de Amazon EC2 debe permitir las acciones `s3:GetBucketAcl`, `s3:GetBucketPolicy`, `s3:GetBucketPolicyStatus` y `s3:PutObject` para el bucket y la ruta de Amazon S3 especificados.

 Note

Esta automatización requiere al menos 500 MB de espacio de disco disponible en el volumen raíz de Amazon Elastic Block Store (Amazon EBS) adjuntado a su instancia de Amazon EC2. Si no hay suficiente espacio en disco disponible en el volumen raíz, la automatización se detiene.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `EnvironmentId`

Tipo: cadena

Descripción: (obligatorio) el ID del entorno de Elastic Beanstalk del que desea recopilar el paquete de registros.

- InstanceId

Tipo: cadena

(obligatorio) el ID de la instancia de Amazon EC2 del entorno de Elastic Beanstalk del que desea recopilar el paquete de registro.

- S3 BucketName

Tipo: cadena

(opcional) el bucket de Amazon S3 en el que desea cargar los registros archivados.

- S3 BucketPath

Tipo: cadena

(opcional) la ruta del bucket de Amazon S3 en la que desea cargar el paquete de registros. Este parámetro es ignorado si especifica un valor para el parámetro S3BucketName.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:SendCommand
- ssm:DescribeInstanceInformation
- ec2:DescribeInstances

Pasos de documentos

- aws:assertAwsResourceProperty: confirma que la instancia de Amazon EC2 que especifique en el parámetro InstanceId está gestionada por AWS Systems Manager.
- aws:assertAwsResourceProperty: confirma que la instancia de Amazon EC2 que especifique en el parámetro InstanceId es una instancia Windows Server.

- `aws:runCommand`: comprueba si la instancia forma parte de un entorno de Elastic Beanstalk, si hay suficiente espacio en disco para agrupar los registros y si el bucket de Amazon S3 en el que se cargarían los registros es público.
- `aws:runCommand`: recopila los archivos de registro y carga el archivo en el bucket de Amazon S3 especificado en el parámetro `S3BucketName` o en el bucket predeterminado de su entorno de Elastic Beanstalk si no se especifica ningún valor.

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

Descripción

El `AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming` runbook permite iniciar sesión en el entorno AWS Elastic Beanstalk (Elastic Beanstalk) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `EnvironmentId`

Tipo: cadena

Descripción: (obligatorio) el ID del entorno de Elastic Beanstalk en el que desea habilitar el inicio de sesión.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Pasos de documentos

- `aws:executeAwsApi`: permite el registro en el entorno de Elastic Beanstalk que especifique en el parámetro `EnvironmentId`.
- `aws:waitForAwsResourceProperty`: espera a que el estado del entorno cambie a `Ready`.
- `aws:executeScript`: verifica que el registro está habilitado en el entorno de Elastic Beanstalk.

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

Descripción

El `AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications` runbook habilita las notificaciones para el entorno AWS Elastic Beanstalk (Elastic Beanstalk) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- EnvironmentId

Tipo: cadena

Descripción: (obligatorio) el ID del entorno de Elastic Beanstalk para el que desea habilitar las notificaciones.

- TopicArn

Tipo: cadena

Descripción: (obligatorio) el ARN del tema de Amazon Simple Notification Service (Amazon SNS) al que desea enviar notificaciones.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

Pasos de documentos

- `aws:executeAwsApi`: activa las notificaciones para el entorno de Elastic Beanstalk que especifique en el parámetro `EnvironmentId`.
- `aws:waitForAwsResourceProperty`: espera a que el estado del entorno cambie a `Ready`.
- `aws:executeScript`: verifica que las notificaciones estén habilitadas para el entorno de Elastic Beanstalk.

AWSSupport-TroubleshootElasticBeanstalk

Descripción

El `AWSSupport-TroubleshootElasticBeanstalk` manual le ayuda a solucionar los posibles motivos por los que su AWS Elastic Beanstalk entorno se encuentra en un estado `Degraded` o `Severe`. Esta automatización comprueba los siguientes AWS recursos asociados al entorno de Elastic Beanstalk:

- Detalles de configuración de un balanceador de carga, una AWS CloudFormation pila, un grupo de Amazon EC2 Auto Scaling, instancias de Amazon Elastic Compute Cloud (Amazon EC2) y nube privada virtual (VPC).
- Problemas de configuración de red con las reglas de los grupos de seguridad, las tablas de enrutamiento y las listas de control de acceso a la red (ACLs) asociadas a las subredes.
- Verifica la conectividad con los puntos de conexión de Elastic Beanstalk y el acceso público a Internet.
- Verifica el estado del equilibrador de carga.
- Verifica el estado de las instancias de Amazon EC2.
- Recupera un paquete de registros del entorno de Elastic Beanstalk y, si lo desea, carga los archivos en él. Soporte

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `ApplicationName`

Tipo: cadena

Descripción: (obligatorio) el nombre de su aplicación Elastic Beanstalk.

- `EnvironmentName`

Tipo: cadena

Descripción: (obligatorio) el nombre de su entorno de Elastic Beanstalk.

- `AWSS3UploaderLink`

Tipo: cadena

Descripción: (opcional) URL que le proporcionó Soporte para cargar el paquete de registros desde su entorno de Elastic Beanstalk a. Esta opción solo está disponible para los clientes que hayan comprado un Soporte plan y hayan abierto un caso de Support.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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*`

Pasos de documentos

- `aws:executeScript`- Comprueba que el director AWS Identity and Access Management (IAM) que inició la automatización tiene los permisos necesarios para realizar todas las acciones definidas en el manual.
- `aws:branch`: ramifica el flujo de trabajo en función de los resultados del paso anterior.
- `aws:executeScript`- Recopila información sobre el entorno de Elastic Beanstalk, incluidos el balanceador de carga CloudFormation , la pila, el grupo de Auto Scaling, las instancias de Amazon EC2 y la configuración de la VPC.
- `aws:executeScript`- Comprueba si hay problemas de conectividad de red con las tablas de enrutamiento y las ACLs asociadas a las subredes de la VPC.

- `aws:executeScript`: comprueba si hay problemas de conectividad de red con las reglas del grupo de seguridad asociadas a sus instancias de Amazon EC2.
- `aws:executeScript`: verifica las comprobaciones de estado de las instancias de Amazon EC2.
- `aws:executeScript`: genera un enlace para un paquete de registros de su entorno de Elastic Beanstalk.
- `aws:executeScript`- Carga el paquete de registros a. Soporte
- `aws:executeScript`: genera un informe de las medidas a tomar para ayudarle a solucionar problemas que podrían estar afectando al estado de su entorno de Elastic Beanstalk.

Elastic Load Balancing

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para Elastic Load Balancing. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-DropInvalidHeadersForALB](#)
- [AWS-EnableCLBAccessLogs](#)
- [AWS-EnableCLBConnectionDraining](#)
- [AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing](#)
- [AWSConfigRemediation-EnableELBDeletionProtection](#)
- [AWSConfigRemediation-EnableLoggingForALBAndCLB](#)
- [AWSSupport-TroubleshootCLBConnectivity](#)
- [AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing](#)
- [AWS-UpdateALBDesyncMitigationMode](#)
- [AWS-UpdateCLBDesyncMitigationMode](#)
- [AWSSupport-TroubleshootELBHealthChecks](#)

AWSConfigRemediation-DropInvalidHeadersForALB

Descripción

El manual `AWSConfigRemediation-DropInvalidHeadersForALB` de procedimientos permite que el equilibrador de carga de aplicación que especifique elimine los encabezados HTTP con encabezados no válidos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `LoadBalancerArn`

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del equilibrador de carga del que desea eliminar los encabezados no válidos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeAwsApi`: habilita la opción de eliminar encabezados no válidos para el equilibrador de carga que especifique en el parámetro `LoadBalancerArn`.
- `aws:executeScript`: verifica que la opción de eliminar encabezados no válidos esté habilitada en el equilibrador de carga que especifique en el parámetro `LoadBalancerArn`.

AWS-EnableCLBAccessLogs

Descripción

El `AWS-EnableCLBAccessLogs` runbook permite acceder a los registros de acceso de un Classic Load Balancer.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **EmitInterval**

Tipo: entero

Valores válidos: 5 | 60

Predeterminado: 60

Descripción: (opcional) El intervalo de publicación de los registros de acceso en minutos.

- **LoadBalancerNames**

Tipo: cadena

Descripción: (Obligatorio) Una lista separada por comas de los balanceadores de carga clásicos para los que quieres habilitar los registros de acceso.

- **S3 BucketName**

Tipo: cadena

Descripción: (Obligatorio) El nombre del depósito de Amazon Simple Storage Service (Amazon S3) en el que se almacenan los registros de acceso.

- **S3 BucketPrefix**

Tipo: cadena

Descripción: (opcional) La jerarquía lógica que creó para su bucket de Amazon S3, por ejemplo `my-bucket-prefix/prod`. Si no se ha proporcionado el prefijo, el registro se colocan en el nivel raíz del bucket.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeAwsApi`- Habilita los registros de acceso para los balanceadores de carga clásicos que especifique en el `LoadBalancerNames` parámetro.

Salidas

Habilite los `CLBAccess` registros. `SuccessesLoadBalancers` - Lista de nombres de balanceadores de carga en los que los registros de acceso se habilitaron correctamente.

Habilite los `CLBAccess` registros. `FailedLoadBalancers` - `MapList` de los nombres de los balanceadores de carga en los que no se pudo habilitar los registros de acceso y el motivo del error.

AWS-EnableCLBConnectionDraining

Descripción

El `AWS-EnableCLBConnectionDraining` runbook permite agotar la conexión en un Classic Load Balancer (CLB) hasta el valor de tiempo de espera especificado. El agotamiento de las conexiones permite al CLB completar las solicitudes en curso realizadas a instancias que se están cancelando el registro o en mal estado, y el tiempo de espera especificado es el tiempo que mantiene activas las conexiones antes de informar que la instancia está cancelada. Para obtener más información sobre el agotamiento de conexiones CLBs, consulte [Configurar el drenaje de conexiones para el Classic Load Balancer](#) en la Guía del usuario de Classic Load Balancers.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LoadBalancerName

Tipo: cadena

Descripción: (obligatorio) El nombre del equilibrador de carga en el que quieres activar el agotamiento de la conexión.

- ConnectionTimeout

Tipo: entero

Valores válidos: 1-3600

Predeterminado: 300

Descripción: (obligatorio) El valor de tiempo de espera de conexión del balanceador de cargas. El valor de tiempo de espera se puede establecer entre 1 y 3600 segundos.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

Pasos de documentos

- ModifyLoadBalancerConnectionDraining (aws:executeAwsApi): habilita el agotamiento de la conexión y establece el valor de tiempo de espera especificado para el balanceador de cargas que especifique.

- `VerifyLoadBalancerConnectionDrainingEnabled(aws: assertAwsResource Property)`: verifica que el drenaje de conexiones esté habilitado para el balanceador de cargas.
- `VerifyLoadBalancerConnectionDrainingTimeout(aws: assertAwsResource Property)`: verifica que el valor del tiempo de espera de conexión del balanceador de cargas coincida con el valor que especificó.

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` permite el equilibrio de carga entre zonas para el Equilibrador de carga clásico (CLB) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `LoadBalancerName`

Tipo: cadena

Descripción: (obligatorio) el nombre del CLB en el que desea habilitar el equilibrio de carga entre zonas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeAwsApi`: habilita el equilibrio de carga entre zonas para el CLB que especifique en el parámetro `LoadBalancerName`.
- `aws:assertAwsResourceProperty`: verifica que el equilibrio de carga entre zonas esté habilitado en el CLB.

AWSConfigRemediation-EnableELBDeletionProtection

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableELBDeletionProtection` habilita la protección contra la eliminación para el equilibrador de carga elástico (ELB) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- LoadBalancerArn

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del ELB en el que desea habilitar la protección de eliminación.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:ModifyLoadBalancerAttributes

Pasos de documentos

- aws:executeScript: habilita la protección contra la eliminación en el ELB que especifique en el parámetro LoadBalancerArn.

AWSConfigRemediation-EnableLoggingForALBAndCLB

Descripción

El AWSConfigRemediation-EnableLoggingForALBAndCLB runbook permite registrar el AWS Application Load Balancer o el Classic Load Balancer (CLB) especificados.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- LoadBalancerId

Tipo: cadena

Descripción: (obligatorio) el nombre del equilibrador de carga clásico o el ARN del equilibrador de carga de aplicación.

- S3 BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de Amazon S3.

- S3 BucketPrefix

Tipo: cadena

Descripción: (opcional) la jerarquía lógica que creó para su bucket de Amazon Simple Storage Service (Amazon S3), por ejemplo my-bucket-prefix/prod. Si no se ha proporcionado el prefijo, el registro se colocan en el nivel raíz del bucket.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

Pasos de documentos

- aws:executeScript: habilita y verifica el registro del equilibrador de carga clásico o el equilibrador de carga de aplicación.

AWSSupport-TroubleshootCLBConnectivity

Descripción

El manual de procedimientos AWSSupport-TroubleshootCLBConnectivity le ayudará a solucionar problemas de conectividad entre instancias de un equilibrador de carga clásico (CLB) y Amazon Elastic Compute Cloud (Amazon EC2). Además, se revisan los problemas de conectividad entre un cliente y el CLB. Este manual de procedimientos también revisa las comprobaciones de estado del CLB, verifica que se estén siguiendo las mejores prácticas y crea un panel de solución de problemas para usted. Si lo desea, puede cargar la salida de automatización en un bucket de Amazon Simple Storage Service (Amazon S3). Sin embargo, este manual de procedimientos no admite la carga de salida en buckets de S3 que son de acceso público. Recomendamos crear un bucket de S3 temporal para esta automatización.

⚠ Important

El uso de este manual de procedimientos puede conllevar gastos por el panel que se cree. Para obtener más información, consulta los [CloudWatchprecios de Amazon](#)

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InvestigationType

Tipo: cadena

Valores válidos: Best Practices | Connectivity Issues | Troubleshooting Dashboard

Descripción: (obligatorio) las operaciones que desea que realice el manual de procedimientos.

- LoadBalancerName

Tipo: cadena

Descripción: (obligatorio) el nombre del CLB.

- S3Location

Tipo: cadena

Descripción: (opcional) el nombre del bucket de S3 al que desea enviar los resultados de la automatización. No se admiten los buckets de acceso público. Si su bucket de S3 usa el cifrado del lado del servidor, el usuario o rol que ejecute esta automatización debe tener permisos `kms:GenerateDataKey` para la clave AWS KMS .

- S3 LocationPrefix

Tipo: cadena

Descripción: (opcional) el prefijo clave de Amazon S3 (subcarpeta) en el que desea cargar el resultado de la automatización. El formato de salida se almacena en el siguiente formato:
S3LocationPrefix amzn-s3-demo-bucket/ {{}} _ {{automation:*InvestigationType*}} .txt.
EXECUTION_ID

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeScript`: verifica que existe el CLB que especifique en el parámetro `LoadBalancerName`.
- `aws:branch`: se ramifica en función del valor especificado para el parámetro `InvestigationType`.
- `aws:executeScript`: realiza comprobaciones de conectividad con el CLB.
- `aws:executeScript`: verifica que la configuración de CLB cumpla con las mejores prácticas de Elastic Load Balancing.
- `aws:executeScript`- Crea un CloudWatch panel de Amazon para tu CLB.
- `aws:executeScript`: crea un archivo de texto con los resultados de la automatización y lo carga en el bucket de Amazon S3 que especifique en el parámetro `S3Location`.

Salidas

RunBestPractices.Resumen

RunConnectivityChecks.Resumen

CreateTroubleshootingDashboard.Salida

UploadOutputToSalida S3.

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

Descripción

El manual de procedimientos AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing permite el equilibrio de carga entre zonas para el Equilibrador de carga de red (NLB) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- LoadBalancerArn

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del NLB en el que desea habilitar el equilibrio de carga entre zonas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- `aws:executeAwsApi`: habilita el equilibrio de carga entre zonas para el NLB que especifique en el parámetro `LoadBalancerArn`.
- `aws:executeScript`: verifica que el equilibrador de carga entre zonas esté habilitado en el NLB.

AWS-UpdateALBDesyncMitigationMode

Descripción

El `AWS-UpdateALBDesyncMitigationMode` manual actualizará el modo de mitigación desincronizado de un Application Load Balancer (ALB) al modo de mitigación especificado. El modo de mitigación desincronizado determina la forma en que el balanceador de cargas gestiona las solicitudes que puedan suponer un riesgo de seguridad para la aplicación.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LoadBalancerArn

Tipo: cadena

Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) del ALB del que desea modificar el modo de mitigación de desincronización.

- DesyncMitigationMode

Tipo: cadena

Valores válidos: monitor | defensivo | estricto

Descripción: (Obligatorio) El modo de mitigación que desea que utilice el ALB. Para obtener información sobre los modos de mitigación de desincronización, consulte el [modo de mitigación de desincronización](#) en la Guía del usuario de los balanceadores de carga de aplicaciones.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeLoadBalancerAttributes

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Pasos de documentos

- `VerifyLoadBalancerType` (aws: assertAwsResource Property): comprueba que el valor especificado para el parámetro de `LoadBalancerArn` entrada corresponde a un balanceador de carga de aplicaciones antes de continuar con el siguiente paso.
- `ModifyLoadBalancerDesyncMode` (aws:executeAwsApi) - Actualiza el ALB para usar el especificado. `DesyncMitigationMode`
- `VerifyLoadBalancerDesyncMitigationMode` (aws:Executescript) - Verifica que el modo de mitigación de desincronización se haya actualizado para el ALB de destino.

Salidas

`VerifyLoadBalancerDesyncMitigationMode`. `ModificationResult` - Carga útil del mensaje del script que verifica la modificación en su ALB.

AWS-UpdateCLBDesyncMitigationMode

Descripción

El `AWS-UpdateCLBDesyncMitigationMode` manual actualizará el modo de mitigación desincronizado de un Classic Load Balancer (CLB) al modo de mitigación especificado. El modo de mitigación desincronizado determina la forma en que el balanceador de cargas gestiona las solicitudes que puedan suponer un riesgo de seguridad para la aplicación.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LoadBalancerName

Tipo: cadena

Descripción: (obligatorio) El nombre del CLB del que quieres modificar el modo de mitigación de desincronización.

- DesyncMitigationMode

Tipo: cadena

Valores válidos: monitor | defensivo | estricto

Descripción: (obligatorio) El modo de mitigación que desea que utilice el CLB. Para obtener información sobre los modos de mitigación desincronizados, consulte el [modo de mitigación desincronizado](#) en la Guía del usuario de los balanceadores de carga de aplicaciones.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

Pasos de documentos

- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - Actualiza el CLB para usar el especificado. DesyncMitigationMode

- `VerifyLoadBalancerDesyncMitigationMode` (aws:Executescript) - Verifica que el modo de mitigación de desincronización se haya actualizado para el CLB de destino.

Salidas

`VerifyLoadBalancerDesyncMitigationMode`. `ModificationResult` - Carga útil del mensaje del script que verifica la modificación de su CLB.

AWSSupport-TroubleshootELBHealthChecks

Descripción

El `AWSSupport-TroubleshootELBHealthChecks` manual ayuda a solucionar problemas de comprobación de estado de AWS Elastic Load Balancing (Elastic Load Balancing) mediante el análisis de las métricas de Amazon CloudWatch (CloudWatch) relacionadas, la verificación de la conectividad de la red y la ejecución de comandos de diagnóstico en las instancias de destino.

Este manual aborda los siguientes casos de uso:

- Hay instancias en mal estado en las instancias de destino de un balanceador de cargas o de un grupo objetivo.
- Si bien no hay instancias en mal estado, CloudWatch las métricas indican puntos de datos para `UnHealthyHostCounts`

Important

Consideraciones importantes:

- La automatización se centra en la resolución de problemas de los objetivos de tipo instancia.
- El número máximo de instancias permitido para la solución de problemas es de 50.
- Systems Manager debe administrar las instancias de destino para permitir la ejecución de comandos de diagnóstico a nivel de instancia.
- El `S3BucketName` parámetro es opcional, pero algunos resultados de diagnóstico se cargan directamente en el bucket de Amazon S3 especificado y no se muestran en el resultado de la automatización.
- IPv6 no se admite la solución de problemas de conectividad de red.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeTargetGroups`
- `elasticloadbalancing:DescribeTargetHealth`
- `elasticloadbalancing:DescribeInstanceHealth`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `cloudwatch:GetMetricStatistics`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `ssm:DescribeInstanceInformation`
- `s3:GetBucketLocation`
- `s3:GetBucketAcl`
- `s3:PutObject`

Ejemplo de política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeInstanceHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "cloudwatch:GetMetricStatistics",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootELBHealthChecks](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a SSM Automation realizar las acciones en su nombre. Si no se especifica ningún rol, SSM Automation utiliza los permisos del usuario que inicia este manual.

- Tipo: `AWS::IAM::Role::Arn`
- `LoadBalancerOrTargetGroupName` (Obligatorio):
 - Descripción: (obligatorio) El nombre de un Classic Load Balancer o el nombre del grupo objetivo asociado a un Application Load Balancer o Network Load Balancer.
 - Tipo: `String`
 - Valor permitido: `^[a-zA-Z0-9-]+$`
- `ExecutionMode` (Obligatorio):
 - Descripción: (Obligatorio) Controla el modo de ejecución de la automatización. `Complete` ejecuta todos los pasos, incluidos los `runCommands`, en las instancias de Amazon EC2. `SkipRunCommand` ejecuta todos los pasos excepto la ejecución de los comandos en las instancias.
 - Tipo: `String`
 - Valores permitidos: `[Complete, SkipRunCommands]`
- `S3 BucketName` (opcional):
 - Descripción: (opcional) El nombre del depósito de Amazon S3 de su cuenta en el que desea cargar los registros de solución de problemas.
 - Tipo: `String`
 - Valor predeterminado: `""`

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `getBucketPublicEstado`:

Comprueba si el bucket de Amazon S3 de destino puede conceder acceso público de lectura o escritura a sus objetos.

- `getLoadBalancerDetalles`:

Identifica el tipo de balanceador de cargas y devuelve un objeto de detalles del balanceador de cargas unificado.

- `checkLoadBalancerType`:

Comprueba si el equilibrador de cargas existe.

Según los diferentes tipos de balanceadores de carga, las consultas describen cómo devolver un mapa APIs con los detalles de los objetivos en buen estado y en mal estado.

- `checkCloudWatchMétricas`:

Comprueba las CloudWatch métricas `HealthyHostCounts` `UnHealthyHostCounts` y genera los CloudWatch enlaces.

- `checkUnhealthyReasons`:

Comprueba si hay motivos insalubres y filtra los objetivos.

- Compruebe la conectividad:

Comprueba la conectividad entre el balanceador de cargas y sus instancias.

- Ejecute los comandos:

Ejecuta comandos de solución de problemas en las instancias y carga el resultado si se proporciona el nombre del bucket.

- Generar un informe:

Genera el informe final en función del resultado de los pasos anteriores y, si se especifica, carga el informe en el bucket de Amazon S3.

7. Una vez finalizado, revise la sección de resultados para ver los resultados detallados de la ejecución.

Diagnostic Commands

El runbook ejecuta los siguientes comandos de diagnóstico en las instancias:

- Shell de Linux: `top`, `free`, `ss`, `curl`, `iptables`, `tcpdump`
- Windows PowerShell: `Get-CimInstance`, `Get-`, `Get-NetFirewallProfile`, `Invoke-NetFirewallRuleWebRequest`, `netstat`, `netsh`, `pktmon`

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)

- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

Amazon EMR

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon EMR. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSsupport-AnalyzeEMRLogs](#)
- [AWSsupport-DiagnoseEMRLogsWithAthena](#)

AWSsupport -AnalyzeEMRLogs

Descripción

Este manual de procedimientos ayuda a identificar los errores al ejecutar un trabajo en un clúster de Amazon EMR. El manual de procedimientos analiza una lista de registros definidos en el sistema de archivos y busca una lista de palabras clave predefinidas. Estas entradas de registro se utilizan para crear CloudWatch eventos de Amazon Events para que pueda realizar las acciones necesarias en función de los eventos. Si lo desea, el runbook publica las entradas de registro en el grupo de CloudWatch registros de Amazon Logs que elija. Actualmente, este manual de procedimientos busca los siguientes errores y patrones en los archivos de registro:

- `container_out_of_memory`: el contenedor YARN se quedó sin memoria, por lo que es posible que no se ejecute el trabajo.
- `yarn_nodemanager_health`: el nodo MAESTRO o de TAREA se está quedando sin espacio en disco y no podrá ejecutar tareas.
- `node_state_change`: el nodo MAESTRO no puede acceder al nodo MAESTRO o de TAREA.
- `step_failure`: falló un paso de EMR.
- `no_core_nodes_running`: actualmente no hay nodos PRINCIPALES en ejecución, el clúster no está en buen estado.
- `hdfs_missing_blocks`: faltan bloques de HDFS, lo que podría provocar la pérdida de datos.

- `hdfs_high_util`: el uso del HDFS es elevado, lo que puede afectar a los trabajos y al buen estado del clúster.
- `instance_controller_restart`: el proceso del controlador de instancias se ha reiniciado. Este proceso es esencial para el buen estado del clúster.
- `instance_controller_restart_legacy`: el proceso del controlador de instancias se ha reiniciado. Este proceso es esencial para el buen estado del clúster.
- `high_load`: se detectó un promedio de carga alto, lo que puede afectar a los informes sobre el estado de los nodos o provocar tiempos de espera o ralentizaciones.
- `yarn_node_blacklisted`: YARN ha incluido en la lista negra el nodo MAESTRO o de TAREA para que no pueda ejecutar tareas.
- `yarn_node_lost`: YARN ha marcado el nodo MAESTRO o de TAREA como PERDIDO, posibles problemas de conectividad.

Las instancias asociadas al `ClusterID` que especifique deben ser administradas por AWS Systems Manager. Puede ejecutar esta automatización una vez, programar la automatización para que se ejecute en un intervalo de tiempo específico o eliminar una programación creada previamente por una automatización. Este manual de procedimientos es compatible con las versiones 5.20 a 6.30 de Amazon EMR.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ID del clúster

Tipo: cadena

Descripción: (obligatorio) el ID del clúster cuyos registros de nodos desea analizar.

- Operación

Tipo: cadena

Valores válidos: Run Once | Schedule | Remove Schedule

Descripción: (obligatoria) la operación que se debe realizar en el clúster.

- IntervalTime

Tipo: cadena

Valores válidos: 5 minutes | 10 minutes | 15 minutes

Descripción: (opcional) el tiempo transcurrido entre la ejecución de la automatización. Este parámetro solo se aplica si especifica Schedule para el parámetro Operation.

- LogToCloudWatchLogs

Tipo: cadena

Valores válidos: Yes | No

Descripción: (opcional) Si especificas yes el valor de este parámetro, la automatización crea un grupo de CloudWatch registros con el nombre especificado en el CloudWatchLogGroup parámetro para almacenar cualquier entrada de registro que coincida.

- CloudWatchLogGroup

Tipo: cadena

Descripción: (opcional) El nombre del grupo de CloudWatch registros en el que desea almacenar las entradas de registro coincidentes. Este parámetro solo se aplica si especifica `yes` para el parámetro `LogToCloudWatchLogs`.

- `CreateLogInsightsDashboard`

Tipo: cadena

Valores válidos: `Yes` | `No`

Descripción: (opcional) Si lo especifica `yes`, se crea el CloudWatch panel si aún no existe. Este parámetro solo se aplica si especifica `yes` para el parámetro `LogToCloudWatchLogs`.

- `CreateMetricFilters`

Tipo: cadena

Valores válidos: `Yes` | `No`

Descripción: (opcional) Especifique `yes` si desea crear filtros de métricas para el grupo de CloudWatch registros. Este parámetro solo se aplica si especifica `yes` para el parámetro `LogToCloudWatchLogs`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeAwsApi`: recopila información sobre el clúster de Amazon EMR especificado en el parámetro `ClusterID`.
- `aws:branch`: se ramifica en función de la entrada.
 - Si la operación proporcionada es `Run Once` o `Schedule`:
 - `aws:assertAwsResourceProperty`: verifica que el clúster esté disponible.
 - `aws:executeAwsApi`- Reúne todas IDs las instancias que se ejecutan en el clúster.
 - `aws:assertAwsResourceProperty`: verifica que el agente SSM se esté ejecutando en todas las instancias del clúster.

- `aws:branch`: se ramifica en función de si especificó ejecutar la automatización una vez o de forma programada.
- Si la operación proporcionada es `Run Once`:
 - `aws:branch`: se ramifica en función del valor especificado en el parámetro `LogToCloudWatchLogs`.
 - Si el valor `LogToCloudWatchLogs` es `yes`:
 - `aws:executeScript`- Comprueba si `CloudWatchLogGroup` ya existe un grupo de `CloudWatch` registros con el nombre especificado en el parámetro. De lo contrario, el grupo se crea con el nombre especificado.
 - `aws:branch`: se ramifica en función del valor especificado en el parámetro `CreateMetricFilters`.
 - Si el valor `CreateMetricFilters` es `yes`:
 - `aws:executeAwsApi`: se ejecutan 12 pasos para cada filtro métrico
 - `aws:branch`: se ramifica en función del valor especificado en el parámetro `CreateLogInsightsDashboard`.
 - Si el valor `CreateLogInsightsDashboard` es `yes`:
 - `aws:executeAwsApi`- Crea un `CloudWatch` panel con el mismo nombre especificado en el `CloudWatchLogGroup` parámetro, si aún no existe.
 - Si el valor `CreateLogInsightsDashboard` es `no`:
 - `aws:runCommand`: ejecuta un script de intérprete de comandos para buscar patrones de registro en cada instancia en el clúster.
 - Si el valor `CreateMetricFilters` es `no`:
 - `aws:branch`: se ramifica en función del valor especificado en el parámetro `CreateLogInsightsDashboard`.
 - Si el valor `CreateLogInsightsDashboard` es `yes`:
 - `aws:executeAwsApi`- Crea un `CloudWatch` panel con el mismo nombre especificado en el `CloudWatchLogGroup` parámetro, si aún no existe.
 - Si el valor `CreateLogInsightsDashboard` es `no`:
 - `aws:runCommand`: ejecuta un script de intérprete de comandos para buscar patrones de registro en cada instancia en el clúster.
 - Si el valor `LogToCloudWatchLogs` es `no`:

- `aws:executeAwsApi`: ejecuta un script de intérprete de comandos para buscar patrones de registro en cada instancia en el clúster.
- Si la operación proporcionada es `Schedule`:
 - `aws:createStack`- Crea un EventBridge evento de Amazon dirigido a este runbook.
- Si la operación proporcionada es `Remove Schedule`:
 - `aws:executeAwsApi`: verifica la existencia de un horario para el clúster.
 - `aws:deleteStack`: elimina la programación.

Salidas

`GetClusterInformation.ClusterName`

`GetClusterInformation.ClusterState`

`ListingClusterInstances.Instancia IDs`

`CreatingScheduleCloudFormationStack.StackStatus`

`RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus`

`CheckIfLogGroupExists.salida`

`FindLogPatternOnEMRNode.CommandId`

AWSSupport-DiagnoseEMRLogsWithAthena

Descripción

El `AWSSupport-DiagnoseEMRLogsWithAthena` manual ayuda a diagnosticar los registros de Amazon EMR mediante Amazon Athena en integración con Data Catalog. AWS Glue Amazon Athena sirve para consultar los archivos de registro de Amazon EMR que corresponden a contenedores, registros de nodos o ambos. Se pueden aplicar parámetros opcionales para intervalos de fechas específicos o búsquedas basadas en palabras clave.

El runbook puede recuperar automáticamente la ubicación del registro de Amazon EMR de un clúster existente, o puede especificar la ubicación del registro de Amazon S3. Para analizar los registros, el runbook:

- Crea una AWS Glue base de datos y ejecuta consultas del lenguaje de definición de datos (DDL) de Amazon Athena en la ubicación del registro Amazon S3 de Amazon EMR para crear tablas para los registros del clúster y una lista de problemas conocidos.
- Ejecuta consultas de lenguaje de manipulación de datos (DML) para buscar patrones de problemas conocidos en los registros de Amazon EMR. Las consultas devuelven una lista de los problemas detectados, su número de incidencias y el número de palabras clave coincidentes por ruta de archivo de Amazon S3.
- Los resultados se cargan en un bucket de Amazon S3 que especifique bajo el prefijosaw_diagnose_EMR_known_issues.
- El manual muestra los resultados de las consultas de Amazon Athena y destaca los hallazgos, recomendaciones y referencias a los artículos del Amazon Knowledge Center (KC) procedentes de un subconjunto predefinido.
- Al finalizar o fallar, se eliminan la AWS Glue base de datos y los archivos de problemas conocidos cargados en el bucket de Amazon S3.

¿Cómo funciona?

AWSSupport-DiagnoseEMRLogsWithAthena Realice un análisis de los registros de Amazon EMR con Amazon Athena para detectar errores y destacar los hallazgos, recomendaciones y artículos relevantes del Knowledge Center.

El manual lleva a cabo los siguientes pasos:

- Obtenga la ubicación del registro del clúster de Amazon EMR mediante el ID del clúster o introduzca la ubicación de Amazon S3 para recuperar la ubicación y el tamaño del registro.
- Proporcione a Athena una estimación de los costos en función del tamaño de la ubicación del registro.
- Obtenga la aprobación para continuar solicitando la aprobación de los directores de IAM designados antes de ejecutar las consultas de Athena y continuar con los siguientes pasos.
- Sube los problemas conocidos al bucket de Amazon S3 especificado y crea una AWS Glue base de datos y tablas.
- Ejecute consultas de Athena en los datos de los registros de Amazon EMR. Las consultas se pueden buscar por intervalo de fechas, palabras clave o ambos criterios o ejecutarse sin filtros en función de las entradas proporcionadas.
- Analice los resultados para destacar los hallazgos, las recomendaciones y los artículos relevantes de KC.

- Enlaces de salida para los resultados de las consultas de Amazon Athena DML.
- Limpie el entorno eliminando la base de datos creada, las tablas y los problemas conocidos cargados.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

El AutomationAssumeRole parámetro requiere las siguientes acciones para utilizar correctamente el runbook:

- atenea: GetQueryExecution
- atenea: StartQueryExecution
- atenea: GetPreparedStatement
- atenea: CreatePreparedStatement
- pegamento: GetDatabase
- pegamento: CreateDatabase
- pegamento: DeleteDatabase
- pegamento: CreateTable
- pegamento: GetTable
- pegamento: DeleteTable
- elasticmapreduce: DescribeCluster
- s3: ListBucket
- s3: GetBucketVersioning
- s3: ListBucketVersions
- s3: GetBucketPublicAccessBlock
- s3: GetBucketPolicyStatus
- s3: GetObject

- s3: GetBucketLocation
- precios: GetProducts
- precios: GetAttributeValues
- precios: DescribeServices
- precios: ListPriceLists

Important

Para restringir el acceso únicamente a los recursos que necesita esta automatización, asocie la siguiente política a la función de IAM que confía en el servicio SSM. Sustituya la partición, la región y la cuenta por los valores adecuados para la partición, la región y el número de cuenta en los que se ejecuta el libro de ejecuciones.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticmapreduce:DescribeCluster",
        "glue:GetDatabase",
        "athena:GetQueryExecution",
        "athena:StartQueryExecution",
        "athena:GetPreparedStatement",
        "athena:CreatePreparedStatement",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:ListBucketVersions",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "pricing:GetProducts",
        "pricing:GetAttributeValues",
        "pricing:DescribeServices",
        "pricing:ListPriceLists"
      ]
    }
  ]
}
```



```

    ],
    "Resource": "*"
  },
  {
    "Sid": "RestrictPutObjects",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::*/results/*",
      "arn:aws:s3:::*/saw_diagnose_emr_known_issues/*"
    ]
  },
  {
    "Sid": "RestrictDeleteAccess",
    "Effect": "Allow",
    "Action": [
      "s3:DeleteObject",
      "s3:DeleteObjectVersion"
    ],
    "Resource": [
      "arn:aws:s3:::*/saw_diagnose_emr_known_issues/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "glue:GetDatabase",
      "glue:CreateDatabase",
      "glue:DeleteDatabase"
    ],
    "Resource": [
      "arn:aws:glue:us-east-1:111122223333:database/saw_diagnose_emr_database_*",
      "arn:aws:glue:us-east-1:111122223333:table/saw_diagnose_emr_database_*/*",
      "arn:aws:glue:us-east-1:111122223333:userDefinedFunction/saw_diagnose_emr_database_*/*",
      "arn:aws:glue:us-east-1:111122223333:catalog"
    ]
  },
  {
    "Effect": "Allow",

```

```

        "Action": [
            "glue:CreateTable",
            "glue:GetTable",
            "glue>DeleteTable"
        ],
        "Resource": [
            "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/saw_diagnose_emr_known_issues",
            "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/saw_diagnose_emr_logs_table",
            "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/j_*",
            "arn:aws:glue:us-east-1:111122223333:database/
saw_diagnose_emr_database_*",
            "arn:aws:glue:us-east-1:111122223333:catalog"
        ]
    }
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue por [AWSSupport-DiagnoseEMRLogsWithAthena](#) a la parte AWS Systems Manager inferior de Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ClusterID (obligatorio):

El ID del clúster de Amazon EMR.

- S3 LogLocation (opcional):

La ubicación del registro de Amazon EMR de Amazon S3. Introduzca la URL de estilo Path (ubicación de Amazon S3), por ejemplo: `s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/`. Proporcione este parámetro si el clúster de Amazon EMR ha estado cerrado durante más 30 de unos días.

- S3 BucketName (obligatorio):

El nombre del bucket de Amazon S3 para cargar una lista de problemas conocidos y el resultado de las consultas de Amazon Athena. El bucket debe tener [activado el acceso público en bloque](#) y estar en la misma AWS región y cuenta que el clúster de Amazon EMR.

- Aprobadores (obligatorio):

La lista de directores AWS autenticados que pueden aprobar o rechazar la acción. Puede especificar los principales mediante cualquiera de los siguientes formatos: nombre de usuario, ARN de usuario, ARN del rol de IAM o ARN de asumir rol de IAM. El número máximo de aprobadores es 10.

- FetchNodeLogsOnly (Opcional):

Si se establece en `true`, la automatización diagnostica los registros de contenedores de la aplicación Amazon EMR. El valor predeterminado es `false`.

- FetchContainersLogsOnly(Opcional):

Si se establece en `true`, la automatización diagnostica los registros de contenedores de Amazon EMR. El valor predeterminado es `false`.

- EndSearchDate (Opcional):

La fecha de finalización de las búsquedas en los registros. Si se proporciona, la automatización buscará exclusivamente los registros generados hasta la fecha especificada en el formato YYYY-MM-DD (por ejemplo: 2024-12-30).

- DaysToCheck (Opcional):

Si EndSearchDate se proporciona, este parámetro es necesario para determinar el número de días necesarios para buscar retrospectivamente los registros especificados EndSearchDate. El valor máximo es de 30 días. El valor predeterminado es 1.

- SearchKeywords (Opcional):

La lista de palabras clave para buscar en los registros, separadas por comas. Las palabras clave no pueden contener comillas simples o dobles.

Input parameters

AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. SSMAutomation	ClusterID (Required) The Amazon EMR cluster ID. j-1K48XXXXXXHCB
S3LogLocation (Optional) The Amazon S3 URL that contains the Amazon EMR logs. Provide this parameter if the Amazon EMR cluster has been terminated for more than 30 days. Provide the full Amazon S3 path prefix for the EMR logs. Example <code>s3://mybucket/myfolder/j-1K48XXXXXXHCB/</code>. String	S3BucketName (Required) The Amazon S3 bucket name to upload a list of known issues, and the output of Amazon Athena queries. The bucket should have [Block Public Access Enabled](https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html) and be in the same AWS region as the Amazon EMR cluster provided. String
Approvers (Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats: 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN. arn:awsiam::[redacted]:role/Approver	FetchNodeLogsOnly (Optional) If set to "true", the automation diagnoses the Amazon EMR node logs. false
FetchContainersLogsOnly (Optional) If set to "true", the automation diagnoses the Amazon EMR containers logs related to applications on the cluster. false	EndSearchDate (Optional) The end date for log searches. If provided, the automation will exclusively search for logs generated up to the specified date in the format YYYY-MM-DD (for example: "2024-12-30"). String
DaysToCheck (Optional) When "EndSearchDate" is provided, this parameter is required to determine the number of days to retrospectively search for logs from the specified "EndSearchDate". The maximum value is "30" days. 1	SearchKeywords (Optional) The list of keywords to search in the logs, separated by commas. The keywords cannot contain single or double quotes. StringList

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **getLogLocation:**

Recupera la ubicación del registro de Amazon S3 consultando el ID de clúster de Amazon EMR especificado. Si la automatización no puede consultar la ubicación del registro desde el ID del clúster de Amazon EMR, el runbook utiliza el `S3LogLocation` parámetro de entrada.

- **branchOnValidRegistro:**

Verifica la ubicación de los registros de Amazon EMR. Si la ubicación es válida, proceda a estimar los posibles costes de Amazon Athena al ejecutar consultas en los registros de Amazon EMR.

- **estimateAthenaCosts:**

Determina el tamaño de los registros de Amazon EMR y proporciona una estimación del costo de ejecutar los escaneos de Athena en el conjunto de datos de registros. Para las regiones no comerciales (sin AWS particiones), este paso solo proporciona el tamaño del registro sin estimar los costos. Los costes se pueden calcular utilizando la documentación de precios de Athena en la región especificada.

- **Apruebe la automatización:**

Espera la aprobación del director de IAM designado para continuar con los siguientes pasos de la automatización. La notificación de aprobación contiene el costo estimado del escaneo de Amazon Athena en los registros de Amazon EMR y detalles sobre los recursos que aprovisiona la automatización.

- `uploadKnownIssuesExecuteAthenaQueries`:

Carga los problemas conocidos predefinidos en el bucket de Amazon S3 especificado en el `S3BucketName` parámetro. Crea AWS Glue bases de datos y tablas. Ejecuta las consultas de Amazon Athena en AWS Glue la base de datos en función de los parámetros de entrada.

- `getQueryExecutionEstado`:

Espera hasta que la ejecución de la consulta de Amazon Athena esté `SUCCEEDED` activa. La consulta DML de Amazon Athena busca errores y excepciones en los registros del clúster de Amazon EMR.

- `analyzeAthenaResults`:

Analiza los resultados de Amazon Athena para proporcionar hallazgos, recomendaciones y artículos del Knowledge Center (KC) procedentes de un conjunto predefinido de mapeos.

- `getAnalyzeResultsConsulta 1: ExecutionStatus`

Espera hasta que la ejecución de la consulta esté en estado. `SUCCEEDED` La consulta de DML de Amazon Athena analiza los resultados de la consulta de DML anterior. Esta consulta de análisis devolverá las excepciones coincidentes con las resoluciones y los artículos de KC

- `getAnalyzeResultsConsulta 2: ExecutionStatus`

Espera hasta que la ejecución de la consulta esté en estado. `SUCCEEDED` La consulta de DML de Amazon Athena analiza los resultados de la consulta de DML anterior. Esta consulta de análisis devolverá una lista de lo exceptions/errors detectado en cada ruta de registro de Amazon S3.

- `printAthenaQueriesMensaje`:

Imprime enlaces para los resultados de las consultas de Amazon Athena DML.

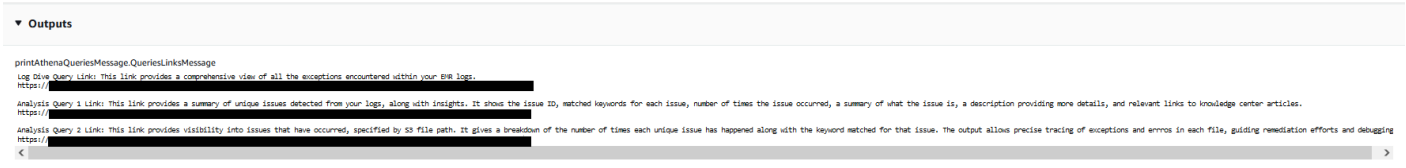
- Recursos de limpieza:

Limpia los recursos eliminando la AWS Glue base de datos creada y eliminando los archivos de problemas conocidos que se crearon en el depósito de registros de Amazon EMR.

7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución:

El resultado proporciona tres enlaces para los resultados de las consultas de Athena:

- Lista de todos los errores y excepciones frecuentes que se encuentran en los registros del clúster de Amazon EMR, junto con las ubicaciones de registro correspondientes (prefijo Amazon S3).
- Resumen de las excepciones conocidas únicas que coinciden en los registros de Amazon EMR, junto con las resoluciones recomendadas y los artículos de KC para ayudar a solucionar problemas.
- Detalles sobre dónde aparecen errores y excepciones específicos en las rutas de registro de Amazon S3, para facilitar un diagnóstico más detallado.



Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS documentación de servicio

- Consulte [Solución de problemas de clústeres de Amazon EMR](#) para obtener más información

OpenSearch Servicio Amazon

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon OpenSearch Service. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-DeleteOpenSearchDomain](#)

- [AWSConfigRemediation-EnforceHTTPSONOpenSearchDomain](#)
- [AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups](#)
- [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#)
- [AWSSupport-TroubleshootOpenSearchHighCPU](#)

AWSConfigRemediation-DeleteOpenSearchDomain

Descripción

El AWSConfigRemediation-DeleteOpenSearchDomain runbook elimina el dominio de Amazon OpenSearch Service en cuestión mediante la [DeleteDomain](#) API.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- DomainName

Tipo: cadena

Valores permitidos: `(\d{12})/[a-z]{1}[a-z0-9-]{2,28}`

Descripción: (Obligatorio) El nombre del dominio de Amazon OpenSearch Service que quieres eliminar.

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es>DeleteDomain`
- `es:DescribeDomain`

Pasos de documentos

- `aws:executeScript`- Acepta el nombre de dominio de Amazon OpenSearch Service como entrada, lo elimina y verifica la eliminación.

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

Descripción

El `AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain` runbook se habilita `EnforceHTTPS` en un dominio de Amazon OpenSearch Service determinado mediante la [UpdateDomainConfig](#) API.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `DomainName`

Tipo: cadena

Valores permitidos: `(\d{12})?[a-z]{1}[a-z0-9-]{2,28}`

Descripción: (Obligatorio) El nombre del dominio de Amazon OpenSearch Service que quieres usar para aplicar HTTPS.

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Pasos de documentos

- `aws:executeScript`- Activa la opción de `EnforceHTTPS` punto final en el dominio OpenSearch de Amazon Service que especifiques en el `DomainName` parámetro.

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

Descripción

El AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups runbook actualiza la configuración del grupo de seguridad en un dominio de Amazon OpenSearch Service determinado mediante la [UpdateDomainConfigAPI](#).

Note

AWS Los grupos de seguridad solo se pueden aplicar a los dominios de Amazon OpenSearch Service configurados para Amazon Virtual Private Cloud (VPC) y no a los dominios de Amazon OpenSearch Service configurados para Public Access.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- DomainName

Tipo: cadena

Descripción: (obligatorio) El nombre del dominio de Amazon OpenSearch Service que quieres usar para actualizar los grupos de seguridad.

- SecurityGroupList

Tipo: StringList

Descripción: (Obligatorio) El grupo de seguridad IDs que quieres asignar al dominio de Amazon OpenSearch Service.

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

Pasos de documentos

- aws:executeScript- Actualiza la configuración del grupo de seguridad en el dominio OpenSearch de Amazon Service que especifiques en el DomainName parámetro.

AWSSupport-TroubleshootOpenSearchRedYellowCluster

Descripción

AWSSupport-TroubleshootOpenSearchRedYellowClusterEl manual de automatización se utiliza para identificar la causa del estado de salud de los clústeres [rojos](#) o [amarillos](#) y sirve de guía para cambiar el clúster a verde.

¿Cómo funciona?

El manual le `AWSSupport-TroubleshootOpenSearchRedYellowCluster` ayuda a solucionar la causa del clúster rojo o amarillo y proporciona los siguientes pasos para resolver este problema mediante el análisis de la configuración del clúster y el uso de los recursos.

El manual de ejecución lleva a cabo los siguientes pasos:

- Llama a la [DescribeDomain](#) API en el dominio de destino para obtener la configuración del clúster.
- Comprueba si el dominio del OpenSearch servicio está basado en Internet (público) o en [Amazon Virtual Private Cloud \(VPC\)](#).
- Crea una función pública o [basada en Amazon VPC en](#) AWS Lambda función de la configuración del clúster. Nota: La función Lambda contiene el código de solución de problemas que ejecuta el OpenSearch Servicio en APIs el clúster para determinar por qué el clúster está en estado rojo o amarillo.
- Elimina la función Lambda.
- Muestra las comprobaciones realizadas y los siguientes pasos recomendados para resolver el problema del clúster rojo o amarillo.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

El `LambdaExecutionRole` parámetro requiere las siguientes acciones para utilizar correctamente el runbook:

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`

Descripción general de la `LambdaExecutionRole` política:

A continuación, se muestra un ejemplo del rol de ejecución de una función Lambda (rol AWS Identity and Access Management (IAM)) que otorga a la función permiso para acceder a los AWS servicios

y recursos que requiere este manual. Para obtener más información, consulte [Rol de ejecución de Lambda](#).

Note

Los `ec2:DescribeNetworkInterfaces` y `ec2:CreateNetworkInterface`, y solo `ec2>DeleteNetworkInterface` son necesarios si el clúster de OpenSearch servicio está [basado en Amazon VPC](#) para permitir que la función Lambda cree y gestione las interfaces de red de Amazon VPC. Para obtener más información, consulte [Conexión de redes salientes a recursos en una función de ejecución de Amazon VPC](#) y [Lambda](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "es:ESHttpGet",
      "Resource": [
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cluster/health",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cat/indices",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cat/allocation",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cluster/allocation/explain"
      ]
    },
    {
      "Condition": {
        "ArnLikeIfExists": {
          "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/vpc_id"
        }
      },
      "Action": [
        "ec2>DeleteNetworkInterface",
        "ec2>CreateNetworkInterface",

```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta la consola [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#). AWS Systems Manager
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LambdaExecutionRole (Obligatorio):

El ARN de la función de IAM que Lambda utilizará para firmar las solicitudes a tu clúster de Amazon Service. OpenSearch

- DomainName (Obligatorio):

El nombre del dominio del OpenSearch servicio con el estado de salud del clúster en rojo o amarillo.

- UtilizationThreshold (Opcional):

El porcentaje del umbral de utilización utilizado para comparar las métricas CPUUtilization y las de JVMMemory presión. El valor predeterminado es 80.

Input parameters

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

Select an existing IAM Role

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

DomainName
(Required) The name of the Amazon OpenSearch Service domain is red or yellow status.

opensearch-red-yellow-sample

LambdaExecutionRole
(Required) The ARN of the IAM role that the AWS Lambda will use to sign requests to your Amazon OpenSearch Service cluster.

Select an existing IAM Role

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

UtilizationThreshold
(Optional) The utilization threshold in percentage used to compare the 'CPUUtilization' and 'JVMMemoryPressure' metrics. Default value is '80'.

80

4. Si ha habilitado un [control de acceso detallado](#) en un clúster de OpenSearch servicios, asegúrese de que el LambdaExecutionRole rol arn esté asignado a un rol con al menos permiso.

`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. Seleccione Ejecutar.
6. Se inicia la automatización.
7. El manual de procedimientos de automatización realiza los siguientes pasos:

- GetClusterConfiguration:

Obtiene la configuración del clúster de servicios. OpenSearch

- Crea AWSLambdaFunctionStack:

Crea una función Lambda temporal en su cuenta mediante. CloudFormation La función Lambda se utiliza para ejecutar el OpenSearch servicio. APIs

- WaitForAWSLambdaFunctionStack:

Espera a que se complete la CloudFormation pila.

- **GetClusterMetricsFromCloudWatch:**

Obtiene las métricas relacionadas con los clústeres OpenSearch de Amazon CloudWatch ClusterStatus y JVMMemory Pressure Service y su fecha de creación. CPUUtilization

- **RunOpenSearchAPIs:**

Utiliza la función Lambda para llamar al OpenSearch Servicio APIs y analizar los datos de las métricas del clúster para diagnosticar la causa del estado rojo o amarillo del clúster.

- **Eliminar AWSLambdaFunctionStack:**

Elimina la función Lambda creada por esta automatización en su cuenta.

8. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.

- **RootCause:**

Proporciona una descripción general de la causa identificada por la que el estado del clúster está en rojo o amarillo.

- **IssueDescription:**

Proporciona detalles sobre por qué el clúster está en estado rojo o amarillo y las posibles medidas para devolverlo al estado verde.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS documentación de servicio

- Consulta [Solución de problemas de Amazon OpenSearch Service](#) para obtener más información.

AWSSupport-TroubleshootOpenSearchHighCPU

Descripción

El AWSSupport-TroubleshootOpenSearchHighCPU manual proporciona una solución automatizada para recopilar datos de diagnóstico de un dominio de Amazon OpenSearch Service a fin de solucionar problemas de [CPU elevados](#).

¿Cómo funciona?

El AWSSupport-TroubleshootOpenSearchHighCPU runbook ayuda a solucionar problemas de uso elevado de la CPU en el dominio de Amazon OpenSearch Service.

El manual de ejecución lleva a cabo los siguientes pasos:

- Ejecuta la [DescribeDomain](#) API en el dominio de Amazon OpenSearch Service proporcionado para obtener los metadatos del clúster.
- Comprueba si el dominio de Amazon OpenSearch Service es público o está basado en Amazon VPC y, con la ayuda de CloudFormation, crea una función pública o basada en [Amazon AWS Lambda VPC](#).
- La función Lambda obtiene datos de diagnóstico de los dominios de Amazon OpenSearch Service.
- Utiliza una máquina de AWS Step Functions estados para organizar múltiples ejecuciones de funciones Lambda a fin de recopilar datos más completos.
- De forma predeterminada, almacena los datos recopilados en un grupo de CloudWatch registros de Amazon durante 24 horas.
- Elimina los recursos creados, excepto el grupo de CloudWatch registros.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudformation:CreateStack`
- `cloudformation:CreateStack`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `cloudformation>DeleteStack`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:InvokeFunction`
- `lambda:GetFunction`
- `lambda:TagResource`
- `es:DescribeDomain`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:AttachNetworkInterface`
- `ec2>DeleteNetworkInterface`
- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:TagResource`
- `states:CreateStateMachine`
- `states>DeleteStateMachine`
- `states:StartExecution`

- `states:TagResource`
- `states:DescribeStateMachine`
- `states:DescribeExecution`
- `iam:PassRole`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam>DeleteRolePolicy`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

 Note

Los `iam:CreateRole` parámetros `iam>DeleteRole`, `iam:GetRole`, `iam:PutRolePolicy` y solo `iam>DeleteRolePolicy` son necesarios si no se utiliza una función de IAM existente como parámetro `LambdaInvocationRoleForStepFunctions`

El `LambdaExecutionRole` parámetro requiere las siguientes acciones para utilizar correctamente el runbook:

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2>DeleteNetworkInterface`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

La función de ejecución de Lambda otorga a la función permiso para acceder a AWS los servicios y recursos que requiere este manual. Para obtener más información, consulte [Rol de ejecución de Lambda](#).

Note

Los `ec2:DescribeNetworkInterfaces` y `ec2:CreateNetworkInterface`, y solo `ec2:DeleteNetworkInterface` son necesarios si el clúster de OpenSearch servicio está [basado en Amazon VPC](#) para permitir que la función Lambda cree y gestione las interfaces de red de Amazon VPC. Para obtener más información, consulte [Conexión de redes salientes a recursos en una función de ejecución de Amazon VPC](#) y [Lambda](#).

El `LambdaInvocationRoleForStepFunctions` parámetro concede los permisos para que la máquina de AWS Step Functions estado invoque la función Lambda. El siguiente es un ejemplo de política de IAM que otorga permiso a Step Functions para invocar la función Lambda que obtiene datos de diagnóstico del dominio de servicio. OpenSearch Para obtener más información, consulte [Creación de una función de IAM en una máquina de estado](#) en la Guía para desarrolladores. AWS Step Functions

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": [
        "arn:aws:lambda:us-east-1:111122223333:function:AWSSupport-
HighCPU-*"
      ]
    }
  ]
}
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootOpenSearchHighCPU](#) la AWS Systems Manager consola.

2. Elija **Execute automation** (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - **AutomationAssumeRole** (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **DomainName** (Obligatorio):

El nombre del dominio de Amazon OpenSearch Service que quieres solucionar en caso de problemas de CPU elevada.

- **LambdaExecutionRoleForOpenSearch**(Obligatorio):

El ARN de la función de IAM que se va a adjuntar a la función Lambda. La función Lambda usa las credenciales de este rol para firmar las solicitudes al dominio de Amazon OpenSearch Service. Si el control de acceso detallado está habilitado en el dominio de Amazon OpenSearch Service, debes asignar este rol a un rol de backend de OpenSearch Service Dashboards con un permiso mínimo de «cluster_monitor».

- **LambdaInvocationRoleForStepFunctions**(Opcional):

(Opcional) El ARN del rol de IAM que se va a adjuntar al flujo de trabajo de Step Functions. La máquina de estados usa las credenciales de este rol para invocar la función Lambda que obtiene los datos de diagnóstico del dominio del OpenSearch servicio. Si no se especifica ningún rol, esta automatización creará un rol de IAM para Step Functions en su cuenta.

- **DataRetentionDays** (Opcional):

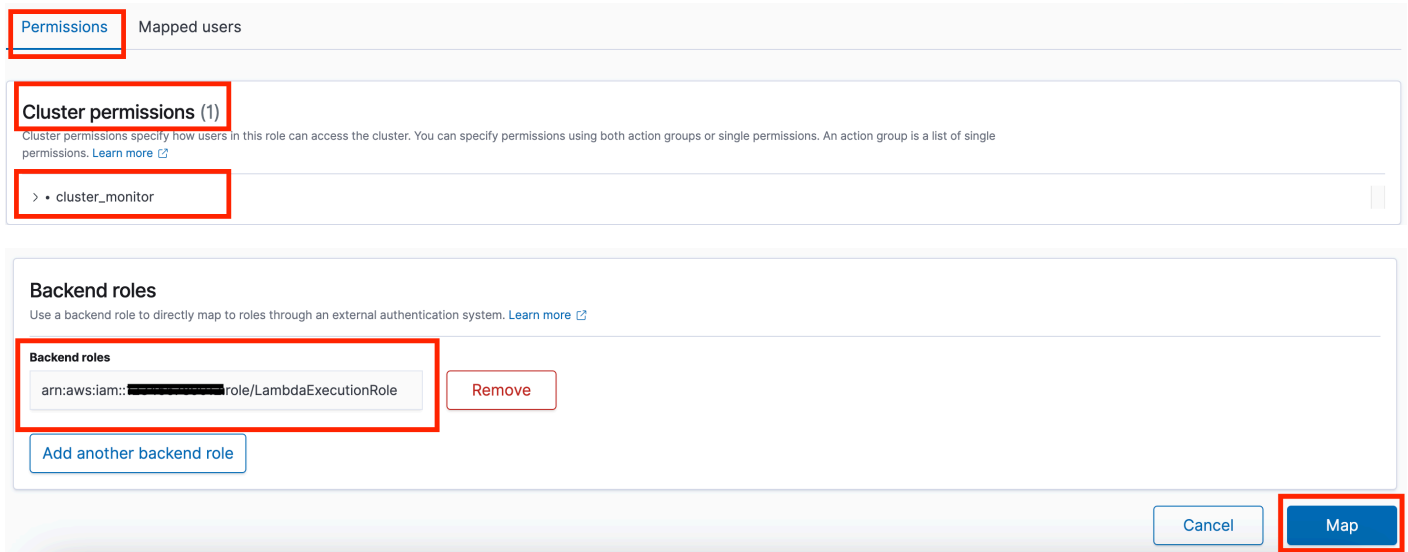
El número de días que se conservarán los datos de diagnóstico recopilados del dominio de Amazon OpenSearch Service. De forma predeterminada, los datos se conservan durante 24 horas (un día). Puede optar por conservar los datos durante un máximo de 30 días.

- **NumberOfDataSamples** (Opcional):

El número de muestras de datos que se van a recopilar del dominio OpenSearch de Amazon Service. De forma predeterminada, se recopilan 5 muestras de datos. Puede recopilar hasta 10 muestras y se invocará la función Lambda para cada colección de muestras.

4. Si ha habilitado un [control de acceso detallado](#) en un clúster de OpenSearch servicios, asegúrese de que el LambdaExecutionRole rol arn esté asignado a un rol con al menos permiso.

cluster_monitor



The screenshot shows the AWS IAM console interface. At the top, there are two tabs: 'Permissions' (highlighted with a red box) and 'Mapped users'. Below the tabs, there is a section titled 'Cluster permissions (1)' (highlighted with a red box). This section contains a description of cluster permissions and a list of permissions, which includes 'cluster_monitor' (highlighted with a red box). Below this, there is a section titled 'Backend roles'. It contains a list of roles, with one role 'arn:aws:iam::[redacted]:role/LambdaExecutionRole' (highlighted with a red box) and a 'Remove' button. At the bottom right, there are two buttons: 'Cancel' and 'Map' (highlighted with a red box).

5. Seleccione Ejecutar.

6. Se inicia la automatización.

7. El manual de procedimientos de automatización realiza los siguientes pasos:

- Compruebe la simultaneidad:

Garantiza que solo haya una ejecución de este runbook dirigida al dominio de Amazon OpenSearch Service especificado. Si el runbook encuentra otra ejecución dirigida al mismo nombre de dominio, devuelve un error y finaliza.

- getDomainConfig:

Obtiene los detalles de configuración del dominio de OpenSearch servicio de destino.

- Recursos de aprovisionamiento:

Aprovisiona los recursos para la recopilación de datos mediante CloudFormation.

- waitForStackCreación:

Espera a que se complete la CloudFormation pila.

- describeStackResources:

Describe la CloudFormation pila y obtiene el ARN de la máquina de estados.

- runStateMachine:

Invoca la función Lambda del recopilador de datos una o más veces mediante la ejecución de una máquina de estados Step Functions.

- `describeErrorsFromStackEvents`:

Describe los errores de la CloudFormation pila de errores.

- `unstageOpenSearchAltoCPUAutomation`:

Elimina la `AWSSupport-TroubleshootOpenSearchHighCPU` CloudFormation pila.

- `describeErrorsFromStackDeletion`:

Describe los errores encontrados al eliminar la CloudFormation pila.

- Estado final:

Devuelve el resultado final del runbook. `AWSSupport-TroubleshootOpenSearchHighCPU`

8. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.

- Estado final. `FinalOutput`:

Proporciona el grupo de CloudWatch registros en el que se almacenan los datos de diagnóstico.

▼ Outputs
<code>finalStatus.FinalOutput</code> Hot thread data collection completed. Please check the custom CloudWatch log group <code>/aws/lambda/AWSSupport-HighCPU-df52ba5d-8773-4038-a908-b67ecd9c9d11</code> for more information.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS documentación de servicio

- Consulta [Solución de problemas de Amazon OpenSearch Service](#) para obtener más información

EventBridge

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon EventBridge. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-AddOpsItemDedupStringToEventBridgeRule](#)
- [AWS-DisableEventBridgeRule](#)

AWS-AddOpsItemDedupStringToEventBridgeRule

Descripción

El AWS-AddOpsItemDedupStringToEventBridgeRule runbook añade una cadena de deduplicación para todas las AWS Systems Manager OpsItems asociadas a una regla de Amazon EventBridge . Este manual de procedimientos no agrega una cadena de deduplicación si una regla ya tiene una. Para obtener más información sobre las cadenas de deduplicación OpsItems, consulte [Reducir la duplicación OpsItems](#) en la Guía del AWS Systems Manager usuario.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DedupString

Tipo: cadena

Descripción: (obligatorio) la cadena de deduplicación que desea agregar a la regla.

- RuleName

Tipo: cadena

Descripción: (obligatorio) el nombre de la regla a la que desea agregar la cadena de deduplicación.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- events:ListTargetsByRule
- events:PutTargets

Pasos de documentos

- aws:executeScript- Añade una cadena de deduplicación a la EventBridge regla que especifique en el RuleName parámetro.

AWS-DisableEventBridgeRule

Descripción

El *AWS-DisableEventBridgeRule* manual desactiva la EventBridge regla de Amazon que especifiques. Para obtener más información sobre las reglas EventBridge , consulta las reglas de Amazon [EventBridge en la Guía del usuario](#) de Amazon. EventBridge

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- EventBusName

Tipo: cadena

Valor predeterminado: default

Descripción: (opcional) el bus de eventos asociado a la regla que desea deshabilitar.

- RuleName

Tipo: cadena

Descripción: (obligatorio) el nombre de la regla que desea deshabilitar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

Pasos de documentos

- `aws:executeAwsApi`- Desactiva la EventBridge regla que especifique en el parámetro.
`RuleName`

AWS Glue

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Glue Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-TroubleshootGlueConnection](#)

AWSSupport-TroubleshootGlueConnection

Descripción

El AWSSupport-TroubleshootGlueConnectionsmanual ayuda a solucionar problemas AWS Glue de conexión. El destino de la conexión probada debe alcanzarse a través de una conexión JDBC y puede ser un clúster/instancia de Amazon Relational Database Service (Amazon RDS), un clúster de Amazon Redshift o cualquier otro destino al que se pueda acceder a través de JDBC. En los dos primeros casos, se utiliza la herramienta Reachability Analyzer para determinar si se concede la conectividad entre la fuente AWS Glue() y el destino (Amazon RDS o Amazon Redshift).

Si el destino de la conexión no es Amazon RDS ni Amazon Redshift, la conectividad se sigue probando creando AWS Lambda una función en la misma subred que la conexión (un punto de presencia de AWS Glue la red) y comprobando si el nombre del destino se puede resolver y si se puede acceder a él en el puerto de destino.

⚠ Important

Para ejecutar las comprobaciones del [Reachability Analyzer](#), se crearán interfaces de [red elásticas](#) en cada una de las subredes de fuentes de datos de la conexión. Asegúrese de disponer de suficiente espacio libre IPs en esas subredes y de que el consumo de una IP no afecte a su carga de trabajo antes de ejecutar esta automatización.

⚠ Important

Todos los recursos creados por esta automatización están etiquetados para que se puedan encontrar fácilmente. Las etiquetas utilizadas son:

- `AWSSupport-TroubleshootGlueConnection: true`
- `AutomationExecutionId: Amazon EC2 Systems Manager Execution Id`

¿Cómo funciona?

El manual de instrucciones realiza los siguientes pasos:

- Describe la AWS Glue conexión para obtener la información de origen (subred y grupos de seguridad) para las comprobaciones de conectividad.
- Obtiene la información de destino (subred y grupos de seguridad) de la fuente de datos a la que se hace referencia en la URL del JDBC o de los `DatasourceSecurityGroups` parámetros y, si están presentes, `DatasourceSubnets`.
- Si la fuente de datos presente en la URL de JDBC es una instancia o un clúster de Amazon RDS o un clúster de Amazon Redshift, esta automatización se crea ENIs a partir de la información de origen y de destino recopilada en los pasos anteriores y utiliza Reachability Analyzer para realizar una comprobación de conectividad entre ambos.
- Se utiliza una función Lambda (punto de presencia de la red, en el contexto de esta automatización) para realizar comprobaciones de conectividad L4 y resolución de nombres.
- La misma función Lambda se utiliza para realizar las comprobaciones en el punto de conexión Amazon S3.
- El simulador de políticas se utiliza para determinar si la función de IAM utilizada en la conexión tiene los permisos necesarios.

- La automatización comprueba si el grupo de seguridad utilizado por la conexión tiene la configuración esperada.
- Se genera un informe que contiene las posibles causas del error en la operación de prueba de and/or la conexión y las pruebas realizadas con éxito.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `ec2:CreateNetworkInsightsPath`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `ec2>DeleteNetworkInsightsAnalysis`
- `ec2>DeleteNetworkInsightsPath`
- `ec2>DeleteNetworkInterface`
- `ec2:StartNetworkInsightsAnalysis`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`

- `iam:DetachRolePolicy`
- `iam:PutRolePolicy`
- `iam:TagRole`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:TagResource`
- `logs:CreateLogGroup`
- `logs>DeleteLogGroup`
- `logs:PutRetentionPolicy`
- `logs:TagResource`
- `glue:GetConnection`
- `glue:GetDataCatalogEncryptionSettings`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `ec2:DescribeDhcpOptions`
- `ec2:DescribeNetworkInsightsPaths`
- `ec2:DescribeNetworkInsightsAnalyses`
- `ec2:DescribeSecurityGroupRules`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpcAttribute`
- `iam:GetRole`
- `iam>ListAttachedRolePolicies`
- `iam:SimulatePrincipalPolicy`
- `kms:DescribeKey`
- `lambda:InvokeFunction`
- `lambda:GetFunction`
- `s3:GetEncryptionConfiguration`
- `iam:PassRole`

⚠ Important

Además de las acciones mencionadas anteriormente, AutomationAssumeRole deben tener [Amazon VPCReachability AnalyzerFullAccessPolicy](#) como [política gestionada adjunta](#) para que las pruebas del [Reachability Analyzer se realicen correctamente](#).

Este es un ejemplo de una política que podría concederse para: AutomationAssumeRole

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "TaggedAWSResourcesPermissions",
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
      }
    },
    "Action": [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam>DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:TagRole",
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda:TagResource",
      "logs>DeleteLogGroup",
      "logs>CreateLogGroup",
      "logs:PutRetentionPolicy",
      "logs:TagResource",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack"
    ],
    "Resource": "*"
  }],
}
```



```

    {
      "Sid": "TaggedEC2ResourcesPermissions",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
        }
      },
      "Action": [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "*"
    },
    {
      "Sid": "PutRolePolicy",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "iam:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
        }
      },
      "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "InvokeFunction",
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Resource": "arn:*:lambda:*:*:function:point-of-presence-*"
    },
    {
      "Sid": "UnTaggedActions",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",

```

```

        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:StartNetworkInsightsAnalysis",
        "glue:GetConnection",
        "glue:GetDataCatalogEncryptionSettings",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:SimulatePrincipalPolicy",
        "kms:DescribeKey",
        "lambda:GetFunction",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "arn*:iam::*:role/point-of-presence-*",
    "Condition": {
      "StringLikeIfExists": {
        "iam:PassedToService": "lambda.amazonaws.com"
      }
    }
  }
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootGlueConnection](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- TestConnectionRole (Obligatorio)

El nombre de recurso de Amazon (ARN) de la función de IAM que se utiliza durante la prueba de conexión.

- ConnectionName (Obligatorio)

AWS Glue no se pudo comprobar el nombre de la conexión que desea solucionar.

- PersistReachabilityAnalyzerResults(Opcional)

El indicador que informa si los resultados de la ejecución del Reachability Analyzer deben conservarse o no. Valor predeterminado: `false`.

- PointOfPresenceLogRetentionPeriod(Opcional)

La cantidad de días durante los que se almacenarán los registros del punto de presencia Lambda. Predeterminado: 7.

- DatasourceSubnets (Opcional)

Si la fuente de datos original no está disponible, utilice este parámetro para proporcionar las subredes que utilizó, de modo que se sigan realizando las pruebas de conectividad. Debe usarse con. DatasourceSecurityGroups Ejemplo: subnet-1, subnet-2.

- DatasourceSecurityGroups (Opcional)

Si la fuente de datos original no está disponible, utilice este parámetro para proporcionar los grupos de seguridad que utilizó, de modo que se sigan realizando las pruebas de conectividad. Debe usarse con. DatasourceSubnets Ejemplo: sg-1, sg-2.

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.	ConnectionName (Required) The name of the AWS Glue Connection you want to troubleshoot the failed test connection attempt. String
TestConnectionRole (Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that is used during the connection test.	PersistReachabilityAnalyzerResults (Optional) The flag informing if the results of the VPC Reachability Analyzer execution should be kept or not. Default: false. false
PointOfPresenceLogRetentionPeriod (Optional) The amount of days the logs for the point of presence AWS Lambda will be stored for. Default: 7. 7	DatasourceSubnets (Optional) If the original datasource is not available, use this parameter to provide the subnets that it used so that the connectivity tests are still performed. **Must** be used with <code>DatasourceSecurityGroups</code>. Example: subnet-1,subnet-2. StringList
DatasourceSecurityGroups (Optional) If the original datasource is not available, use this parameter to provide the security groups it used so that the connectivity tests are still performed. **Must** be used with <code>DatasourceSubnets</code>. Example: sg-1,sg-2. StringList	

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. El manual de procedimientos de automatización realiza los siguientes pasos:

- ParseInputs:

Este paso valida la combinación de entradas. Si `DatasourceSubnets` se proporcionan ambos `DatasourceSecurityGroups` y, son válidos y se devuelven tal cual. Si no se proporciona ninguna, se devuelven dos listas vacías. Si solo se proporciona una de ellas, el escalón genera una `ValueException`.

- GetConnectionDetails:

Este paso devuelve los detalles de la AWS Glue conexión proporcionada.

- ParseSecurityGroupList:

Este paso se utiliza para concatenar lo que se utilizará `SecurityGroupIdList` en un `String` futuro en esta automatización.

- GetConnectionData:

Determina, en función de la URL del JDBC, qué tipo de conexión entre:, y. `RedShift` `RdsInstance` `RdsCluster` `Other` Además, devuelve el dominio y el puerto utilizados en la conexión JDBC, la Amazon VPC de la conexión y sus servidores de nombres de dominio.

- GetNetworkDetails:

Obtiene la información de la subred y el grupo de seguridad del objetivo de Amazon RDS o Amazon Redshift.

- Crear: ENITemplate

Genera la AWS CloudFormation plantilla utilizada para crear las interfaces de red que se utilizan para probar la conectividad. Esto es necesario para ejecutar la herramienta Reachability Analyzer.

- Crear: ENIStack

Crea la CloudFormation pila a partir de la plantilla creada en el paso anterior.

- GetStackDetails:

Describe la CloudFormation pila creada en la pila anterior y recupera la SourceNetworkInterface TargetNetworkInterfaces información.

- RunSourceToTargetCheck:

Ejecuta comprobaciones entre el origen y el destino ENIs creados en el paso anterior mediante la herramienta Reachability Analyzer.

- Eliminar: ENIStack

Elimina la CloudFormation pila que crea las interfaces de red

- CreateNetworkPointOfPresence:

CloudFormation crea la función Lambda utilizada como punto de presencia de la red.

- GetFunctionName:

Realiza una llamada a la API CloudFormation describe stack para recuperar el nombre de la función Lambda creada en el paso anterior.

- RunEndpointChecks:

Utiliza el punto de presencia de la red para determinar si el punto final presente en la conexión JDBC se puede resolver y se puede acceder a él en el puerto declarado.

- Comprueba la conectividad de 3:

Comprueba la conectividad de red desde la AWS Glue conexión al servicio Amazon S3.

- DeletePointOfPresence:

Elimina la CloudFormation pila que crea el punto de presencia de la red Lambda.

- **Permisos de pruebaIAMRole:**

Comprueba si la función de IAM utilizada para la prueba tiene los permisos necesarios para ejecutarla.

- **CheckConnectionSecurityGroupReferencingRule:**

Comprueba si el grupo de seguridad utilizado en la AWS Glue conexión permite que todo el tráfico de entrada provenga de él mismo. Devolverá una lista de los grupos de seguridad sin esta regla, si la hubiera.

- **GenerateReport:**

Genera un informe que contiene una lista de los resultados (posibles motivos del error en la prueba de conexión) y los pasos a seguir (intentos de resolver el error de la prueba de conexión).

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución:

- **Resultados de la automatización**

En esta sección, encontrará escenarios que describen las posibles causas del fallo de la operación de conexión de prueba (hallazgos) y cómo pueden solucionarse (pasos siguientes). Si la automatización no puede encontrar la causa del fallo de la prueba, también se explicará en esta sección.

- **Pruebas exitosas**

En esta sección, encontrará escenarios que indican lo que esta automatización ha probado satisfactoriamente. Las pruebas realizadas correctamente son útiles en caso de que la automatización no pueda identificar la causa del fallo en la conexión de prueba, ya que reducen el alcance de la investigación al informar sobre lo que no contribuye al problema.

- **Errores de automatización**

En esta sección, encontrará escenarios que describen los problemas que se produjeron durante la automatización y que pueden haber limitado el número de pruebas que la automatización podía realizar. La descripción del escenario indicará qué paso falló.

```

TroubleshootGlueConnection
-----
Automation Results
Below are possible causes for the issue being troubleshoot and their fixes.
-----

# Scenario: AWS Glue connection's VPC using Amazon Provided DNS
🔍 Findings:
- The JDBC URL's endpoint dummy-instance.c3c3tj8ogvmj.us-east-1.rds.amazonaws.com could not be resolved from the AWS Glue
  connection's subnet subnet-
- Glue connection's VPC (vpc- ) is using AWS DNS Resolver but no issue could be found.
➔ Next steps:
- Please check the following links for further DNS troubleshooting:
- https://repost.aws/knowledge-center/vpc-find-cause-of-failed-dns-queries.
- https://repost.aws/knowledge-center/vpc-peering-troubleshoot-dns-resolution
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-support

# Scenario: Checking AWS Glue connection IAM role trust relationship
🔍 Findings:
- The IAM role arn:aws:iam:: :role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi used for
  the AWS Glue connection test has no trust relationship with the AWS Glue service.
➔ Next steps:
- Please add the AWS Glue service to the arn:aws:iam:: :role/SAW-Core-Test-AWSSupport-Trou-
  IncorrectGlueTestRole-1Lu7FYAp9bfi trust relationship. More details on the following link:
- https://docs.aws.amazon.com/directoryservice/latest/admin-guide/edit_trust.html

# Scenario: Glue test connection role IAM check
🔍 Findings:
- The IAM role (arn:aws:iam:: :role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi) used to
  test the connection is not allowed to perform 'glue:TestConnection'.
➔ Next steps:
- Please add the 'glue:TestConnection' action to the role used for the AWS Glue connection test:
  arn:aws:iam:: :role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-1Lu7FYAp9bfi.

-----
✓ Successful Tests
Below are the successful tests performed by the automation, for further troubleshooting.
-----

# Scenario: Datasource security group
✓ The target's security group(s) allow(s) inbound connections from the Glue connection.

# Scenario: Checking connection security group self referencing rule
✓ The AWS Glue connection has a self referencing inbound rule allowing all traffic.

```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

Amazon FSx

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon FSx. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-ValidateFSxWindowsADConfig](#)

AWSSupport-ValidateFSxWindowsADConfig

Descripción

El `AWSSupport-ValidateFSxWindowsADConfig` runbook se utiliza para validar la configuración autogestionada de Active Directory (AD) de un servidor de archivos de Amazon FSx para Windows

¿Cómo funciona?

El runbook `AWSSupport-ValidateFSxWindowsADConfig` ejecuta el script de validación de Amazon FSx en la instancia temporal de Windows de Amazon Elastic Compute Cloud (Amazon EC2) lanzada por el runbook en la subred de Amazon FSx. El script realiza varias comprobaciones para validar la conectividad de la red con los AD/DNS servidores autogestionados y los permisos de la cuenta de FSx servicio de Amazon. El runbook puede validar un servidor de archivos de Amazon FSx para Windows con errores o mal configurado o crear un nuevo servidor de archivos de Amazon FSx para Windows con AD autogestionado.

De forma predeterminada, el runbook crea la instancia de Windows de Amazon EC2, el grupo de seguridad AWS Systems Manager para el acceso (SSM) AWS Identity and Access Management , la función (IAM) y la política que se utilizan en CloudFormation la subred de Amazon FSx. Si desea ejecutar el script en una instancia Amazon EC2 existente, proporcione el ID en el parámetro. `InstanceId` Si se ejecuta correctamente, elimina los CloudFormation recursos. Sin embargo, para conservar los recursos, defina `true` el `RetainCloudFormationStack` parámetro en.

La CloudFormation plantilla crea un rol de IAM en su nombre con los permisos necesarios para adjuntarlo a la instancia de Amazon EC2 y ejecutar el script de validación de FSx Amazon. Para especificar un perfil de instancia de IAM existente para la instancia temporal, utilice el parámetro. `InstanceProfileName` La función de IAM asociada debe contener los siguientes permisos:

- `ec2:DescribeSubnets` y `ec2:DescribeVpcs` permisos y la Política de gestión de `AmazonAmazonSSMManagedInstanceCore`.
- Permisos para obtener el nombre de usuario y la contraseña de la cuenta de FSx servicio de Amazon desde Systems Manager mediante una llamada a la `GetSecretValue` API.
- Permisos para colocar el objeto en el bucket de Amazon Simple Storage Service (Amazon S3) para la salida del script.

Requisitos previos

La subred en la que se crea la instancia temporal de Amazon EC2 (o la instancia existente proporcionada en InstanceId el parámetro) debe permitir el acceso a AWS Systems Manager los puntos de enlace AWS Secrets Manager, y Amazon S3 para poder ejecutar AmazonFSxADValidation el script mediante SSM Run Command.

AWS Secrets Manager configurar

El script de validación se conecta al dominio de Microsoft AD recuperando el nombre de usuario y la contraseña de la cuenta de FSx servicio de Amazon con una llamada en tiempo de ejecución a Secrets Manager. Sigue los pasos de [Crear un AWS Secrets Manager secreto](#) para crear un nuevo secreto de Secrets Manager. Asegúrese de que el nombre de usuario y la contraseña estén key/value guardados en el mismo formato{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}". Consulte [Autenticación y control de acceso AWS Secrets Manager para](#) obtener información sobre cómo proteger el acceso a los secretos.

Para obtener más información sobre la herramienta, consulta los README.md archivos TROUBLESHOOTING.md y del FSx ADValidation archivo de [Amazon](#).

Ejecución del manual

Ejecuta el runbook con los parámetros de Amazon FSx ID o AD. El siguiente es el flujo de trabajo del runbook:

- Obtiene los parámetros del Amazon FSx ID o utiliza los parámetros de entrada de AD.
- Crea la instancia Amazon EC2 de Windows de validación temporal en la FSx subred de Amazon, el grupo de seguridad para el acceso SSM, el rol de IAM y el uso de políticas (condicionales). CloudFormation Si se especifica el InstanceId parámetro, se utiliza.
- Descarga y ejecuta el script de validación en la instancia Amazon EC2 de destino de la subred principal de FSx Amazon.
- Proporciona el código del resultado de la validación de AD en el resultado de la automatización. Además, el resultado completo del script se carga en el bucket de Amazon S3.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackResources`
- `cloudformation:DescribeStackEvents`
- `ec2:CreateTags`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `ec2:CreateLaunchTemplate`
- `ec2>DeleteLaunchTemplate`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeLaunchTemplateVersions`
- `ec2:CreateSecurityGroup`
- `ec2>DeleteSecurityGroup`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupEgress`

- iam:CreateRole
- iam:CreateInstanceProfile
- iam:GetInstanceProfile
- iam:getRolePolicy
- iam>DeleteRole
- iam>DeleteInstanceProfile
- iam:AddRoleToInstanceProfile
- iam:RemoveRoleFromInstanceProfile
- iam:AttachRolePolicy
- iam:DetachRolePolicy
- iam:PutRolePolicy
- iam>DeleteRolePolicy
- iam:GetRole
- iam:PassRole
- ssm:SendCommand
- ssm:StartAutomationExecution
- ssm:DescribeInstanceInformation
- ssm:DescribeAutomationExecutions
- ssm:GetDocument
- ssm:GetAutomationExecution
- ssm:DescribeAutomationStepExecutions
- ssm:ListCommandInvocations
- ssm:GetParameters
- ssm:ListCommands
- ssm:GetCommandInvocation
- fsx:DescribeFileSystems
- ds:DescribeDirectories
- s3:GetEncryptionConfiguration
- s3:GetBucketPublicAccessBlock
- s3:GetAccountPublicAccessBlock

- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:GetBucketLocation

Ejemplo de política de IAM para el rol Automation Assume

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribe",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudFormation",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack"
      ],
    },
```

```

        "Resource": "arn::cloudformation:::stack/
AWSsupport-ValidateFSxWindowsADConfig-*"
    },
    {
        "Sid": "AllowCreateLaunchTemplate",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateLaunchTemplate",
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:::launch-template/*"
        ]
    },
    {
        "Sid": "AllowEC2RunInstances",
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances",
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:::image/*",
            "arn:aws:ec2:::snapshot/*",
            "arn:aws:ec2:::subnet/*",
            "arn:aws:ec2:::network-interface/*",
            "arn:aws:ec2:::security-group/*",
            "arn:aws:ec2:::key-pair/*",
            "arn:aws:ec2:::launch-template/*"
        ]
    },
    {
        "Sid": "AllowEC2RunInstancesWithTags",
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances",
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:::instance/*",
            "arn:aws:ec2:::volume/*"
        ]
    },
    {

```

```

        "Sid": "EC2SecurityGroup",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateSecurityGroup",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:*:ec2:*:*:security-group/*",
            "arn:*:ec2:*:*:vpc/*"
        ]
    },
    {
        "Sid": "EC2Remove",
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances",
            "ec2>DeleteLaunchTemplate",
            "ec2>DeleteSecurityGroup"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ec2:*:*:launch-template/*",
            "arn:*:ec2:*:*:security-group/*"
        ]
    },
    {
        "Sid": "IAMInstanceProfile",
        "Effect": "Allow",
        "Action": [
            "iam:CreateInstanceProfile",
            "iam>DeleteInstanceProfile",
            "iam:GetInstanceProfile",
            "iam:AddRoleToInstanceProfile",
            "iam:RemoveRoleFromInstanceProfile"
        ],
        "Resource": "arn:*:iam:*:*:instance-profile/*"
    },
    {
        "Sid": "IAM",
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",

```

```

        "iam:DeleteRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:getRolePolicy",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:GetRole",
        "iam:TagRole"
    ],
    "Resource": "arn*:iam::*:role/*"
},
{
    "Sid": "SSM",
    "Effect": "Allow",
    "Action": [
        "ssm:StartAutomationExecution",
        "ssm:GetDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:GetCommandInvocation"
    ],
    "Resource": "*"
},
{
    "Sid": "SSMSendCommand",
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": "arn:aws:ssm::*:document/AWS-RunPowerShellScript"
},
{
    "Sid": "SSMSendCommandOnlyFsxInstance",
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": [
        "arn:aws:ec2::*:instance/*"
    ],
    "Condition": {

```

```

        "StringLike": {
            "ssm:resourceTag/CreatedBy": [
                "AWSSupport-ValidateFSxWindowsADConfig"
            ]
        }
    },
    {
        "Sid": "AllowPassRoleToEC2",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:*:iam:*:role/AWSSupport-ValidateFSxWindowsADConfig-*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:GetEncryptionConfiguration",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
        ],
        "Resource": "*"
    }
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-ValidateFSxWindowsADConfig](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para validar el AD autogestionado con un Amazon existente con errores o mal configurado FSx, introduce los siguientes parámetros:

- AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- FSxID (condicional):

El ID del servidor de archivos de Amazon FSx para Windows. Esto es necesario para validar un Amazon FSx existente con errores o mal configurado.

- SecretArn (Obligatorio):

El ARN del secreto de Secrets Manager que contiene el nombre de usuario y la contraseña de la cuenta FSx de servicio de Amazon. Asegúrese de que el nombre de usuario y la contraseña se almacenen con un key/value par en el formato `{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}`. La CloudFormation pila crea la instancia de validación con permisos para `GetSecretValue` realizar este ARN.

- FSxSecurityGroupId (Obligatorio):

El ID del grupo de seguridad del servidor de archivos de Amazon FSx para Windows.

- BucketName (Obligatorio):

El bucket de Amazon S3 en el que cargar los resultados de la validación. Asegúrese de que el depósito esté configurado con el cifrado del lado del servidor (SSE) y de que la política del depósito no conceda read/write permisos innecesarios a las partes que no necesitan acceder a los registros. Asegúrese también de que la instancia Amazon EC2 para Windows tenga el acceso necesario al bucket de Amazon S3.

Input parameters**InstanceId**

(Optional) The ID of an existing AWS Systems Manager managed Windows Server Amazon EC2 instance where you intend to run the validation script. The instance requires the [AWS Tools for PowerShell](https://docs.aws.amazon.com/powershell/) to be installed. ****Caution**:** The script will temporarily modify the DNS configuration of the instance, which may result in loss of network connectivity. To avoid disruptions, ****do not use a production instance****. Ensure the selected instance is designated for testing purposes only. Please ensure that access to the contents of the instance's volume is not exposed to parties that do not need to access the logs.

☐ Show interactive instance picker

`AWS::EC2::Instance::Id`

AutomationAssumeRole

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

`fsx-test`

BucketName

(Required) The Amazon S3 bucket to upload the validation results to. Please make sure the bucket is configured with server-side encryption (SSE), and the bucket policy does not grant unnecessary read/write permissions to parties that do not need to access the logs. Also please make sure EC2 Windows instance has necessary access to the S3 Bucket.

`test-for-customer`

RetainCloudFormationStack

(Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

`false`

SecretArn

(Required) The ARN of your AWS Secrets Manager secret containing the FSx service account username and password. Make sure that the username and password are stored using a key/value pair in the format `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`.

`arn:aws:secretsmanager:us-west-2:123456789012:secret:fsx-test`

FSxSecurityGroupId

(Required) The security group ID of the Amazon FSx for Windows File Server.

`sg-examplesg1234`

FSxId

(Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.

`fs-abcdef123456789`

4. Para validar la configuración de AD autogestionada para una nueva FSx creación de Amazon, introduce los siguientes parámetros:

- AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- SecretArn (Obligatorio):

El ARN del secreto de Secrets Manager que contiene el nombre de usuario y la contraseña de la cuenta FSx de servicio de Amazon. Asegúrese de que el nombre de usuario y la contraseña se almacenen con un key/value par en el formato `{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}`. La CloudFormation pila crea la instancia de validación con permisos para `GetSecretValue` realizar este ARN.

- FSxSecurityGroupId (Obligatorio):

El ID del grupo de seguridad del servidor de archivos de Amazon FSx para Windows.

- BucketName (Obligatorio):

El bucket de Amazon S3 en el que cargar los resultados de la validación. Asegúrese de que el depósito esté configurado con el cifrado del lado del servidor (SSE) y de que la política del

depósito no conceda read/write permisos innecesarios a las partes que no necesitan acceder a los registros. Asegúrese también de que la instancia Amazon EC2 para Windows tenga el acceso necesario al bucket de Amazon S3.

- **FSxPreferredSubnetId(Condicional):**

La subred preferida de Amazon FSx for Windows File Server.

- **DomainName (Condicional):**

El nombre de dominio completo de tu dominio autogestionado de Microsoft AD.

- **DnsIpAddresses (Condicional):**

Una lista de hasta dos direcciones IP de servidor DNS o controlador de dominio en tu dominio AD autogestionado. Para un máximo de dos IPs, introdúzcalas separadas por una coma.

- **FSxAdminsGroup (Condicional):**

El grupo de administradores de sistemas de archivos delegados de Amazon FSx para Windows File Server. De forma predeterminada, este es Domain Admins.

- **FSxOrganizationalUnit(Condicional):**

La unidad organizativa (OU) a la que desea unir su sistema de archivos. Proporcione el nombre de la ruta distinguida de la OU. Ejemplo: OU=org,DC=example,DC=com.

RetainCloudFormationStack

(Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

false

TestServiceAccountPermissions

(Optional) Enable service account permission validation. This validation will create test Active Directory computer objects in the Microsoft Active Directory Organizational Unit. The resources are cleaned up by the script unless delete permissions are not properly configured on the provided service account in which case manual cleanup may be necessary.

true

DnsIpAddresses

(Conditional) A list of up to two DNS server or domain controller IP addresses in your self-managed AD domain. Required if the `FSxId` parameter is not specified. For up to two IPs, enter them separated by a comma.

10.0.1.10

FSxSecondarySubnetId

(Conditional) The Amazon FSx for Windows File Server secondary subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Optional if the `FSxId` parameter is not specified.

String

FSxOrganizationalUnit

(Conditional) The Organizational Unit (OU) within which you want to join your file system. Provide the distinguished path name of the OU. Example: `OU=org,DC=example,DC=com`. Optional if the `FSxId` parameter is not specified.

OU=testou,DC=example,DC=com

FSxId

(Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.

String

DomainName

(Conditional) The fully qualified domain name of your self-managed Microsoft Active Directory domain. Required if the `FSxId` parameter is not specified.

example.com

FSxPreferredSubnetId

(Conditional) The Amazon FSx for Windows File Server preferred subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Required if the `FSxId` parameter is not specified.

subnet-test1234example

FSxAdminsGroup

(Conditional) The Amazon FSx for Windows File Server delegated file system administrators group. Optional if the `FSxId` parameter is not specified. By default, this is `Domain Admins`.

Domain Admins

InstanceKeyPairName

(Conditional) An existing Amazon EC2 key pair you want to associate to the temporary Amazon EC2 instance. Optional when the `InstanceId` parameter is not specified.

String

5. Seleccione Ejecutar.

6. Se inicia la automatización.

7. Este documento realiza los siguientes pasos:

- `CheckBucketPublicStatus(AWS:ExecuteScript)`:

Comprueba si el bucket de Amazon S3 de destino puede conceder acceso público de lectura y and/or escritura a sus objetos.

- `BranchOnInputParameters(aws:branch)`:

Se basa en los parámetros de entrada proporcionados, como el Amazon FSx ID o FSx los parámetros de Amazon.

- `AssertFileSystemTypelsWindows(leyes: assertAwsResource Propiedad)`:

Si se proporciona el Amazon FSx ID, valida que el tipo de sistema de archivos sea Amazon FSx for Windows File Server.

- `GetValidationInputs(AWS:ExecuteScript)`:

Devuelve la configuración autogestionada de Microsoft AD requerida por la CloudFormation plantilla para crear la instancia de Amazon EC2.

- `BranchOnInstanceId (aws:branch)`:

Se ramifica en la entrada proporcionada. `InstanceId` Si `InstanceId` se proporciona, el script de validación se ejecuta en la instancia Amazon EC2 de destino desde la automatización.
`step:RunValidationScript`

- `Crear EC2 InstanceStack (aws:CreateStack)`:

Crea la instancia de Amazon EC2 en la subred preferida utilizando el CloudFormation lugar donde se ejecutará la `AmazonFSxADValidation` herramienta

- `DescribeStackResources(aws:): executeAwsApi`

Describe la CloudFormation pila para obtener el ID de instancia temporal de Amazon EC2.

- `WaitForEC2InstanceToBeManaged(aws: waitForAwsResourceProperty)`:

Espera a que Systems Manager administre la instancia de Amazon EC2 para ejecutar el script de validación mediante SSM Run Command.

- `GetAmazonFSxADValidationAdjunto (aws): executeAwsApi`

Obtiene la URL de la AmazonFSxADValidation herramienta de los archivos adjuntos del runbook.

- RunValidationScript(AWS: comando RUN):

Ejecuta la AmazonFSxADValidation herramienta en la instancia temporal de Amazon EC2 y almacena el resultado en el bucket de Amazon S3 especificado en el BucketName parámetro.

- DescribeErrorsFromStackEvents(AWS:ExecuteScript):

Describe los eventos de la CloudFormation pila si los runbooks no logran crear la pila.

- BranchOnRetainCloudFormationStack(aws:branch):

Ramifica los InstanceId parámetros RetainCloudFormationStack y para determinar si se debe CloudFormation eliminar la pila.

- DeleteCloudFormationStack(AWS: DeleteStack):

Elimina la pila CloudFormation .

8. Una vez finalizada, revise la sección de resultados para ver los resultados de la ejecución:

```

▼ Outputs

DescribeInstanceAndSubnet.InstanceId
i-06: [REDACTED]

CreateEC2InstanceStack.CloudFormationStackId
arn:aws:cloudformation:us-east-1:3[REDACTED]:stack/AWSSupport-ValidateFSxWindowsADConfig-3428bd96-f8ca-4c8d-9b02-57d81560bac8/67c23cc0-3585-11ef-868f-0efb7b77b54b

RunValidationScript.Output
AmazonFSxADValidation tool downloaded and extracted successfully.
RSAT-AD-PowerShell installed successfully.

Running Test-FSxADConfiguration with parameters:
DomainDNSRoot: self.msfc.com
DnsIPAddresses: 10.10.1.191
SubnetIds: subnet-0[REDACTED]
TestServiceAccountPermissions: True
TranscriptDirectory: C:\ProgramData\Amazon\AmazonFSxADValidation\3428bd96-f8ca-4c8d-9b02-57d81560bac8
AdminGroup: Domain Admins
OrganizationalUnit:

=====
The validation details and logs can be found in the bucket test-for-customer.

ERRORS: 1
- InvalidCredentials

WARNINGS: 0

For detailed information about a given warning or error, see C:\ProgramData\Amazon\AmazonFSxADValidation\AmazonFSxADValidation\TROUBLESHOOTING.md.

=====
The local DNS configuration has been reset successfully.

```

El runbook cargará los resultados de la ejecución del script de validación en el bucket de Amazon S3.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS documentación de servicio

- [¿Qué es Amazon FSx para Windows File Server?](#)
- [Validación de la configuración de AD autogestionada FSx para Amazon para Windows File Server](#)

GuardDuty

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon GuardDuty. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-CreateGuardDutyDetector](#)

AWSConfigRemediation-CreateGuardDutyDetector

Descripción

El AWSConfigRemediation-CreateGuardDutyDetector manual crea un detector Amazon GuardDuty (GuardDuty) en el Región de AWS lugar donde se ejecuta la automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- guardduty:CreateDetector
- guardduty:GetDetector

Pasos de documentos

- aws:executeAwsApi- Crea un GuardDuty detector.
- aws:assertAwsResourceProperty: verifica que el Status del detector sea ENABLED.

IAM

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Identity and Access Management Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-TroubleshootIAMAccessDeniedEvents](#)
- [AWS-AttachIAMToInstance](#)
- [AWS-DeleteIAMInlinePolicy](#)
- [AWSConfigRemediation-DeleteIAMRole](#)
- [AWSConfigRemediation-DeleteIAMUser](#)
- [AWSConfigRemediation-DeleteUnusedIAMGroup](#)
- [AWSConfigRemediation-DeleteUnusedIAMPolicy](#)
- [AWSConfigRemediation-DetachIAMPolicy](#)
- [AWSConfigRemediation-EnableAccountAccessAnalyzer](#)
- [AWSSupport-GrantPermissionsToIAMUser](#)
- [AWSConfigRemediation-RemoveUserPolicies](#)
- [AWSConfigRemediation-ReplaceIAMInlinePolicy](#)
- [AWSConfigRemediation-RevokeUnusedIAMUserCredentials](#)
- [AWSConfigRemediation-SetIAMPasswordPolicy](#)
- [AWSSupport-ContainIAMPrincipal](#)
- [AWSSupport-TroubleshootSAMLIssues](#)

AWSSupport - TroubleshootIAMAccessDeniedEvents

Descripción

El manual de `AWSSupport-TroubleshootIAMAccessDeniedEvents` automatización ayuda a solucionar problemas de acceso AWS Identity and Access Management denegado (IAM). El manual consulta CloudTrail eventos de acceso denegado recientes relacionados con la entidad de IAM y AWS la fuente de eventos de servicio especificadas. Analiza los eventos en un intervalo de tiempo configurable de hasta 24 horas y procesa hasta 10 eventos por ejecución. Cada evento de acceso denegado identificado se examina para ayudar a comprender el contexto de la denegación y las acciones intentadas. La automatización analiza las políticas de IAM basadas en la identidad y en los recursos. En el caso de las políticas basadas en la identidad, examina las políticas integradas y gestionadas asociadas a la entidad de IAM. En el caso de las políticas basadas en recursos, evalúa las políticas de varios servicios, AWS incluidos Amazon Simple Storage Service (Amazon S3), AWS Key Management Service (AWS KMS), AWS Lambda Amazon Simple Notification Service (Amazon SNS), Amazon Elastic Container Registry (Amazon ECR), Amazon API Gateway, Amazon Elastic CodeArtifact File System (Amazon EFS), Amazon Simple Queue Servicio (Amazon Queue SQS),

Amazon Service, Signer y. AWS Cloud9 OpenSearch AWS AWS Serverless Application Repository
AWS Secrets Manager

El manual utiliza las capacidades de simulación de políticas de IAM para evaluar estas políticas frente a las acciones denegadas que se encuentran en los CloudTrail eventos. El manual aprovecha las capacidades de simulación de políticas de la IAM, tanto [SimulatePrincipalPolicy](#) para los usuarios como para las funciones de la IAM, a fin de evaluar estas políticas comparándolas con las acciones denegadas detectadas en los eventos. [SimulateCustomPolicy](#) CloudTrail La automatización genera un informe que ayuda a identificar las acciones específicas que se denegaron, diferenciando entre denegaciones implícitas y explícitas, enumerando las políticas responsables de las denegaciones de acceso y proporcionando explicaciones para cada denegación. El informe también sugiere posibles soluciones, como identificar las declaraciones de autorización que faltan o las declaraciones de denegación contradictorias

¿Cómo funciona?

El manual lleva a cabo los siguientes pasos:

- Describe y valida `RequesterARN` (rol o usuario) para obtener información como el tipo de entidad de IAM y el ID de IAM.
- Obtiene los CloudTrail eventos asociados a `RequesterARN`, y si se proporcionan `EventSource.ResourceARN`
- Analiza los CloudTrail eventos para obtener la acción que se llevó a cabo cuando se devolvió el error de acceso denegado y, a continuación, examina todas las políticas de IAM, como las políticas integradas y gestionadas asociadas a la entidad de IAM, así como las políticas basadas en los recursos. A continuación, simula estas políticas comparándolas con las acciones detectadas en los errores de acceso denegado de los CloudTrail eventos en cuestión para determinar la causa del error.
- Genera un informe en el que se determina el tipo de error de acceso denegado, las políticas responsables de los errores y se ofrecen sugerencias para una posible solución al error.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `apigateway:GetRestApis`
- `cloudtrail:LookupEvents`
- `cloud9:GetEnvironment`
- `codeartifact:GetRepositoryPermissionsPolicy`
- `ecr:GetRepositoryPolicy`
- `elasticfilesystem:GetFileSystemPolicy`
- `es:DescribeDomain`
- `iam:GetPolicy`
- `iam:GetPolicyVersion`
- `iam:GetRole`
- `iam:GetRolePolicy`
- `iam:GetUser`
- `iam:GetUserPolicy`
- `iam:ListAttachedRolePolicies`
- `iam:ListAttachedUserPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`
- `iam:SimulatePrincipalPolicy`
- `iam:SimulateCustomPolicy`
- `kms:GetKeyPolicy`
- `lambda:GetPolicy`
- `secretsmanager:GetResourcePolicy`
- `serverlessrepo:GetApplication`

- signer:GetSigningProfile
- sns:GetTopicAttributes
- ssm:StartAutomationExecution
- ssm:StopAutomationExecution
- sqs:GetQueueAttributes
- s3:GetBucketPolicy

Ejemplo de política:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:GetUser",
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "iam:ListUserPolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetUserPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedUserPolicies",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "cloudtrail:LookupEvents",
        "iam:SimulateCustomPolicy"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetBucketPolicy",
        "kms:GetKeyPolicy",
```

```

        "lambda:GetPolicy",
        "sns:GetTopicAttributes",
        "ecr:GetRepositoryPolicy",
        "apigateway:GET",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "sqs:GetQueueAttributes",
        "cloud9:DescribeEnvironmentStatus",
        "es:DescribeDomain",
        "signer:GetSigningProfile",
        "serverlessrepo:GetApplication",
        "secretsmanager:GetResourcePolicy"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSsupport-TroubleshootIAMAccessDeniedEvents](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a SSM Automation realizar las acciones en su nombre. El rol debe añadirse a la entrada de acceso al clúster de Amazon EKS o al permiso RBAC para permitir las llamadas a la API de Kubernetes.
 - Tipo: `AWS::IAM::Role::Arn`
 - ARN de solicitud (obligatorio):
 - Descripción: (obligatorio) El ARN del usuario o rol de IAM para el que desea investigar los permisos de acceso a un recurso específico. AWS
 - Tipo: `String`

- Patrón de permisos: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`
- ResourceArn (opcional):
 - Descripción: (opcional) Se evalúa el ARN del recurso para AWS el que se ha denegado el acceso. El recurso de AWS destino debe estar en la misma región en la que se ejecuta el manual de automatización.
 - Tipo: String
 - Permitir patrón: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:([a-zA-Z0-9\\-]{1,63}):([a-z0-9\\-]{0,63})?:([\\d]{12})?:([a-zA-Z0-9\\-_/:.]{1,1024})$`
- EventSource (Obligatorio):
 - Descripción: (obligatorio) El punto de enlace de la API de Amazon en el que se originó el CloudTrail evento. Por ejemplo: `s3.amazonaws.com`.
 - Tipo: String
 - Patrón de permisos: `^([a-zA-Z0-9.-]+)\\.amazonaws\\.com$`
- EventName (Opcional):
 - Descripción: (opcional) El nombre de la acción de la API de Amazon asociado al CloudTrail evento. Por ejemplo: `s3:CreateBucket`.
 - Tipo: String
 - Patrón de permisos: `^$|^([a-z0-9]+:[A-Za-z0-9])+$`
- LookBackHours (Opcional):
 - Descripción: (opcional) El número de horas para revisar los CloudTrail eventos al Access Denied buscarlos. Intervalo válido: de 12 a 248 horas.
 - Tipo: entero
 - Patrón de permiso: `^([1-9]|1[0-9]|2[0-4])$`
 - Predeterminado: 12
- MaxEvents (Opcional):
 - Descripción: (opcional) El número máximo de CloudTrail Access Denied eventos que se devuelve al buscar eventos. Rango válido: 1 hasta 5 eventos.
 - Tipo: entero
 - Patrón de permiso: `^([1-9]|1[0-9]|2[0-4])$`
 - Predeterminado: 3

- `UseContextEntries` (Opcional):
 - Descripción: (opcional) Si lo especifica `true`, la automatización extrae los detalles sobre el contexto de la solicitud de API del CloudTrail evento y los incluye en la simulación de políticas de IAM.
 - Tipo: Booleano
 - Patrón de permisos: `^( [1-9] | 1[0-9] | 2[0-4] )$`
 - Predeterminado: 3

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `ValidateRequesterArn`

Valida y deconstruye el `RequesterArn` ARN, recuperando información sobre el usuario o rol de IAM objetivo.

- `GetCloudTrailEventsWithAccessDeniedError`

Consulta los CloudTrail eventos en busca de `Access Denied` eventos recientes relacionados con la entidad y el servicio de IAM especificados. `AWS EventSource`

- `Evalúe las políticas IAMRequester`

Evalúa los permisos de IAM de la entidad de IAM solicitante comparándolos con las acciones de los eventos. CloudTrail Esta evaluación incluye el análisis de las políticas basadas en la identidad y en los recursos asociadas al solicitante. La automatización utiliza las capacidades de simulación de políticas de IAM para evaluar estas políticas en el contexto de las acciones denegadas identificadas en los eventos. CloudTrail

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución:

- `PermissionEvaluationResults`

Genera un informe que ayuda a identificar las acciones específicas que se denegaron, diferenciando entre denegaciones implícitas y explícitas. También enumera las políticas responsables de las denegaciones de acceso y proporciona explicaciones para cada denegación. El informe también sugiere posibles soluciones, como identificar las declaraciones de autorización que faltan o las declaraciones de denegación contradictorias

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS-AttachIAMToInstance

Descripción

Adjunta un rol AWS Identity and Access Management (de IAM) a una instancia gestionada.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ForceReplace

Tipo: Booleano

Descripción: (opcional) marcar para especificar si reemplazar el perfil de existente o no.

Predeterminado: true

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia en la que desea asignar un rol de IAM.

- RoleName

Tipo: cadena

Descripción: (obligatorio) el nombre del rol de IAM que se va a añadir a la instancia administrada.

Pasos de documentos

1. `aws:executeAwsApi- DescribeInstanceProfile` - Busque el perfil de instancia de IAM adjunto a la instancia EC2.
2. `aws:branch- CheckInstanceProfileAssociations` - Compruebe el perfil de la instancia de IAM adjunto a la instancia EC2.
 - a. Si un perfil de instancia de IAM se encuentra adjunto y `ForceReplace` está establecido en `true`:
 - i. `aws:executeAwsApi- DisassociateIAMInstanceProfile` - Desasocie el perfil de instancia de IAM de la instancia EC2.
 - b. `aws:executeAwsApi- ListInstanceProfilesForRole` - Enumere los perfiles de instancia para la función de IAM proporcionada.
 - c. `aws:branch- CheckInstanceProfileCreated` - Compruebe si el rol de IAM proporcionado tiene un perfil de instancia asociado.
 - i. Si el rol de IAM tiene un perfil de instancia asociado:
 - A. `aws:executeAwsApi- attachIAMProfileToInstance` : asocie el rol de perfil de instancia de IAM a la instancia EC2.
 - i. Si el rol de IAM no tiene un perfil de instancia asociado:
 - A. `aws:executeAwsApi- CreateInstanceProfileForRole` - Cree un rol de perfil de instancia para el rol de IAM especificado.

- B. `aws:executeAwsApi- AddRoleToInstanceProfile` - Adjunte el rol del perfil de instancia al rol de IAM especificado.
- C. `aws:executeAwsApi- GetInstanceProfile` - Obtenga los datos del perfil de la instancia para el rol de IAM especificado.
- D. `aws:executeAwsApi- attachIAMProfileToInstanceWithRetry` : asocie el rol de perfil de instancia de IAM a la instancia EC2.

Salidas

Adjuntar. IAMProfile ToInstanceWithRetry AssociationId

GetInstanceProfile.InstanceProfileName

GetInstanceProfile.InstanceProfileArn

Adjuntar IAMProfileToInstance. AssociationId

ListInstanceProfilesForRole.InstanceProfileName

ListInstanceProfilesForRole.InstanceProfileArn

AWS-DeleteIAMInlinePolicy

Descripción

El AWS-DeleteIAMInlinePolicy manual elimina todas las políticas integradas AWS Identity and Access Management (IAM) asociadas a las identidades de IAM que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- **AutomationAssumeRole**

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **IamArns**

Tipo: cadena

Descripción: (Obligatorio) Una lista separada por comas de las identidades de IAM ARNs de las que desea eliminar las políticas integradas. Esta lista puede incluir usuarios, grupos o roles de IAM.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

Pasos de documentos

- `aws:executeScript`- Elimina las políticas integradas de IAM asociadas a las identidades de IAM de destino.

AWSConfigRemediation-DeleteIAMRole

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteIAMRole` elimina el rol de AWS Identity and Access Management (IAM) que especifique. Esta automatización no elimina los perfiles de instancia asociados al rol de IAM ni los roles vinculados al servicio.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `IAMRoleID`

Tipo: cadena

Descripción: (obligatorio) el ID del rol de IAM que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfilesForRole`
- `iam:ListRolePolicies`
- `iam:ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

Pasos de documentos

- `aws:executeScript`: recopila el nombre del rol de IAM que especifique en el parámetro `IAMRoleID`.
- `aws:executeScript`: recopila las políticas y los perfiles de instancia asociados al rol de IAM.
- `aws:executeScript`: elimina las políticas adjuntas.
- `aws:executeScript`: elimina el rol de IAM y verifica que el rol se haya eliminado.

AWSConfigRemediation-DeleteIAMUser

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteIAMUser` elimina el usuario de AWS Identity and Access Management (IAM) que especifique. Esta automatización elimina o separa los siguientes recursos asociados al usuario de IAM:

- Claves de acceso
- Políticas administradas asociadas
- Credenciales de Git
- Membresías a grupos de IAM
- Contraseña de usuario de IAM
- Políticas insertadas
- Uso de dispositivos de autenticación multifactor (MFA)
- Firma de certificados

- Clave SSH pública

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- IAMUserID

Tipo: cadena

Descripción: (obligatorio) el ID del usuario de IAM que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Pasos de documentos

- `aws:executeScript`: recopila el nombre de usuario del usuario de IAM que especifique en el parámetro `IAMUserId`.
- `aws:executeScript`: recopila las claves de acceso, los certificados, las credenciales, los dispositivos MFA y las claves SSH asociadas al usuario de IAM.
- `aws:executeScript`: recopila las membresías a grupos y las políticas del usuario de IAM.
- `aws:executeScript`: elimina las claves de acceso, los certificados, las credenciales, los dispositivos MFA y las claves SSH asociadas al usuario de IAM.
- `aws:executeScript`: elimina las membresías a grupos y las políticas del usuario de IAM.
- `aws:executeScript`: elimina el usuario de IAM y verifica que el usuario se haya eliminado.

AWSConfigRemediation-DeleteUnusedIAMGroup

Descripción

El manual de procedimientos AWSConfigRemediation-DeleteUnusedIAMGroup elimina un grupo de IAM que no contenga ningún usuario.

El manual de procedimientos AWSConfigRemediation-DeleteUnusedIAMGroup elimina un grupo de IAM que no contenga ningún usuario.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- GroupName

Tipo: cadena

Descripción: (obligatorio) el nombre del grupo de IAM que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam>DeleteGroup`
- `iam>DeleteGroupPolicy`
- `iam:DetachGroupPolicy`

Pasos de documentos

- `aws:executeScript`: elimina las políticas de IAM gestionadas e insertadas asociadas al grupo de IAM de destino y, a continuación, elimina el grupo de IAM.

AWSConfigRemediation-DeleteUnusedIAMPolicy

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedIAMPolicy` elimina una política (de IAM) AWS Identity and Access Management que no está asociada a ningún usuario, grupo o función.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- IAMResourceId

Tipo: cadena

Descripción: (obligatorio) el identificador de recurso de la política de IAM que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam>DeletePolicy
- iam>DeletePolicyVersion
- iam:GetPolicy
- iam:ListEntitiesForPolicy
- iam:ListPolicyVersions

Pasos de documentos

- aws:executeScript: elimina la política que especifique en el parámetro IAMResourceId y verifica que se haya eliminado.

AWSConfigRemediation-DetachIAMPolicy

Descripción

El manual de procedimientos AWSConfigRemediation-DetachIAMPolicy desvincula la política (de IAM) AWS Identity and Access Management que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- IAMResourceID

Tipo: cadena

Descripción: (obligatorio) el ID de la política de IAM que desea separar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DetachGroupPolicy
- iam:DetachRolePolicy

- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`

Pasos de documentos

- `aws:executeScript`: separa la política de IAM de todos los recursos.

AWSConfigRemediation-EnableAccountAccessAnalyzer

Descripción

El `AWSConfigRemediation-EnableAccountAccessAnalyzer` manual crea un analizador de acceso AWS Identity and Access Management (IAM) en su. Cuenta de AWS Para obtener información acerca de Access Analyzer, consulte [Cómo utilizar IAM Access Analyzer de AWS](#) en la Guía del usuario de IAM.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AnalyzerName`

Tipo: cadena

Descripción: (obligatorio) nombre de la analizadora que se va a crear.

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

Pasos de documentos

- `aws:executeAwsApi`: crea un analizador de acceso para su cuenta.
- `aws:waitForAwsResourceProperty`: espera a que el estado del analizador de acceso sea `ACTIVE`.
- `aws:assertAwsResourceProperty`: confirma que el estado del analizador de acceso sea `ACTIVE`.

AWSSupport-GrantPermissionsToIAMUser

Descripción

Este manual de procedimientos concede los permisos especificados a un grupo de IAM (nuevo o existente) y añade el usuario de IAM existente. Las políticas que puede elegir: [Billing](#) o [Support](#). Para habilitar el acceso de facturación para IAM, recuerde activar también el [acceso del usuario de IAM y del usuario federado a las páginas de facturación y administración de costos](#).

Important

Si proporciona un grupo de IAM existente, todos los usuarios actuales de IAM en el grupo de reciben los nuevos permisos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- IAMGroupName

Tipo: cadena

Predeterminado: ExampleSupportAndBillingGroup

Descripción: (obligatorio) puede ser un grupo nuevo o existente. Debe cumplir con [Límites de nombres de entidades de IAM](#).

- IAMUserName

Tipo: cadena

Predeterminado: ExampleUser

Descripción: (obligatorio) debe ser un usuario existente.

- LambdaAssumeRole

Tipo: cadena

Descripción: (opcional) el ARN del rol asumido por Lambda.

- Permisos

Tipo: cadena

Valores válidos: `SupportFullAccess` | `BillingFullAccess` | `SupportAndBillingFullAccess`

Predeterminado: `SupportAndBillingFullAccess`

Descripción: (obligatorio) elija una de estas opciones: `SupportFullAccess` concede acceso completo al centro de soporte | `BillingFullAccess` concede acceso completo al panel de facturación | `SupportAndBillingFullAccess` concede acceso completo tanto al centro de soporte como al panel de facturación. Más información sobre las políticas en Detalles del documento.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Los permisos necesarios dependen de cómo se ejecute `AWSSupport-GrantPermissionsToIAMUser`.

En ejecución como usuario o rol que ha iniciado sesión actualmente

Se recomienda tener asociada la política administrada `AmazonSSMAutomationRole` de Amazon y los siguientes permisos adicionales para poder crear la función de Lambda y el rol de IAM que pasar a Lambda:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:lambda:*:111122223333:function:AWSSupport-*",
    "Effect": "Allow"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:CreateGroup",
      "iam:AddUserToGroup",
      "iam:ListAttachedGroupPolicies",
      "iam:GetGroup",
      "iam:GetUser"
    ],
    "Resource": [
      "arn:aws:iam::*:user/*",
      "arn:aws:iam::*:group/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:AttachGroupPolicy"
    ],
    "Resource": "*",
    "Condition": {
      "ArnEquals": {
        "iam:PolicyArn": [
          "arn:aws:iam::aws:policy/job-function/Billing",
          "arn:aws:iam::aws:policy/AWSSupportAccess"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:ListAccountAliases",
      "iam:GetAccountSummary"
    ],
    "Resource": "*"
  }
]
}

```

Uso AutomationAssumeRole y LambdaAssumeRole

El usuario debe tener los `StartAutomationExecution` permisos `ssm:` en el runbook e `iam: PassRole` en las funciones de IAM transferidas como y. `AutomationAssumeRole` `LambdaAssumeRole` A continuación se incluyen los permisos que necesita cada rol de IAM:

AutomationAssumeRole

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction"
      ],
      "Resource":
"arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
      "Effect": "Allow"
    }
  ]
}
```

LambdaAssumeRole

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateGroup",
        "iam:AddUserToGroup",
        "iam:ListAttachedGroupPolicies",
        "iam:GetGroup",
        "iam:GetUser"
      ],
      "Resource" : [
        "arn:aws:iam:*:user/*",
        "arn:aws:iam:*:group/*"
      ]
    }
  ]
}
```



```

        ]
      },
      {
        "Effect" : "Allow",
        "Action" : [
          "iam:AttachGroupPolicy"
        ],
        "Resource": "*",
        "Condition": {
          "ArnEquals": {
            "iam:PolicyArn": [
              "arn:aws:iam::aws:policy/job-function/Billing",
              "arn:aws:iam::aws:policy/AWSSupportAccess"
            ]
          }
        }
      }
    ],
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "iam:GetAccountSummary"
      ],
      "Resource" : "*"
    }
  ]
}

```

Pasos de documentos

1. `aws:createStack`- Ejecute la CloudFormation plantilla para crear una función Lambda.
2. `aws:invokeLambdaFunction`: para configurar permisos de IAM para Lambda.
3. `aws:deleteStack`- Eliminar CloudFormation plantilla.

Salidas

`configureIAM.Payload`

AWSConfigRemediation-RemoveUserPolicies

Descripción

El manual de procedimientos `AWSConfigRemediation-RemoveUserPolicies` elimina las políticas insertadas de AWS Identity and Access Management (IAM) y separa las políticas gestionadas asociadas al usuario que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `IAMUser- ID`

Tipo: cadena

Descripción: (obligatorio) el ID del usuario del que desea eliminar políticas.

- `PolicyType`

Tipo: cadena

Valores válidos: All | Inline | Managed

Valor predeterminado: All

Descripción: (obligatorio) el tipo de políticas de IAM que desea eliminar del usuario.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam:ListAttachedUserPolicies`
- `iam:ListUserPolicies`
- `iam:ListUsers`

Pasos de documentos

- `aws:executeScript`: elimina y separa las políticas de IAM del usuario que especifique en el parámetro `IAMUserID`.

AWSConfigRemediation-ReplaceIAMInlinePolicy

Descripción

El `AWSConfigRemediation-ReplaceIAMInlinePolicy` manual reemplaza una política en línea AWS Identity and Access Management (IAM) por una política de IAM administrada replicada. En el caso de una política insertada asociada a un usuario, grupo o función, los permisos de la política insertada se clonan en una política de IAM gestionada. La política de IAM gestionada se añade al recurso y la política integrada se elimina. AWS Config debe estar habilitada en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- InlinePolicyName

Tipo: StringList

Descripción: (obligatoria) la política de IAM insertada que desea reemplazar.

- ResourceId

Tipo: cadena

Descripción: (obligatorio) el ID del usuario, grupo o rol de IAM cuya política insertada desea reemplazar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Pasos de documentos

- `aws:executeScript`: sustituya la política de IAM insertada por una política AWS replicada en el recurso que especifique.

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

Descripción

El `AWSConfigRemediation-RevokeUnusedIAMUserCredentials` manual revoca las contraseñas no utilizadas AWS Identity and Access Management (IAM) y las claves de acceso activas. Este manual también desactiva las claves de acceso caducadas y elimina los perfiles de inicio de sesión caducados. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- IAMResourceID

Tipo: cadena

Descripción: (obligatorio) el ID del recurso de IAM del que desea revocar las credenciales no utilizadas.

- MaxCredentialUsageAge

Tipo: cadena

Predeterminado: 90

Descripción: (obligatorio) el número de días en los que se debe haber utilizado la credencial.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:ListDiscoveredResources
- iam>DeleteAccessKey
- iam>DeleteLoginProfile
- iam:GetAccessKeyLastUsed
- iam:GetLoginProfile
- iam:GetUser
- iam:ListAccessKeys
- iam:UpdateAccessKey

Pasos de documentos

- `aws:executeScript`: revoca las credenciales de IAM del usuario especificado en el parámetro `IAMResourceId`. Las claves de acceso caducadas se desactivan y los perfiles de inicio de sesión caducados se eliminan.

Note

Asegúrese de configurar el `MaxCredentialUsageAge` parámetro de esta acción correctiva para que coincida con el `maxAccessKeyAge` parámetro de la AWS Config regla que utiliza para activar esta acción: [access-keys-rotated](#).

AWSConfigRemediation-SetIAMPASSWORDPolicy

Descripción

El manual de procedimientos `AWSConfigRemediation-SetIAMPASSWORDPolicy` establece la política de contraseñas de usuario de AWS Identity and Access Management (IAM) para su Cuenta de AWS.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- AllowUsersToChangePassword

Tipo: Booleano

Predeterminado: false

Descripción: (opcional) Si se establece en true, todos los usuarios de IAM de su cuenta Cuenta de AWS pueden utilizarla Consola de administración de AWS para cambiar sus contraseñas.

- HardExpiry

Tipo: Booleano

Predeterminado: false

Descripción: (opcional) si se establece en true, los usuarios de IAM no pueden restablecer sus contraseñas una vez caducada la contraseña.

- MaxPasswordAge

Tipo: entero

Predeterminado: 0

Descripción: (opcional) el número de días que la contraseña de un usuario de IAM es válida.

- MinimumPasswordLength

Tipo: entero

Valor predeterminado: 6

Descripción: (opcional) el número mínimo de caracteres que puede tener la contraseña de un usuario de IAM.

- PasswordReusePrevention

Tipo: entero

Predeterminado: 0

Descripción: (opcional) el número de contraseñas anteriores que un usuario de IAM no puede reutilizar.

- `RequireLowercaseCharacters`

Tipo: Booleano

Predeterminado: `false`

Descripción: (opcional) si se establece en `true`, la contraseña de un usuario de IAM debe contener una minúscula del alfabeto latino básico ISO (de la a a la z).

- `RequireNumbers`

Tipo: Booleano

Predeterminado: `false`

Descripción: (opcional) si se establece en `true`, la contraseña de un usuario de IAM debe contener un carácter numérico (del 0 al 9).

- `RequireSymbols`

Tipo: Booleano

Predeterminado: `false`

Descripción: (opcional) si se establece en `true`, la contraseña de un usuario de IAM debe contener un carácter que no sea alfanumérico (`! @ # $ % ^ * ( ) _ + - = [ ] { } | ' .`).

- `RequireUppercaseCharacters`

Tipo: Booleano

Predeterminado: `false`

Descripción: (opcional) si se establece en `true`, la contraseña de un usuario de IAM debe contener un carácter en mayúscula del alfabeto latino básico ISO (de la A a la Z).

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

Pasos de documentos

- `aws:executeScript`: establece la política de contraseñas de usuario de IAM en función de los valores que especifique para los parámetros del manual de procedimientos de su Cuenta de AWS.

AWSSupport-ContainIAMPrincipal

Descripción

En caso de que se produzca un incidente de seguridad o se sospeche que un usuario o rol AWS Identity and Access Management (IAM) o un usuario del Centro de Identidad (IDC) están en peligro, es fundamental aislar rápidamente la AWS identidad afectada y, al mismo tiempo, preservar su configuración para su investigación. El `AWSSupport-ContainIAMPrincipal` manual proporciona un enfoque estructurado y reversible para contener las identidades de IAM o IDC comprometidas, lo que bloquea de manera efectiva su acceso a AWS los recursos y evita que la vulnerabilidad se propague.

Este proceso automatizado permite la investigación sin alterar permanentemente la configuración de la identidad, lo que permite restablecer el acceso normal cuando se considere apropiado. El proceso de contención mantiene al usuario o la función dentro de IAM o al usuario dentro de IDC, a la vez que lo aísla eficazmente de todas las actividades de la red. Este aislamiento impide que el recurso de identidad contenido se comunique con los recursos de su Amazon Virtual Private Cloud o acceda a los recursos de Internet. La contención está diseñada para ser reversible, lo que permite restablecer el acceso normal cuando se considere apropiado.

¿Cómo funciona?

El `AWSSupport-ContainIAMPrincipal` manual implementa un proceso de contención integral para los usuarios, las funciones y los usuarios del Centro de Identidad de IAM. Cuando se ejecuta en `Contain` modo, primero valida todos los parámetros de entrada y realiza comprobaciones de seguridad en el bucket de Amazon S3 especificado. A continuación, recopila información detallada sobre el principal de IAM objetivo y aplica las medidas de contención adecuadas en función del

tipo principal. Para los usuarios de IAM, deshabilita las claves de acceso, elimina el acceso a la consola y adjunta una política de denegación. En el caso de las funciones de IAM, incluye una política de denegación que revoca los permisos de las sesiones creadas antes de la contención. Para los usuarios de Identity Center, elimina los conjuntos de permisos y las pertenencias a grupos y aplica una política de denegación. Durante todo el proceso, el runbook hace una copia de seguridad de la configuración original en un bucket de Amazon S3 para su posible restauración. Cuando se ejecuta en Restore modo, intenta revertir el principal a su estado previo a la contención mediante la configuración de la que se ha hecho una copia de seguridad. El manual incluye una DryRun opción para previsualizar los cambios sin necesidad de aplicarlos y proporciona informes exhaustivos sobre las operaciones exitosas y los escenarios de fallo.

 Important

- **Uso de privilegios elevados:** este documento SSM realiza varias operaciones que requieren privilegios elevados, como la modificación de las políticas de identidad de IAM e IDC y la aplicación de configuraciones de cuarentena. Estas acciones podrían provocar una escalada de privilegios o afectar a otras cargas de trabajo que dependen de las identidades objetivo. Debe revisar los permisos otorgados al rol especificado por el `AutomationAssumeRole` parámetro y asegurarse de que son adecuados para el caso de uso previsto. Puede consultar la siguiente AWS documentación para obtener más información sobre los permisos de IAM:
 - [Permisos de Identity and Access Management \(IAM\)](#)
 - [AWS Permisos de automatización de Systems Manager](#)
- **Riesgos de falta de disponibilidad de la carga de trabajo:** este documento de Systems Manager lleva a cabo acciones de aislamiento que podrían provocar la falta de disponibilidad o la interrupción de las cargas de trabajo. Cuando se ejecuta durante un evento de seguridad, restringe el acceso al recurso afectado al revocar los permisos de la AWS API de las identidades de IAM e IDC especificadas, lo que les impide realizar llamadas o realizar acciones a la API. AWS Esto podría afectar a cualquier aplicación o servicio que dependa de estas identidades.
- **Creación de recursos adicionales:** el documento de automatización puede crear recursos adicionales de forma condicional, como un bucket de Amazon Simple Storage Service (Amazon S3) y objetos de Amazon S3 almacenados en él, en función de los parámetros de ejecución. Estos recursos incurrirán en cargos adicionales en función de su AWS uso.
- **Riesgos de restauración:** si el parámetro `Action` está establecido en `Restore`, este documento SSM intenta restaurar la configuración de identidad de IAM o IDC a su estado

original. Sin embargo, existe el riesgo de que el proceso de restauración falle y deje la identidad de IAM o IDC en un estado incoherente. El documento proporciona instrucciones para la restauración manual en caso de que se produzcan estos errores, pero debe estar preparado para gestionar posibles problemas durante el proceso de restauración.

Se recomienda revisar el manual detenidamente, comprender sus posibles impactos y probarlo en un entorno que no sea de producción antes de ejecutarlo en su entorno de producción.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El `AutomationAssumeRole` parámetro requiere los siguientes permisos para utilizar correctamente el manual de ejecución:

- `s3: GetBucketLocation`
- `s3: GetBucket`
- `s3: ListBucket`
- `s3: GetBucketPublicAccessBlocks`
- `s3: GetAccountPublicAccessBlocks`
- `s3: GetBucketPolicyStatus`
- `s3: GetBucketAcl`
- `s3: GetObject`
- `s3: CreateBucket`

- s3: PutObject
- objetivo: GetUser
- objetivo: GetUserPolicy
- objetivo: GetRole
- objetivo: ListUserPolicies
- objetivo: ListAttachedUserPolicies
- objetivo: ListAccessKeys
- objetivo: ListMfaDevices
- objetivo: ListVirtual MFADevices
- objetivo: GetLoginProfile
- objetivo: GetPolicy
- objetivo: GetRolePolicy
- objetivo: ListPolicies
- objetivo: ListAttachedRolePolicies
- objetivo: ListRolePolicies
- objetivo: UpdateAccessKey
- objetivo: CreateAccessKey
- objetivo: DeleteLoginProfile
- objetivo: DeleteAccessKey
- objetivo: PutUserPolicy
- objetivo: DeleteUserPolicy
- IAM: desactivar MFADevice
- Soy: AttachRolePolicy
- objetivo: AttachUserPolicy
- objetivo: DeleteRolePolicy
- Yo soy: Tag MFADevice
- soy: PutRolePolicy
- objetivo: TagPolicy
- objetivo: TagRole
- objetivo: TagUser

- objetivo: UntagUser
- objetivo: UntagRole
- organizaciones: ListAccounts
- así que: ListPermissionSetsProvisionedToAccount
- sso: GetInlinePolicyForPermissionSet
- sso: ListInstances
- directorio sso: SearchUsers
- sso: ListPermissionSets
- sso: ListAccountAssignments
- directorio sso: DescribeUser
- almacén de identidades: ListUsers
- almacén de identidades: ListGroups
- almacén de identidades: IsMemberInGroups
- almacén de identidades: ListGroupMemberships
- administrador de secretos: CreateSecret
- administrador de secretos: DeleteSecret
- así que: DeleteAccountAssignment
- sso: PutInlinePolicyToPermissionSet
- sso: CreateAccountAssignment
- sso: DeleteInlinePolicyFromPermissionSet
- sso: TagResource
- sso: UntagResource
- almacén de identidad: DeleteGroupMembership
- almacén de identidades: CreateGroupMembership

A continuación, se muestra un ejemplo de una política de IAM que concede los permisos necesarios para: `AutomationAssumeRole`

JSON

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

```

"Statement": [
  {
    "Sid": "S3Permissions",
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketAcl",
      "s3:GetObject",
      "s3:CreateBucket",
      "s3:PutObject"
    ],
    "Resource": "*"
  },
  {
    "Sid": "IAMPermissions",
    "Effect": "Allow",
    "Action": [
      "iam:GetUser",
      "iam:GetUserPolicy",
      "iam:GetRole",
      "iam:ListUserPolicies",
      "iam:ListAttachedUserPolicies",
      "iam:ListAccessKeys",
      "iam:ListMfaDevices",
      "iam:ListVirtualMFADevices",
      "iam:GetLoginProfile",
      "iam:GetPolicy",
      "iam:GetRolePolicy",
      "iam:ListPolicies",
      "iam:ListAttachedRolePolicies",
      "iam:ListRolePolicies",
      "iam:UpdateAccessKey",
      "iam:CreateAccessKey",
      "iam:DeleteLoginProfile",
      "iam:DeleteAccessKey",
      "iam:PutUserPolicy",
      "iam:DeleteUserPolicy",
      "iam:DeactivateMFADevice",
      "iam:AttachRolePolicy",
      "iam:AttachUserPolicy",
      "iam:DeleteRolePolicy",

```

```

        "iam:TagMFADevice",
        "iam:PutRolePolicy",
        "iam:TagPolicy",
        "iam:TagRole",
        "iam:TagUser",
        "iam:UntagUser",
        "iam:UntagRole"
    ],
    "Resource": "*"
},
{
    "Sid": "OrganizationsPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:ListAccounts"
    ],
    "Resource": "*"
},
{
    "Sid": "SSOPermissions",
    "Effect": "Allow",
    "Action": [
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListInstances",
        "sso-directory:SearchUsers",
        "sso:ListPermissionSets",
        "sso:ListAccountAssignments",
        "sso-directory:DescribeUser",
        "sso:DeleteAccountAssignment",
        "sso:PutInlinePolicyToPermissionSet",
        "sso:CreateAccountAssignment",
        "sso:DeleteInlinePolicyFromPermissionSet",
        "sso:TagResource",
        "sso:UntagResource"
    ],
    "Resource": "*"
},
{
    "Sid": "IdentityStorePermissions",
    "Effect": "Allow",
    "Action": [
        "identitystore:ListUsers",
        "identitystore:ListGroups",

```



```

        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore>DeleteGroupMembership",
        "identitystore>CreateGroupMembership"
    ],
    "Resource": "*"
},
{
    "Sid": "SecretsManagerPermissions",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager>DeleteSecret"
    ],
    "Resource": "*"
}
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-ContainIAMPrincipal](#) la consola AWS de Systems Manager.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.
 - Tipo: `AWS::IAM::Role::Arn`
 - PrincipalType (Obligatorio):
 - Descripción: (obligatorio) El tipo principal de AWS IAM: usuario de IAM, rol de IAM o usuario de Identity Center.
 - Tipo: cadena
 - Valores permitidos: `IAM user|IAM role|Identity Center user`

- **PrincipalName (Obligatorio):**
 - Descripción: (Obligatorio) El nombre del director de IAM. Para los usuarios de Identity Center, proporcione el nombre de usuario.
 - Tipo: cadena
 - Valor permitido: `^[a-zA-Z0-9\\.\_-\\\\!*'() /+=, @]{1,1024}$`
- **Acción (obligatoria):**
 - Descripción: (Obligatorio) Seleccione `Contain` esta opción para aislar el principal de IAM de destino o `Restore` intentar restaurar el principal de IAM a su configuración original a partir de una copia de seguridad anterior.
 - Tipo: cadena
 - Valores permitidos: `Contain|Restore`
- **DryRun (Opcional):**
 - Descripción: (opcional) Si se configura en `true`, la automatización no realizará ningún cambio en el principal de IAM objetivo, sino que generará datos sobre lo que habría intentado cambiar, detallando cada paso. Valor predeterminado: `true`.
 - Tipo: Booleano
 - Valores permitidos: `true|false`
- **ActivateDisabledKeys(Condicional):**
 - Descripción: (Condicional) Si el parámetro de entrada `Action` está establecido como `Restore` y `PrincipalType` está configurado como usuario de IAM, esta opción determina si esta automatización debe intentar activar las claves de acceso asociadas si está desactivada. Tenga en cuenta que no se puede verificar la integridad de una clave de acceso comprometida. AWS recomienda encarecidamente no reactivar una clave comprometida. En su lugar, es recomendable generar nuevas claves. Valor predeterminado: `false`.
 - Tipo: Booleano
 - Valores permitidos: `true|false`
- **Copias de seguridad 3 BucketName (condicionales):**
 - Descripción: (Condicional) El bucket de Amazon S3 para hacer una copia de seguridad de la configuración principal de IAM cuando la acción está establecida en `Contain` o para restaurar la configuración desde que está `Restore` establecida la acción. Tenga en cuenta que si la acción especificada es `Contain` y el runbook no puede acceder al bucket o no se proporciona un valor, se crea un nuevo bucket en su cuenta con ese nombre. `awssupport-`

`containiamprincipal-<random-string>` Si `DryRun` se establece en `true` este parámetro, es obligatorio.

- Tipo: `AWS::S3::Bucket::Name`
- Copias de seguridad S3 KeyName (condicionales):
 - Descripción: (Condicional) Si `Action` se establece en `Restore`, se especifica la clave de Amazon S3 que la automatización utilizará para intentar restaurar la configuración principal de IAM. La clave Amazon S3 normalmente sigue este formato: `{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json`. La clave se puede obtener del resultado de una ejecución anterior de automatización de contención.
 - Tipo: cadena
 - Valor permitido: `^[a-zA-Z0-9\.\_\-\!\*'()/{0,1024}$`
- Copias de seguridad S3 BucketAccess (condicionales):
 - Descripción: (Condicional) El ARN de los usuarios o roles de IAM a los que se les permitirá acceder al bucket de respaldo de Amazon S3 después de ejecutar las acciones de contención. Este parámetro es obligatorio cuando `Action` es `Contain`. El usuario en cuyo contexto se ejecuta la automatización o `AutomationAssumeRole`, en su defecto, el usuario en cuyo contexto se ejecuta la automatización se añade automáticamente a la lista.
 - Tipo: `StringList`
 - Valor permitido: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:[0-9]{12}:(role|user)\[/[\\w+\\/=,.\@-]+$`
- TagIdentifier (Opcional):
 - Descripción: (opcional) Etiqueta el director de IAM con una etiqueta de su elección utilizando el siguiente formato: `Key=<EXAMPLE_KEY>,Value=<EXAMPLE_VALUE>`. Esta opción le permite realizar un seguimiento de los principios de IAM a los que se ha dirigido este manual. Nota: Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
 - Tipo: cadena
 - Valor permitido: `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{0,128}$`

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

Valida los parámetros de entrada de automatización necesarios en función de lo especificado.

Action

- CheckBackupS3BucketName

Comprueba si el bucket Amazon S3 de Amazon S3 de destino puede conceder `read` acceso `write` público a sus objetos. En el caso de un flujo de trabajo de contención, se crea un nuevo bucket de Amazon S3 si el `BackupS3BucketName` bucket no existe.

- BranchOnAction

Ramifica la automatización en función del valor especificado `Action`.

- BranchOnPrincipalTypeAndDryRun

Ramifica la automatización en función del tipo de principal de IAM (usuario de IAM, rol de IAM o usuario de Identity Center) y si se está ejecutando en modo. `DryRun`

- BranchOnPrincipalTypeForContain

Ramifica la automatización según la `Contain` acción y el tipo principal de IAM (usuario de IAM, rol de IAM o usuario de Identity Center) especificado en la entrada.

- Obtenga IAMUser

Obtiene la hora de creación y el nombre de usuario del usuario de IAM objetivo.

- Obtenga los detalles IAMUser

Obtiene y almacena la configuración del usuario de IAM de destino, incluidas las políticas en línea, las políticas administradas, las claves de acceso, los dispositivos MFA y el perfil de inicio de sesión.

- Actualizaciones 3 KeyForUser

Actualiza la variable de automatización 'S3Key' a partir del resultado del paso.

GetIAMUserDetails

- Obtenga IAMRole

Obtiene la hora de creación, el nombre del rol y la ruta del rol de IAM objetivo.

- Obtenga los detalles IAMRole

Obtiene y almacena la configuración de la función de IAM de destino, incluidas las políticas integradas y las políticas gestionadas asociadas a la función.

- Actualiza S3 KeyForRole

Actualiza la variable de automatización 'S3Key' a partir del resultado del paso.
`GetIAMRoleDetails`

- GetIdentityStoreId

Obtiene el ID de la instancia del AWS IAM Identity Center asociada a la cuenta. AWS

- Obtenga IDCUser

Obtiene el ID de usuario del Identity Center de destino mediante el ID del almacén de identidades.

- Recopile IDCUser los detalles

Obtiene y almacena la configuración del usuario de Identity Center de destino, incluidas las asignaciones de cuentas, los conjuntos de permisos asociados y las políticas integradas.

- Actualiza S3 KeyFor IDCUser

Actualiza la variable de automatización 'S3Key' a partir del resultado del paso.
`GatherIDCUserDetails`

- BranchOnIdentityContain

Ramifica la automatización según el valor `DryRun` y el tipo principal de IAM de la acción.
`Contain`

- BranchOnDisableAccessKeys

Ramifica la automatización en función de si el usuario de IAM tiene claves de acceso que deben deshabilitarse.

- DisableAccessKeys

Desactiva las claves de acceso de los usuarios de IAM activos.

- BranchOnDisableConsoleAccess

Se ramifica en función de si el usuario de IAM tiene habilitado o no el acceso a la consola de AWS administración.

- DisableConsoleAccess

Elimina el acceso mediante contraseña del usuario de IAM a la consola de administración. AWS

Adjunta una política de denegación al usuario de IAM para revocar los permisos de los tokens de sesión anteriores.

- `AttachInlineDenyPolicyToRole`

Adjunta una política de denegación a la función de IAM para revocar los permisos de los tokens de sesión más antiguos.

- `RemovePermissionSets`

Elimina los conjuntos de permisos asociados al usuario de Identity Center.

- `Eliminar IDCUUser de IDCGroups`

Elimina el usuario de Identity Center de los grupos de Identity Center.

- `AttachInlineDenyPolicyToPermissionSet`

Adjunta una política de denegación a los conjuntos de permisos asociados al usuario de Identity Center.

- `BranchOnReactivateKeys`

Durante el proceso de restauración, ramifica la automatización en función del `ActivateDisabledKeys` parámetro.

- `DetachInlineDenyPolicy`

Elimina la política de denegación asociada a la función de IAM durante el proceso de contención.

- `DetachInlineDenyPolicyFromPermissionSet`

Elimina la política de denegación adjunta a los conjuntos de permisos durante el proceso de contención.

- `ReportContain`

Muestra información detallada sobre las acciones de contención que se llevarían a cabo cuando `DryRun` se establezca en. `True`

- `ReportRestore`

Genera información detallada sobre las acciones de restauración que se realizarían cuando `DryRun` esté configurado en. `True`

- `ReportContainFailure`

Proporciona instrucciones completas para restaurar manualmente la configuración original del director de IAM durante un escenario de fallo en el flujo de trabajo de contención.

- `ReportRestoreFailure`

Proporciona instrucciones detalladas para completar manualmente la restauración de la configuración original del principal de IAM durante un escenario de fallo en el flujo de trabajo de restauración.

7. Una vez finalizada la ejecución, consulte la sección de resultados para ver los resultados detallados de la ejecución:

- `Contiene IAMPrincipal .Output`

Proporciona información detallada sobre las acciones de contención que se realizan cuando `Action` está establecida en `Contener` y `DryRun` `False`. Incluye información sobre la ubicación de la copia de seguridad, las políticas de denegación aplicadas y las configuraciones modificadas.

- `RestaurarIAMPrincipal. Salida`

Proporciona información detallada sobre las acciones de restauración que se realizan cuando `Action` está establecida en `Restaurar` y `DryRun` `False`. Incluye información sobre las configuraciones restauradas y cualquier problema que se haya producido durante la restauración.

- `ReportContain.Salida`

Genera información detallada sobre las acciones de contención que se realizarían cuando `Action` se establece en `Contener` y `DryRun` se establece en `True`. Incluye una comparación de las configuraciones actuales y posteriores a la contención.

- `ReportRestore.Salida`

Genera información detallada sobre las acciones de restauración que se realizarían cuando `Action` se establece en `Restore` y `DryRun` en `True`. Muestra la configuración actual y la configuración original que se restauraría.

- `ReportContainFailure.Salida`

Proporciona instrucciones completas para restaurar manualmente la configuración original del director de IAM durante un escenario de fallo en el flujo de trabajo de contención.

- `ReportRestoreFailure4. Salida`

Proporciona instrucciones detalladas para completar manualmente la restauración de la configuración original del principal de IAM durante un escenario de error en el flujo de trabajo de restauración.

Salidas

Una vez finalizada la ejecución, consulte la sección de resultados para ver los resultados detallados:

- `Contiene... IAMPrincipal Salida`

Proporciona información detallada sobre las acciones de contención que se realizan cuando `Action` está establecida en `Contener` y `DryRun` `False`. Incluye información sobre la ubicación de la copia de seguridad, las políticas de denegación aplicadas y las configuraciones modificadas.

- `RestaurarIAMPrincipal. Salida`

Proporciona información detallada sobre las acciones de restauración que se realizan cuando `Action` está establecida en `Restaurar` y `DryRun` `False`. Incluye información sobre las configuraciones restauradas y cualquier problema que se haya producido durante la restauración.

- `ReportContain.Salida`

Genera información detallada sobre las acciones de contención que se realizarían cuando `Action` se establece en `Contener` y `DryRun` se establece en `True`. Incluye una comparación de las configuraciones actuales y posteriores a la contención.

- `ReportRestore.Salida`

Genera información detallada sobre las acciones de restauración que se realizarían cuando `Action` se establece en `Restore` y `DryRun` en `True`. Muestra la configuración actual y la configuración original que se restauraría.

- `ReportContainFailure.Salida`

Proporciona instrucciones completas para restaurar manualmente la configuración original del director de IAM durante un escenario de fallo en el flujo de trabajo de contención.

- `ReportRestoreFailure4. Salida`

Proporciona instrucciones detalladas para completar manualmente la restauración de la configuración original del principal de IAM durante un escenario de error en el flujo de trabajo de restauración.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización sencilla](#)
- [Configuración de la automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWSSupport-TroubleshootSAMLIssues

Descripción

El manual de AWSSupport-TroubleshootSAMLIssues automatización ayuda a diagnosticar problemas relacionados con el lenguaje de marcado de aserciones de seguridad (SAML) mediante el análisis de los archivos de respuesta de SAML almacenados en Amazon Simple Storage Service (Amazon S3). Realiza una validación exhaustiva que incluye la verificación del esquema, la validación de firmas, la verificación de las restricciones de audiencia y la verificación del tiempo de caducidad. El manual decodifica y extrae los elementos clave del SAML, como el emisor, las afirmaciones, el asunto, las condiciones, las firmas y los atributos, de la respuesta del SAML. En los entornos en los que se utiliza SAML para acceder a AWS los recursos (como Amazon Connect o Amazon WorkSpaces Applications) a través de un proveedor de identidad de IAM, verifica si los certificados de las firmas de respuesta de SAML coinciden con los certificados configurados en el proveedor de identidades de IAM.

¿Cómo funciona?

El manual de instrucciones lleva a cabo los siguientes pasos:

- Valida el formato de respuesta de SAML y los elementos necesarios.
- Decodifica y extrae los componentes de la respuesta de SAML (emisor, afirmaciones, asunto, condiciones, firmas y atributos).
- Verifica las firmas digitales con los certificados del proveedor de identidad de IAM cuando se proporcionan.
- Comprueba las restricciones de audiencia y la validez temporal.
- Proporciona información de diagnóstico detallada que muestra la estructura SAML analizada y los resultados de la validación.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

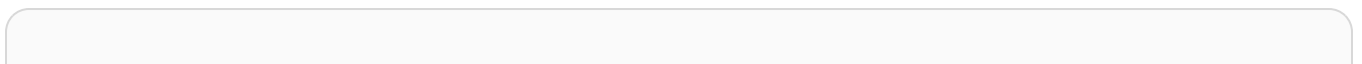
Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `s3:GetBucketLocation`
- `s3:ListBucket`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetAccountPublicAccessBlock`
- `s3:GetObject`
- `s3:GetBucketPolicyStatus`
- `s3:GetEncryptionConfiguration`
- `s3:GetBucketOwnershipControls`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicy`
- `s3:PutObject`
- `iam:GetSAMLProvider`
- `sts:AssumeRole`

Ejemplo de política:

JSON



```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "iam:GetSAMLProvider",
        "sts:AssumeRole"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Antes de usar este manual, debe capturar y almacenar una respuesta SAML codificada en Base64 (archivo txt) en un bucket de S3. [Las instrucciones para capturar las respuestas de SAML se encuentran en este documento](#)
2. Navegue hasta [AWSsupport-TroubleshootSAMLIssues](#) Systems Manager, en Documentos.
3. Elija Execute automation (Ejecutar automatización).
4. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a SSM Automation realizar las acciones en su

nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Tipo: `AWS::IAM::Role::Arn`
- InputFileS3URI (obligatorio):
 - Descripción: URI (obligatorio) de Amazon Simple Storage Service (Amazon S3) del archivo txt de respuesta SAML (p. ej., `s3://bucket name/path/to/file - .txt`).
 - Tipo: cadena
 - Patrón de permisos: `^s3://[a-z0-9][a-z0-9.-][a-z0-9](/. )?$`
- S3 OutputPrefix (opcional):
 - <executionID of the runbook>Descripción: (opcional) Los archivos de salida del análisis se almacenan en el depósito de entrada con el nombre «saml_analysis_ .json». Puede usar este parámetro si desea generar un archivo con un prefijo específico. <executionID of the runbook>El valor predeterminado es «output/», en cuyo caso el URI del archivo que generará el resultado será 's3://bucket - name/output/saml_analysis_ .json'.
 - Tipo: cadena
 - Permitir patrón: `^[a-zA-Z0-9+=, .@\\-_/]*/$`
- ExpectedAudience (Opcional):
 - Descripción: (opcional) Valor de audiencia esperado en la respuesta de SAML. Si no se especifica, utilizamos `urn:amazon:webservices`. Si ha configurado un valor de audiencia específico en su configuración de IdP y SP, proporcione el formato exacto (por ejemplo, `urn:amazon:webservices,https://signin.aws.amazon.com/saml`).
 - Tipo: cadena
 - Predeterminado: `urn:amazon:webservices`
- IamIdProviderArn (Opcional):
 - Descripción: (Opcional) Si utiliza una entidad proveedora de ID de IAM para vincular directamente su IdP AWS con IAM, indique su ARN (por ejemplo, `arn:aws:iam::<account-id>saml-provider/<provider-name>`).
 - Tipo: cadena
 - Patrón de permisos: `^$|^arn:aws:iam::[0-9]{12}:saml-provider/[a-zA-Z0-9_-]+$`
- SAMLAuthenticationHora (opcional):
 - Descripción: (opcional) Fecha y hora en que se realizó la autenticación SAML. La zona horaria debe ser UTC. Debe estar en YYYY-MM-DDThh formato:mm:ss (p. ej., `2025-02-01T`

10:00:00). Si no se proporciona este parámetro, las comprobaciones de caducidad se realizarán comparándolas con la marca de tiempo actual.

- Tipo: cadena
- Patrón de permisos: `^$|^\\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[12]\\d|3[01])T(?:[01]\\d|2[0-3]):[0-5]\\d:[0-5]\\d$`
- S3 BucketOwnerRoleArn (opcional):
 - Descripción: ARN de rol de IAM (opcional) para acceder a los buckets de Amazon S3. El ARN de la función de IAM con permisos para obtener la configuración de acceso público del bucket y el bloqueo de cuentas de Amazon S3, la configuración de cifrado del bucket, el bucket ACLs, el estado de la política del bucket y cargar objetos al bucket. Si no se especifica este parámetro, el runbook utiliza el ``AutomationAssumeRole`` (si se especifica) o el usuario que inicia este runbook (si ``AutomationAssumeRole`` no se especifica).
 - Tipo: `AWS::IAM::Role::Arn`

5. Seleccione Ejecutar.

6. Se inicia la automatización.

7. Este documento realiza los siguientes pasos:

- Validar IAMIDProvider

Valida el ARN del proveedor de ID de IAM proporcionado comprobando si existe y es accesible. Si no se proporciona ningún ARN, se omite la validación y el paso se completa correctamente.

- Compruebe S3 BucketPublicStatus

Comprueba si el bucket de Amazon S3 permite permisos de acceso de lectura o escritura públicos o anónimos. Si el bucket permite estos permisos, la automatización se detiene en este paso.

- Comprueba: 3. ObjectExistence

Valida el acceso a los buckets de Amazon S3. Comprueba si el depósito y el objeto existen y si la automatización tiene los permisos necesarios para leer desde el origen y escribir en el destino.

- Analiza SAMLResponse

Analiza el archivo de respuesta SAML realizando las comprobaciones (validación del esquema, verificación de firmas, validación de audiencia, comprobación de caducidad). Genera un informe JSON detallado y lo guarda en la ubicación de Amazon S3 especificada.

8. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución:
 - La sección de resultados contiene información sobre el objeto Amazon S3 donde se describen los resultados del análisis.
9. El objeto Amazon S3 de los resultados del análisis es un archivo Json que contiene la siguiente información:
 - `validation_result`: contiene los resultados de validación básicos de la respuesta de SAML.
 - `saml_info`: información clave sobre SAML, que incluye el emisor, las firmas y las afirmaciones.
 - `schema_validation`: resultados de la validación del esquema SAML.
 - `verification_result`: proporciona resultados de diagnóstico más detallados.
 - `firma`: resultados de la verificación de la firma.
 - `audiencia`: resultados de la validación de la restricción de audiencia.
 - `caducidad`: resultados de la verificación de la hora de caducidad.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

Detección y respuesta a incidentes

AWS Systems Manager La automatización proporciona manuales predefinidos para la detección y respuesta a AWS incidentes. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSPremiumSupport-OnboardWorkloadToIDR](#)

AWSPremiumSupport-OnboardWorkloadToIDR

Descripción

El AWSPremiumSupport-OnboardWorkloadToIDRmanual ayuda a los clientes de AWS Enterprise Support a incorporar una carga de trabajo para la supervisión y la gestión de incidentes críticos mediante AWS Incident Detection and Response. Una carga de trabajo se puede definir como un conjunto de AWS recursos asociados a un grupo de AWS recursos o a una AppRegistry aplicación AWS de Service Catalog. Si no se especifica un grupo de AWS recursos o una AppRegistry aplicación de AWS Service Catalog, el runbook crea un grupo de recursos en su nombre mediante filtros de etiquetas o el identificador de AWS CloudFormation pila cuyos recursos desee incluir en el grupo. Si estableces el parámetro `CreateApplicationInsights` en `Yes`, la automatización aprovisiona una aplicación de Amazon CloudWatch Application Insights mediante AWS CloudFormation. CloudWatch Application Insights configura las métricas y los registros recomendados para los recursos de la aplicación seleccionados mediante CloudWatch métricas, registros y eventos de Amazon para las notificaciones sobre los problemas detectados.

Important

Este manual realiza las siguientes acciones en su cuenta en función de los parámetros de entrada proporcionados:

- Crea un nuevo grupo AWS de recursos utilizando AWS CloudFormation si se `AppRegistryApplication` especifican `ResourceGroupName` o no. Una vez creada la pila, el runbook intenta establecer la protección de terminación.
- Etiqueta el grupo de AWS recursos asociado a la carga de trabajo, incluida la `aws_idr` etiqueta.
- Crea una CloudWatch aplicación basada en un grupo de recursos de Amazon Application Insights si el parámetro `CreateApplicationInsights` de entrada está establecido en `Yes`. Una vez creada la pila, el runbook intenta establecer la protección de terminación para la pila.
- Instala el rol `AWSServiceRoleForHealth_EventProcessor` vinculado al servicio (SLR) para proporcionar acceso a la detección y respuesta a incidentes para la recepción de alertas si el `InstallServiceLinkedRole` parámetro de entrada está establecido en `Yes`.
- Crea un caso de AWS soporte con AWS detección y respuesta a incidentes.

⚠ Important

Para usar este manual e incorporarse a AWS Incident Detection and Response, necesita una suscripción a AWS Enterprise Support (con cargo adicional) o a Unified Operations. Para obtener más información, consulte [Comparar planes de Soporte](#).

¿Cómo funciona?

El manual incluye los siguientes pasos generales:

- Comprueba si el AWS Account Support Plan actual es Enterprise; de lo contrario, la automatización finaliza.
- Determina si se debe utilizar un grupo de AWS recursos existente o crear uno nuevo en función de los parámetros proporcionados.
- Si crea un nuevo grupo de recursos, genera una AWS CloudFormation plantilla y crea la pila con las etiquetas adecuadas.
- Etiqueta el grupo de recursos con las etiquetas de detección y respuesta a AWS incidentes necesarias.
- Si lo desea, instala la función vinculada al servicio para la detección y respuesta a AWS incidentes.
- Si lo desea, crea una CloudWatch aplicación Amazon Application Insights para mejorar la supervisión.
- Crea un caso de AWS soporte para completar el proceso de incorporación.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudformation:CreateStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateTerminationProtection`
- `iam:CreateServiceLinkedRole`
- `resource-groups:CreateGroup`
- `resource-groups:GetGroup`
- `resource-groups:TagResource`
- `servicecatalog-appregistry:GetApplication`
- `support:CreateCase`
- `support:DescribeSeverityLevels`
- `support:DescribeServices`
- `support:DescribeSupportLevel`

Ejemplo de política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "iam:CreateServiceLinkedRole",
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:TagResource",
        "servicecatalog-appregistry:GetApplication",
        "support:CreateCase",
        "support:DescribeSeverityLevels",
```

```

        "support:DescribeServices",
        "support:DescribeSupportLevel"
    ],
    "Resource": "*"
}
]
}
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSPremiumSupport-OnboardWorkloadToIDR](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
 - Tipo: AWS::IAM::Role::Arn
 - WorkloadName (Obligatorio):
 - Descripción: (obligatorio) Nombre de la carga de trabajo. Si no ResourceGroupName se proporciona, el nombre de la carga de trabajo se utiliza para configurar un nuevo grupo de AWS recursos con ese nombre IDR-AWS-<WorkloadName>.
 - Tipo: String
 - Patrón de permisos: `^[a-zA-Z0-9_-]{1,128}$`
 - WorkloadDescription (Obligatorio):
 - Descripción: (Obligatoria) La descripción de la carga de trabajo. Introduzca una breve descripción para detallar los casos de uso de esta carga de trabajo. Incluya el usuario final principal y la función de esta carga de trabajo.
 - Tipo: String
 - Patrón de permisos: `^[a-zA-Z0-9.:;,-_&() ]{1,1024}$`
 - AppRegistryApplication (Opcional):

- Descripción: (opcional) El nombre o el ID de la AppRegistry aplicación AWS Service Catalog. Si no se proporciona, debe introducir una entrada para `ResourceGroupName`.
- Tipo: `String`
- Permitir patrón: `^[a-zA-Z0-9._-]{1,128}$`
- Valor predeterminado: `""`
- `ResourceGroupName` (Opcional):
 - Descripción: (opcional) El nombre de un grupo de AWS recursos existente si no `AppRegistryApplication` se proporciona. Si desea crear un grupo de recursos, debe proporcionar una entrada `TagFilters` y, si lo desea, `ResourceTypeFilters` crear un nuevo grupo de AWS recursos.
 - Tipo: `String`
 - Permitir patrón: `^[a-zA-Z0-9_.-]{1,128}$`
 - Valor predeterminado: `""`
- `TagFilters` (Condicional):
 - Descripción: (Condicional) La lista de pares key/values (cadena/lista de cadenas) que se comparan con las etiquetas adjuntas a los recursos. AWS Este parámetro se utiliza para crear un nuevo grupo AWS de recursos si no se especifica un o existente `ResourceGroupName`. `AppRegistryApplication`
 - Tipo: `StringMap`
- `ResourceTypeFilters` (Condicional):
 - Descripción: (Condicional) La lista de tipos de recursos compatibles con Resource Groups.
 - Tipo: `StringList`
 - Número máximo de artículos: 10
 - Valor predeterminado: `AWS::AllSupported`
- `InstallServiceLinkedRole` (Opcional):
 - Descripción: (opcional) Seleccione esta opción Yes para instalar la función `AWSServiceRoleForHealth_EventProcessor` vinculada al servicio (SLR).
 - Tipo: `String`
 - Valores permitidos: `[Yes, No]`
 - Valor predeterminado: `No`
- `CreateApplicationInsights` (Opcional):

- Descripción: (opcional) Seleccione esta opción Yes para crear una aplicación basada en un grupo de recursos de Amazon CloudWatch Application Insights.
- Tipo: String
- Valores permitidos: [Yes, No]
- Valor predeterminado: No
- ComplianceAndRegulatoryRequirements (Obligatorio):
 - Descripción: (Obligatorio) Requisitos and/or normativos de cumplimiento aplicables a esta carga de trabajo y cualquier acción necesaria AWS después de un incidente.
 - Tipo: String
 - Patrón de permisos: `^[a-zA-Z0-9.:;,\_\&() ]{1,1024}$`
- No AWSComponents (opcional):
 - Descripción: (opcional) ¿Detalla algún AWS componente local o ajeno a esta carga de trabajo? Si es así, ¿qué son y qué funciones desempeñan?
 - Tipo: String
 - Permitir patrón: `^$|^[a-zA-Z0-9.:;,\_\&() ]{1,1024}$`
 - Valor predeterminado: ""
- UpstreamDownstreamDependencies (Opcional):
 - Descripción: (opcional) Detalles de cualquier upstream/downstream componente que no esté incorporado y que podría afectar a esta carga de trabajo en caso de producirse una interrupción.
 - Tipo: String
 - Patrón de permisos: `^$|^[a-zA-Z0-9.:;,\_\&() ]{1,1024}$`
 - Valor predeterminado: ""
- FailoverDisasterRecoveryPlan (Opcional):
 - Descripción: (opcional) Proporcione detalles de cualquier plan de failover/disaster recuperación manual o automatizado a nivel regional y de Arizona.
 - Tipo: String
 - Patrón de permisos: `^$|^[a-zA-Z0-9.:;,\_\&() ]{1,1024}$`
 - Valor predeterminado: ""
- BridgeDetails (Opcional):

- Descripción: (opcional) El puente incident/crisis de administración estática establecido por su empresa. Si utiliza un puente no estático, especifique su aplicación preferida y AWS solicitará estos detalles durante un incidente.
- Tipo: String
- Valores permitidos: [Amazon Chime bridge, Non-Static bridge, Static bridge]
- Valor predeterminado: Amazon Chime bridge
- SubscriptionStartDate (Obligatorio):
 - Descripción: (Obligatorio) La fecha en el YYYY-MM-DD formato en que desea iniciar su suscripción a la detección y respuesta a AWS incidentes.
 - Tipo: String
 - Patrón de permisos: $^((202[4-9]|20[3-9][0-9])-(0[1-9]|1[0-2])-(0[1-9]|[12][0-9]|3[01]))$$

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- Compruebe el AWSSupport plan:

Comprueba si el AWS Account Support Plan actual es Enterprise; de lo contrario, la automatización finaliza.

- BranchOnResourceGroup:

Ramifica la automatización en función de si se proporcionó un grupo de AWS recursos existente. Si no se proporciona, la automatización crea un nuevo grupo AWS de recursos.

- GetAppRegistryApplication:

Obtiene la información de metadatos sobre la AppRegistry aplicación AWS Service Catalog, si se proporciona.

- GenerateResourceGroupTemplate:

Genera una AWS CloudFormation plantilla para el grupo AWS de recursos con los filtros de etiquetas especificados.

- CreateResourceGroup:

Crea un nuevo grupo de AWS recursos mediante AWS CloudFormation.

- TagResourceGroup:

Etiqueta el grupo de recursos con las etiquetas requeridas para la detección y respuesta a AWS incidentes (IDR).

- InstallServiceLinkedRole:

Instala la función vinculada al servicio de detección y respuesta a AWS incidentes (IDR) si se solicita.

- CreateApplicationInsightsApplication:

Crea una CloudWatch aplicación Amazon Application Insights si se solicita.

- CreateAwsSupportCase:

Crea un caso de AWS soporte con detección y respuesta a AWS incidentes.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)
- [Comience con la detección y respuesta a AWS incidentes](#)
- [Descubrimiento de la carga de trabajo en la detección y respuesta a incidentes](#)

Amazon Kinesis Data Streams

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Kinesis Data Streams. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-EnableKinesisStreamEncryption](#)

AWS-EnableKinesisStreamEncryption

Descripción

El AWS-EnableKinesisStreamEncryption manual permite el cifrado en Amazon Kinesis Data Streams (Kinesis Data Streams). Las aplicaciones de los productores que escriban en una transmisión cifrada encontrarán errores si no tienen acceso a la clave AWS Key Management Service (AWS KMS).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- KinesisStreamName

Tipo: cadena

Descripción: (obligatorio) El nombre de la transmisión en la que desea habilitar el cifrado.

- KeyId

Tipo: cadena

Valor predeterminado: alias/aws/kinesis

Descripción: (Obligatoria) La AWS KMS clave administrada por el cliente que desea utilizar para el cifrado. Este valor puede ser un identificador único global, un ARN para un alias o una clave, o un nombre de alias con el prefijo «alias/». También puede usar la clave AWS administrada utilizando el valor predeterminado del parámetro.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

Pasos de documentos

- `VerifyKinesisStreamStatus (aws:waitForAwsResourceProperty)` - Comprueba el estado de Kinesis Data Streams.
- `EnableKinesisStreamEncryption (aws:executeAwsApi)` - Habilita el cifrado de Kinesis Data Streams.
- `VerifyKinesisStreamUpdateComplete (aws:waitForAwsResourceProperty)` - Espera a que el estado de Kinesis Data Streams vuelva a ser. ACTIVE
- `VerifyKinesisStreamEncryption (aws:assertAwsResourceProperty)` - Verifica que el cifrado esté habilitado para Kinesis Data Streams.

AWS KMS

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Key Management Service Para obtener información acerca de los manuales de

procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-CancelKeyDeletion](#)
- [AWSConfigRemediation-EnableKeyRotation](#)

AWSConfigRemediation-CancelKeyDeletion

Descripción

El AWSConfigRemediation-CancelKeyDeletion manual cancela la eliminación de la clave gestionada por el cliente AWS Key Management Service (AWS KMS) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- KeyId

Tipo: cadena

Descripción: (obligatorio) el ID de la clave gestionada por el cliente cuya eliminación desea cancelar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CancelKeyDeletion`
- `kms:DescribeKey`

Pasos de documentos

- `aws:executeAwsApi`: cancela la eliminación de la clave gestionada por el cliente que especifique en el parámetro `KeyId`.
- `aws:assertAwsResourceProperty`: confirma que la eliminación de claves está deshabilitada en la clave gestionada por el cliente.

AWSConfigRemediation-EnableKeyRotation

Descripción

El `AWSConfigRemediation-EnableKeyRotation` manual permite la rotación automática de claves para la clave simétrica AWS Key Management Service (AWS KMS) gestionada por el cliente.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- KeyId

Tipo: cadena

Descripción: (obligatorio) el ID de la clave gestionada por el cliente en la que desea activar la rotación automática de claves.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:EnableKeyRotation
- kms:GetKeyRotationStatus

Pasos de documentos

- aws:executeAwsApi: habilita la rotación automática de claves en la clave gestionada por el cliente que especifique en el parámetro KeyId.
- aws:assertAwsResourceProperty: confirma que la rotación automática de claves está habilitada en su clave administrada por el cliente.

Lambda

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Lambda Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing](#)
- [AWSConfigRemediation-DeleteLambdaFunction](#)
- [AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK](#)
- [AWSConfigRemediation-MoveLambdaToVPC](#)
- [AWSSupport-RemediateLambdaS3Event](#)
- [AWSSupport-TroubleshootLambdaInternetAccess](#)
- [AWSSupport-TroubleshootLambdaS3Event](#)

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

Descripción

El AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing manual permite el rastreo AWS X-Ray en tiempo real de la AWS Lambda función que especifique en el parámetro. FunctionName

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- FunctionName

Tipo: cadena

Descripción: (obligatorio) el nombre o ARN de la función de Lambda en la que se habilitará el seguimiento.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- lambda:UpdateFunctionConfiguration
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

Pasos de documentos

- aws:executeAwsApi: permite el trazado de X-Ray en la función de Lambda que especifique en el parámetro FunctionName.
- aws:assertAwsResourceProperty: verifica que el trazado de X-Ray esté activado en la función de Lambda.

Salidas

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Respuesta de la llamada a la UpdateFunctionConfiguration API.

AWSConfigRemediation-DeleteLambdaFunction

Descripción

El manual de procedimientos AWSConfigRemediation-DeleteLambdaFunction elimina la función AWS Lambda que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- LambdaFunctionName

Tipo: cadena

Descripción: (obligatorio) el nombre de la función de Lambda que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

Pasos de documentos

- `aws:executeAwsApi`: elimina la función de Lambda especificada en el parámetro `LambdaFunctionName`.
- `aws:executeScript`: verifica que se ha eliminado la función de Lambda.

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

Descripción

El `AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` runbook cifra, en reposo, las variables de entorno de la función (AWS Lambda Lambda) que especifique mediante una clave AWS Key Management Service (AWS KMS) gestionada por el cliente. Este manual de procedimientos solo debe usarse como referencia para garantizar que las variables de entorno de la función de Lambda estén cifradas de acuerdo con las mejores prácticas de seguridad mínimas recomendadas. Recomendamos cifrar varias funciones con diferentes claves administradas por el cliente.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- FunctionName

Tipo: cadena

Descripción: (obligatorio) el nombre o ARN de la función de Lambda cuyas variables de entorno desea cifrar.

- KMSKeyArn

Tipo: cadena

Descripción: (obligatorio) El ARN de la clave gestionada por el AWS KMS cliente que desea utilizar para cifrar las variables de entorno de la función Lambda.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

Pasos de documentos

- aws:waitForAwsResourceProperty: espera a que el LastUpdateStatus de la propiedad sea Successful.
- aws:executeAwsApi- Cifra las variables de entorno de la función Lambda que especifique en FunctionName el parámetro mediante la clave gestionada por AWS KMS el cliente que especifique en KMSKeyArn el parámetro.

- `aws:assertAwsResourceProperty`: confirma que el cifrado está habilitado en las variables de entorno de la función de Lambda.

AWSConfigRemediation-MoveLambdaToVPC

Descripción

El manual de procedimientos AWSConfigRemediation-MoveLambdaToVPC mueve una función de AWS Lambda (Lambda) a una Amazon Virtual Private Cloud (Amazon VPC).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- FunctionName

Tipo: cadena

Descripción: (obligatorio) el nombre de la función de Lambda que se va a migrar a una Amazon VPC.

- SecurityGroupIds

Tipo: cadena

Descripción: (Obligatorio) El grupo de seguridad IDs que desea asignar a las interfaces de red elásticas (ENIs) asociadas a la función Lambda.

- SubnetIds

Tipo: cadena

Descripción: (Obligatorio) La subred en la IDs que desea crear las interfaces de red elásticas (ENIs) asociadas a la función Lambda.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Pasos de documentos

- `aws:executeAwsApi`: actualiza la configuración de Amazon VPC para la función de Lambda que especifique en el parámetro `FunctionName`.
- `aws:waitForAwsResourceProperty`: espera a que el `LastUpdateStatus` de la función de Lambda sea `successful`.
- `aws:executeScript`: verifica que la configuración de Amazon VPC de la función de Lambda se haya actualizado correctamente.

AWSSupport-RemediateLambdaS3Event

Descripción

El `AWSSupport-TroubleshootLambdaS3Event` manual proporciona una solución automatizada para los procedimientos descritos en los artículos del AWS Knowledge Center [¿Por qué mi notificación de eventos de Amazon S3 no activa mi función Lambda?](#) y [¿Por qué aparece el error](#)

[«No se pueden validar las siguientes configuraciones de destino» al crear una notificación de evento de Amazon S3 para activar mi función Lambda?](#) Este manual le ayuda a identificar y solucionar los motivos por los que una notificación de evento de Amazon Simple Storage Service (Amazon S3) no pudo activar la función que especificó. AWS Lambda Si el resultado del manual de procedimientos sugiere validar y configurar la simultaneidad de la función de Lambda, consulte [Invocación asíncrona](#) y [Escala de funciones de AWS Lambda](#).

 Note

Los errores “Unable to validate the following destination configurations” también pueden producirse debido a configuraciones de eventos incorrectas de Amazon S3 de Amazon Simple Notification Service (Amazon SNS) y Amazon Simple Queue Service (Amazon SQS). Este manual de procedimientos solo comprueba las configuraciones de la función de Lambda. Si, después de usar el manual de procedimientos sigue recibiendo el error “Unable to validate the following destination configurations”, por favor revise las configuraciones de eventos de Amazon S3 de Amazon SNS y Amazon SQS existentes.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `LambdaFunctionArn`

Tipo: cadena

Descripción: (obligatorio) el ARN de la función de Lambda.

- `S3 BucketName`

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de Amazon S3 cuyas notificaciones de eventos activan la función de Lambda.

- `Action`

Tipo: cadena

Valores válidos: `Troubleshoot` | `Remediate`

Descripción: (obligatoria) la acción que desea que realice el manual de procedimientos. La opción `Troubleshoot` ayuda a identificar cualquier problema, pero no realiza ninguna acción de mutación para resolver el problema. La opción `Remediate` ayuda a identificar los problemas e intenta resolverlos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`

- `s3:GetBucketNotification`

Pasos de documentos

- `aws:branch`: se ramifica en función de la entrada especificada para el parámetro `Action`.

Si el valor especificado es `Troubleshoot`:

- `aws:executeAutomation`: ejecuta el manual de procedimientos `AWSSupport-TroubleshootLambdaS3Event`.
- `aws:executeAwsApi`: comprueba el resultado del manual de procedimientos `AWSSupport-TroubleshootLambdaS3Event` que se ejecutó en el paso anterior.

Si el valor especificado es `Remediate`:

- `aws:executeScript`: ejecuta un script para solucionar los problemas descritos en la sección [¿Por qué mi notificación de eventos de Amazon S3 no activa mi función de Lambda?](#) y [¿Por qué aparece el error “Unable to validate the following destination configurations” al crear una notificación de evento de Amazon S3 para activar mi función de Lambda?](#) Artículos del Centro de conocimientos.

Salidas

`checkoutput.Output`

`remediatelambdas3event.Output`

AWSSupport-TroubleshootLambdaInternetAccess

Descripción

El `AWSSupport-TroubleshootLambdaInternetAccess` manual le ayuda a solucionar problemas de acceso a Internet para una AWS Lambda función que se lanzó en Amazon Virtual Private Cloud (Amazon VPC). Se revisan recursos como las rutas de subred, las reglas de los grupos de seguridad y las reglas de la lista de control de acceso (ACL) de red para confirmar que se permite el acceso saliente a Internet.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- FunctionName

Tipo: cadena

Descripción: (obligatorio) el nombre de la función de Lambda para la que desea solucionar problemas de acceso a Internet.

- destinationIp

Tipo: cadena

Descripción: (obligatoria) la dirección IP de destino con la que desea establecer una conexión saliente.

- destinationPort

Tipo: cadena

Predeterminado: 443

Descripción: (opcional) el puerto de destino en el que desea establecer una conexión saliente.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

Pasos de documentos

- `aws:executeScript`: verifica la configuración de varios recursos de VPC en la que se lanzó la función de Lambda.
- `aws:branch`: se ramifica en función de si la función de Lambda especificada está en una VPC o no.
- `aws:executeScript`: revisa las rutas de la tabla de enrutamiento de la subred en la que se lanzó la función de Lambda y verifica que estén presentes las rutas a una puerta de enlace de traducción de direcciones de red (NAT) y a una puerta de enlace de Internet. Confirma que la función de Lambda no está en una subred pública.
- `aws:executeScript`: verifica que el grupo de seguridad asociado a la función de Lambda permita el acceso saliente a Internet en función de los valores especificados para los parámetros `destinationIp` y `destinationPort`.
- `aws:executeScript`: verifica las reglas de ACL asociadas a las subredes de la función de Lambda y la puerta de enlace NAT que permiten el acceso saliente a Internet en función de los valores especificados para los parámetros `destinationIp` y `destinationPort`.

Salidas

`checkVpc.vpc`: el ID de VPC en la que se lanzó la función de Lambda.

`checkVPC.subnet`: la IDs de las subredes en las que se lanzó la función Lambda.

`checkVpc.securityGroups`: grupos de seguridad asociados a la función de Lambda.

`checkNACL.NACL`: mensaje de análisis con nombres de recursos. `LambdaIp` hace referencia a la dirección IP privada de la interfaz de red elástica de la función de Lambda. El objeto

LambdaIpRules solo se genera para las subredes que tienen una ruta a una puerta de enlace NAT. A continuación se muestra un ejemplo de la salida.

```
{
  "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: análisis del grupo de seguridad asociado a la función Lambda. A continuación se muestra un ejemplo de la salida.

```
{
  "sg-123456789":{
    "Status":"Allowed",
    "Analysis":"This security group has allowed destintion IP and port in its
outbuond rule."
  }
}
```

checkSubnet.subnets: análisis de las subredes de su VPC asociadas con su función de Lambda. A continuación se muestra un ejemplo de la salida.


```
{
  "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

Descripción

El AWSSupport-TroubleshootLambdaS3Event manual proporciona una solución automatizada para los procedimientos descritos en los artículos del AWS Knowledge Center [¿Por qué mi notificación de eventos de Amazon S3 no activa mi función Lambda?](#) y [¿Por qué aparece el error «No se pueden validar las siguientes configuraciones de destino» al crear una notificación de evento de Amazon S3 para activar mi función Lambda?](#) Este manual le ayuda a identificar por qué una notificación de evento de Amazon Simple Storage Service (Amazon S3) no pudo activar AWS Lambda la función que especificó. Si el resultado del manual de procedimientos sugiere validar y configurar la simultaneidad de la función de Lambda, consulte [Invocación asíncrona](#) y [Escalado de funciones de AWS Lambda](#).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LambdaFunctionArn

Tipo: cadena

Descripción: (obligatorio) el ARN de la función de Lambda que activa la notificación de eventos de Amazon S3.

- S3 BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de Amazon S3 cuyas notificaciones de eventos activan la función de Lambda.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- lambda:GetPolicy
- s3:GetBucketNotification

Pasos de documentos

- aws:executeScript: ejecuta el script para validar los ajustes de configuración de la notificación de eventos de Amazon S3. Valida la política de IAM basada en recursos para la función Lambda y genera un comando AWS Command Line Interface (AWS CLI) para añadir los permisos necesarios si faltan los permisos necesarios en la política. Valida las políticas de recursos de otras funciones de Lambda que forman parte de las notificaciones de eventos para el mismo bucket de S3 y genera AWS CLI un comando como resultado si faltan los permisos necesarios.

Salidas

lambdaS3Event.output

Amazon Managed Workflows para Apache Airflow

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Managed Workflows para Apache Airflow. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-TroubleshootMWAAEnvironmentCreation](#)

AWSSupport-TroubleshootMWAAEnvironmentCreation

Descripción

El `AWSSupport-TroubleshootMWAAEnvironmentCreation` manual proporciona información para depurar los problemas de creación del entorno Amazon Managed Workflows for Apache Airflow (Amazon MWAA) y realizar comprobaciones junto con los motivos documentados haciendo todo lo posible para ayudar a identificar el error.

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Recupera los detalles del entorno de Amazon MWAA.
- Verifica los permisos de la función de ejecución.
- Comprueba si el entorno tiene permisos para usar la AWS KMS clave proporcionada para el registro y si existe el grupo de CloudWatch registros requerido.
- Analiza los registros del grupo de registros proporcionado para localizar cualquier error.
- Comprueba la configuración de la red para comprobar si el entorno Amazon MWAA tiene acceso a los puntos de conexión necesarios.
- Genera un informe con los resultados.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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

Instrucciones

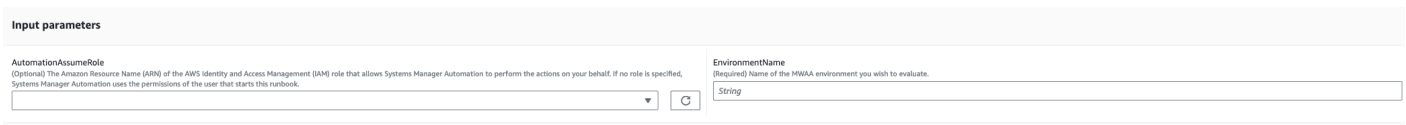
Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootMWAAEnvironmentCreation](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- EnvironmentName (Obligatorio):

Nombre del entorno de Amazon MWAA que desea evaluar.



Input parameters

AutomationAssumeRole	EnvironmentName
(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.	(Required) Name of the MWAA environment you wish to evaluate.

4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:
 - **GetMWAAEnvironmentDetails:**

Recupera los detalles del entorno de Amazon MWAA. Si este paso no funciona, el proceso de automatización se detendrá y aparecerá como. Failed

- **CheckIAMPermissionsOnExecutionRole:**

Verifica que la función de ejecución tenga los permisos necesarios para los recursos de Amazon MWAA, Amazon S3 CloudWatch, CloudWatch Logs y Amazon SQS. Si detecta una clave gestionada por el cliente AWS Key Management Service (AWS KMS), la automatización valida los permisos necesarios de la clave. En este paso, se emplea la `iam:SimulateCustomPolicy` API para determinar si la función de ejecución de la automatización cumple con todos los permisos necesarios.

- **CheckKMSPolicyOnKMSKey:**

Comprueba si la política de AWS KMS claves permite que el entorno MWAA de Amazon utilice la clave para cifrar CloudWatch los registros. Si la AWS KMS clave está AWS gestionada, la automatización omite esta comprobación.

- **CheckIfRequiredLogGroupsExists:**

Comprueba si existen los grupos de CloudWatch registros necesarios para el entorno Amazon MWAA. Si no es así, la automatización comprueba si hay CloudTrail eventos `CreateLogGroup`. `DeleteLogGroup` En este paso también se comprueban los `CreateLogGroup` eventos.

- **BranchOnLogGroupsFindings:**

Las ramificaciones se basan en la existencia de grupos de CloudWatch registros relacionados con el entorno de Amazon MWAA. Si existe al menos un grupo de registros, la automatización lo analiza para localizar los errores. Si no hay ningún grupo de registros, la automatización omite el siguiente paso.

- **CheckForErrorsInLogGroups:**

Analiza los grupos de CloudWatch registros para localizar los errores.

- **GetRequiredEndpointsDetails:**

Recupera los puntos de enlace del servicio utilizados por el entorno Amazon MWAA.

- **CheckNetworkConfiguration:**

Verifica que la configuración de red del entorno Amazon MWAA cumpla con los requisitos, incluidas las comprobaciones de las configuraciones de grupos de seguridad, redes ACLs, subredes y tablas de enrutamiento.

- **CheckEndpointsConnectivity:**

Invoca la automatización `AWSSupport-ConnectivityTroubleshooter` secundaria para validar la conectividad de la MWAA de Amazon con los puntos de conexión necesarios.

- **CheckS3BlockPublicAccess:**

Comprueba si el bucket Amazon S3 del entorno de Amazon MWAA está `Block Public Access` activado y también revisa la configuración general de Amazon S3 Block Public Access de la cuenta.

- **GenerateReport:**

Recopila información de la automatización e imprime el resultado o la salida de cada paso.

7. Una vez completado, revise la sección de resultados para ver los resultados detallados de la ejecución:

- Comprobación de los permisos de ejecución del entorno Amazon MWAA:

Comprueba si la función de ejecución tiene los permisos necesarios para los recursos de Amazon MWAA, Amazon S3 CloudWatch, CloudWatch Logs y Amazon SQS. Si se detecta una AWS KMS clave gestionada por el cliente, la automatización valida los permisos necesarios de la clave.

- Comprobación de la política AWS KMS clave del entorno de Amazon MWAA:

Comprueba si la función de ejecución posee los permisos necesarios para los recursos de Amazon MWAA, Amazon S3 CloudWatch, CloudWatch Logs y Amazon SQS. Además, si se detecta una AWS KMS clave administrada por el cliente, la automatización comprueba los permisos necesarios para la clave.

- Comprobar los grupos de CloudWatch registros del entorno de Amazon MWAA:

Comprueba si existen los grupos de CloudWatch registros necesarios para el entorno Amazon MWAA. Si no es así, la automatización comprueba la ubicación de `CloudTrail CreateLogGroup` los `DeleteLogGroup` eventos.

- Comprobación de las tablas de enrutamiento del entorno Amazon MWAA:

Comprueba si las tablas de enrutamiento de Amazon VPC del entorno Amazon MWAA están configuradas correctamente.

- Comprobación de los grupos de seguridad del entorno Amazon MWAA:

Comprueba si los grupos de seguridad de Amazon VPC del entorno MWAA están configurados correctamente.

- Comprobación de la red del entorno Amazon MWAA: ACLs

Comprueba si los grupos de seguridad de Amazon VPC del entorno de Amazon MWAA están configurados correctamente.

- Comprobación de las subredes del entorno Amazon MWAA:

Comprueba si las subredes del entorno Amazon MWAA son privadas.

- Para comprobar el entorno de Amazon MWAA, se requería la conectividad de los puntos finales:

Verifica si el entorno Amazon MWAA puede acceder a los puntos de enlace necesarios. Para ello, la automatización invoca la automatización. `AWSSupport-ConnectivityTroubleshooter`

- Comprobación del bucket Amazon S3 del entorno MWAA:

Comprueba si el bucket Amazon S3 del entorno de Amazon MWAA está `Block Public Access` activado y también revisa la configuración de Amazon S3 `Block Public Access` de la cuenta.

- La comprobación de los CloudWatch registros del entorno de Amazon MWAA agrupa errores:

Analiza los grupos de CloudWatch registros existentes del entorno Amazon MWAA para localizar los errores.

▼ Outputs

GenerateReportAutomationReport
Troubleshooting report for MWAA environment

🔍 The automation found no issues with the MWAA environment configuration ✓

🔍 Checking the MWAA environment execution role permissions
All the required permissions for the MWAA environment execution role are in place ✓

🔍 Checking the MWAA environment KMS key policy
KMS key is an AWS managed key ✓

🔍 Checking the MWAA environment CloudWatch logs groups
The number of CloudWatch log groups found is 5 and the number of enabled log groups for the MWAA environment is 5. This suggests that all log groups were created successfully ✓

🔍 Checking the MWAA environment Route Tables
NAT GW has Internet route: subnet- → nat- → igw- ✓
NAT GW has Internet route: subnet- → nat- → igw- ✓

🔍 Checking the MWAA environment Security Groups
Security group has self-referencing rules for all traffic. ✓

🔍 Checking the MWAA environment Network ACLs
NACL: allows port 5432 on egress ✓ and allows port 5432 on ingress ✓

🔍 Checking the MWAA environment Subnets
Subnet: subnet- is private ✓
Subnet: subnet- is private ✓

🔍 Checking the MWAA environment required endpoints connectivity

✓ Testing connectivity with sqs.eu-west-1.amazonaws.com:
Connectivity test between ENI- and sqs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the sqs.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with api.ecr.eu-west-1.amazonaws.com:
Connectivity test between ENI- and api.ecr.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.ecr.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with monitoring.eu-west-1.amazonaws.com:
Connectivity test between ENI- and monitoring.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the monitoring.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with kms.eu-west-1.amazonaws.com:
Connectivity test between ENI- and kms.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the kms.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with s3.eu-west-1.amazonaws.com:
Connectivity test between ENI- and s3.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the s3.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI- and env.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI- and env.airflow.eu-west-1.amazonaws.com on port 5432 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with api.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI- and api.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with logs.eu-west-1.amazonaws.com:
Connectivity test between ENI- and logs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the logs.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

✓ Testing connectivity with ops.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI- and ops.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the ops.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: <https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/> region=eu-west-1

🔍 Checking the MWAA environment S3 bucket
Environment's S3 bucket and/or account block public access ✓

🔍 Checking the MWAA environment CloudWatch logs groups errors

Parsed log group	DAGProcessing - no errors found ✓
Parsed log group	Scheduler - no errors found ✓
Parsed log group	Task - no errors found ✓
Parsed log group	WebServer - no errors found ✓
Parsed log group	Worker - no errors found ✓

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

Neptune

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Neptune. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-EnableNeptuneDbAuditLogsToCloudWatch](#)
- [AWS-EnableNeptuneDbBackupRetentionPeriod](#)
- [AWS-EnableNeptuneClusterDeletionProtection](#)

AWS-EnableNeptuneDbAuditLogsToCloudWatch

Descripción

El AWS-EnableNeptuneDbAuditLogsToCloudWatch runbook le ayuda a enviar los registros de auditoría de un clúster de base de datos de Amazon Neptune a Amazon CloudWatch Logs.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `DbClusterResourceId`

Tipo: cadena

Descripción: (obligatorio) El ID de recurso del clúster de base de datos de Neptune para el que desea habilitar los registros de auditoría.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Pasos de documentos

- `GetNeptuneDbClusterIdentifier` (`aws:executeAwsApi`) - Devuelve el ID del clúster de base de datos de Neptune.
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`) - Verifica que el tipo de motor Neptune DB sea. `neptune`
- `EnableNeptuneDbAuditLogs` (`aws:executeAwsApi`) - Permite enviar CloudWatch registros de auditoría para el clúster de base de datos de Neptune.
- `VerifyNeptuneDbStatus` (`aws:waitAwsResourceProperty`) - Verifica que el estado del clúster de base de datos de Neptune sea. `available`
- `VerifyNeptuneDbAuditLogs` (`aws:executeScript`) - Verifica que los registros de auditoría se hayan configurado correctamente para enviarlos a Logs. CloudWatch

AWS-EnableNeptuneDbBackupRetentionPeriod

Descripción

El AWS-EnableNeptuneDbBackupRetentionPeriod runbook le ayuda a habilitar las copias de seguridad automatizadas con un período de retención de las copias de seguridad de entre 7 y 35 días para un clúster de base de datos de Amazon Neptune.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DbClusterResourceId

Tipo: cadena

Descripción: (Obligatorio) El ID de recurso del clúster de base de datos de Neptune para el que desea habilitar las copias de seguridad.

- BackupRetentionPeriod

Tipo: entero

Valores válidos: 7-35

Descripción: (Obligatorio) El número de días que se conservan las copias de seguridad.

- PreferredBackupWindow

Tipo: cadena

Descripción: (opcional) Un período de tiempo diario de al menos 30 minutos para realizar las copias de seguridad. El valor debe estar en hora universal coordinada (UTC) y usar el formato:hh24:mm-hh24:mm. El período de retención de la copia de seguridad no puede entrar en conflicto con el período de mantenimiento preferido.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

Pasos de documentos

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Devuelve el ID del clúster de base de datos de Neptune.
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty) - Verifica que el tipo de motor Neptune DB sea. neptune
- VerifyNeptuneDbStatus (aws:waitAwsResourceProperty) - Verifica que el estado del clúster de base de datos de Neptune sea. available
- ModifyNeptuneDbRetentionPeriod (aws:executeAwsApi) - Establece el período de retención del clúster de base de datos Neptune.
- VerifyNeptuneDbBackupsEnabled (aws:executeScript) - Verifica que el período de retención y la ventana de respaldo se hayan establecido correctamente.

AWS-EnableNeptuneClusterDeletionProtection

Descripción

El `AWS-EnableNeptuneClusterDeletionProtection` runbook permite la protección contra la eliminación del clúster de Amazon Neptune que especifique.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `DbClusterResourceId`

Tipo: cadena

Descripción: (Obligatorio) El ID del clúster de Neptune en el que desea habilitar la protección contra la eliminación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`

- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Pasos de documentos

- `GetNeptuneDbClusterIdentifier` (`aws:executeAwsApi`) - Devuelve el ID del clúster de base de datos de Neptune.
- `VerifyNeptuneDbEngine` (`aws:assertAwsResourceProperty`) - Verifica el tipo de motor del clúster de base de datos especificado. `neptune`
- `VerifyNeptuneStatus` (`aws:waitForAwsResourceProperty`) - Verifica que el estado del clúster sea. `available`
- `EnableNeptuneDbDeletionProtection` (`aws:executeAwsApi`) - Activa la protección contra la eliminación en el clúster de base de datos Neptune.
- `VerifyNeptuneDbDeletionProtection` (`aws:assertAwsResourceProperty`) - Verifica que la protección contra la eliminación esté habilitada en el clúster de base de datos.

Salidas

- `EnableNeptuneDbDeletionProtection`. `EnableNeptuneDbDeletionProtectionResponse` - El resultado de la operación de la API.

Amazon RDS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Relational Database Service. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-CreateEncryptedRdsSnapshot](#)

- [AWS-CreateRdsSnapshot](#)
- [AWSConfigRemediation-DeleteRDSCluster](#)
- [AWSConfigRemediation-DeleteRDSClusterSnapshot](#)
- [AWSConfigRemediation-DeleteRDSInstance](#)
- [AWSConfigRemediation-DeleteRDSInstanceSnapshot](#)
- [AWSConfigRemediation-DisablePublicAccessToRDSInstance](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster](#)
- [AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance](#)
- [AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance](#)
- [AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance](#)
- [AWSConfigRemediation-EnableMultiAZOnRDSInstance](#)
- [AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance](#)
- [AWSConfigRemediation-EnableRDSClusterDeletionProtection](#)
- [AWSConfigRemediation-EnableRDSInstanceBackup](#)
- [AWSConfigRemediation-EnableRDSInstanceDeletionProtection](#)
- [AWSConfigRemediation-ModifyRDSInstancePortNumber](#)
- [AWSSupport-ModifyRDSSnapshotPermission](#)
- [AWSPremiumSupport-PostgreSQLWorkloadReview](#)
- [AWS-RebootRdsInstance](#)
- [AWSSupport-ShareRDSSnapshot](#)
- [AWS-StartRdsInstance](#)
- [AWS-StartStopAuroraCluster](#)
- [AWS-StopRdsInstance](#)
- [AWSSupport-TroubleshootConnectivityToRDS](#)
- [AWSSupport-TroubleshootRDSIAMAuthentication](#)
- [AWSSupport-ValidateRdsNetworkConfiguration](#)

AWS-CreateEncryptedRdsSnapshot

Descripción

El AWS-CreateEncryptedRdsSnapshot runbook crea una instantánea cifrada a partir de una instancia no cifrada de Amazon Relational Database Service (Amazon RDS).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DBInstanceIdentificador

Tipo: cadena

Descripción: (obligatorio) El ID de la instancia de Amazon RDS de la que desea crear una instantánea.

- DBSnapshotIdentificador

Tipo: cadena

Descripción: (opcional) La plantilla de nombres de la instantánea de Amazon RDS. La plantilla de nombres predeterminada es *DBInstanceIdentifier-yyyymmddhhmmss*.

- DBSnapshotIdentificador cifrado

Tipo: cadena

Descripción: (opcional) Nombre de la instantánea cifrada. El nombre predeterminado es el valor que especifique para el `DBSnapshotIdentifier` parámetro adjunto. `-encrypted`

- `InstanceTags`

Tipo: cadena

Descripción: etiquetas (opcionales) para añadir a la instancia de base de datos. (Ejemplo: `key=tagkey1, value=tagvalue1; key=tagkey2, value=tagValue2`) '

- `KmsKeyId`

Tipo: cadena

Valor predeterminado: `alias/aws/rds`

Descripción: (opcional) El ARN, el identificador de clave o el alias de la clave gestionada por el cliente que desee utilizar para cifrar la instantánea.

- `SnapshotTags`

Tipo: cadena

Descripción: (opcional) Etiquetas para añadir a la instantánea. (Ejemplo: `key=tagKey1, value=tagValue1; key=TagKey2, value=tagValue2`) '

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds>CreateDBSnapshot`
- `rds>DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Pasos de documentos

- `aws:executeScript`- Crea una instantánea de la instancia de base de datos que especifique en el parámetro. `DBInstanceIdentifier`
- `aws:executeScript`- Comprueba que la instantánea creada en el paso anterior existe y `existeavailable`.
- `aws:executeScript`- Copia la instantánea creada anteriormente en una instantánea cifrada.
- `aws:executeScript`- Verifica la existencia de la instantánea cifrada creada en el paso anterior.

Salidas

`CopyRdsSnapshotToEncryptedRdsSnapshot`. `EncryptedSnapshotId` - El ID de la instantánea cifrada de Amazon RDS.

AWS-CreateRdsSnapshot

Descripción

Crea una instantánea de Amazon Relational Database Service (Amazon RDS) de una instancia de Amazon RDS.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DBInstanceIdentificador

Tipo: cadena

Descripción: (obligatorio) El DBInstance ID de la instancia de RDS desde la que se va a crear la instantánea.

- DBSnapshotIdentificador

Tipo: cadena

Descripción: (opcional) El DBSnapshot identificador de la instantánea de RDS que se va a crear.

- InstanceTags

Tipo: cadena

Descripción: (opcional) etiquetas que se van a crear para la instancia.

- SnapshotTags

Tipo: cadena

Descripción: (opcional) etiquetas que se van a crear para la instantánea.

Pasos de documentos

crearRDSSnapshot : crea la instantánea de RDS y devuelve el ID de la instantánea.

verificarRDSSnapshot : comprueba que existe la instantánea creada en el paso anterior.

Salidas

crearRDSSnapshot. SnapshotId — El ID de la instantánea creada.

AWSConfigRemediation-DeleteRDSCluster

Descripción

El AWSConfigRemediation-DeleteRDSCluster runbook elimina el clúster de Amazon Relational Database Service (Amazon RDS) que especifique. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DBClusterID

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos del clúster de base de datos en el que desea habilitar la protección contra la eliminación.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds>DeleteDBCluster
- rds>DeleteDBInstance
- rds:DescribeDBClusters

Pasos de documentos

- `aws:executeScript`: elimina el clúster de base de datos que especifique en el parámetro `DBClusterId`.

AWSConfigRemediation-DeleteRDSClusterSnapshot

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteRDSClusterSnapshot` elimina la instantánea del clúster de Amazon Relational Database Service (Amazon RDS) determinada.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `DBClusterSnapshotId`

Tipo: cadena

Descripción: (obligatorio) el identificador de la instantánea del clúster de Amazon RDS que se va a eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

Pasos de documentos

- `aws:branch`: comprueba si la instantánea del clúster está en estado `available`. Si no está disponible, el flujo finaliza.
- `aws:executeAwsApi`: elimina la instantánea de clúster de Amazon RDS determinada mediante el identificador de la instantánea del clúster de la base de datos (DB).
- `aws:executeScript`: verifica que se haya eliminado la instantánea determinada del clúster de Amazon RDS.

AWSConfigRemediation-DeleteRDSInstance

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteRDSInstance` elimina la instancia de Amazon Relational Database Service (Amazon RDS) que especifique. Al eliminar una instancia de base de datos (DB), se eliminan todas las copias de seguridad automatizadas para esa instancia y no se pueden recuperar. Las instantáneas DB manuales no se eliminan. Si la instancia de base de datos que desea eliminar se encuentra en estado `failed`, `incompatible-network` o `incompatible-restore`, debe establecer el parámetro `SkipFinalSnapshot` en `true`.

Note

Si la instancia de base de datos que desea eliminar está en un clúster de base de datos de Amazon Aurora, el manual de procedimientos no eliminará la instancia de base de datos si es una réplica de lectura y la única instancia del clúster de base de datos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DbResourceId

Tipo: cadena

Descripción: (obligatorio) el identificador de recurso de la instancia de base de datos que desea eliminar.

- SkipFinalSnapshot

Tipo: Booleano

Predeterminado: false

Descripción: (opcional) si se establece en true, no se crea una instantánea final antes de eliminar la instancia de base de datos.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds>DeleteDBInstance`
- `rds:DescribeDBInstances`

Pasos de documentos

- `aws:executeAwsApi`: recopila el nombre de la instancia de base de datos a partir del valor que especifique en el parámetro `DbiResourceId`.
- `aws:branch`: se ramifica en función del valor que especifique en el parámetro `SkipFinalSnapshot`.
- `aws:executeAwsApi`: elimina la instancia de base de datos que especifique en el parámetro `DbiResourceId`.
- `aws:executeAwsApi`: elimina la instancia de base de datos que especifique en el parámetro `DbiResourceId` una vez creada la instantánea final.
- `aws:assertAwsResourceProperty`: verifica que la instancia de base de datos se haya eliminado.

AWSConfigRemediation-DeleteRDSInstanceSnapshot

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteRDSInstanceSnapshot` elimina la instantánea de la instancia de Amazon Relational Database Service (Amazon RDS) que especifique. Solo se eliminan las instantáneas que estén en estado `available`. Este manual de procedimientos no admite la eliminación de instantáneas de las instancias de bases de datos de Amazon Aurora.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DbSnapshotId

Tipo: cadena

Descripción: (obligatorio) ID de la instantánea que quiere eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds>DeleteDBSnapshot
- rds:DescribeDBSnapshots

Pasos de documentos

- aws:executeAwsApi: recopila el estado de la instantánea especificada en el parámetro DbSnapshotId.
- aws:assertAwsResourceProperty: confirma que el estado de la instantánea es available.
- aws:executeAwsApi: elimina la instantánea especificada en el parámetro DbSnapshotId.
- aws:executeScript: verifica que se haya eliminado la instantánea.

AWSConfigRemediation-DisablePublicAccessToRDSInstance

Descripción

El manual de procedimientos AWSConfigRemediation-DisablePublicAccessToRDSInstance deshabilita la accesibilidad pública de la instancia de base de datos (DB) de Amazon Relational Database Service (Amazon RDS) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DbiResourceId

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos para la que desea deshabilitar la accesibilidad pública.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: verifica que las instancias de base de datos estén en un estado AVAILABLE.
- `aws:executeAwsApi`: deshabilita la accesibilidad pública en su instancia de base de datos.
- `aws:waitForAwsResourceProperty`: espera a que la instancia de base de datos cambie al estado MODIFYING.
- `aws:waitForAwsResourceProperty`: espera a que la instancia de base de datos cambie al estado AVAILABLE.
- `aws:assertAwsResourceProperty`: confirma que la accesibilidad pública está deshabilitada en la instancia de base de datos.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` habilita la configuración `CopyTagsToSnapshot` del clúster de Amazon Relational Database Service (Amazon RDS) que especifique. Al habilitar esta configuración, se copian todas las etiquetas del clúster de base de datos en instantáneas del clúster de base de datos. El valor predeterminado es no copiarlos. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- `ApplyImmediately`

Tipo: Booleano

Predeterminado: `false`

Descripción: (opcional) si especifica `true` para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente del valor de `PreferredMaintenanceWindow` del clúster de base de datos.

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `DbClusterResourceId`

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos del clúster de base de datos en el que desea habilitar la configuración `CopyTagsToSnapshot`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador del clúster de base de datos a partir del identificador de recursos del clúster de base de datos.
- `aws:assertAwsResourceProperty`: confirma que el clúster de base de datos está en un estado AVAILABLE.
- `aws:executeAwsApi`: activa la configuración CopyTagsToSnapshot en su clúster de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la configuración CopyTagsToSnapshot está habilitada en su clúster de base de datos.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

Descripción

El manual de procedimientos AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance habilita la configuración CopyTagsToSnapshot en la instancia de Amazon Relational Database Service (Amazon RDS) que especifique. Al habilitar esta configuración, se copian todas las etiquetas de la instancia de base de datos en instantáneas de la instancia de base de datos. La opción predeterminada es no copiarlos. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- `ApplyImmediately`

Tipo: Booleano

Predeterminado: `false`

Descripción: (opcional) si especifica `true` para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente de la configuración de `PreferredMaintenanceWindow` de la instancia DB.

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `DbiResourceId`

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos en la que desea habilitar la configuración `CopyTagsToSnapshot`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la instancia de base de datos está en estado AVAILABLE.
- `aws:executeAwsApi`: activa la configuración CopyTagsToSnapshot en su instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la configuración CopyTagsToSnapshot está habilitada en su instancia de base de datos.

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

Descripción

El manual de procedimientos AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance permite la monitorización mejorada en la instancia de base de datos de Amazon RDS que especifique. Para obtener información sobre la monitorización mejorada, consulte la [Monitorización mejorada](#) en la Guía del usuario de Amazon RDS.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- MonitoringInterval

Tipo: entero

Valores válidos: 1 | 5 | 10 | 15 | 30 | 60

Descripción: (obligatorio) el intervalo en segundos en el que se recopilan las métricas de supervisión mejoradas de la instancia de base de datos.

- MonitoringRoleArn

Tipo: cadena

Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) de la función de IAM que permite a Amazon RDS enviar métricas de monitorización mejorada a Amazon Logs. CloudWatch

- ResourceId

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos en la que desea activar la supervisión mejorada.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la instancia de base de datos está en estado AVAILABLE.
- `aws:executeAwsApi`: permite una supervisión mejorada en su instancia de base de datos.
- `aws:executeScript`: confirma que la supervisión mejorada está habilitada en su instancia de base de datos.

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance

Descripción

El manual de procedimientos AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS habilita la configuración AutoMinorVersionUpgrade en la instancia de base de datos de Amazon RDS que especifique. Habilitar esta opción indica que las actualizaciones de versión secundarias se aplican automáticamente a la instancia de base de datos durante el periodo de mantenimiento.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `DbiResourceId`

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos que desea configurar `AutoMinorVersionUpgrade`.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la instancia de base de datos está en estado `AVAILABLE`.
- `aws:executeAwsApi`: activa la configuración `AutoMinorVersionUpgrade` en su instancia de base de datos.
- `aws:executeScript`: confirma que la configuración `AutoMinorVersionUpgrade` está habilitada en su instancia de base de datos.

AWSConfigRemediation-EnableMultiAZOnRDSInstance

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableMultiAZOnRDSInstance` cambia su instancia de base de datos (DB) de Amazon Relational Database Service (Amazon RDS) a una implementación multi-AZ. Cambiar este ajuste no produce una interrupción. El cambio se aplicará durante el siguiente período de mantenimiento, salvo que el parámetro `ApplyImmediately` esté establecido en `true`.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `ApplyImmediately`

Tipo: Booleano

Predeterminado: `false`

Descripción: (opcional) si especifica `true` para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente de la configuración de `PreferredMaintenanceWindow` de la instancia DB.

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `DbiResourceId`

Tipo: cadena

Descripción: (obligatorio) El identificador Región de AWS Único e inmutable de la instancia de base de datos para habilitar la configuración. MultiAZ

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Pasos de documentos

- `aws:executeAwsApi`: recupera el nombre de la instancia de base de datos mediante el valor proporcionado en el parámetro `DBInstanceId`.
- `aws:executeAwsApi`: verifica que `DBInstanceStatus` esté `available`.
- `aws:branch`: comprueba si `MultiAZ` ya está establecido `true` en la instancia de base de datos que especifique en el parámetro `DbiResourceId`.
- `aws:executeAwsApi`: cambia la configuración `MultiAZ` a `true` en la instancia de base de datos que especifique en el parámetro `DbiResourceId`.
- `aws:assertAwsResourceProperty`: verifica que `MultiAZ` esté configurado como `true` en la instancia de base de datos que especifique en el parámetro `DbiResourceId`.

AWSConfigRemediation- EnablePerformanceInsightsOnRDSInstance

Descripción

El manual de procedimientos `AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance` habilita Performance Insights en la instancia de base de datos de Amazon RDS que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DbiResourceId

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos en la que desea habilitar Performance Insights.

- PerformanceInsightsKMSKeyId

Tipo: cadena

Valor predeterminado: `alias/aws/rds`

Descripción: (opcional) El nombre del recurso de Amazon (ARN), el identificador de clave o el alias clave de la AWS Key Management Service (AWS KMS) clave gestionada por el cliente que desea que Performance Insights utilice para cifrar todos los datos potencialmente confidenciales. Si introduce el alias de la clave para este parámetro, ponga el prefijo **alias/** al valor. Si no especifica un valor para este parámetro, Clave administrada de AWS se utiliza el.

- PerformanceInsightsRetentionPeriod

Tipo: entero

Valores válidos: 7, 731

Valor predeterminado: 7

Descripción (opcional): el número de días durante los que se retienen los datos de Información de rendimiento.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que el estado de la instancia de base de datos sea `available`.
- `aws:executeAwsApi`- Recopila el ARN de la clave gestionada AWS KMS por el cliente especificada en `PerformanceInsightsKMSKeyId` el parámetro.
- `aws:branch`: comprueba si ya hay un valor asignado a la propiedad `PerformanceInsightsKMSKeyId` de la instancia de base de datos.
- `aws:executeAwsApi`: habilita Performance Insights en la instancia de base de datos que especifique en el parámetro `DbiResourceId`.
- `aws:assertAwsResourceProperty`: confirma que el valor especificado para el parámetro `PerformanceInsightsKMSKeyId` se utilizó para habilitar el cifrado de Performance Insights en la instancia de base de datos.

- `aws:assertAwsResourceProperty`: confirma que Performance Insights está habilitado en la instancia de base de datos.

AWSConfigRemediation-EnableRDSClusterDeletionProtection

Descripción

El `AWSConfigRemediation-EnableRDSClusterDeletionProtection` runbook permite la protección contra la eliminación en el clúster de Amazon Relational Database Service (Amazon RDS) que especifique. AWS Config debe estar habilitado en el Región de AWS lugar donde se ejecuta esta automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `ClusterId`

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos del clúster de base de datos en el que desea habilitar la protección contra la eliminación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Pasos de documentos

- `aws:executeAwsApi`: recopila el nombre del clúster de base de datos a partir del identificador de recursos del clúster de base de datos.
- `aws:assertAwsResourceProperty`: verifica que el estado del clúster de base de datos sea `available`.
- `aws:executeAwsApi`: activa la protección contra la eliminación en el clúster de base de datos que especifique en el parámetro `ClusterId`.
- `aws:assertAwsResourceProperty`: verifica que la protección contra la eliminación esté habilitada en el clúster de base de datos.

AWSConfigRemediation-EnableRDSInstanceBackup

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRDSInstanceBackup` permite realizar copias de seguridad para la instancia de base de datos de Amazon Relational Database Service (Amazon RDS) que especifique. Este manual de procedimientos no admite la habilitación de copias de seguridad para las instancias de bases de datos de Amazon Aurora.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- ApplyImmediately

Tipo: Booleano

Predeterminado: false

Descripción: (opcional) si especifica true para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente de la configuración de PreferredMaintenanceWindow de la instancia DB.

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BackupRetentionPeriod

Tipo: entero

Valores válidos: 1-35

Descripción: (obligatorio) el número de días que se conservan las copias de seguridad.

- DbInstanceIdentifier

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos para la que desea habilitar las copias de seguridad.

- PreferredBackupWindow

Tipo: cadena

Descripción: (opcional) el intervalo de tiempo diario (en UTC) durante el cual se crean las copias de seguridad.

Restricciones:

- Tiene que tener el formato hh24:mi-hh24:mi
- Debe estar en tiempo universal coordinado (UTC)
- No debe entrar en conflicto con la ventana de mantenimiento preferida.
- Debe durar al menos 30 minutos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeScript`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos. Habilita las copias de seguridad para su instancia de base de datos. Confirma que las copias de seguridad estén habilitadas en la instancia de base de datos.

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRDSInstanceDeletionProtection` permite la protección contra la eliminación en la instancia de base de datos de Amazon RDS que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- `ApplyImmediately`

Tipo: Booleano

Predeterminado: `false`

Descripción: (opcional) si especifica `true` para este parámetro, las modificaciones de esta solicitud y todas las modificaciones pendientes se asignan de manera asincrónica en cuanto sea posible, independientemente de la configuración de `PreferredMaintenanceWindow` de la instancia DB.

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `DbInstanceResourceId`

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos en la que desea habilitar la protección contra la eliminación.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Pasos de documentos

- `aws:executeAwsApi`: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- `aws:executeAwsApi`: activa la protección contra la eliminación en su instancia de base de datos.
- `aws:assertAwsResourceProperty`: confirma que la protección contra la eliminación está habilitada en la instancia de base de datos.

AWSConfigRemediation-ModifyRDSInstancePortNumber

Descripción

El manual de procedimientos `AWSConfigRemediation-ModifyRDSInstancePortNumber` modifica el número de puerto en el que la instancia de Amazon Relational Database Service (Amazon RDS) acepta conexiones. Al ejecutar esta automatización se reiniciará la base de datos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- PortNumber

Tipo: cadena

Descripción: (opcional) el número de puerto en el que desea que la instancia de base de datos acepte conexiones.

- RDSDBInstanceResourceId

Tipo: cadena

Descripción: (obligatorio) el identificador de recursos de la instancia de base de datos cuyo número de puerto de entrada desea modificar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

Pasos de documentos

- aws:executeAwsApi: recopila el identificador de la instancia de base de datos a partir del identificador de recursos de la instancia de base de datos.
- aws:assertAwsResourceProperty: confirma que la instancia de base de datos está en estado AVAILABLE.
- aws:executeAwsApi: modifica el número de puerto de entrada en el que la instancia de base de datos acepta conexiones.

- `aws:waitForAwsResourceProperty`: espera a que la instancia de base de datos esté en estado `MODIFYING`.
- `aws:waitForAwsResourceProperty`: espera a que la instancia de base de datos esté en estado `AVAILABLE`.

AWSSupport-ModifyRDSSnapshotPermission

Descripción

El manual de procedimientos `AWSSupport-ModifyRDSSnapshotPermission` le ayuda a modificar permisos para varias instantáneas de Amazon Relational Database Service (Amazon RDS). Con este manual de procedimientos, puede crear instantáneas `Public` o `Private` y compartirlas con otras Cuentas de AWS. Las instantáneas cifradas con una clave de KMS predeterminada no se pueden compartir con otras cuentas que utilicen este manual de procedimientos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AccountIds

Tipo: StringList

Predeterminado: none

Descripción: (opcional) Las IDs cuentas con las que quieres compartir las instantáneas. Este parámetro es obligatorio si especifica un valor No para el parámetro Private.

- AccountPermissionOperation

Tipo: cadena

Valores válidos: add | remove

Predeterminado: none

Descripción: (opcional) el tipo de operación que se va a realizar.

- Private

Tipo: cadena

Valores válidos: Yes | No

Descripción: (obligatorio) introduzca No para el valor si desea compartir instantáneas con cuentas específicas.

- SnapshotIdentifiers

Tipo: StringList

Descripción: (obligatorio) los nombres de las instantáneas de Amazon RDS cuyo permiso desea modificar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBSnapshots

- `rds:ModifyDBSnapshotAttribute`

Pasos de documentos

1. `aws:executeScript`- Verifica IDs las instantáneas proporcionadas en el parámetro. `SnapshotIdentifiers` Tras verificarlas IDs, el script comprueba si hay instantáneas cifradas y genera una lista si encuentra alguna.
2. `aws:branch`: ramifica la automatización en función del valor que introduzca para el parámetro `Private`.
3. `aws:executeScript`: modifica los permisos de las instantáneas especificadas para compartirlas con las cuentas especificadas.
4. `aws:executeScript`: modifica los permisos de las instantáneas para cambiarlos de `Public` a `Private`.

Salidas

`ValidateSnapshots.EncryptedSnapshots`

`SharewithOtherAccounts.Resultado`

`MakePrivate.Resultado`

`MakePrivate.Comandos`

AWSPremiumSupport-PostgreSQLWorkloadReview

Descripción

El manual de procedimientos `AWSPremiumSupport-PostgreSQLWorkloadReview` captura varias instantáneas de las estadísticas de uso de base de datos de PostgreSQL de Amazon Relational Database Service (Amazon RDS). Las estadísticas recopiladas son necesarias para que un experto de Soporte [Proactive Services](#) realice una revisión operativa. Las estadísticas se recopilan mediante un conjunto de scripts SQL y de intérprete de comandos personalizados. Estos scripts se descargan en una instancia temporal de Amazon Elastic Compute Cloud (Amazon EC2) creada por este runbook. Cuenta de AWS El manual de procedimientos requiere que proporcione credenciales mediante un secreto AWS Secrets Manager que contenga un par de clave-valor de

nombre de usuario y contraseña. El nombre de usuario debe tener permisos para consultar las vistas y funciones de estadísticas estándar de PostgreSQL.

Este manual crea automáticamente los siguientes AWS recursos Cuenta de AWS mediante una pila. AWS CloudFormation Puede supervisar la creación de la pila mediante la consola CloudFormation .

- Una nube privada virtual (VPC) y una instancia de Amazon EC2 lanzadas en una subred privada de VPC con conectividad opcional a Internet mediante una puerta de enlace NAT.
- Un rol AWS Identity and Access Management (IAM) asociado a la instancia temporal de Amazon EC2 con permisos para recuperar el valor secreto de Secrets Manager. El rol también proporciona permisos para cargar archivos en un bucket de Amazon Simple Storage Service (Amazon S3) que elija y, opcionalmente, en un caso. Soporte
- Una conexión de emparejamiento de VPC para permitir la conectividad entre la instancia de base de datos y la instancia temporal de Amazon EC2.
- Puntos de conexión de VPC Systems Manager, Secrets Manager y Amazon S3 que están conectados a la VPC temporal.
- Un período de mantenimiento con tareas registradas que inician y detienen periódicamente la instancia temporal de Amazon EC2, ejecutan scripts de recopilación de datos y suben archivos a un bucket de Amazon S3. También se crea un rol de IAM para la ventana de mantenimiento que proporciona permisos para realizar las tareas registradas.

Cuando se complete el runbook, se eliminará la CloudFormation pila que se utilizó para crear los AWS recursos necesarios y el informe se cargará en el bucket de Amazon S3 que elija y, opcionalmente, en un Soporte caso.

Note

De forma predeterminada, se conserva el volumen raíz de Amazon EBS de la instancia temporal de Amazon EC2. Puede invalidar esta configuración seleccionando el `EbsVolumeDeleteOnTermination` con el parámetro `true`.

Requisitos previos

- Suscripción a Enterprise Support Este manual de procedimientos y los diagnósticos y revisiones de la carga de trabajo de Proactive Services requieren una suscripción a Enterprise Support. Antes de utilizar este manual de procedimientos, póngase en contacto con su administrador técnico de

cuentas (TAM) o con un especialista en TAM (STAM) para obtener instrucciones. Para obtener más información, consulte [Servicios proactivos de Soporte](#).

- Cuenta y Región de AWS cuotas Asegúrese de no haber alcanzado el número máximo de instancias de Amazon EC2 o de crearlas en la cuenta y la región en las VPCs que utiliza este runbook. Si necesita solicitar un aumento de los límites, utilice el [formulario de aumento de los límites de servicio](#).
- Configuración de las bases de datos
 1. La base de datos que especifique en el parámetro DatabaseName debe tener la extensión `pg_stat_statements` configurada. Si no ha configurado `pg_stat_statements` en `shared_preload_libraries`, debe editar el valor en el grupo de parámetros de base de datos y aplicar los cambios. Los cambios en el parámetro `shared_preload_libraries` requieren que reinicie su instancia de base de datos. Para obtener más información, consulte [Trabajo con los grupos de parámetros](#). Si se añade `pg_stat_statements` a `shared_preload_libraries`, se añadirá cierta sobrecarga de rendimiento. Sin embargo, esto es útil para realizar un seguimiento del rendimiento de las declaraciones individuales. Para obtener más información acerca de la extensión `pg_stat_statements`, consulte la [documentación de PostgreSQL](#). Si no configura la extensión `pg_stat_statements` o si la extensión no está presente en la base de datos que se utiliza para la recopilación de estadísticas, el análisis a nivel de declaración no se presentará en la revisión operativa.
 2. Asegúrese de que los parámetros `track_counts` y `track_activities` no estén desactivados. Si estos parámetros están desactivados en el grupo de parámetros de la base de datos, no habrá estadísticas significativas disponibles. Para cambiar estos parámetros, deberá reiniciar su instancia de base de datos. Para obtener más información, consulte [Uso de parámetros en su instancia de base de datos de Amazon RDS para PostgreSQL](#).
 3. Si el `track_io_timing` parámetro está desactivado, las estadísticas de I/O nivel no se incluirán en la revisión operativa. El cambio `track_io_timing` requerirá reiniciar la instancia de base de datos y generará una sobrecarga de rendimiento adicional en función de la carga de trabajo de la instancia de base de datos. A pesar de la sobrecarga de rendimiento de las cargas de trabajo críticas, este parámetro proporciona información útil relacionada con el I/O tiempo por consulta.

Facturación y cargos Se le Cuenta de AWS cobrarán los costos asociados a la instancia temporal de Amazon EC2, el volumen de Amazon EBS asociado, la puerta de enlace NAT y los datos transferidos durante la ejecución de esta automatización. De forma predeterminada, este manual de

procedimientos crea una instancia de `t3.micro` Amazon Linux 2 para recopilar las estadísticas. El manual de procedimientos inicia y detiene la instancia entre los pasos para reducir los costos.

Seguridad y gobernanza de datos Este manual de procedimientos recopila estadísticas consultando las vistas y funciones estadísticas de [PostgreSQL](#). Asegúrese de que las credenciales proporcionadas en el parámetro `SecretId` solo concedan permisos de solo lectura para las vistas y funciones de estadísticas. Como parte de la automatización, los scripts de recopilación se cargan en su bucket de Amazon S3 y se pueden encontrar en `s3://amzn-s3-demo-bucket/automation execution id/queries/`.

Estos scripts recopilan datos que un AWS especialista utiliza para revisar los indicadores clave de rendimiento a nivel de objeto. El script recopila información como el nombre de la tabla, el nombre del esquema y el nombre del índice. Si parte de esta información contiene información confidencial, como indicadores de ingresos, nombre de usuario, dirección de correo electrónico o cualquier otra información de identificación personal, le recomendamos que deje de revisar la carga de trabajo. Póngase en contacto con su AWS TAM para analizar un enfoque alternativo para la revisión de la carga de trabajo.

Asegúrese de contar con la aprobación y la autorización necesarias para compartir con usted las estadísticas y los metadatos recopilados por esta automatización AWS.

Consideraciones de seguridad Si establece el parámetro `UpdateRdsSecurityGroup` en `yes`, el manual de procedimientos actualiza el grupo de seguridad asociado a la instancia de base de datos para permitir el tráfico entrante desde la dirección IP privada de la instancia temporal de Amazon EC2.

Si establece el parámetro `UpdateRdsRouteTable` en `yes`, el manual de procedimientos actualiza la tabla de enrutamiento asociada a la subred en la que se ejecuta su instancia de base de datos para permitir el tráfico a la instancia temporal de Amazon EC2 a través de la conexión de emparejamiento de VPC.

Creación de usuarios Para permitir que el script de recopilación se conecte a su base de datos de Amazon RDS, debe configurar un usuario con permisos para leer las vistas de las estadísticas. Debe almacenar estas credenciales en Secrets Manager. Recomendamos crear un nuevo usuario dedicado para esta automatización. La creación de un usuario independiente le permite auditar y realizar un seguimiento de las actividades realizadas por esta automatización.

1. Cree un nuevo usuario.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. Asegúrese de que este usuario solo pueda realizar conexiones de solo lectura.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. Establezca límites a nivel de usuario.

```
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. Conceda permisos `pg_monitor` al nuevo usuario para que pueda acceder a las estadísticas de la base de datos. (El rol `pg_monitor` es miembro de `pg_read_all_settings`, `pg_read_all_stats` y `pg_stat_scan_table`.)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

Permisos añadidos al perfil de instancia temporal de Amazon EC2 por esta automatización de Systems Manager. Los siguientes permisos se añaden al rol de IAM asociado a la instancia temporal de Amazon EC2. La política `AmazonSSMManagedInstanceCore` gestionada también está asociada al rol de IAM para permitir que Systems Manager gestione la instancia de Amazon EC2.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeTags"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/automation-execution-  
id/*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-  
east-1:111122223333:secret:secret-id",
    "Effect": "Allow"
  },
  {
    "Action": [
      "support:AddAttachmentsToSet",
      "support:AddCommunicationToCase",
      "support:DescribeCases"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
]
}

```

Permisos agregados a la ventana de mantenimiento temporal por esta automatización de Systems Manager. Los siguientes permisos se agregan automáticamente al rol de IAM asociado a las tareas.

de mantenimiento de Windows. Las tareas de mantenimiento de Windows inician, detienen y envían comandos a la instancia temporal de Amazon EC2.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:GetAutomationExecution",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation",
        "ssm:GetCalendarState",
        "ssm:CancelCommand",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ssm:SendCommand",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ssm:StartAutomationExecution"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/temporary-instance-  
id",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:111122223333:automation-execution/*"
      ],
      "Effect": "Allow"
    },
    {
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ssm.amazonaws.com"
        }
      },

```

```
        "ArnLike": {
            "iam:AssociatedResourceARN": "arn:aws:ssm:*:*:document/AWS-*"
        },
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::111122223333:role/SSM-*",
        "Effect": "Allow"
    }
}
```

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DBInstanceIdentificador

Tipo: cadena

Descripción: (obligatorio) ID de la instancia DB.

- DatabaseName

Tipo: cadena

Descripción: (obligatorio) el nombre de la base de datos alojada en su instancia de base de datos.

- SecretId

Tipo: cadena

Descripción: (obligatorio) el ARN de su secreto de Secrets Manager que contenga un par de clave-valor de nombre de usuario y contraseña. La CloudFormation pila crea una política de IAM con permisos para la GetSecretValue operación en este ARN. Las credenciales se utilizan para permitir que la instancia temporal recopile las estadísticas de la base de datos. Póngase en contacto con su TAM o STAM para hablar sobre los permisos mínimos requeridos.

- Acknowledge

Tipo: cadena

Descripción: (obligatorio) introduzca **yes** si reconoce que este manual de procedimientos creará recursos temporales en su cuenta para recopilar estadísticas de su instancia de base de datos. Le recomendamos que se ponga en contacto con su TAM o STAM antes de ejecutar esta automatización.

- SupportCase

Tipo: cadena

Descripción: (opcional) El número de Soporte caso proporcionado por su TAM o STAM. Si se proporciona, el manual de procedimientos actualiza el caso y adjunta los datos recopilados. Esta opción requiere que la instancia temporal de Amazon EC2 tenga conectividad a Internet para acceder al punto final de la Soporte API. El parámetro AllowVpcInternetAccess debe estar establecido en true. El asunto del caso debe contener la frase AWSPremiumSupport-PostgreSQLWorkloadReview.

- S3 BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de Amazon S3 de su cuenta en la que desea cargar los datos recopilados por la automatización. Verifique que la política del bucket no conceda permisos de lectura o escritura innecesarios a las entidades principales que no necesiten acceso al contenido del bucket. Recomendamos crear un nuevo bucket temporal de Amazon S3 para

esta automatización. El manual de procedimientos proporciona permisos para la operación API de `s3:PutObject` al rol de IAM asociado a la instancia de Amazon EC2 temporal. Los archivos cargados se ubicarán en `s3://bucket name/automation execution id/`.

- `InstanceType`

Tipo: cadena

Descripción: (opcional) el tipo de instancia temporal de Amazon EC2 que ejecutará los scripts SQL y de intérprete de comandos personalizados.

Valores válidos: `t2.micro` | `t2.small` | `t2.medium` | `t2.large` | `t3.micro` | `t3.small` | `t3.medium` | `t3.large`

Valor predeterminado: `t3.micro`

- `VpcCidr`

Tipo: cadena

Descripción: (opcional) el rango de dirección IP en notación CIDR para la nueva VPC (por ejemplo, `172.31.0.0/16`). Asegúrese de seleccionar un CIDR que no se superponga ni coincida con ninguna VPC existente con conectividad a su instancia de base de datos. La VPC más pequeña que puede crear utiliza una máscara de subred `/28` y la VPC mayor utiliza una máscara de subred `/16`.

Valor predeterminado: `172.31.0.0/16`

- `StackResourcesNamePrefix`

Tipo: cadena

Descripción: (opcional) El nombre, el prefijo y la etiqueta de los recursos de la CloudFormation pila. El manual crea los recursos de la CloudFormation pila utilizando este prefijo como parte del nombre y la etiqueta que se aplican a los recursos. La estructura del par clave-valor de etiqueta es `StackResourcesNamePrefix:{{automation:EXECUTION_ID}}`.

Predeterminado: Revisar `AWSPostgre SQLWorkload`

- `Schedule`

Tipo: cadena

Descripción: (opcional) el horario del período de mantenimiento. Especifica la frecuencia con la que la ventana de mantenimiento ejecuta las tareas. El valor predeterminado es `1 hour`.

Valores válidos: 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 12 hours | 1 day | 2 days | 4 days

Valor predeterminado: 1 hora

- Duración

Tipo: entero

Descripción: (opcional) el tiempo máximo, en minutos, que desea permitir que se ejecute la automatización. La duración máxima admitida es de 8640 minutos (6 días). El valor predeterminado es 4320 minutos (3 días).

Valores válidos: 30-8640

Predeterminado: 4320

- UpdateRdsRouteTable

Tipo: cadena

Descripción: (opcional) si se establece en `true`, el manual de procedimientos actualiza la tabla de enrutamiento asociada a la subred en la que se ejecuta la instancia de base de datos. Se agrega una ruta IPv4 para enrutar el tráfico a la dirección IPV4 privada temporal de la instancia Amazon EC2 a través de la conexión de emparejamiento de VPC recién creada.

Valores válidos: `true` | `false`

Predeterminado: `false`

- AllowVpcInternetAccess

Tipo: cadena

Descripción: (opcional) Si se establece en `true`, el runbook crea una puerta de enlace NAT para proporcionar conectividad a Internet a la instancia temporal de Amazon EC2 para comunicarse con el punto de enlace de Soporte la API. Puede dejar este parámetro como `false` si solo quiere que el manual de procedimientos cargue la salida en su bucket de Amazon S3.

Valores válidos: `true` | `false`

Predeterminado: `false`

- `UpdateRdsSecurityGroup`

Tipo: cadena

Descripción: (opcional) si se establece en `true`, el manual de procedimientos actualiza el grupo de seguridad asociado a su instancia de base de datos para permitir el tráfico desde la dirección IP privada de la instancia temporal.

Valores válidos: Falso | Verdadero

Predeterminado: `false`

- `EbsVolumeDeleteOnTermination`

Tipo: cadena

Descripción: (Opcional) Si se establece en `true`, el volumen raíz de la instancia temporal de Amazon EC2 se elimina una vez que el runbook complete y elimine la pila. CloudFormation

Valores válidos: Falso | Verdadero

Predeterminado: `false`

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStackEvents`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateStack`
- `ec2:AcceptVpcPeeringConnection`
- `ec2:AllocateAddress`
- `ec2:AssociateRouteTable`
- `ec2:AssociateVpcCidrBlock`

- `ec2:AttachInternetGateway`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateEgressOnlyInternetGateway`
- `ec2:CreateInternetGateway`
- `ec2:CreateNatGateway`
- `ec2:CreateRoute`
- `ec2:CreateRouteTable`
- `ec2:CreateSecurityGroup`
- `ec2:CreateSubnet`
- `ec2:CreateTags`
- `ec2:CreateVpc`
- `ec2:CreateVpcEndpoint`
- `ec2:CreateVpcPeeringConnection`
- `ec2>DeleteEgressOnlyInternetGateway`
- `ec2>DeleteInternetGateway`
- `ec2>DeleteNatGateway`
- `ec2>DeleteRoute`
- `ec2>DeleteRouteTable`
- `ec2>DeleteSecurityGroup`
- `ec2>DeleteSubnet`
- `ec2>DeleteTags`
- `ec2>DeleteVpc`
- `ec2>DeleteVpcEndpoints`
- `ec2:DescribeAddresses`
- `ec2:DescribeEgressOnlyInternetGateways`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeInternetGateways`

- `ec2:DescribeNatGateways`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcPeeringConnections`
- `ec2:DescribeVpcs`
- `ec2:DetachInternetGateway`
- `ec2:DisassociateRouteTable`
- `ec2:DisassociateVpcCidrBlock`
- `ec2:ModifySubnetAttribute`
- `ec2:ModifyVpcAttribute`
- `ec2:RebootInstances`
- `ec2:ReleaseAddress`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam>DeleteInstanceProfile`
- `iam>DeleteRole`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`

- `iam:GetRolePolicy`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `iam:RemoveRoleFromInstanceProfile`
- `iam:TagPolicy`
- `iam:TagRole`
- `rds:DescribeDBInstances`
- `s3:GetAccountPublicAccessBlock`
- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:GetBucketPublicAccessBlock`
- `s3:ListBucket`
- `ssm:AddTagsToResource`
- `ssm:CancelMaintenanceWindowExecution`
- `ssm:CreateDocument`
- `ssm:CreateMaintenanceWindow`
- `ssm>DeleteDocument`
- `ssm>DeleteMaintenanceWindow`
- `ssm:DeregisterTaskFromMaintenanceWindow`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeDocument`
- `ssm:DescribeInstanceInformation`
- `ssm:DescribeMaintenanceWindowExecutions`
- `ssm:GetCalendarState`
- `ssm:GetDocument`
- `ssm:GetMaintenanceWindowExecution`
- `ssm:GetParameters`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:ListTagsForResource`

- `ssm:RegisterTaskWithMaintenanceWindow`
- `ssm:RemoveTagsFromResource`
- `ssm:SendCommand`
- `support:AddAttachmentsToSet`
- `support:AddCommunicationToCase`
- `support:DescribeCases`

Pasos de documentos

1. `aws:assertAwsResourceProperty`: confirma que la instancia de base de datos está en estado `available`.
2. `aws:executeAwsApi`: recopila detalles sobre la instancia de base de datos.
3. `aws:executeScript`: comprueba si el bucket de Amazon S3 especificado en el campo `S3BucketName` permite permisos de acceso de lectura o escritura públicos o anónimos.
4. `aws:executeScript`- Obtiene el contenido de la CloudFormation plantilla del archivo adjunto del manual de automatización que se utiliza para crear los recursos temporales AWS en su archivo. Cuenta de AWS
5. `aws:createStack`- Crea la CloudFormation pila de recursos.
6. `aws:waitForAwsResourceProperty`- Espera a que se ejecute la instancia de Amazon EC2 creada por CloudFormation la plantilla.
7. `aws:executeAwsApi`: obtiene los ID de la instancia temporal de Amazon EC2 y de la conexión de emparejamiento de VPC creada por CloudFormation.
8. `aws:executeAwsApi`: obtiene la dirección IP de la instancia temporal de Amazon EC2 para configurar la conectividad con su instancia de base de datos.
9. `aws:executeAwsApi`: etiqueta el volumen de Amazon EBS adjunto a la instancia temporal de Amazon EC2.
10. `aws:waitForAwsResourceProperty`: espera hasta que la instancia temporal de Amazon EC2 supere las comprobaciones de estado.
11. `aws:waitForAwsResourceProperty`: espera hasta que Systems Manager gestione la instancia temporal de Amazon EC2. Si se agota el tiempo de espera de este paso o se produce un error, el manual de procedimientos reinicia la instancia.
 - a. `aws:executeAwsApi`: reinicia la instancia temporal de Amazon EC2 si el paso anterior ha fallado o se ha agotado el tiempo de espera.

- b. `aws:waitForAwsResourceProperty`: espera hasta que Systems Manager gestione la instancia temporal de Amazon EC2 tras el reinicio.
12. `aws:runCommand`: instala los requisitos de la aplicación recopiladora de metadatos en la instancia temporal de Amazon EC2.
13. `aws:runCommand`: configura el acceso a la instancia de base de datos mediante la creación de un archivo de configuración en la instancia temporal de Amazon EC2.
14. `aws:executeAwsApi`: crea una ventana de mantenimiento para ejecutar periódicamente la aplicación recopiladora de metadatos mediante Run Command. La ventana de mantenimiento inicia y detiene la instancia entre comandos.
15. `aws:waitForAwsResourceProperty`- Espera a que la ventana de mantenimiento creada por la CloudFormation plantilla esté lista.
16. `aws:executeAwsApi`- Obtiene la ventana IDs de mantenimiento y el calendario de cambios creados por CloudFormation.
17. `aws:sleep`: espera hasta la fecha de finalización del período de mantenimiento.
18. `aws:executeAwsApi`: desactiva la ventana de mantenimiento.
19. `aws:executeScript`: obtiene los resultados de las tareas ejecutadas durante el período de mantenimiento.
20. `aws:waitForAwsResourceProperty`: espera a que el período de mantenimiento finalice la última tarea antes de continuar.
21. `aws:branch`: ramifica el flujo de trabajo en función de si ha proporcionado un valor para el parámetro `SupportCase`.
- a. `aws:changeInstanceState`: inicia la instancia temporal de Amazon EC2 y espera a que se superen las comprobaciones de estado antes de cargar el informe.
 - b. `aws:waitForAwsResourceProperty`: espera hasta que Systems Manager gestione la instancia temporal de Amazon EC2. Si se agota el tiempo de espera de este paso o se produce un error, el manual de procedimientos reinicia la instancia.
 - i. `aws:executeAwsApi`: reinicia la instancia temporal de Amazon EC2 si el paso anterior ha fallado o se ha agotado el tiempo de espera.
 - ii. `aws:waitForAwsResourceProperty`: espera hasta que Systems Manager gestione la instancia temporal de Amazon EC2 tras el reinicio.
 - c. `aws:runCommand`: adjunta el informe de metadatos al caso Soporte si ha proporcionado un valor para el parámetro `SupportCase`. El script comprime y divide el informe en archivos de 5 MB. El número máximo de archivos que el script adjunta a un caso Soporte es 12.

22.aws:changeInstanceState- Detiene la instancia temporal de Amazon EC2 en caso de que la CloudFormation pila no se elimine.

23.aws:executeAwsApi- Describe los eventos de la CloudFormation pila si los runbooks no pueden crear o actualizar la CloudFormation pila.

24.aws:waitForAwsResourceProperty- Espera a que la CloudFormation pila esté en estado terminal antes de eliminarla.

25.aws:executeAwsApi- Elimina la CloudFormation pila excluyendo la ventana de mantenimiento. El volumen raíz de Amazon EBS asociado a la instancia temporal de Amazon EC2 se conserva si el valor del parámetro `EbsVolumeDeleteOnTermination` se estableció en `false`.

AWS-RebootRdsInstance

Descripción

El manual de procedimientos AWS-RebootRdsInstance reinicia una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) si aún no se está reiniciando.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia de Amazon RDS DB que desea reiniciar.

Pasos de documentos

RebootInstance - Reinicia la instancia de base de datos si aún no se está reiniciando.

WaitForAvailableState - Espera a que la instancia de base de datos complete el proceso de reinicio.

Salidas

Esta automatización no tiene salidas.

AWSSupport-ShareRDSSnapshot

Descripción

El manual de procedimientos AWSSupport-ShareRDSSnapshot proporciona una solución automatizada para el procedimiento descrito en el artículo del Centro de Conocimiento [¿Cómo puedo compartir una instantánea de base de datos de Amazon RDS cifrada con otra cuenta?](#)

Si la instantánea de Amazon Relational Database Service (Amazon RDS) se cifró con la Clave administrada de AWS configuración predeterminada, no podrá compartir la instantánea. En este caso, debe copiar la instantánea con una clave administrada por el cliente y, a continuación, compartir la instantánea con la cuenta de destino. Esta automatización realiza estos pasos utilizando el valor que especifique en el parámetro SnapshotName o la última instantánea encontrada para la instancia de base de datos o el clúster de base de datos de Amazon RDS seleccionados.

Note

Si no especifica un valor para el KMSKey parámetro, la automatización crea una nueva clave administrada por el AWS KMS cliente en su cuenta que se utiliza para cifrar la instantánea.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AccountIds

Tipo: StringList

Descripción: (obligatorio) Lista de cuentas separadas por comas con las IDs que compartir la instantánea.

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Base de datos

Tipo: cadena

Descripción: (obligatorio) el nombre de la instancia de base de datos o el clúster de Amazon RDS cuya instantánea desea compartir. Este parámetro es opcional si especifica un valor para el parámetro SnapshotName.

- KMSKey

Tipo: cadena

Descripción: (opcional) el nombre de recurso de Amazon (ARN) completo de la clave de AWS KMS administrada por el cliente que se utiliza para cifrar la instantánea.

- **SnapshotName**

Tipo: cadena

Descripción: (opcional) el ID del clúster o instantánea de instancia de base de datos que desea utilizar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:DescribeDBSnapshots`
- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

`AutomationAssumeRole` requiere las siguientes acciones para iniciar correctamente el manual de procedimientos de un clúster de base de datos.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBClusters`
- `rds:DescribeDBClusterSnapshots`
- `rds:CopyDBClusterSnapshot`
- `rds:ModifyDBClusterSnapshotAttribute`

El rol de IAM utilizado para ejecutar la automatización debe agregarse como usuario clave para usar la clave de KMS especificada en el parámetro `ARNKmsKey`. Para obtener información sobre cómo añadir usuarios de clave a la clave KMS, consulte [Modificación de una política de claves](#) en la Guía del desarrollador de AWS Key Management Service .

Si no se especifica un valor para el parámetro `KMSKey`, `AutomationAssumeRole` requiere realizar las siguientes acciones adicionales para iniciar correctamente el manual de procedimientos.

- `kms:CreateKey`

- kms:ScheduleKeyDeletion
- kms:CreateGrant
- kms:DescribeKey

Pasos de documentos

1. `aws:executeScript`- Comprueba si se ha proporcionado un valor para el `KMSKey` parámetro y crea una clave gestionada por el AWS KMS cliente si no se encuentra ningún valor.
2. `aws:branch`: comprueba si se ha proporcionado un valor para el parámetro `SnapshotName` y se ramifica en consecuencia.
3. `aws:executeAwsApi`: comprueba si la instantánea proporcionada proviene de una instancia de base de datos.
4. `aws:executeScript`: formatea el parámetro `SnapshotName` sustituyendo los dos puntos por un guion.
5. `aws:executeAwsApi`: copia la instantánea utilizando el `KMSKey` especificado.
6. `aws:waitForAwsResourceProperty`: espera a que finalice la operación de copia de la instantánea.
7. `aws:executeAwsApi`: comparte la nueva instantánea con la `AccountIds` especificada.
8. `aws:executeAwsApi`: comprueba si la instantánea proporcionada proviene de un clúster de base de datos.
9. `aws:executeScript`: formatea el parámetro `SnapshotName` sustituyendo los dos puntos por un guion.
10. `aws:executeAwsApi`: copia la instantánea utilizando el `KMSKey` especificado.
11. `aws:waitForAwsResourceProperty`: espera a que finalice la operación de copia de la instantánea.
12. `aws:executeAwsApi`: comparte la nueva instantánea con la `AccountIds` especificada.
13. `aws:executeAwsApi`: comprueba si el valor proporcionado para el parámetro `Database` es una instancia de base de datos.
14. `aws:executeAwsApi`: comprueba si el valor proporcionado para el parámetro `Database` es un clúster de base de datos.
15. `aws:executeAwsApi`: recupera una lista de instantáneas de la `Database` especificada.
16. `aws:executeScript`: determina la última instantánea disponible de la lista recopilada en el paso anterior.

- 17 `aws:executeAwsApi`: copia la instantánea de la instancia de base de datos utilizando la KMSKey especificada.
- 18 `aws:waitForAwsResourceProperty`: espera a que finalice la operación de copia de la instantánea.
- 19 `aws:executeAwsApi`: comparte la nueva instantánea con la AccountIds especificada.
- 20 `aws:executeAwsApi`: recupera una lista de instantáneas de la Database especificada.
- 21 `aws:executeScript`: determina la última instantánea disponible de la lista recopilada en el paso anterior.
- 22 `aws:executeAwsApi`: copia la instantánea de la instancia de base de datos utilizando la KMSKey especificada.
- 23 `aws:waitForAwsResourceProperty`: espera a que finalice la operación de copia de la instantánea.
- 24 `aws:executeAwsApi`: comparte la nueva instantánea con la AccountIds especificada.
- 25 `aws:executeScript`- Elimina la clave gestionada por el AWS KMS cliente creada por la automatización si no se especificó un valor para el KMSKey parámetro y la automatización falla.

AWS-StartRdsInstance

Descripción

Inicia una instancia de Amazon Relational Database Service (Amazon RDS).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia Amazon RDS que comenzar.

AWS-StartStopAuroraCluster

Descripción

Este manual inicia o detiene un clúster de Amazon Aurora.

 Note

Para iniciar un clúster, debe estar en un stopped estado. Para detener un clúster, debe estar en un available estado. Este manual de ejecución no se puede utilizar para iniciar o detener un clúster que sea un clúster Aurora Serverless v1, un clúster de varios maestros de Aurora, parte de una base de datos global de Aurora o un clúster que utilice Aurora parallel Query. El runbook se puede utilizar para detener e iniciar un clúster Aurora Serverless v2.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ClusterName

Tipo: cadena

Descripción: (Obligatorio) El nombre del clúster de Aurora que desea detener o iniciar.

- Action

Tipo: cadena

Valores válidos: Start | Stop

Predeterminado: Inicio

Descripción: (Obligatorio) El nombre del clúster de Aurora que desea detener o iniciar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- rds:DescribeDBClusters
- rds:StartDBCluster
- rds:StopDBCluster

Pasos de documentos

- aws:executeScript- Inicia o detiene el clúster en función de los valores que especifique para el.

Salidas

StartStopAuroraCluster. ClusterName - El nombre del cúmulo de Aurora

StartStopAuroraCluster. CurrentStatus - El estado actual del cúmulo Aurora

StartStopAuroraCluster.Message: detalles de la automatización

AWS-StopRdsInstance

Descripción

Detenga una instancia de Amazon Relational Database Service (Amazon RDS).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia de Amazon RDS que se va a detener.

AWSSupport-TroubleshootConnectivityToRDS

Descripción

El manual de procedimientos AWSSupport-TroubleshootConnectivityToRDS diagnostica los problemas de conectividad entre una instancia EC2 y una instancia de Amazon Relational Database Service. La automatización garantiza que la instancia de base de datos esté disponible y, a continuación, comprueba las reglas de los grupos de seguridad asociados, las listas de control de acceso a la red (red ACLs) y las tablas de enrutamiento para detectar posibles problemas de conectividad.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DBInstanceIdentificador

Tipo: cadena

Descripción: (obligatorio) el ID de instancia de base de datos para probar la conectividad.

- SourceInstance

Tipo: cadena

Patrón permitido: `^[a-z0-9]{8,17}$`

Descripción: (obligatorio) el ID de la instancia EC2 desde la que probar la conectividad.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el estado de la instancia de base de datos sea `available`.
- `aws:executeAwsApi`: obtiene información de resumen acerca de la instancia DB.
- `aws:executeAwsApi`- Obtiene información sobre la red de instancias de base de datos ACLs.
- `aws:executeAwsApi`: obtiene el CIDR de la subred de la instancia de base de datos.
- `aws:executeAwsApi`: obtiene información acerca de la instancia EC2.
- `aws:executeAwsApi`- Obtiene información sobre la red ACLs de instancias EC2.
- `aws:executeAwsApi`: obtiene información sobre los grupos de seguridad asociados a la instancia EC2.
- `aws:executeAwsApi`: obtiene información sobre los grupos de seguridad asociados a la instancia de base de datos.
- `aws:executeAwsApi`: obtiene información sobre las tablas de ruteo asociadas a la instancia EC2.

- `aws:executeAwsApi`: obtiene información sobre la tabla de enrutamiento principal asociada con el Amazon VPC para la instancia EC2.
- `aws:executeAwsApi`: obtiene información sobre las tablas de enrutamiento asociadas a la instancia de base de datos.
- `aws:executeAwsApi`: obtiene información sobre la tabla de enrutamiento principal asociada con el Amazon VPC para la instancia de base de datos.
- `aws:executeScript`: evalúa las reglas de los grupos de seguridad.
- `aws:executeScript`- Evalúa la red. ACLs
- `aws:executeScript`: evalúa las tablas de enrutamiento.
- `aws:sleep`: finaliza la automatización.

Salidas

obtener RDSInstance propiedades. DBInstanceIdentificador: la instancia de base de datos utilizada en la automatización.

obtener RDSInstance propiedades. DBInstanceEstado: el estado actual de DBInstance.

evalSecurityGroupReglas. SecurityGroupEvaluation - Resultados de la comparación de las reglas del grupo SourceInstance de seguridad con las reglas del grupo de seguridad de la instancia de base de datos.

evalNetworkAclReglas. NetworkAclEvaluation - Resultados de la comparación de la SourceInstance red con ACLs la red de instancias de base de datos ACLs.

evalRouteTableEntradas. RouteTableEvaluation - Resultados de la comparación de la tabla de SourceInstance rutas con las rutas de la instancia de base de datos.

AWSSupport-TroubleshootRDSIAMAuthentication

Descripción

AWSSupport-TroubleshootRDSIAMAuthentication Ayuda a solucionar problemas de autenticación AWS Identity and Access Management (IAM) para instancias de Amazon RDS for PostgreSQL, Amazon RDS for MySQL, Amazon RDS for MariaDB, Amazon Aurora PostgreSQL y Amazon Aurora MySQL. Utilice este manual para verificar la configuración necesaria para la autenticación de IAM con una instancia de Amazon RDS o un clúster Aurora. También proporciona pasos para corregir los problemas de conectividad con la instancia Amazon RDS o el clúster Aurora.

⚠ Important

Este manual no es compatible con Amazon RDS for Oracle ni Amazon RDS for Microsoft SQL Server.

⚠ Important

Si se proporciona una instancia Amazon EC2 de origen y la base de datos de destino es Amazon RDS, `AWSSupport-TroubleshootConnectivityToRDS` se invoca una automatización secundaria para solucionar los problemas de conectividad TCP. El resultado también proporciona comandos que puede ejecutar en su instancia Amazon EC2 o máquina de origen para conectarse a las instancias de Amazon RDS mediante la autenticación de IAM.

¿Cómo funciona?

Este manual consta de seis pasos:

- Paso 1: `ValidateInputs`: valida las entradas de la automatización.
- Paso 2: `branchOnSource EC2 proporcionado`: verifica si se proporciona un ID de instancia de Amazon EC2 de origen en los parámetros de entrada.
- Paso 3: `validarRDSConnectivity`: valida la conectividad de Amazon RDS desde la instancia Amazon EC2 de origen, si se proporciona.
- Paso 4: `validarRDSIAMAuthentication`: valida si la función de autenticación de IAM está habilitada.
- Paso 5: `validarIAMPolicies`: verifica si los permisos de IAM necesarios están presentes en el usuario o rol de IAM proporcionado.
- Paso 6: Generar un informe: genera un informe con los resultados de los pasos ejecutados anteriormente.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- RDSType

Tipo: cadena

Descripción: (Obligatorio): Seleccione el tipo de base de datos relacional a la que está intentando conectarse y autenticarse.

Valores permitidos: o Amazon RDS Amazon Aurora Cluster.

- DBInstanceIdentificador

Tipo: cadena

Descripción: (obligatorio) El identificador de la instancia de base de datos Amazon RDS o del clúster de base de datos Aurora de destino.

Valor permitido: $^[A-Za-z0-9]+(-[A-Za-z0-9]+)*\$$

Número máximo de caracteres: 63

- SourceEc2InstanceIdentifier

Tipo: AWS::EC2::Instance::Id

Descripción: (opcional) El ID de instancia de Amazon EC2 si se conecta a la instancia de base de datos Amazon RDS desde una instancia de Amazon EC2 que se ejecuta en la misma cuenta y

región. No especifique este parámetro si la fuente no es una instancia de Amazon EC2 o si el tipo de Amazon RDS de destino es un clúster de base de datos Aurora.

Valor predeterminado: ""

- DBIAMRoleNombre

Tipo: cadena

Descripción: (opcional) El nombre de la función de IAM que se utiliza para la autenticación basada en IAM. Indíquelo solo si no DBIAMUserName se proporciona el parámetro; de lo contrario, déjelo vacío. Se debe proporcionar DBIAMRoleName o DBIAMUserName.

Valor permitido: `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

Número máximo de caracteres: 64

Valor predeterminado: ""

- DBIAMUserName

Tipo: cadena

Descripción: (opcional) El nombre de usuario de IAM utilizado para la autenticación basada en IAM. Indíquelo solo si no se proporciona el DBIAMRoleName parámetro; de lo contrario, déjelo vacío. Se debe proporcionar DBIAMRoleName o DBIAMUserName.

Valor permitido: `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

Número máximo de caracteres: 64

Valor predeterminado: ""

- DBUserName

Tipo: cadena

Descripción: (opcional) El nombre de usuario de la base de datos asignado a un IAM role/user para la autenticación basada en el IAM dentro de la base de datos. La opción predeterminada * evalúa si el `rds-db:connect` permiso está permitido para todos los usuarios de la base de datos.

Valor permitido: `^[a-zA-Z0-9+=, .@*_]{1,64}$`

Número máximo de caracteres: 64

Valor predeterminado: *

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Instrucciones

1. Navega hasta [AWS Support-TroubleshootRDSIAMAuthentication](#) la AWS Systems Manager consola.
2. Elija Ejecutar automatización
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole(Opcional):

El nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- RDSType(Obligatorio):

Seleccione el tipo de Amazon RDS al que intenta conectarse y autenticarse. Elija uno de los dos valores permitidos: o Amazon RDS Amazon Aurora Cluster.

- DBInstanceIdentificador (obligatorio):

Introduzca el identificador de la instancia de base de datos Amazon RDS de destino o del clúster Aurora al que intenta conectarse y utilice las credenciales de IAM para la autenticación.

- SourceEc2 InstanceIdentifier (opcional):

Proporcione el ID de instancia de Amazon EC2 si se conecta a la instancia de base de datos de Amazon RDS desde una instancia de Amazon EC2 presente en la misma cuenta y región. Déjelo en blanco si el origen no es Amazon EC2 o si el tipo de Amazon RDS de destino es un clúster Aurora.

- DBIAMRoleNombre (opcional):

Introduzca el nombre del rol de IAM utilizado para la autenticación basada en IAM. Indíquelo solo si no DBIAMUserName se proporciona; de lo contrario, déjelo en blanco. Se debe proporcionar DBIAMRoleName o DBIAMUserName.

- DBIAMUserName (opcional):

Introduzca el usuario de IAM utilizado para la autenticación basada en IAM. Indique solo si no DBIAMRoleName se proporciona; de lo contrario, déjelo en blanco. Se debe proporcionar DBIAMRoleName o DBIAMUserName.

- DBUserName (opcional):

Introduzca el usuario de la base de datos asignado a un rol o usuario de IAM para la autenticación basada en IAM dentro de la base de datos. La opción predeterminada * se utiliza para evaluar; no se proporciona nada en este campo.

Input parameters

SourceEC2InstanceIdentifier
(Optional) The Amazon EC2 Instance ID if you are connecting to the RDS DB instance from an EC2 Instance running in the same account and region. Do not specify this parameter if the source is not an EC2 instance or if the target RDS type is an Aurora DB cluster.

☒ Show interactive instance picker

Name	Instance ID	State	Availability zone	Platform
There are no managed instances in this account. We recommend using Quick Setup to configure your instances for Systems Manager. After configuring your instances for Systems Manager, the instances will be displayed here in a few minutes.				

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the role that allows the Automation runbook to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your current IAM user permissions context to execute this runbook.

RDSType
(Required) The type of Relational Database.

DBInstanceIdentifier
(Required) The identifier of the target Amazon RDS DB instance or Amazon Aurora DB cluster.

DBIAMRoleName
(Optional) The IAM role name being used for IAM-based authentication. Provide only if the parameter 'DBIAMUserName' is not provided, otherwise leave it empty. Either 'DBIAMRoleName' or 'DBIAMUserName' must be provided.

DBIAMUserName
(Optional) The IAM user name used for IAM-based authentication. Provide only if the 'DBIAMRoleName' parameter is not provided, otherwise leave it empty. Either 'DBIAMRoleName' or 'DBIAMUserName' must be provided.

DBUserName
(Optional) The database user name mapped to an IAM role/user for IAM-based authentication within the database. The default option "" evaluates if the 'rds-db:connect' permission is allowed for all users in the DB.

4. Seleccione Ejecutar.

5. Observe que se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- Paso 1: Validar las entradas:

Valida las entradas de la automatización: `SourceEC2InstanceIdentifier` (opcional), `DBInstanceIdentifier` o, y o `ClusterID`. `DBIAMRoleName` `DBIAMUserName` Verifica si los parámetros de entrada ingresados están presentes en su cuenta y región. También verifica si el usuario ingresó uno de los parámetros de IAM (por ejemplo, `DBIAMRoleName` o). `DBIAMUserName` Además, realiza otras verificaciones, por ejemplo, si la base de datos mencionada está en estado Disponible.

- Paso 2: `branchOnSource EC2` Siempre que:

Verifica si se proporciona Amazon EC2 de origen en los parámetros de entrada y si la base de datos es Amazon RDS. En caso afirmativo, continúa con el paso 3. De lo contrario, se salta el paso 3, que es la validación de la conectividad entre Amazon EC2 y Amazon RDS, y pasa al paso 4.

- Paso 3: validar: `RDSConnectivity`

Si se proporciona el Amazon EC2 de origen en los parámetros de entrada y la base de datos es Amazon RDS, el paso 2 inicia el paso 3. En este paso, `AWSSupport -`

TroubleshootConnectivityToRDS se invoca la automatización secundaria para validar la conectividad de Amazon RDS desde Amazon EC2 de origen. El manual de automatización secundaria AWSSupport-TroubleshootConnectivityToRDS verifica si las configuraciones de red requeridas (Amazon Virtual Private Cloud [Amazon VPC], grupos de seguridad, lista de control de acceso a la red [NACL], disponibilidad de Amazon RDS) están implementadas para que pueda conectarse desde la instancia de Amazon EC2 a la instancia de Amazon RDS.

- Paso 4: validar: RDSIAMAuthentication

Valida si la función de autenticación de IAM está habilitada en la instancia de Amazon RDS o en el clúster Aurora.

- Paso 5: validar: IAMPolicies

Comprueba si los permisos de IAM necesarios están presentes en el IAM user/role transferido para permitir que las credenciales de IAM se autenticuen en la instancia de Amazon RDS para el usuario de base de datos especificado (si lo hubiera).

- Paso 6: Generar un informe:

Obtiene toda la información de los pasos anteriores e imprime el resultado o la salida de cada paso. También se enumeran los pasos a seguir y realizar para conectarse a la instancia de Amazon RDS mediante las credenciales de IAM.

7. Cuando se complete la automatización, consulte la sección de resultados para ver los resultados detallados:

- Comprobar el permiso de usuario o rol de IAM para conectarse a la base de datos:

Comprueba si los permisos de IAM necesarios están presentes en el IAM user/role transferido para permitir que las credenciales de IAM se autenticuen en la instancia de Amazon RDS para el usuario de base de datos especificado (si lo hubiera).

- Comprobación del atributo de autenticación basado en IAM para la base de datos:

Comprueba si la función de autenticación de IAM está habilitada para la base de datos Amazon RDS o el clúster Aurora especificados.

- Comprobación de la conectividad de una instancia de Amazon EC2 a una instancia de Amazon RDS:

Verifica si las configuraciones de red requeridas (Amazon VPC, grupos de seguridad, NACL, disponibilidad de Amazon RDS) están implementadas para que pueda conectarse desde la instancia de Amazon EC2 a la instancia de Amazon RDS.

- Pasos siguientes:

Enumera los comandos y los pasos que se deben consultar y ejecutar para conectarse a la instancia de Amazon RDS mediante las credenciales de IAM.

Outputs

```
ScriptExecutionId
2e1d[REDACTED]a4

Output
[Troubleshooting Results]

1. Checking the IAM user/role permissions to connect to database:
✓ [PASSED]: Found permission 'rds-db:connect' for the resource 'a[REDACTED]-db1'.

2. Checking IAM-based authentication attribute for the database:
✓ [PASSED]: IAM-based authentication attribute is enabled for the database 'a[REDACTED]-db1'.

3. Checking connectivity from the EC2 instance to RDS instance:
✗ [SKIPPED]: No Source EC2 instance provided.
Run these commands to troubleshoot connectivity to your aurora-mysql DB instance:
$ telnet a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com 3306
$ nc -vz a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com 3306

[Next Steps]

1. Verify if the database user exists and have the required permissions to connect to the database using IAM authentication:
- Connect to DB a[REDACTED]-db1 using admin/master db user.
- Run the following query/command in your database:
  SELECT user, plugin, host from mysql.user WHERE user LIKE '%<name of the DB user>%';
- From the output, verify if the user has the AWSAuthenticationPlugin.

2. Download the SSL bundle and connect to aurora-mysql database using IAM authentication by running the following commands:
$ wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
$ export DBPASS=$(aws rds generate-db-auth-token --hostname a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com --port 3306 --region us-[REDACTED]-2 --username <name of the DB user>)
mysql --host=a[REDACTED]-db1.cluster-[REDACTED].rds.amazonaws.com --port=3306 --ssl-ca=global-bundle.pem --enable-cleartext-plugin --user=<name of the DB user> --password=$DBPASS

Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html
```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSSupport-ValidateRdsNetworkConfiguration

Descripción

AWSSupport-ValidateRdsNetworkConfiguration la automatización ayuda a evitar un estado de red incompatible para su instancia existente de Amazon Relational Database Service (Amazon RDS), Amazon Aurora o Amazon DocumentDB antes de realizar u operar. ModifyDBInstance StartDBInstance Si la instancia ya se encuentra en un estado de red incompatible, el manual explicará el motivo.

¿Cómo funciona?

Este manual determina si la instancia de base de datos de Amazon RDS pasará a un estado de red incompatible o, si lo ha hecho, determina el motivo por el que se encuentra en un estado de red incompatible.

El runbook realiza las siguientes comprobaciones en la instancia de base de datos de Amazon RDS:

- Cuota de Amazon Elastic Network Interface (ENI) por región.
- Existen todas las subredes del grupo de subredes de la base de datos.
- Hay suficientes direcciones IP libres disponibles para las subredes.
- (Para instancias de Amazon RDS de acceso público) Configuración de los atributos de VPC `enableDnsSupport` (`enableDnsHostnames`).

Important

Cuando utilice este documento en clústeres de Amazon Aurora o Amazon DocumentDB, asegúrese de utilizar `DBInstanceIdentifier` en lugar de `ClusterIdentifier`. De lo contrario, el documento fallará en el primer paso.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `rds:DescribeDBInstances`

- servicequotas:GetServiceQuota
- ec2:DescribeNetworkInterfaces
- ec2:DescribeVpcAttribute
- ec2:DescribeSubnets

Ejemplo de política:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ValidateRdsNetwork",
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "servicequotas:GetServiceQuota",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets"
      ],
      "Resource": [
        "arn:aws:rds:us-east-1:111122223333:db:db-instance-name"
      ]
    }
  ]
}
```

Instrucciones

1. Navegue hasta [AWSSupport-ValidateRdsNetworkConfiguration](#) la AWS Systems Manager consola.
2. Elija Ejecutar automatización
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole(Opcional):

El nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no

se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DBInstanceIdentificador (obligatorio):

Introduzca el identificador de instancia de Amazon Relational Database Service.

The screenshot shows the 'Input parameters' section of an AWS Systems Manager Automation runbook. It contains two fields: 'AutomationAssumeRole' and 'DBInstanceIdentifier'. The 'AutomationAssumeRole' field is a dropdown menu with the selected value 'arn:aws:iam::123456789012:role/automation-assume-role-SSM'. The 'DBInstanceIdentifier' field is a text input containing the value 'my-rds-instance-01'.

4. Seleccione Ejecutar.

5. Observe que se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- Paso 1: assertRdsState

Comprueba si el identificador de instancia proporcionado existe y tiene alguno de los siguientes estados: `available`, `stopped`, o `incompatible-network`.

- Paso 2 gatherRdsInformation:

Recopila la información necesaria sobre la instancia de Amazon RDS para utilizarla más adelante en la automatización.

- Paso 3: checkEniQuota

Comprueba la cuota actual disponible de Amazon ENI para la región.

- Paso 4 validateVpcAttributes:

Valida que los parámetros de DNS (`enableDnsSupport` y `enableDnsHostnames`) de la VPC de Amazon estén configurados en `true` (o no si la instancia de Amazon RDS lo está). `PubliclyAccessible`

- Paso 5: validateSubnetAttributes

Valida la existencia de subredes en `DBSubnetGroup` y comprueba si están disponibles IPs para cada subred.

- Paso 6: Generar un informe:

Obtiene toda la información de los pasos anteriores e imprime el resultado o la salida de cada paso. También se enumeran los pasos a seguir y realizar para conectarse a la instancia de

7. Cuando se complete la automatización, consulte la sección de resultados para ver los resultados detallados:

Instancia de Amazon RDS con una configuración de red válida:

▼ 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.
```

Instancia de Amazon RDS con una configuración de red incorrecta (el enableDnsHostnames atributo de VPC está establecido en false):

▼ Outputs

```

generateReport.Report
# AWS RDS Network Configuration Checks: test-fail-sazrds-vpcattr (stopped)
### 🚫 Issue(s) Found!!!

### [Troubleshooting Results]
1. Checking ENI Quota for region the RDS Instance is in:
  ✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4996) is sufficient at the moment.

2. Checking VPC Attribute ('enableDnsHostname' & 'enableDnsSupport') settings:
  ❌ [FAILED] : Value for 'enableDnsHostnames' VPC Attribute is 'false'.

3. Checking if subnets required for RDS exists or not:
  ✅ [PASSED] : All subnets in 'ap-south-1b' availability zone exists.

4. Checking if Available IPs are sufficient per subnets that are required:
  ⚠️ [WARNING] : There are sufficient available IPs in 'ap-south-1b' availability zone, but it is recommended to have more than 9 IPs.

5. Checking if other Availability zone satisfy Check No# 3 & 4:
  * Availability Zone: ap-south-1a
    i. Subnet Existence Check: ✅ [PASSED]
    ii. Available IP Check: ⚠️ [WARNING]

### [Next Steps]
o Please set the value of 'enableDnsHostnames' VPC attribute to 'true'.
  [+] View and update DNS attributes for your VPC: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-updating
o Please free up some IPs before performing Modify/Stop operation on the instance.
  [+] Learn why a subnet in your VPC has insufficient IP addresses : https://repost.aws/knowledge-center/subnet-insufficient-ips

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.

```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS documentación de servicio

- [¿Cómo resuelvo los problemas con una base de datos de Amazon RDS que se encuentra en un estado de red incompatible?](#)
- [¿Cómo resuelvo los problemas con una instancia de Amazon DocumentDB que se encuentra en un estado de red incompatible?](#)

Amazon Redshift

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Redshift. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-DeleteRedshiftCluster](#)
- [AWSConfigRemediation-DisablePublicAccessToRedshiftCluster](#)
- [AWSConfigRemediation-EnableRedshiftClusterAuditLogging](#)
- [AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot](#)
- [AWSConfigRemediation-EnableRedshiftClusterEncryption](#)
- [AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting](#)
- [AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster](#)
- [AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings](#)
- [AWSConfigRemediation-ModifyRedshiftClusterNodeType](#)

AWSConfigRemediation-DeleteRedshiftCluster

Descripción

El manual de procedimientos AWSConfigRemediation-DeleteRedshiftCluster elimina el clúster de Amazon Redshift que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- ClusterIdentifier

Tipo: cadena

Descripción: (obligatorio) el ID del clúster de Amazon Redshift que desea eliminar.

- SkipFinalClusterSnapshot

Tipo: Booleano

Predeterminado: false

Descripción: (opcional) si se establece en `false`, la automatización crea una instantánea antes de eliminar el clúster de Amazon Redshift. Si se establece en `true`, no se crea una instantánea final del clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift>DeleteCluster`
- `redshift:DescribeClusters`

Pasos de documentos

- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `SkipFinalClusterSnapshot`.

- `aws:executeAwsApi`: elimina el clúster de Amazon Redshift especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: verifica que el clúster de Amazon Redshift se haya eliminado.

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

Descripción

El manual de procedimientos `AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` deshabilita la accesibilidad pública para el clúster de Amazon Redshift que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `ClusterIdentifier`

Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster para el que desea deshabilitar la accesibilidad pública.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Pasos de documentos

- `aws:executeAwsApi`: desactiva la accesibilidad pública para el clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:waitForAwsResourceProperty`: espera a que el estado del clúster cambie a `available`.
- `aws:assertAwsResourceProperty`: confirma que la configuración de accesibilidad pública está deshabilitada en el clúster.

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRedshiftClusterAuditLogging` permite el registro de auditorías para el clúster de Amazon Redshift que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de Amazon Simple Storage Service (Amazon S3) al que desea cargar los registros.

- ClusterIdentifier

Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el registro de auditoría.

- S3 KeyPrefix

Tipo: cadena

Descripción: (opcional) el prefijo clave de Amazon S3 (subcarpeta) en el que desea cargar los registros.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution

- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

Pasos de documentos

- `aws:branch`: se ramifica en función de si se especificó un valor para el parámetro `S3KeyPrefix`.
- `aws:executeAwsApi`: habilita el registro de auditoría en el clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: verifica que el registro de auditoría fue habilitado en el clúster.

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` permite realizar instantáneas automatizadas para el clúster de Amazon Redshift que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- AutomatedSnapshotRetentionPeriod

Tipo: entero

Valores válidos: 1-35

Descripción: (obligatorio) el número de días que se conservan las instantáneas automatizadas.

- ClusterIdentifier

Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar las instantáneas automatizadas.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

Pasos de documentos

- aws:executeAwsApi: activa las instantáneas de automatización en el clúster especificado en el parámetro ClusterIdentifier.
- aws:waitForAwsResourceProperty: espera a que el estado del clúster cambie a available.
- aws:executeScript: confirma que las instantáneas automatizadas estaban habilitadas en el clúster.

AWSConfigRemediation-EnableRedshiftClusterEncryption

Descripción

El AWSConfigRemediation-EnableRedshiftClusterEncryption runbook permite el cifrado en el clúster de Amazon Redshift que especifique mediante AWS Key Management Service una clave gestionada por el cliente AWS KMS(). Este manual de procedimientos solo debe utilizarse como referencia para garantizar que los clústeres de Amazon Redshift estén cifrados de acuerdo con las prácticas recomendadas de seguridad mínimas. Recomendamos cifrar varios clústeres con diferentes claves administradas por el cliente. Este manual no puede cambiar la clave administrada por el AWS KMS cliente que se utiliza en un clúster ya cifrado. Para cambiar la clave gestionada por el AWS KMS cliente que se utiliza para cifrar un clúster, primero debe deshabilitar el cifrado en el clúster.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- ClusterIdentifier

Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el cifrado.

- KMSKeyARN

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) de la clave AWS KMS administrada por el cliente que desea utilizar para cifrar los datos del clúster.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Pasos de documentos

- `aws:executeAwsApi`: habilita el cifrado en el clúster de Amazon Redshift especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: verifica que el cifrado esté habilitado en el clúster.

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

Descripción

El manual de procedimientos `AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` permite un enrutamiento mejorado de la nube privada virtual (VPC) para el clúster de Amazon Redshift que especifique. Para obtener información acerca del enrutamiento mejorado de VPC, consulte [Enrutamiento mejorado VPC de Amazon Redshift](#) en la Guía de administración de Amazon Redshift.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- ClusterIdentifier

Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el enrutamiento de VPC mejorado.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

Pasos de documentos

- `aws:executeAwsApi`: permite un enrutamiento de VPC mejorado en el clúster especificado en el parámetro `ClusterIdentifier`.
- `assertAwsResourceProperty`: confirma que el enrutamiento de VPC mejorado estaba habilitado en el clúster.

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

Descripción

El manual de procedimientos `AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` requiere que las conexiones entrantes usen SSL para el clúster de Amazon Redshift que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `ClusterIdentifier`

Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el enrutamiento de VPC mejorado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

Pasos de documentos

- `aws:executeAwsApi`: recopila los detalles de los parámetros del clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:executeAwsApi`: activa la configuración `require_ssl` en el clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: confirma que la configuración `require_ssl` estaba habilitada en el clúster.
- `aws:executeScript`: verifica la configuración `require_ssl` del clúster.

AWSConfigRemediation- ModifyRedshiftClusterMaintenanceSettings

Descripción

El manual de procedimientos `AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` modifica la configuración de mantenimiento del clúster de Amazon Redshift que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AllowVersionUpgrade

Tipo: Booleano

Descripción: (obligatorio) si se establece en `true`, las actualizaciones de las versiones principales se aplican automáticamente al clúster durante el período de mantenimiento.

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- AutomatedSnapshotRetentionPeriod

Tipo: entero

Valores válidos: 1-35

Descripción: (obligatorio) el número de días que se conservan las instantáneas automatizadas.

- ClusterIdentifier

Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster en el que desea habilitar el enrutamiento de VPC mejorado.

- PreferredMaintenanceWindow

Tipo: cadena

Descripción: (obligatorio) el intervalo de tiempo semanal (en UTC) durante el cual puede llevarse a cabo el mantenimiento del sistema.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Pasos de documentos

- `aws:executeAwsApi`: modifica la configuración de mantenimiento del clúster especificado en el parámetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty`: confirma que los ajustes de mantenimiento modificados se configuraron para el clúster.

AWSConfigRemediation-ModifyRedshiftClusterNodeType

Descripción

El manual de procedimientos `AWSConfigRemediation-ModifyRedshiftClusterNodeType` modifica el tipo de nodo y la cantidad de nodos del clúster de Amazon Redshift que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Bases de datos

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- Classic

Tipo: Booleano

Descripción: (opcional) si se establece en `true`, la operación de cambio de tamaño utiliza el proceso de cambio de tamaño clásico.

- ClusterIdentifier

Tipo: cadena

Descripción: (obligatorio) el identificador único del clúster cuyo tipo de nodo desea modificar.

- ClusterType

Tipo: cadena

Valores válidos: `single-node` | `multi-node`

Descripción: (obligatorio) el tipo de clúster que desea asignar a su clúster.

- NodeType

Tipo: cadena

Valores válidos: `ds2.xlarge` | `ds2.8xlarge` | `dc1.large` | `dc1.8xlarge` | `dc2.large` | `dc2.8xlarge` | `ra3.4xlarge` | `ra3.16xlarge`

Descripción: (obligatorio) el tipo de nodo que desea asignar a su clúster.

- **NumberOfNodes**

Tipo: entero

Valores válidos: 2-100

Descripción: (opcional) la cantidad de nodos que desea asignar a su clúster. Si su clúster es de un tipo `single-node`, no especifique un valor para este parámetro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

Pasos de documentos

- `aws:executeScript`: modifica el tipo de nodo y el número de nodos del clúster especificados en el parámetro `ClusterIdentifier`.

Amazon S3

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Simple Storage Service. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-ArchiveS3BucketToIntelligentTiering](#)
- [AWS-ConfigureS3BucketLogging](#)
- [AWS-ConfigureS3BucketVersioning](#)

- [AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock](#)
- [AWSConfigRemediation-ConfigureS3PublicAccessBlock](#)
- [AWS-CreateS3PolicyToExpireMultipartUploads](#)
- [AWS-DisableS3BucketPublicReadWrite](#)
- [AWS-EnableS3BucketEncryption](#)
- [AWS-EnableS3BucketKeys](#)
- [AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy](#)
- [AWSConfigRemediation-RestrictBucketSSLRequestsOnly](#)
- [AWSSupport-TroubleshootS3PublicRead](#)
- [AWSSupport-ConfigureS3ReplicationSameAndCrossAccount](#)
- [AWSSupport-EmptyS3Bucket](#)
- [AWSSupport-TroubleshootS3EventNotifications](#)
- [AWSSupport-ContainS3Resource](#)

AWS-ArchiveS3BucketToIntelligentTiering

Descripción

El AWS-ArchiveS3BucketToIntelligentTiering runbook crea o reemplaza una configuración de organización inteligente por niveles para el bucket de Amazon Simple Storage Service (Amazon S3) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

Tipo: cadena

Descripción: (obligatorio) El nombre del depósito de S3 para el que desea crear una configuración de estratificación inteligente.

- ConfigurationId

Tipo: cadena

Descripción: (obligatorio) El ID de la configuración de organización inteligente por niveles. Puede ser un ID de configuración nuevo o el ID de una configuración existente.

- NumberOfDaysToArchive

Tipo: cadena

Valores válidos: 90-730

Descripción: (Obligatorio) El número de días consecutivos transcurridos desde que un objeto de su depósito pueda pasar al nivel Archive Access.

- NumberOfDaysToDeepArchive

Tipo: cadena

Valores válidos: 180-730

Descripción: (obligatorio) El número de días consecutivos transcurridos desde que un objeto de tu depósito pueda pasar al nivel de Deep Archive Access.

- S3Prefix

Tipo: cadena

Descripción: (opcional) El prefijo del nombre clave de los objetos a los que desea aplicar la configuración.

- Tags

Tipo: MapList

Descripción: (opcional) Metadatos asignados a los objetos a los que desea aplicar la configuración. Las etiquetas constan de una clave y un valor definidos por el usuario.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

Pasos de documentos

- `PutBucketIntelligentTieringConfiguration` (AWS:ExecuteScript): crea o actualiza una configuración de Amazon S3 Intelligent-Tiering para el bucket especificado.
- `VerifyBucketIntelligentTieringConfiguration` (aws: assertAwsResource Property): verifica que la configuración inteligente del bucket de S3 se haya aplicado al bucket especificado.

AWS-ConfigureS3BucketLogging

Descripción

Activa el registro en un bucket de Amazon Simple Storage Service (Amazon S3).

Important

Tenga en cuenta la siguiente información importante sobre la ACL del concesionario de correo electrónico para la [PutBucketLogging](#) API de Amazon S3, que se utiliza en este manual:

Aviso de fin de soporte: a partir del 1 de octubre de 2025, Amazon S3 dejará de dar soporte a la creación de nuevas listas de control de acceso (ACL) de beneficiarios de correo electrónico. El concesionario de correo electrónico ACLs creado antes de esta fecha seguirá funcionando y seguirá siendo accesible a través de la Consola de administración de AWS(AWS CLI CLI) y la API SDKs REST. Sin embargo, ya no podrás crear un nuevo concesionario de correo electrónico. ACLs Entre el 15 de julio de 2025 y el 1 de octubre de 2025, empezará a observar un aumento en la tasa de errores HTTP 405 en las solicitudes a Amazon S3 al intentar crear un nuevo destinatario de correo electrónico. ACLs

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de Amazon S3 para el que desea configurar el registro.

- GrantedPermission

Tipo: cadena

Valores permitidos: FULL_CONTROL | READ | WRITE

Descripción: (obligatorio) permisos de registro asignados al beneficiario para el bucket.

- GranteeEmailAddress

Tipo: cadena

(Opcional) Dirección de correo electrónico del beneficiario.

- GranteeId

Tipo: cadena

Descripción: (opcional) ID de usuario canónico del beneficiario.

- GranteeType

Tipo: cadena

Valores válidos: CanonicalUser | Grupo AmazonCustomerByEmail

Descripción: (obligatorio) tipo de beneficiario.

- GranteeUri

Tipo: cadena

Descripción: (opcional) URI del grupo de beneficiarios.

- TargetBucket

Tipo: cadena

Descripción: (obligatorio) especifica el bucket en el que desea que Amazon S3 almacene los registros de acceso al servidor. Puede hacer que los registros se entreguen en cualquier bucket de su propiedad. También puede configurar varios buckets para entregar sus registros en el mismo bucket de destino. En este caso, debe elegir uno diferente TargetPrefix para cada depósito de origen, de modo que los archivos de registro entregados se puedan distinguir por clave.

- TargetPrefix

Tipo: cadena

Valor predeterminado: /

Descripción: (opcional) especifica un prefijo para las claves en las que se almacenarán los archivos de registro.

AWS-ConfigureS3BucketVersioning

Descripción

Configure el control de versiones para un bucket de Amazon Simple Storage Service (Amazon S3).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de Amazon S3 para el que desea configurar el control de versiones.

- VersioningState

Tipo: cadena

Valores permitidos: Enabled | Suspended

Predeterminado: habilitado

Descripción: (opcional) Aplicada al VersioningConfiguration .Status. Cuando se establece en “Enabled”, este proceso permite el control de versiones para los objetos en el bucket, todos los objetos agregados al bucket reciben un ID de versión único. Cuando se establece en Suspended, este proceso deshabilita el control de versiones para los objetos en el bucket. Todos los objetos añadidos al bucket reciben el ID de versión null.

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Descripción

El manual de procedimientos AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock configura los ajustes del bloque de acceso público de Amazon Simple Storage Service (Amazon S3) para un bucket de Amazon S3 en función de los valores que especifique en los parámetros del manual de procedimientos.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BlockPublicAcls

Tipo: Booleano

Predeterminado: true

Descripción: (Opcional) Si se establece en true, Amazon S3 bloquea las listas de control de acceso público (ACLs) del bucket de S3 y los objetos almacenados en el bucket de S3 que especifique en el BucketName parámetro.

- BlockPublicPolicy

Tipo: Booleano

Predeterminado: true

Descripción: (opcional) si se establece en true, Amazon S3 bloquea las políticas de bucket públicos para el bucket de S3 que especifique en el parámetro BucketName.

- BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de S3 que desea configurar.

- IgnorePublicAcls

Tipo: Booleano

Predeterminado: true

Descripción: (Opcional) Si se establece en true, Amazon S3 ignora todos ACLs los públicos del bucket de S3 que especifique en el BucketName parámetro.

- RestrictPublicBuckets

Tipo: Booleano

Predeterminado: true

Descripción: (opcional) si se establece en true, Amazon S3 restringe las políticas de bucket públicos para el bucket de S3 que especifique en el parámetro BucketName.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetAccountPublicAccessBlock
- s3:PutAccountPublicAccessBlock
- s3:GetBucketPublicAccessBlock
- s3:PutBucketPublicAccessBlock

Pasos de documentos

- aws:executeAwsApi: crea o modifica la configuración PublicAccessBlock del bucket de S3 especificado en el parámetro BucketName.
- aws:executeScript: regresa la configuración PublicAccessBlock del bucket de S3 especificado en el parámetro BucketName y verifica que los cambios se hayan realizado correctamente en función de los valores especificados en los parámetros del manual de procedimientos.

AWSConfigRemediation-ConfigureS3PublicAccessBlock

Descripción

El AWSConfigRemediation-ConfigureS3PublicAccessBlock runbook configura la configuración de un bloque de acceso público de Cuenta de AWS Amazon Simple Storage Service (Amazon S3) en función de los valores que especifique en los parámetros del runbook.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AccountId`

Tipo: cadena

Descripción: (obligatorio) El ID del propietario del bucket de S3 Cuenta de AWS que está configurando.

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `BlockPublicAcls`

Tipo: Booleano

Predeterminado: `true`

Descripción: (Opcional) Si se establece en `true`, Amazon S3 bloquea las listas de control de acceso público (ACLs) para los buckets S3 que pertenecen a los Cuenta de AWS que especifique en el `AccountId` parámetro.

- `BlockPublicPolicy`

Tipo: Booleano

Predeterminado: `true`

Descripción: (Opcional) Si se establece en `true`, Amazon S3 bloquea las políticas de bucket públicos para los buckets S3 propiedad de los Cuenta de AWS que especifique en el `AccountId` parámetro.

- `IgnorePublicAcls`

Tipo: Booleano

Predeterminado: `true`

Descripción: (Opcional) Si se establece en `true`, Amazon S3 ignora todos los buckets públicos ACLs de S3 que pertenezcan a los Cuenta de AWS que especifique en el `AccountId` parámetro.

- `RestrictPublicBuckets`

Tipo: Booleano

Predeterminado: `true`

Descripción: (Opcional) Si se establece en `true`, Amazon S3 restringe las políticas de bucket públicos para los buckets S3 que sean propiedad de los Cuenta de AWS que especifique en el `AccountId` parámetro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

Pasos de documentos

- `aws:executeAwsApi`: crea o modifica la configuración `PublicAccessBlock` de la Cuenta de AWS especificada en el parámetro `AccountId`.
- `aws:executeScript`- Devuelve la `PublicAccessBlock` configuración de lo Cuenta de AWS especificado en el `AccountId` parámetro y verifica que los cambios se hayan realizado correctamente en función de los valores especificados en los parámetros del runbook.

AWS-CreateS3PolicyToExpireMultipartUploads

Descripción

El AWS-CreateS3PolicyToExpireMultipartUploads manual crea una política de ciclo de vida para un segmento específico que vence de forma incompleta y las cargas de varias partes en curso transcurridos un número de días definido. Este manual combina la nueva política de ciclo de vida con cualquier política de ciclo de vida existente que ya exista.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de S3 que desea configurar.

- DaysUntilExpire

Tipo: entero

Descripción: (Obligatorio) El número de días que Amazon S3 espera antes de eliminar permanentemente todas las partes de la carga.

- RuleId

Tipo: cadena

Descripción: (obligatorio) El identificador utilizado para identificar la regla del ciclo de vida. Debe ser un valor único.

- S3Prefix

Tipo: cadena

Descripción: (opcional) El prefijo del nombre clave de los objetos a los que desea aplicar la configuración.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration

Pasos de documentos

- ConfigureExpireMultipartUploads (AWS:ExecuteScript): configura la política de ciclo de vida del depósito.
- VerifyExpireMultipartUploads (AWS:ExecuteScript): verifica que la política de ciclo de vida se haya configurado para el depósito.

Salidas

- VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse
- VerifyExpireMultipartUploads.LifecycleConfigurationRule

AWS-DisableS3BucketPublicReadWrite

Descripción

Use Amazon Simple Storage Service (Amazon S3) Block Public Access para deshabilitar el acceso de lectura y escritura a un bucket de S3 público. Para obtener más información, consulte [Uso de Bloqueo de acceso público de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- S3 BucketName

Tipo: cadena

Descripción: (obligatorio) bucket de S3 cuyo acceso desea restringir.

AWS-EnableS3BucketEncryption

Descripción

Configura el cifrado por defecto de un bucket de Amazon Simple Storage Service (Amazon S3).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de S3 donde desea cifrar el contenido.

- SSEAlgorithm

Tipo: cadena

Predeterminado: AES256

Descripción: (opcional) el algoritmo de cifrado del lado del servidor que se va a utilizar para el cifrado predeterminado.

AWS-EnableS3BucketKeys

Descripción

El AWS-EnableS3BucketKeys runbook habilita las claves de bucket en el bucket de Amazon Simple Storage Service (Amazon S3) que especifique. Esta clave de nivel de depósito crea claves de datos para nuevos objetos durante su ciclo de vida. Si no especifica un valor para el KmsKeyId parámetro, se utiliza el cifrado del lado del servidor mediante claves gestionadas de Amazon S3 (SSE-S3) como configuración de cifrado predeterminada.

Note

Las claves de bucket de Amazon S3 no son compatibles con el cifrado de doble capa del lado del servidor con claves AWS Key Management Service (AWS KMS) (DSSE-KMS).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **BucketName**

Tipo: cadena

Descripción: (obligatorio) El nombre del bucket de S3 para el que desea habilitar las claves de bucket.

- **KMSKeyId**

Tipo: cadena

Descripción: (opcional) El nombre del recurso de Amazon (ARN), el ID de clave o el alias de clave de la clave gestionada por el cliente AWS Key Management Service (AWS KMS) que desea utilizar para el cifrado del lado del servidor.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

Pasos de documentos

- `ChooseEncryptionType` (aws:branch): evalúa el valor proporcionado para el `KmsKeyId` parámetro para determinar si se utilizará SSE-S3 () o SSE-KMS. AES256
- `PutBucketKeysKMS` (aws:executeAwsApi): establece la `BucketKeyEnabled` propiedad en el bucket de S3 especificado utilizando el `true` valor especificado. `KmsKeyId`
- `PutBucketKeysAES256` (aws:executeAwsApi) - Establece la `BucketKeyEnabled` propiedad en `true` el bucket de S3 especificado con AES256 cifrado.
- `VerifyS3 BucketKeysEnabled` (aws: assertAwsResource Property): verifica que las claves de bucket estén habilitadas en el bucket S3 de destino.

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

Descripción

El manual de procedimientos AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy elimina las principales declaraciones de políticas que contienen caracteres comodín (Principal: * o Principal: "AWS": *) para acciones Allow de su política de bucket de Amazon Simple Storage Service (Amazon S3). También se eliminan las declaraciones de política con condiciones.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de Amazon S3 cuya política desea modificar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

Pasos de documentos

- `aws:executeScript`: modifica la política del bucket y verifica que las principales declaraciones de política con caracteres comodín se hayan eliminado del bucket de Amazon S3 que especificó en el parámetro `BucketName`.

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

Descripción

El manual de procedimientos `AWSConfigRemediation-RestrictBucketSSLRequestsOnly` crea una declaración de política de bucket de Amazon Simple Storage Service (Amazon S3) que deniega de forma explícita las solicitudes HTTP al bucket de Amazon S3 que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket de S3 al que desea denegar las solicitudes HTTP.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:DeleteBucketPolicy
- s3:GetBucketPolicy
- s3:PutEncryptionConfiguration
- s3:PutBucketPolicy

Pasos de documentos

- aws:executeScript: crea una política de bucket para el bucket de S3 especificado en el parámetro BucketName que deniega de forma explícita las solicitudes HTTP.

AWSSupport-TroubleshootS3PublicRead

Descripción

El manual de procedimientos AWSSupport-TroubleshootS3PublicRead diagnostica problemas al leer objetos del bucket público de Amazon Simple Storage Service (Amazon S3) que especifique en el parámetro S3BucketName. También se analiza un subconjunto de configuraciones para detectar los objetos del bucket de S3.

[Ejecuta esta automatización \(consola\)](#)

Limitaciones

- Esta automatización no comprueba los puntos de acceso que permiten el acceso público a los objetos.
- Esta automatización no evalúa las claves de condición de la política de bucket de S3.
- Si la utiliza AWS Organizations, esta automatización no evalúa las políticas de control de servicios para confirmar que se permite el acceso a Amazon S3.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- CloudWatchLogGroupName

Tipo: cadena

Descripción: (opcional) El grupo de CloudWatch registros de Amazon Logs al que desea enviar el resultado de la automatización. Si no se encuentra ningún grupo de registro que coincida con el valor que ha especificado, la automatización creará un grupo de registro con este valor de parámetro. El período de retención del grupo de registro creado por esta automatización es de 14 días.

- **CloudWatchLogStreamName**

Tipo: cadena

Descripción: (opcional) El flujo de registro de CloudWatch Logs al que desea enviar el resultado de la automatización. Si no se encuentra un flujo de registro que coincida con el valor especificado, la automatización creará un flujo de registro con este valor de parámetro. Si no especifica un valor para este parámetro, la automatización utilizará el `ExecutionId` como nombre del flujo de registro.

- **HttpGet**

Tipo: Booleano

Valores válidos: `true` | `false`

Predeterminado: `true`

Descripción: (opcional) si este parámetro está establecido en `true`, la automatización realiza una solicitud HTTP parcial a los objetos en el `S3BucketName` que especifique. Solo se regresa el primer byte del objeto mediante el encabezado HTTP Range.

- **IgnoreBlockPublicAccess**

Tipo: Booleano

Valores válidos: `true` | `false`

Predeterminado: `false`

Descripción: (opcional) si este parámetro está establecido en `true`, la automatización ignora la configuración del bloque de acceso público del bucket de S3 que especifique en el parámetro `S3BucketName`. No se recomienda cambiar este parámetro del valor predeterminado.

- **MaxObjects**

Tipo: entero

Valores válidos: 1-25

Valor predeterminado: 5

Descripción: (opcional) el número de objetos que se van a analizar en el bucket de S3 que especifique en el parámetro S3BucketName.

- S3 BucketName

Tipo: cadena

Descripción: (obligatorio) el nombre del bucket S3 para solucionar problemas.

- S3 PrefixName

Tipo: cadena

Descripción: (opcional) el prefijo del nombre clave de los objetos que desea analizar en su bucket de S3. Para obtener más información, consulte el tema para [Claves de objetos](#) en la Guía del usuario de Amazon Simple Storage Service.

- StartAfter

Tipo: cadena

Descripción: (opcional) el nombre de la clave del objeto en el que desea que la automatización comience a analizar los objetos del bucket de S3.

- ResourcePartition

Tipo: cadena

Valores válidos: aws | aws-us-gov | aws-cn

Valor predeterminado: aws

Descripción: (obligatorio) la partición donde está ubicado su bucket de S3.

- Detallado

Tipo: Booleano

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) para obtener información más detallada durante la automatización, defina este parámetro en `true`. Si el parámetro está establecido en `false`, solo se regresarán los mensajes de advertencia y error.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Los `logs:PutLogEvents` permisos `logs:CreateLogGroup``logs:CreateLogStream`, y solo son necesarios si deseas que la automatización envíe datos de registro a CloudWatch Logs.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:SimulateCustomPolicy",
        "iam:GetContextKeysForCustomPolicy",
        "s3:ListAllMyBuckets",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
      "Effect": "Allow"
    }
  ]
}
```

```

        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketRequestPayment",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPolicy",
            "s3:GetBucketAcl"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
        "Effect": "Allow"
    }
}

```

Pasos de documentos

- `aws:assertAwsResourceProperty`: confirma que el bucket de S3 existe y es accesible.
- `aws:executeScript`: regresa la ubicación del bucket de S3 y su ID de usuario canónico.
- `aws:executeScript`: regresa la configuración de bloqueo de acceso público de su cuenta y del bucket de S3.
- `aws:assertAwsResourceProperty`: confirma que el pagador de bucket de S3 está configurado en `BucketOwner`. Si `Requester Pays` está habilitado en el bucket de S3, la automatización finaliza.
- `aws:executeScript`: regresa el estado de la política del bucket de S3 y determina si se considera público. Para obtener más información acerca de los buckets S3 públicos, consulte [El significado de "público"](#) en la Guía del usuario de Amazon Simple Storage Service.
- `aws:executeAwsApi`: regresa la política de bucket de S3.
- `aws:executeAwsApi`: regresa todas las claves de contexto que se encuentran en la política de bucket de S3.
- `aws:assertAwsResourceProperty`: confirma si hay una denegación explícita en la política del bucket de S3 para la acción de la API `GetObject`.
- `aws:executeAwsApi`: regresa la lista de control de acceso (ACL) para el bucket de S3.
- `aws:executeScript`: Crea un grupo de CloudWatch registros y un flujo de registros si se especifica un valor para el `CloudWatchLogGroupName` parámetro.

- `aws:executeScript`: en función de los valores que especifique en los parámetros de entrada del manual de procedimientos, evalúa si alguna de las configuraciones del bucket de S3 recopiladas durante la automatización impide que el público acceda a los objetos. Este script realiza las siguientes funciones:
 - Evalúa la configuración de los bloques de acceso público
 - Regresa los objetos de su bucket de S3 en función de los valores que especifique en los parámetros `MaxObjects`, `S3PrefixName` y `StartAfter`.
 - Regresa la política del bucket de S3 para simular una política de IAM personalizada para los objetos regresados desde su bucket de S3.
 - Realiza una solicitud HTTP parcial a los objetos regresados si el parámetro `HttpGet` está establecido en `true`. Solo se regresa el primer byte del objeto mediante el encabezado HTTP `Range`.
 - Comprueba el nombre clave del objeto regresado para confirmar si termina con uno o dos puntos. Los nombres de claves de objeto que terminan en puntos no se pueden descargar de la consola de Amazon S3.
 - Comprueba si el propietario del objeto regresado coincide con el propietario del bucket de S3.
 - Comprueba si la ACL del objeto concede permisos de `READ` o `FULL_CONTROL` a usuarios anónimos.
 - Regresa las etiquetas asociadas al objeto.
 - Utiliza la política de IAM simulada para confirmar si hay una denegación explícita de este objeto en la política de bucket de S3 para la acción de la API `GetObject`.
 - Regresa los metadatos del objeto para confirmar que se admite la clase de almacenamiento.
 - Comprueba la configuración de cifrado del lado del servidor del objeto para confirmar si el objeto está cifrado mediante una AWS Key Management Service (AWS KMS) clave gestionada por el cliente.

Salidas

`AnalyzeObjects.bucket`

`AnalyzeObjects.objeto`

AWSsupport-ConfigureS3ReplicationSameAndCrossAccount

Descripción

`AWSsupport-ConfigureS3ReplicationSameAndCrossAccount`

El manual de `AWSSupport-ConfigureS3ReplicationSameAndCrossAccount` automatización configura la replicación de buckets de Amazon Simple Storage Service (Amazon S3) entre un bucket de origen y un bucket de destino para cuentas iguales o cruzadas. Esta automatización admite la replicación de cubos cifrados con el cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3) y el cifrado del lado del servidor con (SSE-KMS). AWS Key Management Service También admite el filtrado de replicación selectiva basado en prefijos y etiquetas, el control del tiempo de replicación de Amazon S3 (Amazon S3 RTC) con un SLA de 15 minutos y la replicación de marcadores de eliminación. La automatización realiza las siguientes acciones:

- Valida los parámetros de entrada y las configuraciones de los cubos para garantizar su compatibilidad.
- Comprueba la configuración de cifrado en los depósitos de origen y destino.
- Crea un nuevo rol AWS Identity and Access Management (IAM) con los permisos adecuados para la replicación si no se proporciona como entrada.
- Configura las reglas de replicación en función de parámetros específicos (prefijo, etiquetas o conjunto completo).
- Habilita el control de versiones en cubos si aún no está habilitado.
- Establece la configuración de replicación con funciones opcionales, como el control del tiempo de replicación (RTC) y la replicación de marcadores eliminados.

Important

- Esta automatización no admite buckets con las reglas de replicación existentes. El bucket de origen no debe tener ninguna configuración de replicación existente.
- Esta automatización crea una nueva función de IAM con los permisos adecuados para la replicación si no se proporciona la `ReplicationRole` entrada de S3.
- Esta automatización no replica los objetos existentes. La replicación de Amazon S3 solo se aplica a los objetos una `uploaded/created` vez habilitada la configuración de replicación.
- Para la replicación entre cuentas, debe proporcionar un rol de IAM en la cuenta de destino con los permisos adecuados para las operaciones y AWS KMS operaciones de Amazon S3 (si el bucket usa AWS KMS cifrado).
- Esta automatización utiliza la `aws:approve` acción, que detiene temporalmente la ejecución hasta que los responsables designados aprueben los cambios de configuración. Consulte [Ejecutar una automatización con aprobadores](#) para obtener más información.

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- `ValidateInputParameters`: valida todos los parámetros de entrada para garantizar su corrección y compatibilidad a fin de garantizar una configuración de replicación adecuada.
- `PrepareApprovalMessage`: Prepara un mensaje de aprobación con todos los parámetros de configuración de la replicación para que el usuario lo revise.
- `RequestApproval`: Solicita la aprobación de los usuarios autorizados antes de añadir la configuración de replicación de Amazon S3 al bucket de origen.
- `CheckBucketEncryption`: Comprueba la configuración de cifrado de los buckets de Amazon S3 de origen y destino para determinar la configuración de replicación compatible.
- `BranchOnEncryptionType`: La ejecución de ramificaciones se basa en el tipo de cifrado de buckets de Amazon S3 para aplicar la configuración de replicación adecuada a los buckets cifrados con SSE-S3 o SSE-KMS.
- `Configurar la SSES3 replicación`: configura la replicación de Amazon S3 para depósitos cifrados con cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3), incluidas las funciones de IAM y las reglas de replicación.
- `Configurar SSEKMSReplication`: configura la replicación de Amazon S3 para buckets cifrados con cifrado del lado del servidor con AWS KMS (SSE-KMS), incluidas las funciones de IAM, los permisos de clave de KMS y las reglas de replicación.
- `CleanupResources`: Limpia la función de IAM creada durante una configuración de replicación fallida cuando no se proporciona S3 como entrada. `ReplicationRole`

[Ejecuta esta automatización \(consola\)](#)

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `s3: ListBucket`
- `s3: GetBucketVersioning`
- `s3: GetEncryptionConfiguration`
- `s3: GetBucketLocation`
- `s3: GetReplicationConfiguration`

- s3: PutBucketVersioning
- s3: PutReplicationConfiguration
- objetivo: ListRoles
- objetivo: GetRole
- objetivo: GetRolePolicy
- objetivo: ListRoleTags
- objetivo: ListAttachedRolePolicies
- objetivo: ListRolePolicies
- objetivo: SimulatePrincipalPolicy
- objetivo: CreateRole
- objetivo: TagRole
- objetivo: PassRole
- objetivo: DeleteRole
- objetivo: DeleteRolePolicy
- objetivo: DetachRolePolicy
- objetivo: PutRolePolicy
- conjuntos: GetCallerIdentity
- sns: Publish
- kms: GetKeyPolicy (cuando los buckets usan SSE-KMS, replicación en la misma cuenta)
- kms: DescribeKey (cuando los buckets usan SSE-KMS, replicación en la misma cuenta)
- kms: PutKeyPolicy (cuando los buckets usan SSE-KMS, replicación en la misma cuenta)
- sts: AssumeRole (para la replicación entre cuentas)

CrossAccountReplicationRole (para escenarios con varias cuentas):

Para la replicación entre cuentas, debe proporcionar a CrossAccountReplicationRole la cuenta de destino los siguientes permisos:

- s3: ListBucket
- s3: GetBucketVersioning
- s3: GetBucketLocation
- s3: GetBucketPolicy

- s3: GetEncryptionConfiguration
- s3: PutBucketVersioning
- s3: PutBucketPolicy
- kms: GetKeyPolicy (cuando el depósito de destino multicuenta usa SSE-KMS)
- kms: DescribeKey (cuando el depósito de destino multicuenta usa SSE-KMS)
- kms: PutKeyPolicy (cuando el depósito de destino multicuenta usa SSE-KMS)

S3 ReplicationRole (función proporcionada por el cliente):

Si proporciona un S3 existenteReplicationRole, debe tener los siguientes permisos:

- s3: ListBucket
- s3: GetBucketLocation
- s3: GetReplicationConfiguration
- s3: GetObjectVersionAcl
- s3: GetObjectVersionTagging
- s3: GetObjectVersionForReplication
- s3: GetObjectTagging
- s3: ReplicateObject
- s3: ReplicateDelete
- s3: ReplicateTags
- s3: ObjectOwnerOverrideToBucketOwner
- KMS:Decrypt (para escenarios de SSE-KMS, clave KMS de origen)
- KMS:Encrypt (para escenarios de SSE-KMS, clave KMS de destino)
- kms: GenerateDataKey (para escenarios de SSE-KMS, clave KMS de destino)
- kms: ReEncrypt * (para escenarios de SSE-KMS, clave KMS de destino)

Ejemplo de AutomationAssumeRolepolítica para la replicación en la misma cuenta:

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



```

        "Sid": "S3Permissions",
        "Effect": "Allow",
        "Action": [
            "s3:GetBucketVersioning",
            "s3:GetEncryptionConfiguration",
            "s3:GetBucketLocation",
            "s3:GetReplicationConfiguration",
            "s3:ListBucket",
            "s3:PutBucketVersioning",
            "s3:PutReplicationConfiguration"
        ],
        "Resource": [
            "arn:aws:s3:::SOURCE_BUCKET",
            "arn:aws:s3:::DESTINATION_BUCKET"
        ]
    },
    {
        "Sid": "IAMReadOperations",
        "Effect": "Allow",
        "Action": [
            "iam:GetRole",
            "iam:GetRolePolicy",
            "iam:ListRoleTags",
            "iam:ListAttachedRolePolicies",
            "iam:ListRolePolicies",
            "iam:SimulatePrincipalPolicy"
        ],
        "Resource": "*"
    },
    {
        "Sid": "IAMListRolesForCleanup",
        "Effect": "Allow",
        "Action": "iam:ListRoles",
        "Resource": "*"
    },
    {
        "Sid": "IAMCreateAndTagRole",
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:TagRole"
        ],
        "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {

```

```

        "StringLike": {
            "aws:RequestTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
        }
    },
    {
        "Sid": "IAMPassRole",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "s3.amazonaws.com"
            }
        }
    },
    {
        "Sid": "TaggedIAMRoleModifyAndDeleteOperations",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringLike": {
                "aws:ResourceTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
            }
        }
    },
    {
        "Sid": "STSGetCallerIdentity",
        "Effect": "Allow",
        "Action": "sts:GetCallerIdentity",
        "Resource": "*"
    },
    {
        "Sid": "SNSPublish",
        "Effect": "Allow",
        "Action": "sns:Publish",

```

```

        "Resource": "SNS_TOPIC_ARN"
    },
    {
        "Sid": "KMSKeyReadOperations",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey"
        ],
        "Resource": [
            "arn:aws:kms:REGION:ACCOUNT_ID:key/SOURCE_KMS_KEY_ID",
            "arn:aws:kms:REGION:ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
        ]
    },
    {
        "Sid": "KMSKeyMutatingOperations",
        "Effect": "Allow",
        "Action": "kms:PutKeyPolicy",
        "Resource": [
            "arn:aws:kms:REGION:ACCOUNT_ID:key/SOURCE_KMS_KEY_ID",
            "arn:aws:kms:REGION:ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
        ],
        "Condition": {
            "StringEquals": {
                "kms:CallerAccount": "ACCOUNT_ID"
            }
        }
    }
]
}

```

Note

Las declaraciones de política (KMSKeyReadOperations y KMSKeyMutatingOperations) solo son obligatorias cuando los buckets utilizan el cifrado SSE-KMS.

Ejemplo de AutomationAssumeRolepolítica para la replicación entre cuentas:

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "S3SourceBucketOperations",
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketVersioning",
      "s3:GetEncryptionConfiguration",
      "s3:GetBucketLocation",
      "s3:GetReplicationConfiguration",
      "s3:ListBucket",
      "s3:PutBucketVersioning",
      "s3:PutReplicationConfiguration"
    ],
    "Resource": "arn:aws:s3:::SOURCE_BUCKET"
  },
  {
    "Sid": "IAMReadOperations",
    "Effect": "Allow",
    "Action": [
      "iam:GetRole",
      "iam:GetRolePolicy",
      "iam:ListRoleTags",
      "iam:ListAttachedRolePolicies",
      "iam:ListRolePolicies",
      "iam:SimulatePrincipalPolicy"
    ],
    "Resource": "*"
  },
  {
    "Sid": "IAMListRolesForCleanup",
    "Effect": "Allow",
    "Action": "iam:ListRoles",
    "Resource": "*"
  },
  {
    "Sid": "IAMCreateAndTagRole",
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:TagRole"
    ],
    "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
    "Condition": {

```

```

        "StringLike": {
            "aws:RequestTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
        }
    },
    {
        "Sid": "IAMPassRole",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "s3.amazonaws.com"
            }
        }
    },
    {
        "Sid": "TaggedIAMRoleModifyAndDeleteOperations",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringLike": {
                "aws:ResourceTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
            }
        }
    },
    {
        "Sid": "CrossAccountRoleAssumption",
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "CROSS_ACCOUNT_REPLICATION_ROLE_ARN"
    },
    {
        "Sid": "STSGetCallerIdentity",
        "Effect": "Allow",
        "Action": "sts:GetCallerIdentity",

```

```

        "Resource": "*"
    },
    {
        "Sid": "SNSPublish",
        "Effect": "Allow",
        "Action": "sns:Publish",
        "Resource": "SNS_TOPIC_ARN"
    },
    {
        "Sid": "KMSSourceKeyReadOperations",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey"
        ],
        "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID"
    },
    {
        "Sid": "KMSSourceKeyMutatingOperations",
        "Effect": "Allow",
        "Action": "kms:PutKeyPolicy",
        "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID",
        "Condition": {
            "StringEquals": {
                "kms:CallerAccount": "SOURCE_ACCOUNT_ID"
            }
        }
    }
]
}

```

Note

- Las declaraciones de política (KMSSourceKeyReadOperations y KMSSourceKeyMutatingOperations) solo son obligatorias cuando el bucket de origen utiliza el cifrado SSE-KMS.
- Sustituya CROSS_ACCOUNT_REPLICATION_ROLE_ARN por el valor de parámetro real que haya proporcionado a la automatización. CrossAccountReplicationRole

CrossAccountReplicationRoleEjemplo de política:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3DestinationBucketReadOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetEncryptionConfiguration",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "s3:PutBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::DESTINATION_BUCKET"
    },
    {
      "Sid": "KMSDestinationKeyReadOperations",
      "Effect": "Allow",
      "Action": [
        "kms:GetKeyPolicy",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
    },
    {
      "Sid": "KMSDestinationKeyMutatingOperations",
      "Effect": "Allow",
      "Action": "kms:PutKeyPolicy",
      "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID",
      "Condition": {
        "StringEquals": {
          "kms:CallerAccount": "DESTINATION_ACCOUNT_ID"
        }
      }
    }
  ]
}

```

 Note

Las sentencias KMS (`KMSDestinationKeyReadOperations` y `KMSDestinationKeyMutatingOperations`) solo son necesarias cuando el depósito de destino utiliza el cifrado SSE-KMS. Elimine estas declaraciones para los escenarios de SSE-S3.

Ejemplo de política de `CrossAccountReplicationRole` confianza:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "AUTOMATION_ASSUME_ROLE_ARN"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

 Note

Sustituya `AUTOMATION_ASSUME_ROLE_ARN` por el valor de parámetro real que proporcione a la automatización. `AutomationAssumeRole`

Ejemplo de política `ReplicationRole` de S3:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3SourceBucketPermissions",
      "Effect": "Allow",
```



```

    "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetReplicationConfiguration",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectTagging"
    ],
    "Resource": [
        "arn:aws:s3:::SOURCE_BUCKET",
        "arn:aws:s3:::SOURCE_BUCKET/*"
    ]
},
{
    "Sid": "S3DestinationBucketPermissions",
    "Effect": "Allow",
    "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ReplicateTags"
    ],
    "Resource": "arn:aws:s3:::DESTINATION_BUCKET/*"
},
{
    "Sid": "S3CrossAccountPermissions",
    "Effect": "Allow",
    "Action": "s3:ObjectOwnerOverrideToBucketOwner",
    "Resource": "arn:aws:s3:::DESTINATION_BUCKET/*"
},
{
    "Sid": "KMSSourceKeyPermissions",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID"
},
{
    "Sid": "KMSDestinationKeyPermissions",
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncrypt*"
    ]
}

```

```

    ],
    "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/
DESTINATION_KMS_KEY_ID"
  }
]
}

```

Note

- Las sentencias KMS (KMSSourceKeyPermissions y KMSDestinationKeyPermissions) solo son necesarias cuando los buckets utilizan el cifrado SSE-KMS.
- La CrossAccountPermissions declaración S3 solo es necesaria para la replicación de cubos entre cuentas.

Ejemplo de política de ReplicationRole confianza de S3:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWS Support-Configure S3 Replication Same And Cross Account](#) Systems Manager en Documentos.
2. Elija Execute automation (Ejecutar automatización).

3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Obligatorio):
 - Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
 - Tipo: `AWS::IAM::Role::Arn`
- SourceBucket (Obligatorio):
 - Descripción: (obligatorio) El nombre del depósito de Amazon S3 de origen en el que se crearán o actualizarán las reglas de replicación.
 - Tipo: `AWS::S3::Bucket::Name`
- DestinationBucket (Obligatorio):
 - Descripción: (obligatorio) El nombre del bucket de Amazon S3 de destino en el que se replicarán los objetos.
 - Tipo: `String`
 - Valor permitido: `^[0-9a-z][a-z0-9\\-\\.]{3,63}$`
- SourceAccountId (Obligatorio):
 - Descripción: (obligatorio) El ID de AWS cuenta en el que se encuentra el depósito de origen.
 - Tipo: `String`
 - Valor permitido: `^[0-9]{12,13}$`
- DestinationAccountId (Obligatorio):
 - Descripción: (obligatorio) El identificador de AWS cuenta en el que se encuentra el depósito de destino.
 - Tipo: `String`
 - Valor permitido: `^[0-9]{12,13}$`
- SnsNotificationArn (Obligatorio):
 - Descripción: (Obligatorio) El ARN de un tema de Amazon Simple Notification Service (Amazon SNS) para aprobaciones de automatización.
 - Tipo: `String`
 - Valor permitido: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):sns:[a-z]{2}(-gov)?(-iso[a-z])?-[a-z]{2,10}-[0-9]{1,2}:[0-9a-zA-Z-]{1,256}(.fifo)?$`

- **Aprobadores (obligatorio):**
 - Descripción: (Obligatoria) La lista de los IAM user/role ARNs autorizados a aprobar la ejecución de la automatización.
 - Tipo: `StringList`
 - Valor permitido: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:~\d{12}:(user|role)/[~w+=, .@~-/-/]+$`
- **S3 ReplicationRole (opcional):**
 - Descripción: (opcional) El ARN de un rol de IAM existente que se utilizará en las operaciones de replicación de Amazon S3. Esta función debe tener permisos para leer el bucket de origen y escribir en el bucket de destino, incluidos los permisos de KMS si los buckets utilizan el cifrado SSE-KMS. Si no se proporciona, la automatización creará un nuevo rol con los permisos adecuados.
 - Tipo: `String`
 - Valor permitido: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:~\d{12}:role/[~w+=, .@~-/-/]+$`
 - Valor predeterminado: `""`
- **CrossAccountReplicationRole (Opcional):**
 - Descripción: (opcional) El ARN de una función de IAM en la cuenta de destino que puede asumir la automatización. Esto es necesario para la replicación entre cuentas. Para la replicación en la misma cuenta, deje este campo en blanco.
 - Tipo: `String`
 - Valor permitido: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:~\d{12}:role/[~w+=, .@~-/-/]+$`
 - Valor predeterminado: `""`
- **ReplicateEntireBucket (Opcional):**
 - Descripción: (opcional) Si se establece en `true`, se replicará todo el depósito y tanto el prefijo como las etiquetas deberán estar vacíos. Si es falso, la replicación se basará en el prefijo o las etiquetas especificados.
 - Tipo: `Boolean`
 - Valores permitidos: `[true, false]`
 - Valor predeterminado: `true`
- **ReplicationRuleStatus (Opcional):**

- Descripción: (Opcional) Si se establece en `true`, se habilitarán las reglas de replicación creadas. Si se establece en `false`, las reglas de replicación creadas se establecerán en Deshabilitadas.
- Tipo: `Boolean`
- Valores permitidos: `[true, false]`
- Valor predeterminado: `true`
- `DeleteMarkerReplicationStatus` (Opcional):
 - Descripción: (Opcional) Si se establece en `true`, la automatización permite la replicación de marcadores de eliminación.
 - Tipo: `Boolean`
 - Valores permitidos: `[true, false]`
 - Valor predeterminado: `false`
- `ReplicationTimeControl` (Opcional):
 - Descripción: (Opcional) Si se establece en `true`, habilita Amazon S3 Replication Time Control (Amazon S3 RTC) con un SLA de 15 minutos para tiempos de replicación predecibles.
 - Tipo: `Boolean`
 - Valores permitidos: `[true, false]`
 - Valor predeterminado: `false`
- `ReplicaModifications` (Opcional):
 - Descripción: (Opcional) Si se establece en `true`, habilita la replicación de los cambios de metadatos realizados en los objetos de réplica, lo que permite que las modificaciones de los objetos replicados se sincronicen de nuevo con el origen.
 - Tipo: `Boolean`
 - Valores permitidos: `[true, false]`
 - Valor predeterminado: `false`
- Prefijo (opcional):
 - Descripción: (opcional) Filtro de prefijos para la replicación selectiva de objetos con prefijos clave específicos. El prefijo debe terminar con una barra al final (/) para que el filtrado de prefijos de Amazon S3 sea correcto.
 - Tipo: `String`
 - Valor permitido: `^[a-zA-Z0-9!_'()\-\ ]*/+$`
 - Valor predeterminado: `""`

- Etiquetas (opcionales):
 - Descripción: matriz JSON de etiquetas (opcional) para filtrar los objetos y replicarlos. Formato para una sola etiqueta: [{"Key»:» TagKey «, "Value»:» TagValue «}] y para varias etiquetas: [{"Key»:» TagKey 1", "Value»:» TagValue 1"}, {"Key»:» TagKey 2", "Value»:» TagValue 2"}].
 - Tipo: String
 - Valor permitido: `^\\[((\\{\\\"Key\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{1,128}\\\", \\\"Value\\\":\\\"[a-zA-Z0-9+\\-\\.:/@\\s]{0,256}\\\"\\})\\),\\{\\\"Key\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{1,128}\\\", \\\"Value\\\":\\\"[a-zA-Z0-9+\\-\\.:/@\\s]{0,256}\\\"\\})\\})?\\$`
 - Valor predeterminado: []

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `ValidateInputParameters`:

Valida todos los parámetros de entrada para comprobar su exactitud y compatibilidad a fin de garantizar una configuración de replicación adecuada.

- `PrepareApprovalMessage`:

Prepara el mensaje de aprobación con todos los parámetros de configuración de la replicación para que el usuario lo revise.

- `RequestApproval`:

Solicita la aprobación de los usuarios autorizados antes de proceder con los cambios en la configuración de replicación de Amazon S3.

- `CheckBucketEncryption`:

Comprueba la configuración de cifrado de los buckets de Amazon S3 de origen y destino para determinar la configuración de replicación compatible.

- `BranchOnEncryptionType`:

La ejecución de ramificaciones se basa en el tipo de cifrado de buckets de Amazon S3 para aplicar la configuración de replicación adecuada a los buckets cifrados de SSE-S3 o SSE-KMS.

- `SSES3Configure` la replicación:

Configura la replicación de Amazon S3 para depósitos cifrados con cifrado del lado del servidor con claves gestionadas por Amazon S3 (SSE-S3), incluidas las funciones de IAM y las reglas de replicación.

- SSEKMSReplicationConfigure:

Configura la replicación de Amazon S3 para buckets cifrados con cifrado del lado del servidor con AWS KMS (SSE-KMS), incluidas las funciones de IAM, los permisos de clave de KMS y las reglas de replicación.

- CleanupResources:

Limpia las funciones de IAM creadas durante una configuración de replicación fallida cuando el cliente no proporcionó S3. ReplicationRole

7. Una vez finalizada, revise los resultados de la ejecución en los pasos de configuración de la SSES3 replicación (para los depósitos cifrados con SSE-S3) o del SSEKMSReplication paso de configuración (para los depósitos cifrados con SSE-KMS) para ver los resultados de la ejecución, incluido el estado de la configuración de la replicación y la función de IAM utilizada para la replicación.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

AWSSupport-EmptyS3Bucket

Descripción

El manual de AWSSupport-EmptyS3Bucket automatización vacía un bucket existente de Amazon Simple Storage Service (Amazon S3) mediante una regla de configuración de caducidad del ciclo de vida.

 Important

- No se admiten los buckets de Amazon S3 con la autenticación multifactor (MFA) habilitada.
- Las reglas del ciclo de vida modificadas por este runbook eliminan permanentemente todos los objetos y sus versiones del bucket de Amazon S3 especificado. No puede recuperar objetos eliminados permanentemente. Para obtener más información, consulte [Expiring Objects](#).

¿Cómo funciona?

El manual de instrucciones `AWSSupport-EmptyS3Bucket` lleva a cabo los siguientes pasos de alto nivel:

- Suspende el control de versiones de bucket, si está activado.
- Actualiza la política de buckets para denegar cualquier llamada a la `s3:PutObject` API (para evitar nuevas subidas mientras se vacía).
- Actualiza las reglas del ciclo de vida para eliminar todos los objetos según los días de caducidad especificados en los parámetros de entrada.

 Note

- Las configuraciones del ciclo de vida no eliminan ni sobrescriben las versiones de objetos protegidas con Amazon S3 Object Lock.
- El proceso de eliminación es asíncrono y puede tardar un tiempo en completarse una vez finalizada la ejecución del runbook.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

El `AutomationAssumeRole` parámetro requiere las siguientes acciones para utilizar correctamente el runbook:

- `ssm: DescribeAutomationExecutions`
- `ssm: GetAutomationExecution`
- `s3: GetBucketVersioning`
- `s3: PutBucketVersioning`
- `s3: GetBucketPolicy`
- `s3: GetBucketLifecycleConfiguration`
- `s3: GetLifecycleConfiguration`
- `s3: PutBucketPolicy`
- `s3: PutBucketLifecycleConfiguration`
- `s3: PutLifecycleConfiguration`
- `s3: DeleteBucketPolicy`
- `s3: DeleteBucketLifecycle`

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-EmptyS3Bucket](#) Systems Manager, en Documentos.
2. Elija `Execute automation` (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - `AutomationAssumeRole` (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se

especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- **S3BucketName:**

El nombre del depósito de Amazon S3 que quieres vaciar.

- **SNSTopicArn:**

Proporcione el ARN del tema de Amazon SNS para la notificación de aprobación. Este tema de Amazon SNS se utiliza para enviar las notificaciones de aprobación necesarias durante la ejecución de la automatización.

- **Nombre de usuario de aprobación:**

Proporcione una lista de los directores AWS autenticados que puedan aprobar o rechazar la acción. El número máximo de aprobadores es. 10 Puede especificar los principales mediante cualquiera de estos formatos: un nombre de usuario AWS Identity and Access Management (IAM), un ARN de usuario de IAM, un ARN de rol de IAM o un ARN de usuario que asume el rol de IAM.

- **MinimumRequiredApprovals(Opcional):**

El número mínimo de aprobaciones requeridas para reanudar la automatización. Si no especifica ningún valor, el sistema tomará el valor predeterminado. 1 El valor de este parámetro debe ser un número positivo. El valor de este parámetro no puede superar el número de aprobadores definido por el parámetro `approverIAM`.

- **NoncurrentVersionExpirationDays(Opcional):**

Especifique el número de días en los que caducan las versiones de objetos no actuales. Cuando expiran, Amazon S3 elimina de forma permanente las versiones de objetos no actuales.

- Valor predeterminado: 1
- Valor máximo: 365
- **ExpirationDays (Opcional):**

Especifique la caducidad del ciclo de vida del objeto en los días del formulario.

- Valor predeterminado: 1
- Valor máximo: 365
- **AbortIncompleteMultipartUpload(Opcional):**

Especifique los días transcurridos desde el inicio de una carga multiparte incompleta que Amazon S3 esperará antes de eliminar permanentemente todas las partes de la carga.

- Valor predeterminado: 1
- Valor máximo: 365
- Reconocimiento:

Lea los detalles completos de las acciones realizadas en este manual de automatización y dé su consentimiento Yes, I understand and acknowledge si reconoce los pasos.

Input parameters

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

SNSTopicArn
(Required) The ARN of the Amazon Simple Notification Service (Amazon SNS) Topic for approval notification. This SNS topic is used to send the approval notifications required during the automation execution.

MinimumRequiredApprovals
(Optional) The minimum number of approvals required to resume the automation. If you don't specify a value, the system defaults to one. The value for this parameter must be a positive number. The value for this parameter can't exceed the number of approvers defined in the `ApproverIAM` parameter.

ExpirationDays
(Optional) Specify the expiration for the lifecycle of the object in days. Default value is 1 and max value is 365.

Acknowledgement
(Required) Please read the complete details of the actions performed by this automation runbook and write 'Yes, I understand and acknowledge' if you acknowledge the steps. ****Important**** You cannot recover permanently removed objects. For more information please review [Expiring objects] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-expire-general-considerations.html>).

S3BucketName
(Required) The name of the Amazon S3 bucket you want to empty.

ApproverIAM
(Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats, 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN.

NoncurrentVersionExpirationDays
(Optional) Specify the number of days when noncurrent object versions expire. Upon expiration, Amazon S3 permanently deletes the noncurrent object versions. Default value is 1 and max value is 365.

AbortIncompleteMultipartUpload
(Optional) Specify the days since the initiation of an incomplete multipart upload that Amazon S3 will wait before permanently removing all parts of the upload. Default value is 1 and max value is 365.

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **checkConcurrency:**

Garantiza que solo haya una ejecución de este runbook dirigida al bucket de Amazon S3 especificado. Si el runbook encuentra otra ejecución en curso dirigida al mismo nombre de bucket, devuelve un error y finaliza.

- **getBucketVersioningConfiguration:**

Obtiene el estado del control de versiones del bucket de Amazon S3 especificado.

- **branchOnStoppingIfMFADeleteEnabled**(condicional):

Detiene la automatización si la autenticación multifactor (MFA) está habilitada en el bucket de Amazon S3 especificado.

- **approvalToMakeChangesToTheProvidedS3Bucket**:

Espera la aprobación de los directores designados para deshabilitar el control de versiones de los buckets y actualizar la configuración de la política del bucket y las reglas del ciclo de vida del bucket de Amazon S3 especificado.

- **branchOnBucketVersioningStatus**(condicional):

Si el control de versiones está habilitado en el bucket de Amazon S3 especificado, deshabilítelo; de lo contrario, continúe actualizando la política del bucket y la configuración del ciclo de vida.

- **suspendBucketVersioning**:

Suspende el estado de control de versiones del bucket de Amazon S3 especificado.

- **updateBucketPolicyAndLifeCycleConfiguration**:

Añade o actualiza la política de bucket para denegar todas las `s3:PutObject` solicitudes y actualiza la configuración del ciclo de vida para que los objetos caduquen en función de los parámetros de entrada proporcionados por el usuario.

- **branchOnFailingIfBucketPropertiesNotUpdated**(condicional):

Comprueba el estado del `updateBucketPolicyAndLifeCycleConfiguration` paso e intenta revertir el estado original del control de versiones del bucket si lo modifica la automatización.

- **branchOnFailureOriginalVersioningStatus**(condicional):

En caso de error, se ramifica para determinar el estado original del control de versiones. Si esta automatización la activó y suspendió, intenta volver a habilitarla.

- **onFailureRestoreBucketVersioning**

Restaura el estado de control de versiones activado del bucket de Amazon S3 especificado.

7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución:

✓ Execution has been initiated.

Execution detail: AWSSupport-EmptyS3Bucket

Cancel executionActions

► Execution description

▼ Outputs

updateBucketPolicyAndLifecycleConfiguration.Message

===== Execution Result =====

INFO: Getting the configured lifecycle rules for the S3 Bucket: sample-not-empty-bucket
INFO: Getting bucket policy for S3 Bucket: sample-not-empty-bucket
INFO: Creating new bucket policy to deny any s3:PutObject API calls (to prevent new uploads while it is being emptied).
INFO: Creating a new lifecycle rule to delete all the objects according to the expiration days specified in the input parameters
INFO: The bucket updates have been successfully completed.
Upon the expiration of items, as specified in the parameters, the bucket will be emptied.
Meanwhile, S3 'put object' requests are denied by the bucket policy to prevent the upload of new items.

Execution status

Overall status

✓ Success

Failed

0

All executed steps

7

Cancelled

0

Succeeded

7

TimedOut

0

Executed steps (10)

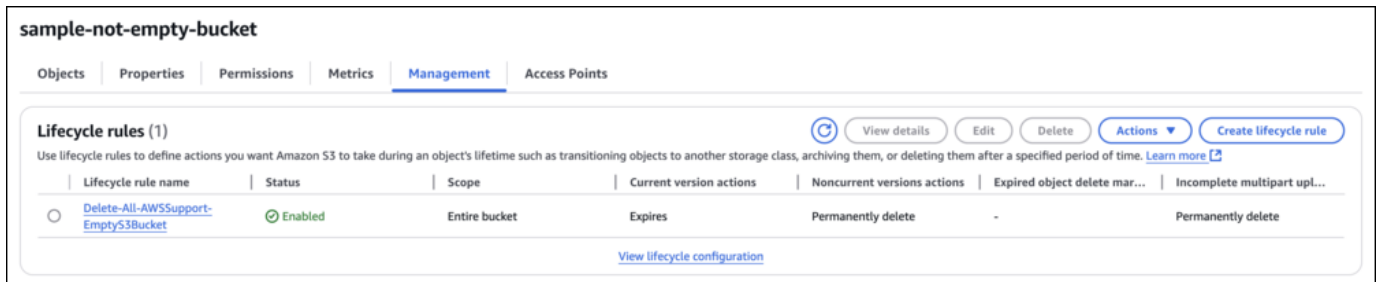
Find Steps

< 1 >

Step ID	Step #	Step name	Action	Status	Start time
17e09354-6a90-4216-9797-a9d6fa18d57c	1	checkConcurrency	aws:executeScript	✓ Success	Wed, 18 Dec 2024 08:01:54 GM
44bc75db-0bd9-44c1-9537-0b9ff9eea87a	2	getBucketVersioningConfiguration	aws:executeAwsApi	✓ Success	Wed, 18 Dec 2024 08:02:08 GM
1e942013-e886-4fce-b685-bc8e578bcb2a	3	branchOnStoppingIfMFADeleteEnabled	aws:branch	✓ Success	Wed, 18 Dec 2024 08:02:09 GM
742066ac-39a8-4699-8aa4-13a7a8b0239f	4	approvalToMakeChangesToTheProvidedS3Bucket	aws:approve	✓ Success	Wed, 18 Dec 2024 08:02:09 GM
34c276bb-f7e3-43f8-a89f-8d457040cc31	5	branchOnBucketVersioningStatus	aws:branch	✓ Success	Wed, 18 Dec 2024 08:03:24 GM
5f3efb16-d6f8-441e-b090-ab6c88ab2a9d	6	updateBucketPolicyAndLifecycleConfiguration	aws:executeScript	✓ Success	Wed, 18 Dec 2024 08:03:25 GM
739dd72a-e7de-42d9-900a-7a0aa5e826d0	7	branchOnFailingIfBucketPropertiesNotUpdated	aws:branch	✓ Success	Wed, 18 Dec 2024 08:03:29 GM
f97fc493-3d62-4884-901f-dcc2a2a3bcd0	8	suspendBucketVersioning	aws:executeAwsApi	⌚ Pending	-
4b02a204-8de7-49c8-b079-e94741c40a37	9	branchOnFailureOriginalVersioningStatus	aws:branch	⌚ Pending	-
92645daf-8587-4947-bc53-b4c440d07f84	10	onFailureRestoreBucketVersioning	aws:executeAwsApi	⌚ Pending	-

- Ejecución exitosa

Este flujo de trabajo actualiza la regla del ciclo de vida del depósito. Los objetos se eliminarán de acuerdo con la política de Delete-All-AWSSupport-EmptyS3-Bucket ciclo de vida.



- Fallo en la ejecución

No se realizará una eliminación parcial. Si se produce un error en la ejecución, se revierten el ciclo de vida y otros ajustes del depósito.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

Para obtener más información sobre la administración de buckets y objetos de Amazon S3, consulte [Vaciar un bucket](#).

AWSSupport-TroubleshootS3EventNotifications

Descripción

El manual de AWSSupport-TroubleshootS3EventNotifications AWS Systems Manager automatización ayuda a solucionar problemas con las notificaciones de eventos de bucket de Amazon Simple Storage Service (Amazon S3) configuradas con funciones AWS Lambda , temas del Amazon Simple Notification Service (Amazon SNS) o Amazon Simple Queue Service (Amazon SQS). Proporciona un informe de los ajustes de configuración de los diferentes recursos configurados con el bucket de Amazon S3 como notificación de eventos de destino.

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Comprueba si el bucket de Amazon S3 existe en la misma cuenta en la que `AWSSupport-TroubleshootS3EventNotifications` se ejecuta.
- Obtiene los recursos de destino (AWS Lambda función, tema de Amazon SNS o cola de Amazon SQS) configurados como notificaciones de eventos para el bucket de Amazon S3 mediante la API. [GetBucketNotificationConfiguration](#)
- Valida la existencia del recurso de destino y, a continuación, revisa la política basada en recursos de los recursos de destino para determinar si Amazon S3 puede publicar en el destino.
- Si ha cifrado el destino con una clave AWS Key Management Service (AWS KMS), se comprueba la política de claves para determinar si se permite el acceso a Amazon S3.
- Genera un informe de todas las comprobaciones de los recursos de destino.

Important

- Este runbook solo puede evaluar las configuraciones de notificaciones de eventos si el propietario del bucket de Amazon S3 es el mismo Cuenta de AWS propietario en el que se ejecuta el runbook de automatización.
- Además, este manual no puede evaluar las políticas sobre los recursos de destino que están alojados en otro. Cuenta de AWS

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- S3 BucketName

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

Descripción: (Obligatorio) El nombre del bucket de Amazon S3 configurado con las notificaciones de eventos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:GetBucketNotification`
- `sqs:GetQueueAttributes`
- `sqs:GetQueueUrl`
- `sns:GetTopicAttributes`
- `kms:GetKeyPolicy`
- `kms:DescribeKey`
- `kms:ListAliases`
- `lambda:GetPolicy`
- `lambda:GetFunction`
- `iam:GetContextKeysForCustomPolicy`
- `iam:SimulateCustomPolicy`
- `iam:ListRoles`
- `ssm:DescribeAutomationStepExecutions`

Ejemplo de política de IAM para el rol `Automation Assume`

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permission",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3PermissionGetBucketNotification",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketNotification"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "SQSPermission",
      "Effect": "Allow",
      "Action": [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource": "arn:aws:sqs:us-east-1:111122223333:"
    },
    {
      "Sid": "SNSPermission",
      "Effect": "Allow",
      "Action": [
        "sns:GetTopicAttributes"
      ],
      "Resource": "arn:aws:sns:us-east-1:111122223333:"
    }
  ]
}

```

```

        "Sid": "KMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey",
            "kms:ListAliases"
        ],
        "Resource": "arn:aws:kms:us-  

east-1:111122223333:key/key-id"
    },
    {
        "Sid": "LambdaPermission",
        "Effect": "Allow",
        "Action": [
            "lambda:GetPolicy",
            "lambda:GetFunction"
        ],
        "Resource": "arn:aws:lambda:us-  

east-1:111122223333:function:*"
    },
    {
        "Sid": "IAMPermission",
        "Effect": "Allow",
        "Action": [
            "iam:GetContextKeysForCustomPolicy",
            "iam:SimulateCustomPolicy",
            "iam:ListRoles"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SSMPermission",
        "Effect": "Allow",
        "Action": [
            "ssm:DescribeAutomationStepExecutions"
        ],
        "Resource": "*"
    }
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSsupport-TroubleshootS3EventNotifications](#) Systems Manager, en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:

- AutomationAssumeRole (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- S3 BucketName (obligatorio):

El nombre del bucket de Amazon S3 configurado con las notificaciones de eventos.

The screenshot shows the 'Input parameters' section of the AWS Systems Manager Automation console. It contains two parameters: 'AutomationAssumeRole' and 'S3BucketName'. 'AutomationAssumeRole' is optional and has a dropdown menu with 'AWS-SystemsManager-AutomationAdministrationRole' selected. 'S3BucketName' is required and has an empty text input field. Both fields have a refresh icon (circular arrow) to the right.

4. Seleccione Ejecutar.
5. Se inicia la automatización.
6. Este documento realiza los siguientes pasos:

- ValidateInputs

Valida que el bucket de Amazon S3 proporcionado pertenece a la misma cuenta en la que se ejecuta la automatización y busca la región en la que se aloja el bucket.

- GetBucketNotificationConfiguration

Llama a la GetBucketNotificationConfiguration API para revisar las notificaciones de eventos configuradas con el bucket de Amazon S3 y formatea el resultado.

- BranchOnSQSResourcePolítica

Depende de si hay recursos de Amazon SQS en las notificaciones de eventos.

- SQSResourceValide la política

Valida la política de recursos en los atributos de Amazon SQS Queue con permiso para Amazon sqs:SendMessage S3. Si el recurso de Amazon SQS está cifrado, comprueba que el cifrado

no utilice la AWS KMS clave predeterminada, es decir, `aws/sqs` y compruebe que la política de AWS KMS claves tiene permisos para Amazon S3.

- `BranchOnSNSResourcePolítica`

Depende de si hay recursos de Amazon SNS en las notificaciones de eventos.

- `SNSResourceValide` la política

Valida la política de recursos en Amazon SNS Topic Attributes `sns:Publish` con permiso para Amazon S3. Si el recurso de Amazon SNS está cifrado, comprueba que el cifrado no utilice la AWS KMS clave predeterminada, es decir, `aws/sns` y compruebe que la política de AWS KMS claves tiene permisos para Amazon S3.

- `BranchOnLambdaFunctionResourcePolicy`

Depende de si hay AWS Lambda funciones en las notificaciones de eventos.

- `ValidateLambdaFunctionResourcePolicy`

Valida la política de recursos si AWS Lambda la función tiene `lambda:InvokeFunction` permiso para Amazon S3.

- `GenerateReport`

Devuelve los detalles del manual, los pasos, los resultados y las recomendaciones para resolver cualquier problema con las notificaciones de eventos configuradas con el bucket de Amazon S3.

7. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución:

- Notificaciones de eventos de Amazon SQS

Si hay notificaciones de destino de Amazon SQS configuradas con el bucket de Amazon S3, se muestra una lista de las colas de Amazon SQS junto con los resultados de las comprobaciones. El informe incluye la verificación de recursos de Amazon SQS, la verificación de la política de acceso de Amazon SQS, la verificación de claves AWS KMS, la verificación del estado de las claves AWS KMS y la verificación de la política de claves. AWS KMS

- Notificaciones de eventos de Amazon SNS

Si hay notificaciones de destino de Amazon SNS configuradas con el bucket de Amazon S3, se muestra una lista de los temas de Amazon SNS junto con los resultados de las comprobaciones. El informe incluye la verificación de recursos de Amazon SNS, la verificación

de la política de acceso de Amazon SNS, la verificación de claves AWS KMS, la verificación del estado de las claves AWS KMS y la verificación de la política de claves. AWS KMS

- AWS Lambda Notificaciones de eventos

Si hay notificaciones de AWS Lambda destino configuradas con el bucket de Amazon S3, se muestra una lista de las funciones de Lambda junto con los resultados de las comprobaciones. El informe incluye la comprobación de recursos de Lambda y la comprobación de la política de acceso de Lambda.

```

▼ Outputs
generateReport.Output
-----
| Amazon S3 Event Notification Troubleshooting Results for S3 Bucket |
|-----|
| Amazon S3 Event Notifications |
|-----|
| SQS Queue: 1. arn:aws:sqs:us-east-1:354647335354:SAW-Core-TroubleshootS3EventNotification-EncryptedQueue | KMS Key: |
| SQS resource check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| SQS access policy check | ✓ [PASSED]: The resource policy is properly configured for use with S3 Bucket. |
| KMS key check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| KMS key status check | ✗ [FAILED]: The KMS key is disabled. |
| KMS key policy check | ✓ [PASSED]: The resource policy is properly configured for use with S3 Bucket. |
|-----|
| Amazon SNS Event Notifications |
|-----|
| SNS Topic: 1. arn:aws:sns:us-east-1:354647335354:CoreInfra-TestSNSTopic-1dW0EaySLdmr | KMS Key: alias/aws/sns |
| SNS resource check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| SNS access policy check | ✓ [PASSED]: The resource policy is properly configured for use with S3 Bucket. |
| KMS key check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| KMS key status check | ! [INFO]: Not Applicable. |
| KMS key policy check | ✗ [FAILED]: Amazon S3 Event Notifications does not support using SQS or SNS targets encrypted using AWS managed keys, i.e., aws/sns or aws/sqs respectively. |
|-----|
| AWS Lambda Event Notifications |
|-----|
| Lambda Function: 1. arn:aws:lambda:us-east-1:354647335354:function:SAW-Core-TroubleshootS3EventNotification-LambdaFunction |
| Lambda resource check | ✓ [PASSED]: The resource exists in the S3 Bucket Region. |
| Lambda access policy check | ✗ [FAILED]: No resource policies found on the resource. Please update the resource with a valid policy using this guide: https://docs.aws.amazon.com/AmazonS3/latest/userguide/grant-destin

```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSSupport-ContainS3Resource

Descripción

El AWSSupport-ContainS3Resource manual proporciona una solución automatizada para el procedimiento descrito en el artículo [Manual de ejecución de Support Automation Workflow \(SAW\): Contener un bucket de AWS Amazon S3 comprometido](#)

Important

- Este manual realiza varias operaciones que requieren privilegios elevados, como la modificación de las políticas de bucket, las etiquetas y las configuraciones de acceso público de Amazon S3. Estas acciones podrían provocar una escalada de privilegios o afectar a otras cargas de trabajo que dependen del bucket de Amazon S3 de destino. Debe revisar los permisos otorgados al rol especificado por el `AutomationAssumeRole` parámetro y asegurarse de que son adecuados para el caso de uso previsto. Puede consultar la siguiente AWS documentación para obtener más información sobre los permisos de IAM: [Identity and Access Management \(IAM\) PermissionsAWS AWS Systems Manager Automation Permissions](#).
- Este manual realiza acciones mutativas que podrían provocar la falta de disponibilidad o la interrupción de sus cargas de trabajo. En concreto, la `Contain` acción bloquea todo el acceso al bucket de Amazon S3 especificado, excepto los roles especificados en el `SecureRoles` parámetro. Esto podría afectar a cualquier aplicación o servicio que dependa del bucket de Amazon S3 de destino.
- Durante la `Contain` acción, este runbook puede crear un bucket de Amazon S3 adicional (especificado por el `BackupS3BucketName` parámetro) para almacenar la copia de seguridad de la configuración del bucket original, si aún no existe.
- Si el `Action` parámetro está establecido en `Restore`, este runbook intenta restaurar la configuración del bucket de Amazon S3 a su estado original en función de la copia de seguridad almacenada en el `BackupS3BucketName` bucket. Sin embargo, existe el riesgo de que el proceso de restauración falle y deje el bucket de Amazon S3 en un estado incoherente. El manual proporciona instrucciones para la restauración manual en caso de que se produzcan estos errores, pero debe estar preparado para gestionar posibles problemas durante el proceso de restauración.

Se recomienda revisar el manual detenidamente, comprender sus posibles impactos y probarlo en un entorno que no sea de producción antes de ejecutarlo en su entorno de producción.

¿Cómo funciona?

Este manual funciona de forma diferente según el tipo de recurso y la acción:

- Para el bucket de uso general de Amazon S3Containment: la automatización bloquea el acceso público al bucket, inhabilita la configuración de la ACL, impone la propiedad del objeto propietario del bucket y aplica una política restrictiva que niega todas las acciones de Amazon S3 al bucket, excepto las funciones de IAM permitidas enumeradas.
- Para el objeto de uso general de Amazon S3Containment: la automatización bloquea el acceso público al bucket, deshabilita la configuración de la ACL, impone la propiedad del objeto propietario del bucket e implementa una política de bucket restrictiva que niega todas las acciones de Amazon S3 en el objeto, excepto las funciones de IAM permitidas enumeradas.
- Para el bucket de directorio de Amazon S3Containment: la automatización aplica una política de bucket restrictiva que niega todas las acciones de Amazon S3 al bucket, excepto las funciones de IAM que figuran en la lista de permisos.
- Para el bucket de uso general de Amazon S3Restore: la automatización restaura la configuración inicial de Block Public Access, Bucket ACL, Bucket Owner Object y Bucket Policy a la configuración inicial antes de la contención.
- Para el objeto de uso general de Amazon S3Restore: la automatización restaura la configuración de acceso público en bloque, la configuración de ACL de bucket, la configuración de ACL de objetos, la propiedad del objeto propietario del bucket y la política de bucket a la configuración inicial antes de la contención.
- Para Amazon S3 Directory BucketRestore: la automatización restaura la política de bucket a la configuración inicial antes de la contención.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataforma

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- s3: CreateBucket
- s3: DeleteBucketPolicy
- s3: DeleteObjectTagging
- s3: GetAccountPublicAccessBlock
- s3: GetBucketAcl
- s3: GetBucketLocation
- s3: GetBucketOwnershipControls
- s3: GetBucketPolicy
- s3: GetBucketPolicyStatus
- s3: GetBucketTagging
- s3: GetEncryptionConfiguration
- s3: GetObject
- s3: GetObjectAcl
- s3: GetObjectTagging
- s3: GetReplicationConfiguration
- s3: ListBucket
- s3: PutAccountPublicAccessBlock
- s3: PutBucket ACL
- s3: PutBucketOwnershipControls
- s3: PutBucketPolicy
- s3: PutBucketPublicAccessBlock
- s3: PutBucketTagging
- s3: PutBucketVersioning
- s3: PutObject
- s3: PutObjectAcl
- s3 express: CreateSession
- s3express: DeleteBucketPolicy
- s3express: GetBucketPolicy
- s3express: PutBucketPolicy
- ssm: DescribeAutomationExecutions

A continuación, se muestra un ejemplo de una política de IAM que concede los permisos necesarios para: `AutomationAssumeRole`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetEncryptionConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketACL",
        "s3:PutBucketOwnershipControls",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ExpressPermissions",
      "Effect": "Allow",
```

```

        "Action": [
            "s3express:CreateSession",
            "s3express:DeleteBucketPolicy",
            "s3express:GetBucketPolicy",
            "s3express:PutBucketPolicy"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SSMPermissions",
        "Effect": "Allow",
        "Action": [
            "ssm:DescribeAutomationExecutions"
        ],
        "Resource": "*"
    }
]
}

```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-ContainS3Resource](#) Systems Manager en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - BucketName (Obligatorio):
 - Descripción: (Obligatorio) El nombre del bucket de Amazon S3.
 - Tipo: AWS::S3::Bucket::Name
 - Acción (obligatoria):
 - Descripción: (Obligatorio) Seleccione Contain esta opción para aislar el recurso de Amazon S3 o Restore intentar restaurar la configuración del recurso a su estado original a partir de una copia de seguridad anterior.
 - Tipo: cadena
 - Valores permitidos: Contain|Restore
 - DryRun (Opcional):

- Descripción: (opcional) Si se establece en `true`, la automatización no realizará ningún cambio en el recurso Amazon S3 de destino, sino que generará lo que hubiera intentado cambiar.
Valor predeterminado: `true`.
- Tipo: Booleano
- Valores permitidos: `true` | `false`
- BucketKeyName (Opcional):
 - Descripción: (opcional) La clave del objeto de Amazon S3 que desea contener o restaurar. Se utiliza durante la contención a nivel de objeto.
 - Tipo: cadena
 - Valor permitido: `^[a-zA-Z0-9\\.\_-\\\\\!*\'()/]{0,1024}$`
- BucketRestrictAccess(Condicional):
 - Descripción: (Condicional) El ARN de los usuarios o roles de IAM a los que se les permitirá acceder al recurso Amazon S3 de destino después de ejecutar las acciones de contención. Este parámetro es necesario cuando `Action` se establece en `Contain`.
 - Tipo: StringList
 - Valor permitido: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=, .@-]+$`
- TagIdentifier (Opcional):
 - Descripción: (opcional) Una etiqueta con el formato `Key=BatchId, Value=78925` que se añadirá a los recursos creados o modificados por este manual de instrucciones durante el flujo de trabajo de contención.
 - Tipo: cadena
 - Valor permitido: `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{0,128}$`
- Copias de seguridad S3 (condicionales): BucketName
 - Descripción: (Condicional) El bucket de Amazon S3 para hacer una copia de seguridad de la configuración del recurso de destino cuando `Action` está establecido en `Contain` o para restaurar la configuración desde cuando `Action` está establecido en `Restore`.
 - Tipo: `AWS::S3::Bucket::Name`
- BackupS3 KeyName (condicional):

- Descripción: (Condicional) Si `Action` se establece en `Restore`, especifica la clave de Amazon S3 que utilizará la automatización para intentar restaurar la configuración de los recursos de destino.
- Tipo: cadena
- Valor permitido: `^[a-zA-Z0-9\\.\_\-\!\*'()/{0,1024}]$`
- BackupS3 BucketAccess (condicional):
 - Descripción: (Condicional) El ARN de los usuarios o roles de IAM a los que se les permitirá acceder al bucket de respaldo de Amazon S3 después de ejecutar las acciones de contención. Este parámetro es obligatorio cuando lo es. `Action Contain`
 - Tipo: `StringList`
 - Valor permitido: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam:[0-9]{12}:(role|user)\\/[\\w+\\/=, .@-]+$`
- AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) de la función de IAM que permite a Systems Manager Automation realizar las acciones en su nombre.
 - Tipo: `AWS::IAM::Role::Arn`

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `validateRequiredInputs`

Valida los parámetros de entrada de automatización necesarios en función de la acción especificada.

- `assertBucketExists`

Comprueba si el bucket de Amazon S3 de destino existe y es accesible.

- `backupBucketPreComprueba`

Comprueba si el bucket de Amazon S3 de respaldo puede conceder acceso público de lectura o escritura a sus objetos.

- `backupTargetBucketMetadatos`

Describe la configuración actual del bucket de Amazon S3 de destino y carga la copia de seguridad en el bucket de Amazon S3 de respaldo especificado.

- `Contenga un cubo`

Realiza operaciones a nivel de bucket para contener el bucket de Amazon S3 de destino.

- `BranchOnActionAndMode`

Ramifica la automatización en función de los parámetros de entrada `Action` y `DryRun`.

- `RestoreInstanceConfiguration`

Restaura la configuración del bucket de Amazon S3 desde la copia de seguridad.

- `containFinalOutput`

Consolida la actividad de contención en un formato legible.

- `ReportContain`

Muestra los detalles del simulacro de las acciones de contención.

- `ReportRestore`

Muestra los detalles del ensayo en seco para las acciones de restauración.

- `ReportRestoreFailure`

Proporciona instrucciones para restaurar la configuración original del bucket de Amazon S3 durante un escenario de error en el flujo de trabajo de restauración.

- `ReportContainmentFailure`

Proporciona instrucciones para restaurar la configuración original del bucket de Amazon S3 durante un escenario de fallo en el flujo de trabajo de contención.

- `FinalOutput`

Muestra los detalles de las acciones de contención.

7. Una vez completada la ejecución, revise la sección de resultados para ver los resultados detallados de la ejecución:

- `ContainFinalOutput.Salida`

Muestra los detalles de las acciones de contención realizadas por este manual cuando se establece en `DryRun False`.

- `RestoreFinalOutput.Salida`

Muestra los detalles de las acciones de restauración realizadas por este runbook cuando se establece en DryRun False.

- Contiene 3ResourceDryRun. Salida

Muestra los detalles de las acciones de contención realizadas por este manual cuando DryRun se establece en True.

- Restaura S3. Salida ResourceDryRun

Muestra los detalles de las acciones de restauración realizadas por este runbook cuando DryRun se establece en True.

- ReportContainmentFailure.Salida

Proporciona instrucciones para restaurar la configuración original del recurso Amazon S3 de destino durante un escenario de error en el flujo de trabajo de contención.

- ReportRestoreFailure.Salida

Proporciona instrucciones para restaurar la configuración original del recurso Amazon S3 de destino durante un escenario de error en el flujo de trabajo de restauración.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Flujos de trabajo de automatización de Support](#)

Amazon SES

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Simple Email Service. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSSupport-AnalyzeSESMessagesSendingStatus](#)
- [AWSSupport-DeploySESSendingLogsToCloudWatchLogs](#)

AWSSupport - AnalyzeSESMessagesSendingStatus

Description (Descripción)

El manual de AWSSupport-AnalyzeSESMessagesSendingStatus automatización resume el estado de entrega del correo electrónico de los mensajes de correo electrónico no entregados y le brinda consejos para resolver por qué no se entregaron. El manual recupera los eventos de envío de correo electrónico de Amazon Simple Email Service (Amazon SES) almacenados en un grupo de Amazon CloudWatch Logs publicado por Amazon SES. Para obtener información sobre la publicación de eventos de Amazon SES, consulte [Supervisión mediante la publicación de eventos de Amazon Simple Email Service](#). El manual también proporciona un resumen y el cronograma de las entregas de correo electrónico, así como recomendaciones que pueden afectar a los mensajes de correo electrónico no entregados. Puedes encontrar esos mensajes en la sección de resultados de cada ejecución. Tenga en cuenta que este manual solo puede solucionar los problemas de los eventos después de la implementación del almacén de eventos.

¿Cómo funciona?

El manual de ejecución lleva a cabo los siguientes pasos:

- Comprueba las ejecuciones de automatización simultáneas para el mismo grupo de CloudWatch registros.
- Analice los eventos de Amazon SES correspondientes al mensaje IDs proporcionado por el parámetro de automatización.
- Envíe los resúmenes de entrega a la sección de resultados de la ejecución de la automatización.

Important

- Antes de ejecutar este runbook, debe almacenar los eventos de Amazon SES publicados en un grupo de CloudWatch registros especificado por el parámetro de automatización.

Este runbook solo analiza los eventos de Amazon SES almacenados en el grupo de registros.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `logs:StartQuery`
- `logs:GetQueryResults`
- `ses:GetIdentityMailFromDomainAttributes`
- `ses:GetSendQuota`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSsupport-AnalyzeSESMessagesSendingStatus](#) Systems Manager, en Documentos.

2. Elija **Execute automation** (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - **AutomationAssumeRole** (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que inicia este runbook.

- **MessageIds** (Obligatorio)

Mensaje de Amazon Simple Email Service separado por comas IDs de los eventos de Amazon Simple Email Service que desee analizar.

- **CloudWatchLogsGroup** (Opcional)

El grupo Amazon CloudWatch Logs que almacena los eventos de Amazon Simple Email Service. El nombre predeterminado del grupo de registros es `/ses/sending_event_logs``. Si desea utilizar un grupo de registros distinto del grupo de registros predeterminado, introduzca el nombre del grupo de registros en este campo. «,

- **QueryStartTime** (Opcional)

La hora de inicio del intervalo de tiempo para el análisis del evento. El formato de hora válido es ISO8601 (por ejemplo, ``YYY-MM-DDTHH:MM:SS``, ``1970-01-01T 00:00:00 ``). La fecha y hora por defecto es de hace 30 días.

- **QueryEndTime** (Opcional)

La hora de finalización del intervalo de tiempo para el análisis del evento. El formato de hora válido es ISO8601 (por ejemplo, ``YYY-MM-DDTHH:MM:SS``, ``1970-01-01T 00:00:00 ``). La fecha y hora por defecto es la hora actual.

Input parameters**AutomationAssumeRole**

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

 
CloudWatchLogsGroup

(Optional) The Amazon CloudWatch Logs group which stores Amazon SES events. The default log group name is `/ses/sending_event_logs`. If you would like to utilize another log group than the default log group, please enter your log group name in this field.

QueryEndTime

(Optional) The end time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is the current time.

MessageIds

(Required) Comma separated Amazon SES message IDs of the Amazon SES events that you would like to analyze.

QueryStartTime

(Optional) The start time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is 30 days ago.

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **CheckConcurrency:**

Garantiza que solo haya una ejecución de este runbook dirigida al grupo Amazon CloudWatch Logs. Si el runbook encuentra otra ejecución dirigida al mismo grupo de registros, devuelve un error y finaliza.

- **AnalyzeSesEvents:**

Analice los eventos de Amazon Simple Email Service almacenados en el grupo Amazon CloudWatch Logs especificado por el parámetro de automatización.

- **OutputFailureReason:**

Muestra mensajes de error en el paso de ejecución cuando el `AnalyzeSESMessagesSendingStatus` paso ha fallado.

7. Una vez completado, revise la sección de resultados para ver los resultados detallados de la ejecución:

- Resultado del análisis de un mensaje de correo electrónico no entregado debido a un rebote

Resultado de una ejecución automática de un mensaje de correo electrónico que no llegó al buzón de destino debido a un rebote.

▼ Outputs

OutputFailureReason.FailureReason

No output available yet because the step is not successfully executed

AnalyzeSesEvents.ResultMessage

```
==== Delivery summary of the message ID [REDACTED] ====
SES received bounces or complaints.
```

```
==== Timeline of [REDACTED] =====
```

```
[2024-08-21 06:22:58.193000+00:00] Your email message was sent from SES.
```

```
[2024-08-21 06:22:58.193000+00:00] SES received a bounce from [REDACTED].
```

```
Bounce type: Permanent(General)
```

```
Bounce sources:
```

```
- email address: [REDACTED] diagnostic code: "smtp; 550 5.1.1 user unknown"
```

```
==== Next Action ====
```

```
Please fix the issues described in the delivery error messages returned from the destination email servers in the Timeline section. In the case you received s
```

```
===== Recommendations for arn:aws:ses:[REDACTED] =====
```

```
- The SES account in this region seems to be in the sandbox environment. If you haven't requested the production access, please consider to move out of the san
```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSSupport-DeploySESSendingLogsToCloudWatchLogs

Descripción

El manual de AWSSupport-DeploySESSendingLogsToCloudWatchLogs automatización ayuda a configurar la infraestructura necesaria para la publicación de eventos de Amazon Simple Email Service (Amazon SES) en CloudWatch Amazon Logs CloudWatch (Logs). Este manual configura los componentes necesarios para capturar los eventos de envío de correos electrónicos y almacenarlos en CloudWatch registros para su monitoreo y análisis. Para obtener más información sobre la publicación de eventos de Amazon SES, consulte [Supervisar el envío de correos electrónicos mediante la publicación de eventos de Amazon SES](#).

Cuando el ApproveDeployAnalyticEnvironment parámetro se establece en approve, este manual crea nuevos AWS recursos en su AWS cuenta. La CloudFormation pila se elimina

automáticamente después del tiempo especificado en el `SleepTime` parámetro, a menos que se establezca en. `0`

¿Cómo funciona?

Este manual realiza las siguientes acciones:

- Muestra los conjuntos de configuración existentes que tienen destinos de eventos configurados para temas o transmisiones de entrega del Amazon Simple Notification Service (Amazon SNS).
- Crea la infraestructura necesaria para la publicación de eventos de Amazon SES en CloudWatch Logs cuando el `ApproveDeployAnalyticEnvironment` parámetro está establecido en `approve`.

Cuando el `ApproveDeployAnalyticEnvironment` parámetro se establece en `approve`, el runbook crea los siguientes recursos:

- Un nombre de CloudFormation pila `AWSSupport-SESSendingLogsToCloudWatchLogs` que incluye:
 - Tema de Amazon SNS con cifrado AWS Key Management Service (AWS KMS)
 - Cola de Amazon Simple Queue Service (Amazon SQS)
 - AWS Lambda función para procesar eventos de envío de correo electrónico
 - AWS Identity and Access Management Función de ejecución (IAM) con permisos para Amazon CloudWatch SQS y Logs
 - CloudWatch Grupo de registros
 - AWS KMS clave de cifrado
 - Conjunto de configuraciones de Amazon SES con destinos de eventos
- La infraestructura procesa los eventos de envío de correo electrónico en el siguiente flujo: Amazon SES Email Sending Events → Amazon SES Configuration Set → Tema de Amazon SNS → Amazon SQS Queue → Función Lambda → Registros CloudWatch
- Asocia el conjunto de configuraciones creado como el conjunto de configuraciones predeterminado para una identidad de Amazon SES específica cuando se proporciona el `SesIdentity` parámetro.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

/

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStackEvents`
- `cloudformation:DescribeStacks`
- `iam:CreateRole`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `kms:CreateKey`
- `kms:CreateAlias`
- `lambda:CreateFunction`
- `lambda:AddPermission`
- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `ses:CreateConfigurationSet`
- `ses:CreateConfigurationSetEventDestination`
- `ses:ListConfigurationSets`
- `ses:PutEmailIdentityConfigurationSetAttributes`
- `sns:CreateTopic`
- `sns:Subscribe`
- `sqs:CreateQueue`

- `sqs:SetQueueAttributes`
- `ssm:DescribeAutomationExecutions`

Ejemplo de política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "kms:CreateKey",
        "kms:CreateAlias",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "ses:CreateConfigurationSet",
        "ses:CreateConfigurationSetEventDestination",
        "ses:ListConfigurationSets",
        "ses:PutEmailIdentityConfigurationSetAttributes",
        "sns:CreateTopic",
        "sns:Subscribe",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "ssm:DescribeAutomationExecutions"
      ],
      "Resource": "*"
    }
  ]
}
```

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-DeploySESSendingLogsToCloudWatchLogs](#) Systems Manager en Documentos.
2. Elija Execute automation (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole (Opcional):
 - Descripción: (opcional) El nombre del recurso de Amazon (ARN) de la función de IAM que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.
 - Tipo: `AWS::IAM::Role::Arn`
 - ApproveDeployAnalyticEnvironment (Opcional):
 - Descripción: (opcional) Aprobación para implementar la infraestructura de publicación de eventos de Amazon SES. Ingrese approve para crear la CloudFormation pila y los recursos relacionados. Si se deja vacío, el runbook solo muestra los conjuntos de configuración existentes o los destinos de eventos de Amazon SNS en la región actual.
 - Tipo: `String`
 - Patrón de permisos: `^$|^approve$`
 - Valor predeterminado: `""`
 - SesIdentity (Opcional):
 - Descripción: (opcional) Identidad de Amazon SES (dirección de correo electrónico o dominio) para asociarla al conjunto de configuraciones recién creado como conjunto de configuraciones predeterminado. Esto sobrescribirá cualquier conjunto de configuraciones predeterminado existente para la identidad especificada.
 - Tipo: `String`
 - Valor predeterminado: `""`
 - CloudWatchLogGroupName (Opcional):
 - Descripción: (opcional) Nombre del grupo de CloudWatch registros que se va a crear para almacenar los eventos de envío de correo electrónico de Amazon SES.
 - Tipo: `String`
 - Patrón de permisos: `^[0-9a-zA-Z_.#/\-]{1,512}$`
 - Valor predeterminado: `/ses/sending_event_logs`

- Descripción: (opcional) Especifique si desea ocultar en los CloudWatch registros los datos de información de identificación personal (PII), como las direcciones de correo electrónico de destino y los asuntos del correo electrónico. `False` Configúrelo para incluir esta información en los registros.
- Tipo: `String`
- Valores permitidos: `[True, False]`
- Valor predeterminado: `True`
- `SleepTime` (Opcional):
 - Descripción: (opcional) Número de minutos que hay que esperar antes de eliminar automáticamente la CloudFormation pila. El valor predeterminado es 24 horas (1440 minutos) y el máximo es 7 días (10,080 minutos). Configúrelo en 0 para evitar la eliminación automática.
 - Tipo: `String`
 - Permitir patrón: `^(?:[0-9]|[1-9]\\d{1,3}|100[0-7][0-9])$`
 - Valor predeterminado: `1440`
- `RetainCloudWatchLogsOnDeletion` (Opcional):
 - Descripción: (opcional) Especifique si desea conservar el grupo de CloudWatch registros cuando se elimine la CloudFormation pila. `False` Configúrelo para eliminar el grupo de registros junto con la pila.
 - Tipo: `String`
 - Valores permitidos: `[True, False]`
 - Valor predeterminado: `True`
- `UniqueId` (Opcional):
 - Descripción: (Opcional) un identificador único para el flujo de trabajo.
 - Tipo: `String`
 - Permitir patrón: `\\{\\{ automation:EXECUTION_ID \\}\\}\\}|[a-zA-Z0-9-]+`
 - Valor predeterminado: `{ automation:EXECUTION_ID }`
 - Caracteres máximos: 64

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- `BranchOnValueOfParameterApproveDeployAnalyticEnvironment`

Determina si se debe implementar la infraestructura de publicación de eventos de Amazon SES en función del valor del `ApproveDeployAnalyticEnvironment` parámetro.

- `GetEligibleConfigurationSets`

Recupera los conjuntos de configuración de Amazon SES existentes e identifica aquellos con destinos de eventos configurados para transmisiones de entrega o temas de Amazon SNS.

- `CheckConcurrency`

Verifica que no exista ninguna pila existente y que ninguna otra ejecución simultánea de este runbook esté creando la misma pila.

- `DeploySesEventDestinations`

Crea la CloudFormation pila que contiene la infraestructura de publicación de eventos de Amazon SES, que incluye el tema de Amazon SNS, la cola de Amazon SQS, la función Lambda y el grupo de registros. CloudWatch

- `RelateConfigurationSetAsDefaultConfigurationSet`

Asocia el conjunto de configuraciones de Amazon SES recién creado como el conjunto de configuraciones predeterminado para la identidad de Amazon SES especificada (si se proporciona).

- `SleepBeforeDeleteCloudFormationStack`

Espera el tiempo especificado en el `SleepTime` parámetro antes de proceder a eliminar la CloudFormation pila.

- `DeleteCloudFormationStack`

Elimina la CloudFormation pila una vez transcurrido el período de tiempo especificado.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución.

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)

- [Página de inicio de Support Automation Workflows](#)

SageMaker IA

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon SageMaker AI. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-DisableSageMakerNotebookRootAccess](#)
- [AWSSupport-RequestSageMakerLimitIncrease](#)

AWS-DisableSageMakerNotebookRootAccess

Descripción

El AWS-DisableSageMakerNotebookRootAccess runbook deshabilita el acceso root en una instancia de bloc de notas de Amazon SageMaker AI. Durante la automatización, la instancia del bloc de notas se detiene para realizar los cambios necesarios. SageMaker No se admiten las instancias de bloc de notas de AI Studio.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- NotebookInstanceName

Tipo: cadena

Descripción: (obligatorio) El nombre de la instancia de SageMaker AI notebook a la que se va a deshabilitar el acceso root.

- StartInstanceAfterUpdate

Tipo: Booleano

Predeterminado: true

Descripción: (opcional) Determina si la instancia del bloc de notas se inicia después de deshabilitar el acceso raíz. La configuración predeterminada de este parámetro es `true`. Si se establece en `true`, la instancia se inicia cuando se deshabilita el acceso a la raíz. Si se establece en `false`, la instancia permanece en ese `stopped` estado después de deshabilitar el acceso raíz.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

Pasos de documentos

- `CheckNotebookInstanceStatus` (aws:executeAwsApi): comprueba el estado actual de la instancia del bloc de notas.
- `StopOrUpdateNotebookInstance` (aws:branch): se ramifica según el estado de la instancia del bloc de notas.
- `StopNotebookInstance` (aws:executeAwsApi): inicia la instancia si el estado es. `stopped`
- `WaitForInstanceToStop` (aws: waitForAwsResourceProperty): Comprueba que la instancia es `stopped`.
- `UpdateNotebookInstance` (aws:executeAwsApi): inhabilita el acceso root en la instancia del bloc de notas.
- `WaitForNotebookUpdate` (aws: waitForAwsResourceProperty): verifica que el acceso raíz esté deshabilitado y que la instancia tenga un `stopped` estado.
- `ChooseInstanceStart` (aws:branch): se ramifica en función de si la instancia debe iniciarse.
- `StartNotebookInstance` (aws:executeAwsApi): inicia la instancia del bloc de notas.
- `VerifyNotebookInstanceStatus` (aws: waitForAwsResourceProperty): Comprueba si la instancia está activa `available` antes de deshabilitar el acceso root.
- `VerifyNotebookInstanceRootAccess` (aws: assertAwsResource Property): verifica que la configuración de acceso raíz de la instancia del bloc de notas esté deshabilitada correctamente.

AWSSupport-RequestSageMakerLimitIncrease

Descripción

El `AWSSupport-RequestSageMakerLimitIncrease` manual permite el envío masivo de múltiples solicitudes de aumento de cuota de Amazon SageMaker AI (SageMaker AI) en una sola operación, lo que agiliza la gestión de cuotas para cargas de trabajo de aprendizaje automático a gran escala. El manual valida cada solicitud comparándola con cuotas de servicio de SageMaker IA ajustables, direcciona las solicitudes dentro de los umbrales de aprobación automática para su procesamiento inmediato y crea casos de AWS Support para las solicitudes que requieren una revisión manual. Los aumentos de cuota se aplican en la misma AWS región en la que se ejecuta el manual.

Important

Este manual no admite solicitudes de aumento de cuota para instancias informáticas especializadas, incluidos los tipos de instancias P4, P5 y Trainium. Para estos tipos de

instancias, envía solicitudes de aumento de cuota individuales a través de la consola AWS Service Quotas o AWS Support.

El manual se detiene durante un máximo de una hora mientras espera la aprobación de los directores designados mediante una notificación del Amazon Simple Notification Service (Amazon SNS). Revise detenidamente el resultado del `ApproveQuotaCodeLimitMapping` paso antes de aprobarlo, ya que los aumentos de cuota aprobados no se pueden revertir.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo `AWS::IAM::Role`: `:Arn`

Descripción: (opcional) El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a (Systems AWS Systems Manager Manager) Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- ResourcesMapping

Tipo: `StringList`

Descripción: (Obligatorio) Se aumentarán las cuotas de los servicios de SageMaker IA, especificadas como valores separados por dos puntos. Soporta tres formatos:

- `Category:Resource:NewValue`— cuando están disponibles los nombres de las categorías y de los recursos. Ejemplo: `spot-training-job:ml.c4.xlarge:25`

- `Resource:NewValue`— cuando solo está disponible el nombre del recurso. Ejemplo:
`max_number_of_experiment_trial_associations:501`
- `QuotaCode:NewValue`— cuando se utiliza el código de cuota directa. Ejemplo:
`L-9xAxx23x:25`

Puedes mezclar formatos en la misma solicitud, separados por comas. Máximo 50 artículos. Ejemplo: `studio:CodeEditor-ml.r6id.large:787,spot-training-job:ml.c4.xlarge:34,L-99AEC235:2`

- `SNSTopicArn`

Tipo: cadena

Descripción: (obligatorio) El ARN del tema Amazon SNS utilizado para enviar las notificaciones de aprobación durante la ejecución de la automatización.

- `ApproverIAM`

Tipo: `StringList`

Descripción: (Obligatoria) Una lista de directores AWS autenticados que pueden aprobar o rechazar las solicitudes de aumento de cuota. Máximo 10 aprobadores. Formatos aceptados: nombre de usuario de IAM, ARN de usuario de IAM, ARN de rol de IAM o ARN de usuario de rol de IAM.

- `MinimumRequiredApprovals`

Tipo: entero

Valores válidos: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

Valor predeterminado: 1

Descripción: (opcional) El número mínimo de aprobaciones necesarias para reanudar la automatización. No puede superar el número de aprobadores definido en `ApproverIAM`

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `servicequotas:ListServiceQuotas`

- `servicequotas:RequestServiceQuotaIncrease`
- `servicequotas:GetRequestedServiceQuotaChange`
- `sns:Publish`
- `ssm:SendAutomationSignal`

Pasos de documentos

1. `VerifyCategoriesAndResources`- Valida todas las categorías y los recursos especificados comparándolos con las cuotas de servicio de SageMaker IA ajustables mediante la API AWS Service Quotas. Confirma que cada nombre de categoría y recurso existe y se puede modificar, e identifica las solicitudes en las que el nuevo límite es inferior al valor actual.
2. `BranchOnValidCategoriesFound`- Comprueba si se ha encontrado alguna asignación de cuotas válida. Si existen asignaciones válidas, continúa con `ApproveQuotaCodeLimitMapping`. De lo contrario, salta directamente a `GenerateSummaryReport`.
3. `ApproveQuotaCodeLimitMapping`- Prepara un mensaje de aprobación detallado en el que se muestran las solicitudes válidas listas para su procesamiento, las solicitudes no válidas con explicaciones (por ejemplo, límites inferiores a los valores actuales o códigos de cuota no admitidos) y un desglose completo de todas las solicitudes de aumento de cuota para su revisión antes de su aprobación.
4. `WaitingForApproval`- Detiene la automatización y envía una notificación de aprobación al tema de Amazon SNS especificado. Los aprobadores designados deben revisar el resultado del `ApproveQuotaCodeLimitMapping` paso y aprobar o rechazar las solicitudes. Este paso se agota después de 3600 segundos (una hora) si no se realiza ninguna acción.
5. `RequestQuotaIncreases`- Envía solicitudes individuales de aumento de cuota para cada recurso válido a través de la API AWS Service Quotas. El ritmo de las solicitudes es de una por segundo para evitar la limitación de la API. Maneja las excepciones de la API con reintentos exponenciales.
6. `WaitForRequestQuotaIncreaseResults`- Consulta el estado de todas las solicitudes de aumento de cuota enviadas hasta que no quede ninguna en `PENDING` ese estado. Los estados de los terminales aceptados son `CASE_OPENEDAPPROVED`, `DENIED`, `NOT_APPROVEDCASE_CLOSED`, y `INVALID_REQUEST`.
7. `GetRequestQuotaIncreaseResults`- Recupera el estado final de todas las solicitudes de aumento de cuota enviadas desde la API AWS Service Quotas y asigna el caso de soporte IDs a sus recursos y solicitudes de informes IDs correspondientes.

8. `GenerateSummaryReport`- Recopila un resumen completo de todas las solicitudes de aumento de cuota y sus resultados, que incluye el número total de solicitudes, los detalles de cada solicitud, los casos de soporte IDs para las solicitudes que requieren una revisión manual y los próximos pasos a seguir.

Salidas

`GenerateSummaryReport.SummaryReport`- Un resumen completo de todas las solicitudes de aumento de cuota, sus estados y cualquier caso de soporte IDs creado para su revisión manual.

Secrets Manager

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Secrets Manager Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-DeleteSecret](#)
- [AWSConfigRemediation-RotateSecret](#)

AWSConfigRemediation-DeleteSecret

Descripción

El `AWSConfigRemediation-DeleteSecret` runbook elimina un secreto y todas las versiones almacenadas en él. AWS Secrets Manager Si lo desea, puede especificar el período de recuperación durante el cual puede restaurar el secreto. Si no especifica un valor para el parámetro `RecoveryWindowInDays`, la operación se establece de forma predeterminada en 30 días.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- RecoveryWindowInDays

Tipo: entero

Valores válidos: 7-30

Valor predeterminado: 30

Descripción: (opcional) el número de días durante los que puede restaurar el secreto.

- SecretId

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del secreto que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- secretsmanager>DeleteSecret
- secretsmanager:DescribeSecret

Pasos de documentos

- `aws:executeAwsApi`: elimina el secreto que especifique en el parámetro `SecretId`.
- `aws:executeScript`: verifica que se ha programado la eliminación del secreto.

AWSConfigRemediation-RotateSecret

Descripción

El `AWSConfigRemediation-RotateSecret` runbook rota un secreto almacenado en. AWS Secrets Manager

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `RotationInterval`

Tipo: Interval

Valores válidos: 1-365

Descripción: (obligatorio) el número de días entre las rotaciones del secreto.

- `RotationLambdaArn`

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) de la función AWS Lambda que puede rotar el secreto.

- `SecretId`

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) del secreto que desea rotar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

Pasos de documentos

- `aws:executeAwsApi`: rota el secreto que especifique en el parámetro `SecretId`.
- `aws:executeScript`: verifica que la rotación esté habilitada en el secreto.

CSPM de Security Hub

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Security Hub CSPM Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-EnableSecurityHub](#)

AWSConfigRemediation-EnableSecurityHub

Descripción

El AWSConfigRemediation-EnableSecurityHub runbook habilita AWS Security Hub CSPM (Security Hub CSPM) para la automatización Cuenta de AWS y el Región de AWS lugar donde se ejecuta. Para obtener información sobre Security Hub CSPM, consulte [¿Qué es? AWS Security Hub CSPM](#) en la Guía del AWS Security Hub usuario.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- EnableDefaultStandards

Tipo: Booleano

Predeterminado: true

Descripción: (Obligatorio) Si se establece en true, los estándares de seguridad predeterminados designados por Security Hub CSPM están habilitados.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Pasos de documentos

- `aws:executeAwsApi`- Activa el CSPM de Security Hub en la cuenta corriente y la región.
- `aws:executeAwsApi`- Verifica que el Security Hub CSPM esté habilitado.

AWS Shield

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS Shield Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSPremiumSupport-DDoSResiliencyAssessment](#)

AWSPremiumSupport-DDoSResiliencyAssessment

Descripción

El `AWSPremiumSupport-DDoSResiliencyAssessment` manual de AWS Systems Manager automatización le ayuda a comprobar las vulnerabilidades de DDoS y a configurar los recursos de acuerdo con la AWS Shield Advanced protección que tenga. Cuenta de AWS Proporciona un informe sobre los ajustes de configuración de los recursos que son vulnerables a los ataques distribuidos de denegación de servicio (DDoS). Se utiliza para recopilar, analizar y evaluar los siguientes recursos: Amazon Route 53, Amazon Load Balancers, Amazon CloudFront distributions AWS Global Accelerator y AWS Elastic en IPs cuanto a sus ajustes de configuración, de acuerdo con las prácticas

recomendadas AWS Shield Advanced de protección. El informe de configuración final está disponible en el bucket de Amazon S3 de su elección como archivo HTML.

¿Cómo funciona?

Este manual contiene una serie de comprobaciones para comprobar los distintos tipos de recursos que están habilitados para el acceso público y si tienen las protecciones configuradas según las recomendaciones del documento técnico sobre las [mejores prácticas de Estados AWS DDo Unidos](#). El manual de procedimientos realiza lo siguiente:

- Comprueba si la suscripción a está habilitada. AWS Shield Advanced
- Si está habilitada, busca si hay algún recurso protegido por Shield Advanced.
- Busca todos los recursos mundiales y regionales en Cuenta de AWS y comprueba si están protegidos por Shield.
- Requiere los parámetros del tipo de recurso para la evaluación, el nombre del bucket de Amazon S3 y el Cuenta de AWS ID del bucket de Amazon S3 (S3BucketOwner).
- Regresa los resultados como un informe HTML almacenado en el bucket de Amazon S3 proporcionado.

Los parámetros de entrada AssessmentType deciden si se realizarán las comprobaciones de todos los recursos. De forma predeterminada, el manual de procedimientos comprueba todos los tipos de recursos. Si solo se selecciona el parámetro GlobalResources o RegionalResources, el manual de procedimientos comprueba únicamente los tipos de recursos seleccionados.

Important

- El acceso a AWSPremiumSupport-* los manuales requiere una suscripción a Business + Support, Enterprise Support o Unified Operations. Para obtener más información, consulte [Comparar planes de AWS Support](#).
- Este manual de procedimientos requiere una [suscripción AWS Shield Advanced](#) de ACTIVE.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AssessmentType

Tipo: cadena

Descripción: (opcional) Determina el tipo de recursos que se van a evaluar para la evaluación de resiliencia DDoS. De forma predeterminada, el manual de procedimientos evaluará los recursos tanto globales como regionales. Para los recursos regionales, el manual de procedimientos describe todos los equilibradores de carga de aplicaciones (ALB) y redes (NLB), así como todo el grupo de escalado automático de su Cuenta de AWS/región.

Valores válidos: ['Global Resources', 'Regional Resources', 'Global and Regional Resources']

Predeterminado: recursos globales y regionales

- S3 BucketName

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

Descripción: (obligatorio) el nombre del bucket de Amazon S3 en el que se cargará el informe.

Valor permitido: `^[0-9a-z][a-z0-9\-\.\.]{3,63}$`

- S3 BucketOwnerAccount

Tipo: cadena

Descripción: (Opcional) El Cuenta de AWS propietario del bucket de Amazon S3. Especifique este parámetro si el bucket de Amazon S3 pertenece a otro; de lo contrario Cuenta de AWS, puede dejar este parámetro en blanco.

Valor permitido: `^$|^[0-9]{12,13}$`

- S3 BucketOwnerRoleArn

Tipo: `AWS::IAM::Role::Arn`

Descripción: (opcional) El ARN de un rol de IAM con permisos para describir el bucket de Amazon S3 y Cuenta de AWS bloquear la configuración de acceso público si el bucket está en otro. Cuenta de AWS Si no se especifica este parámetro, el manual de procedimientos utilizará `AutomationAssumeRole` o el usuario de IAM que inició este manual de procedimientos (si `AutomationAssumeRole` no se especifica). Por favor consulte la sección de permisos necesarios en la descripción del manual de procedimientos.

Valor permitido: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam:[0-9]{12,13}:role/.*$`

- S3 BucketPrefix

Tipo: cadena

Descripción: (opcional) el prefijo de la ruta dentro de Amazon S3 para almacenar los resultados.

Valor permitido: `^[a-zA-Z0-9][-. /a-zA-Z0-9]{0,255}$|^$`

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Ejemplo de política de IAM para el rol Automation Assume

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::<bucket-name>",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::<bucket-name>/*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:ListDistributions",
        "ec2:DescribeInstances",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkAcls",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",

```

```

        "globalaccelerator:ListAccelerators",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "route53:ListHostedZones",
        "route53:GetHealthCheck",
        "shield:ListProtections",
        "shield:GetSubscriptionState",
        "shield:DescribeSubscription",
        "shield:DescribeEmergencyContactSettings",
        "shield:DescribeDRTAccess",
        "waf:GetWebACL",
        "waf:GetRateBasedRule",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "waf-regional:GetWebACLForResource",
        "waf-regional:GetWebACL"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": "iam:PassRole",
    "Resource":
    "arn:aws:iam::111122223333:role/automation-assume-role-name",
    "Effect": "Allow"
}
]
}

```

Instrucciones

1. Navegue hasta [AWSPremiumSupport-DDoSResiliencyAssessment](#) la AWS Systems Manager consola.
2. Elija Ejecutar automatización
3. Para los parámetros de entrada, introduzca lo siguiente:
 - AutomationAssumeRole(Opcional):

El nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no

se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **AssessmentType(Opcional):**

Determina el tipo de recursos que se van a evaluar para la evaluación de la resiliencia DDoS. De forma predeterminada, el manual de procedimientos evalúa tanto los recursos globales como los regionales.

- **S3 BucketName (obligatorio):**

El nombre del bucket de Amazon S3 para guardar el informe de evaluación en formato HTML.

- **S3 BucketOwner (opcional):**

El Cuenta de AWS ID del bucket de Amazon S3 para la verificación de propiedad. El Cuenta de AWS ID es obligatorio si el informe debe publicarse en un bucket de Amazon S3 multicuenta y es opcional si el bucket de Amazon S3 se encuentra en el mismo lugar donde se Cuenta de AWS inició la automatización.

- **S3 BucketPrefix (opcional):**

Cualquier prefijo de la ruta dentro de Amazon S3 para almacenar los resultados.

Input parameters

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

Select an existing IAM Role

ssm-admin

arn:aws:iam::[redacted]:role/ssm-admin

S3BucketName
(Required) The name of the Amazon S3 bucket to save the assessment report in HTML format.

Select an existing S3 Bucket

[redacted]

S3BucketPrefix
(Optional) Any prefix for the path inside Amazon S3 for storing the results. Example path with prefix: S3://<BucketName>/<Prefix>

String

ResourceType
(Required) Determines the type of resources to be evaluated for DDoS resiliency assessment. By default, the runbook will evaluate both global and regional resources.

Global and Regional Resources

S3BucketOwner
(Required) The Account ID of the Amazon S3 bucket for ownership verification.

[redacted]

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- **CheckShieldAdvancedState:**

Comprueba si Cuenta de AWS está suscrito AWS Shield Advanced y si el runbook tiene acceso al bucket de Amazon S3.

- **S3: BucketSecurityChecks**

Comprueba si el bucket de Amazon S3 especificado en «S3BucketName» permite permisos de acceso de lectura o escritura anónimos o públicos, si el bucket tiene activado el cifrado en reposo y si el Cuenta de AWS ID proporcionado en «S3BucketOwner» es el propietario del bucket de Amazon S3.

- BranchOnShieldAdvancedStatus:

Las sucursales documentan los pasos según el estado de la AWS Shield Advanced suscripción y el estado de propiedad del bucket de and/or Amazon S3.

- ShieldAdvancedConfigurationReview:

Revisa las configuraciones de Shield Advanced para garantizar que estén presentes los detalles mínimos requeridos. Por ejemplo: el equipo de IAM Access for AWS Shield Response Team (SRT), los detalles de la lista de contactos y el estado de participación proactiva del SRT.

- ListShieldAdvancedProtections:

Muestra los recursos protegidos de Shield y crea un grupo de recursos protegidos para cada servicio.

- BranchOnResourceTypeAndCount:

Ramifica los pasos del documento según el valor del parámetro Resource Type y la cantidad de recursos globales protegidos por Shield.

- ReviewGlobalResources:

Revisa los recursos globales protegidos de Shield Advanced, como las zonas alojadas, las CloudFront distribuciones y los aceleradores globales de Route 53.

- BranchOnResourceType:

Ramifica los pasos del documento en función de las selecciones de tipo de recurso, ya sean globales, regionales o ambas.

- ReviewRegionalResources:

Revisa los recursos regionales protegidos de Shield Advanced, como los balanceadores de carga de aplicaciones, los balanceadores de carga de red, los balanceadores de carga clásicos y las instancias de Amazon Elastic Compute Cloud (Amazon EC2) (Elastic). IPs

- SendReportToS3:

Carga los detalles del informe de evaluación DDoS en el bucket de Amazon S3.

7. Una vez completado, el URI del archivo HTML del informe de evaluación se proporciona en el bucket de Amazon S3:

Enlace a la consola S3 y URI de Amazon S3 para el informe sobre la ejecución correcta del manual de procedimientos

▼ Outputs		
SendReportToS3.AssessmentReportS3ConsoleUrl https://s3.console.aws.amazon.com/s3/object/ddos-readiness-review?region=us-east-1&prefix=ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html		
SendReportToS3.AssessmentReportS3Uri S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html		
Execution status		
Overall status ✔ Success	All executed steps 9	# Succeeded 9
# Failed 0	# Cancelled 0	# TimedOut 0

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS documentación de servicio

- [AWS Shield Advanced](#)

Amazon SNS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Simple Notification Service. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-EnableSNSTopicDeliveryStatusLogging](#)

- [AWSConfigRemediation-EncryptSNSTopic](#)
- [AWS-PublishSNSNotification](#)

AWS-EnableSNSTopicDeliveryStatusLogging

Descripción

El AWS-EnableSNSTopicDeliveryStatusLogging manual configura el registro del estado de la entrega para un punto HTTP final de Amazon Data Firehose, Lambda o Amazon Simple Platform application Queue Service (Amazon SQS). Esto permite a Amazon SNS registrar las alertas fallidas y una muestra del porcentaje de notificaciones de alertas que se han enviado correctamente a Amazon. CloudWatch Si el registro del estado de entrega ya está configurado para el tema, el manual sustituirá la configuración existente por los nuevos valores que especifique para los parámetros de entrada.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- EndpointType

Tipo: cadena

Valores válidos:

- HTTP
- Firehose
- Lambda
- Aplicación
- SQS

Descripción: (Obligatorio) El tipo de punto final temático de Amazon SNS para el que desea registrar los mensajes de notificación del estado de la entrega.

- TopicArn

Tipo: cadena

Descripción: (obligatorio) El ARN del tema de Amazon SNS para el que desea configurar el registro del estado de entrega.

- SuccessFeedbackRoleArn

Tipo: cadena

Descripción: (obligatorio) El ARN de la función de IAM que Amazon SNS utiliza para enviar los registros de los mensajes de notificación correctos. CloudWatch

- SuccessFeedbackSampleRate

Tipo: cadena

Valores válidos: 0-100

Descripción: (Obligatorio) El porcentaje de mensajes correctos que se deben muestrear para el tema de Amazon SNS especificado.

- FailureFeedbackRoleArn

Tipo: cadena

Descripción: (obligatorio) El ARN de la función de IAM que Amazon SNS utiliza para enviar los registros de los mensajes de notificación de errores. CloudWatch

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Pasos de documentos

- `aws:executeAwsApi`- Aplica el valor del `SuccessFeedbackRoleArn` parámetro al tema de Amazon SNS.
- `aws:executeAwsApi`- Aplica el valor del `SuccessFeedbackSampleRate` parámetro al tema de Amazon SNS.
- `aws:executeAwsApi`- Aplica el valor del `FailureFeedbackRoleArn` parámetro al tema de Amazon SNS.
- `aws:executeScript`- Confirma que el registro del estado de la entrega está habilitado en el tema Amazon SNS.

Salidas

`VerifyDeliveryStatusLoggingEnabled`. `GetTopicAttributesResponse` - Respuesta de las operaciones de la `GetTopicAttributes` API.

`VerifyDeliveryStatusLoggingEnabled`. `VerifyDeliveryStatusLoggingEnabled` - Mensaje que indica que se ha verificado correctamente el registro del estado de la entrega.

AWSConfigRemediation-EncryptSNSTopic

Descripción

El `AWSConfigRemediation-EncryptSNSTopic` manual permite el cifrado en el tema del Amazon Simple Notification Service (Amazon SNS) que especifique mediante una clave gestionada por el

cliente AWS Key Management Service (AWS KMS). Este manual de procedimientos solo debe usarse como referencia para garantizar que los temas de Amazon SNS estén cifrados de acuerdo con las mejores prácticas de seguridad mínimas recomendadas. Recomendamos cifrar varios temas con diferentes claves administradas por el cliente.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- KmsKeyArn

Tipo: cadena

Descripción: (obligatorio) el nombre de recurso de Amazon (ARN) de la clave de AWS KMS administrada por el cliente que desea utilizar para cifrar el tema de Amazon SNS.

- TopicArn

Tipo: cadena

Descripción: (obligatorio) el ARN del tema de Amazon SNS que desea cifrar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Pasos de documentos

- `aws:executeAwsApi`: cifra el tema de Amazon SNS que especifique en el parámetro `TopicArn`.
- `aws:assertAwsResourceProperty`: confirma que el cifrado está habilitado en el tema de Amazon SNS.

AWS-PublishSNSNotification

Descripción

Publicar una notificación en Amazon SNS.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Mensaje

Tipo: cadena

Descripción: (obligatorio) el mensaje que se incluirá en la notificación de SNS.

- TopicArn

Tipo: cadena

Descripción: (obligatorio) el ARN del tema de SNS en el que se publicará la notificación.

Amazon SQS

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Simple Queue Service (Amazon SQS). Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-EnableSQSEncryption](#)

AWS-EnableSQSEncryption

Descripción

El AWS-EnableSQSEncryption runbook permite el cifrado en reposo para una cola del Amazon Simple Queue Service (Amazon SQS). Una cola de Amazon SQS se puede cifrar con claves administradas de Amazon SQS (SSE-SQS) o con AWS Key Management Service claves administradas () (SSE-KMS).AWS KMS La clave que asigne a la cola debe tener una política de claves que incluya permisos para todos los principales que estén autorizados a utilizar la cola. Con el cifrado activado, se rechazan ReceiveMessage las solicitudes anónimas SendMessage y las dirigidas a la cola cifrada.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- QueueUrl

Tipo: cadena

Descripción: (Obligatorio) La URL de la cola de Amazon SQS en la que desea activar el cifrado.

- KmsKeyId

Tipo: cadena

Descripción: (opcional) La AWS KMS clave que se utilizará para el cifrado. Este valor puede ser un identificador único global, un ARN para un alias o una clave, o un nombre de alias con el prefijo «alias/». También puede usar la clave AWS administrada especificando el alias aws/sqs.

- KmsDataKeyReusePeriodSeconds

Tipo: cadena

Valores válidos: 60-86400

Predeterminado: 300

Descripción: (opcional) El tiempo, en segundos, que una cola de Amazon SQS puede reutilizar una clave de datos para cifrar o descifrar los mensajes antes de volver a llamar. AWS KMS

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

Pasos de documentos

- `SelectKeyType` (`aws:branch`): Se ramifica según la clave especificada.
- `PutAttributeSseKms` (`aws:executeAwsApi`) - Actualiza la cola de Amazon SQS para usar la AWS KMS clave especificada para el cifrado.
- `PutAttributeSseSqs` (`aws:executeAwsApi`) - Actualiza la cola de Amazon SQS para utilizar la clave de cifrado predeterminada.
- `VerifySqsEncryptionKms` (`aws:assertAwsResourceProperty`) - Verifica que el cifrado esté habilitado en la cola de Amazon SQS.
- `VerifySqsEncryptionDefault` (`aws:assertAwsResourceProperty`) - Verifica que el cifrado esté habilitado en la cola de Amazon SQS.

Step Functions

AWS Systems Manager La automatización proporciona manuales predefinidos para AWS Step Functions (Step Functions). Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-EnableStepFunctionsStateMachineLogging](#)

AWS-EnableStepFunctionsStateMachineLogging

Descripción

El AWS-EnableStepFunctionsStateMachineLogging runbook habilita o actualiza el registro en la máquina de AWS Step Functions estados que especifique. El nivel de registro mínimo debe estar establecido en ALLERROR, oFATAL.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Nivel

Tipo: cadena

Valores válidos: ALL | ERROR | FATAL

Descripción: (Obligatorio) La URL de la cola de Amazon SQS en la que desea activar el cifrado.

- LogGroupArn

Tipo: cadena

Descripción: (obligatorio) El ARN del grupo de CloudWatch registros de Amazon Logs al que desea enviar los registros de las máquinas de estado.

- StateMachineArn

Tipo: cadena

Descripción: (obligatorio) El ARN de la máquina de estado en la que desea habilitar el inicio de sesión.

- IncludeExecutionData

Tipo: Booleano

Valor predeterminado: False

Descripción: (opcional) Determina si los datos de ejecución se incluyen en los registros.

- TracingConfiguration

Tipo: Booleano

Valor predeterminado: False

Descripción: (opcional) Determina si AWS X-Ray el rastreo está habilitado.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- states:DescribeStateMachine
- states:UpdateStateMachine

Pasos de documentos

- `EnableStepFunctionsStateMachineLogging` (`aws:executeAwsApi`)- Actualiza la máquina de estados especificada con la configuración de registro especificada.
- `VerifyStepFunctionsStateMachineLoggingEnabled` (`aws:assertAwsResourceProperty`)- Verifica que el registro esté habilitado en la máquina de estado especificada.

Salidas

- `EnableStepFunctionsStateMachineLogging.Response`: respuesta de la llamada a la `UpdateStateMachine` API.

Systems Manager

AWS Systems Manager La automatización proporciona manuales predefinidos para Systems Manager. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [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

Descripción

El manual de procedimientos AWS-BulkDeleteAssociation le ayuda a eliminar hasta 50 asociaciones de administradores de estados de Systems Manager a la vez.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AssociationIds

Tipo: StringList

Descripción: (Obligatorio) Lista separada por comas IDs de las asociaciones que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:DeleteAssociation`

Pasos de documentos

- `aws:executeScript`: elimina las asociaciones especificadas en el parámetro `AssociationIds`.

AWS-BulkEditOpsItems

Descripción

El `AWS-BulkEditOpsItems` manual le ayuda a editar el estado, la gravedad, la categoría o la prioridad de `AWS Systems Manager OpsItems`. Esta automatización puede editar un máximo de 50 `OpsItems` a la vez.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de `AWS Identity and Access Management (IAM)` que permite a `Systems Manager Automation` realizar las acciones en su nombre. Si no se especifica ningún rol, `Systems Manager Automation` utiliza los permisos del usuario que comienza este manual de procedimientos.

- Categoría

Tipo: cadena

Valores válidos:

- Disponibilidad.
- Costo
- Sin cambios
- Desempeño
- Recuperación
- Seguridad

Predeterminado: sin cambios

Descripción: (opcional) La nueva categoría que desea especificar para los editados OpsItems.

- OpsItemIds

Tipo: StringList

Descripción: (Obligatoria) Lista separada por comas de la OpsItems IDs que desea editar (por ejemplo, OI-xxxxxxxxxxxxx, OI-xxxxxxxxxxxxx).

- Priority (Prioridad)

Tipo: cadena

Valores válidos:

- Sin cambios
- 1
- 2
- 3
- 4
- 5

Predeterminado: sin cambios

Descripción: (opcional) La importancia de lo editado en relación con otros elementos del sistema
OpsItems OpsItems

- Gravedad

Tipo: cadena

Valores válidos:

- Sin cambios
- 1
- 2
- 3
- 4

Predeterminado: sin cambios

Descripción: (opcional) La gravedad de lo editado OpsItems.

- WaitTimeBetweenEditsInSecs

Tipo: cadena

Valores válidos: 0.0-2.0

Valor predeterminado: 0,8

Descripción: (opcional) el tiempo que espera la automatización entre las llamadas a la operación UpdateOpsItems.

- Status

Tipo: cadena

Valores válidos:

- InProgress
- Sin cambios
- Abra
- Resolved (Resuelto)

Predeterminado: sin cambios

Descripción: (opcional) El nuevo estado de lo editado OpsItems.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

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

Pasos de documentos

- `aws:executeScript`- Edita `OpsItems` lo que especificó en el `OpsItemIds` parámetro en función de los valores que especifique para los `Status` parámetros `CategoryPriority`, `Severity`, y.

AWS-BulkResolveOpsItems

Descripción

El `AWS-BulkResolveOpsItems` manual resuelve los filtros AWS Systems Manager `OpsItems` que coincidan con el filtro que especifique. También puede especificar un elemento `OpsItemId` para añadirlo al resuelto `OpsItems` mediante el `OpsInsightsId` parámetro. Si especifica un valor para el parámetro `S3BucketName`, se envía un resumen de los resultados al bucket de Amazon Simple Storage Service (Amazon S3). Para recibir una notificación una vez que se haya enviado el resumen de los resultados al bucket de Amazon S3, especifique un valor para el parámetro `SnsTopicArn`. Esta automatización resolverá un máximo de 1000 `OpsItems` a la vez.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Filtros

Tipo: cadena

Descripción: (Obligatorio) Los pares de filtros clave-valor para devolver OpsItems lo que desea resolver. Por ejemplo, [{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]. Para obtener más información sobre las opciones disponibles para filtrar OpsItems las respuestas, consulta la referencia [OpsItemFilters](#) de la AWS Systems Manager API.

- OpsInsightId

Tipo: cadena

Descripción: (opcional) El identificador de recurso relacionado que quieres añadir a Resolved OpsItems.

- S3 BucketName

Tipo: cadena

Descripción: (opcional) el nombre del bucket de Amazon S3 al que desea enviar el resumen de resultados.

- SnsMessage

Tipo: cadena

Descripción: (opcional) la notificación que desea que Amazon Simple Notification Service (Amazon SNS) envíe cuando se complete la automatización.

- SnsTopicArn

Tipo: cadena

Descripción: (opcional) el ARN del tema de Amazon SNS que desea notificar cuando se envíe el resumen de resultados a Amazon S3.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `s3:GetBucketAcl`
- `s3:PutObject`
- `sns:Publish`
- `ssm:DescribeOpsItems`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

Pasos de documentos

- `aws:executeScript`- Recopila y resuelve en OpsItems función de los filtros que especifique. Si especificó un valor para el parámetro `OpsInsightId`, el valor se añade como un recurso relacionado.
- `aws:executeScript`: si especificó un valor para el parámetro `S3BucketName`, se enviará un resumen de los resultados al bucket de Amazon S3.
- `aws:executeScript`: si especificó un valor para el parámetro `SnsTopicArn`, se enviará una notificación al tema de Amazon SNS después de enviar el resumen de los resultados a Amazon S3, incluyendo el valor del parámetro `SnsMessage` si se ha especificado.

AWS-ConfigureMaintenanceWindows

Descripción

El manual de procedimientos `AWS-ConfigureMaintenanceWindows` le ayuda a habilitar o deshabilitar varias ventanas de mantenimiento de Systems Manager.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- MaintenanceWindows

Tipo: StringList

Descripción: (Obligatorio) Una lista separada por comas de las ventanas IDs de mantenimiento que desea activar o desactivar.

- MaintenanceWindowsStatus

Tipo: cadena

Valores válidos: "True" | "False"

Valor predeterminado: "False"

Descripción: (obligatorio) determina si las ventanas de mantenimiento están habilitadas o deshabilitadas. Especifique "Verdadero" para habilitar las ventanas de mantenimiento y "Falso" para deshabilitarlas.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

Pasos de documentos

- `aws:executeScript`: recopila el estado de las ventanas de mantenimiento que especifique en el parámetro `MaintenanceWindows` y habilita o deshabilita las ventanas de mantenimiento.

AWS-CreateManagedLinuxInstance

Descripción

Cree una instancia EC2 para Linux que esté configurada para Systems Manager.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux

Parámetros

- `Amild`

Tipo: cadena

Descripción: (obligatorio) ID AMI que se va a utilizar para lanzar la instancia.

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- **GroupName**

Tipo: cadena

Predeterminado: SSMSecurity GroupForLinuxInstances

Descripción: (obligatorio) nombre de grupo de seguridad que se va a crear.

- **HttpTokens**

Tipo: cadena

Valores válidos: opcional | obligatorio

Predeterminado: opcional

Descripción: (opcional) IMDSv2 utiliza sesiones respaldadas por tokens. Defina el uso de los tokens HTTP en `optional` o `required` para determinar si IMDSv2 es opcional o obligatorio.

- **InstanceType**

Tipo: cadena

Valor predeterminado: t2.medium

Descripción: (obligatorio) tipo de instancia que se va a lanzar. El valor predeterminado es `t2.medium`.

- **KeyPairName**

Tipo: cadena

Descripción: (obligatorio) par de claves que se utilizará al crear una instancia.

- **RemoteAccessCidr**

Tipo: cadena

Valor predeterminado: 0.0.0.0/0

Descripción: (obligatorio) Crea un grupo de seguridad con un puerto para SSH (rango de puertos 22) abierto según lo IPs especificado por el CIDR (el valor predeterminado es 0.0.0.0/0). Si el grupo de seguridad ya existe no será modificado y no se cambiarán las reglas.

- RoleName

Tipo: cadena

Predeterminado: SSManaged InstanceProfileRole

Descripción: (obligatorio) nombre de rol que se va a crear.

- StackName

Tipo: cadena

Predeterminado: CreateManagedInstanceStack {{Automation:EXECUTION_ID}}

Descripción: (opcional) especificar el nombre de pila que utiliza este manual de procedimientos

- SubnetId

Tipo: cadena

Valor predeterminado: Default

Descripción: (obligatorio) una nueva instancia se implementará en esta subred o en la subred predeterminada si no se especifica.

- VpcId

Tipo: cadena

Valor predeterminado: Default

Descripción: (obligatorio) una nueva instancia se implementará en este Amazon Virtual Private Cloud (Amazon VPC) o en la Amazon VPC predeterminada si no se especifica.

AWS-CreateManagedWindowsInstance

Descripción

Cree una instancia EC2 para la Windows Server que esté configurada para Systems Manager.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Windows

Parámetros

Parámetros

- Amild

Tipo: cadena

Valor predeterminado: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

Descripción: (obligatorio) ID AMI que se va a utilizar para lanzar la instancia.

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- GroupName

Tipo: cadena

Predeterminado: `SSMSecurity GroupForLinuxInstances`

Descripción: (obligatorio) nombre de grupo de seguridad que se va a crear.

- HttpTokens

Tipo: cadena

Valores válidos: opcional | obligatorio

Predeterminado: opcional

Descripción: (opcional) IMDSv2 utiliza sesiones respaldadas por tokens. Defina el uso de los tokens HTTP en `optional` o `required` para determinar si IMDSv2 es opcional o obligatorio.

- `InstanceType`

Tipo: cadena

Valor predeterminado: `t2.medium`

Descripción: (obligatorio) tipo de instancia que se va a lanzar. El valor predeterminado es `t2.medium`.

- `KeyPairName`

Tipo: cadena

Descripción: (obligatorio) par de claves que se utilizará al crear una instancia.

- `RemoteAccessCidr`

Tipo: cadena

Valor predeterminado: `0.0.0.0/0`

Descripción: (obligatorio) Crea un grupo de seguridad con un puerto para RDP (rango de puertos 3389) abierto según lo IPs especificado por el CIDR (el valor predeterminado es `0.0.0.0/0`). Si el grupo de seguridad ya existe no será modificado y no se cambiarán las reglas.

- `RoleName`

Tipo: cadena

Predeterminado: `SSMManaged InstanceProfileRole`

Descripción: (obligatorio) nombre de rol que se va a crear.

- `StackName`

Tipo: cadena

Predeterminado: `CreateManagedInstanceStack {{Automation:EXECUTION_ID}}`

Descripción: (opcional) especificar el nombre de pila que utiliza este manual de procedimientos

- `SubnetId`

Tipo: cadena

Valor predeterminado: `Default`

Descripción: (obligatorio) una nueva instancia se implementará en esta subred o en la subred predeterminada si no se especifica.

- `VpcId`

Tipo: cadena

Valor predeterminado: `Default`

Descripción: (obligatorio) una nueva instancia se implementará en este Amazon Virtual Private Cloud (Amazon VPC) o en la Amazon VPC predeterminada si no se especifica.

AWSConfigRemediation-EnableCWLoggingForSessionManager

Descripción

El `AWSConfigRemediation-EnableCWLoggingForSessionManager` runbook permite que las AWS Systems Manager sesiones del administrador de sesiones (administrador de sesiones) almacenen los registros de salida en un grupo de registros de Amazon CloudWatch (CloudWatch).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DestinationLogGroup

Tipo: cadena

Descripción: (obligatorio) El nombre del grupo de CloudWatch registros.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:UpdateDocument
- ssm>CreateDocument
- ssm:UpdateDefaultDocumentVersion
- ssm:DescribeDocument

Pasos de documentos

- aws:executeScript- Acepta el grupo de CloudWatch registros para actualizar el documento que almacena las preferencias de los registros de salida de las sesiones del Administrador de sesiones, o crea uno si no existe.

AWS-ExportOpsDataToS3

Descripción

Este runbook recupera una lista de OpsData resúmenes en AWS Systems Manager Explorer y los exporta a un objeto de un bucket específico de Amazon Simple Storage Service (Amazon S3).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- columnFields

Tipo: StringList

Descripción: (obligatorio) campos de la columna para escribir en el archivo de salida.

- filters

Tipo: cadena

Descripción: filtros (opcionales) para la solicitud. getOpsSummary

- resultAttribute

Tipo: cadena

Descripción: (opcional) El atributo de resultado de la getOpsSummary solicitud.

- s3 BucketName

Tipo: cadena

Descripción: (obligatorio) el bucket de S3 donde desea descargar el archivo de salida.

- snsSuccessMessage

Tipo: cadena

Descripción: (opcional) mensaje que se envía cuando termine el manual de procedimientos.

- snsTopicArn

Tipo: cadena

Descripción: (obligatorio) el ARN del tema de Amazon Simple Notification Service (Amazon SNS) para notificar cuando se complete la descarga.

- SyncName

Tipo: cadena

Descripción: (opcional) el nombre de la sincronización de datos de recursos.

Pasos de documentos

getOpsSummaryPaso: ahora recupera hasta 5000 resúmenes de operaciones para exportarlos a un archivo CSV.

Salidas

OpsData objeto: si el manual se ejecuta correctamente, encontrarás el OpsData objeto exportado en el depósito S3 de destino.

AWS-ExportPatchReportToS3

Descripción

Este manual de procedimientos recupera listas de datos de resúmenes y detalles de parches en AWS Systems Manager Patch Manager y los exporta a archivos.csv en un bucket de Amazon Simple Storage Service (Amazon S3) específico.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `assumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que ejecuta este documento.

- `s3 BucketName`

Tipo: cadena

Descripción: (obligatorio) el bucket de S3 donde desea descargar el archivo de salida.

- `snsTopicArn`

Tipo: cadena

Descripción: (opcional) el nombre de recurso de Amazon (ARN) del tema de Amazon Simple Notification Service (Amazon SNS) para notificar cuando se completa la descarga.

- `snsSuccessMessage`

Tipo: cadena

Descripción: (opcional) el texto del mensaje que se enviará cuando finalice el manual de procedimientos.

- `destinos`

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia o un carácter comodín (*) para indicar si se deben informar los datos de los parches de una instancia específica o de todas las instancias.

Pasos de documentos

ExportReportStep — La acción de este paso depende del valor del `targets` parámetro. Si `targets` tiene el formato de `instanceids=*`, el paso recupera hasta 10.000 resúmenes de parches para las instancias de su cuenta y exporta los datos a un archivo .csv.

Si `targets` tiene el formato de `instanceids=<instance-id>`, el paso recupera tanto el resumen del parche como todos los parches de la instancia especificada en su cuenta y los exporta a un archivo .csv.

Salidas

PatchSummaryObjeto /Patches: si el runbook se ejecuta correctamente, el objeto de informe de parches exportado se descarga en el depósito S3 de destino.

AWS-SetupInventory

Descripción

Cree una asociación de Systems Manager Inventory para una o varias instancias administradas. El sistema recopila metadatos de sus instancias de acuerdo con la programación en la asociación. Para obtener más información, consulte [AWS Systems Manager Inventory](#).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- Aplicaciones

Tipo: cadena

Predeterminado: habilitado

Descripción: (opcional) recopilar metadatos de las aplicaciones instaladas.

- AssociatedDocName

Tipo: cadena

Valor predeterminado: `AWS-GatherSoftwareInventory`

Descripción: (opcional) nombre del manual de procedimientos de SSM utilizado para recopilar datos del inventario desde la instancia administrada.

- AssociationName

Tipo: cadena

Descripción: (opcional) un nombre para la asociación de inventario que se asignará a la instancia.

- AssocWaitTime

Tipo: cadena

Predeterminado: `M PT5`

Descripción: (opcional) cantidad de tiempo que debe ponerse en pausa la recopilación de inventario cuando se alcanza la hora de inicio de la asociación del inventario. La hora usa el formato ISO 8601.

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AwsComponents

Tipo: cadena

Predeterminado: habilitado

Descripción: (Opcional) Recopile metadatos para AWS componentes como amazon-ssm-agent.

- CustomInventory

Tipo: cadena

Predeterminado: habilitado

Descripción: (opcional) recopilar los metadatos de inventario personalizado.

- Archivos

Tipo: cadena

Descripción: (opcional) recopilar metadatos acerca de archivos en las instancias. Para obtener más información sobre cómo recopilar este tipo de datos de inventario, consulte [Trabajar con el inventario de archivos y del registro de Windows](#). Requiere la versión 2.2.64.0 de SSMAgent o una posterior. Ejemplo de Linux: [{"Path":"/usr/bin", "Pattern":["aws*", "*ssm*"],"Recursive":false}, {"Path":"/var/log", "Pattern":["amazon*.*log"], "Recursive":true, "DirScanLimit":1000}] Windows example: [{"Path":"%PROGRAMFILES%", "Pattern":["*.exe"],"Recursive":true}]

- InstanceDetailedInformation

Tipo: cadena

Predeterminado: habilitado

Descripción: (opcional) recopilar información adicional acerca de la instancia, incluido el modelo de CPU, la velocidad y el número de núcleos, por mencionar algunos.

- InstanceIds

Tipo: cadena

Valor predeterminado: *

Descripción: (obligatorio) instancias EC2 de las que desea crear un inventario.

- LambdaAssumeRole

Tipo: cadena

Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- NetworkConfig

Tipo: cadena

Predeterminado: habilitado

Descripción: (opcional) recopilar metadatos de las configuraciones de red.

- Salidas (3) BucketName

Tipo: cadena

Descripción: (opcional) nombre de un bucket de Amazon S3 en el que desea escribir los datos de registro del inventario.

- Salidas 3 KeyPrefix

Tipo: cadena

Descripción: (opcional) un prefijo de clave de Amazon S3 (subcarpeta) en el que desea escribir los datos de registro del inventario.

- OutputS3Region

Tipo: cadena

Descripción: (opcional) El nombre del Región de AWS lugar donde se encuentra Amazon S3.

- Schedule

Tipo: cadena

Valor predeterminado: cron(0 */30 * * * ? *)

Descripción: (opcional) una expresión cron para la programación de asociación de inventario. El valor predeterminado es cada 30 minutos.

- Services

Tipo: cadena

Predeterminado: habilitado

Descripción: (Opcional, solo para el sistema operativo Windows, requiere la SSMAgent versión 2.2.64.0 y superior) Recopile datos para las configuraciones de los servicios.

- WindowsRegistry

Tipo: cadena

Descripción: (opcional) recopilar metadatos acerca de claves del Registro de Microsoft Windows. Para obtener más información sobre cómo recopilar este tipo de datos de inventario, consulte [Trabajar con el inventario de archivos y del registro de Windows](#). Requiere la versión 2.2.64.0 del SSM Agent o posterior. Ejemplo: [{"Path» : "HKEY_CURRENT_CONFIG\ System», "Recursive» : true}, {"Path» : "HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\ «," «: [» «]}] MachinelImage ValueNames AMIName

- WindowsRoles

Tipo: cadena

Predeterminado: habilitado

Descripción: (opcional) recopilar información acerca de roles de Windows en la instancia. Se aplica solo a sistemas operativos Windows. Requiere la versión 2.2.64.0 de SSMAgent o una posterior.

- WindowsUpdates

Tipo: cadena

Predeterminado: habilitado

Descripción: (opcional) recopilar datos acerca de todas las actualizaciones de Windows en la instancia.

AWS-SetupManagedInstance

Descripción

Configure una instancia con un rol AWS Identity and Access Management (IAM) para el acceso a Systems Manager.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia EC2 que se va a configurar.

- LambdaAssumeRole

Tipo: cadena

Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- RoleName

Tipo: cadena

Predeterminado: SSMRole ForManagedInstance

Descripción: (opcional) nombre del rol de IAM para la instancia EC2. Si este rol no existe, se creará. Cuando especifiques este valor, comprueba que el rol contiene la política SSMMManaged InstanceCore gestionada por Amazon.

AWS-SetupManagedRoleOnEC2Instance

Descripción

Configure una instancia con la función de IAM SSMMRole ForManagedInstance gestionada para el acceso a Systems Manager.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) ID de la instancia EC2 que se va a configurar.

- LambdaAssumeRole

Tipo: cadena

Descripción: (opcional) ARN del rol que permite a la Lambda creada por Automatización para realizar las acciones en su nombre. Si no se especifica, se creará un rol transitorio para ejecutar la función Lambda.

- RoleName

Tipo: cadena

Predeterminado: SSMRole ForManagedInstance

Descripción: (opcional) nombre del rol de IAM para la instancia EC2. Si este rol no existe, se creará. Cuando especifiques este valor, comprueba que el rol contiene la política SSMManged InstanceCore gestionada por Amazon.

AWSSupport-TroubleshootManagedInstance

Descripción

El AWSSupport-TroubleshootManagedInstance manual le ayuda a determinar por qué una instancia de Amazon Elastic Compute Cloud (Amazon EC2) no se presenta como gestionada por AWS Systems Manager. Este manual de procedimientos revisa la configuración de VPC de la instancia, incluyendo las reglas de los grupos de seguridad, los puntos de conexión de VPC, las reglas de la lista de control de acceso (ACL) y las tablas de enrutamiento. También confirma que se ha adjuntado a la instancia un perfil de instancia AWS Identity and Access Management (IAM) que contiene los permisos necesarios.

Important

Este manual de automatización no evalúa IPv6 las reglas.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) El ID de la EC2 instancia de Amazon que no informa como gestionada por Systems Manager.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- 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`

Pasos de documentos

- `aws:executeScript`: recopila el `PingStatus` de la instancia.
- `aws:branch`: se ramifica en función de si la instancia ya está informando como gestionada por Systems Manager.
- `aws:executeAwsApi`: recopila detalles sobre la instancia, incluyendo la configuración de la VPC.
- `aws:executeScript`: si corresponde, recopila detalles adicionales relacionados con los puntos de conexión de VPC que se han implementado para usarlos con Systems Manager y confirma que los grupos de seguridad conectados al punto de conexión de VPC permiten el tráfico entrante en el puerto TCP 443 desde la instancia.
- `aws:executeScript`: comprueba si la tabla de enrutamiento permite el tráfico al punto de conexión de VPC o a los puntos de conexión públicos de Systems Manager.
- `aws:executeScript`: comprueba si las reglas de ACL de la red permiten el tráfico al punto de conexión de VPC o a los puntos de conexión públicos de Systems Manager.
- `aws:executeScript`: comprueba si el grupo de seguridad asociado a la instancia permite el tráfico saliente al punto de conexión de VPC o a los puntos de conexión públicos de Systems Manager.
- `aws:executeScript`: comprueba si el perfil de instancia adjunto a la instancia incluye una política gestionada que proporcione los permisos necesarios.
- `aws:branch`: se ramifica en función del sistema operativo de la instancia.
- `aws:executeScript`: proporciona una referencia al script de `ssmagent-toolkit-linux` del intérprete de comandos.
- `aws:executeScript`: Proporciona una referencia al `ssmagent-toolkit-windows` PowerShell script.

- `aws:executeScript`: genera el resultado final para la automatización.
- `aws:executeScript`: si el `PingStatus` de la instancia es `Online`, regresa que la instancia ya está gestionada por Systems Manager.

AWSSupport-TroubleshootPatchManagerLinux

Descripción

El `AWSSupport-TroubleshootPatchManagerLinux` manual soluciona problemas comunes que pueden provocar un error en los parches en los nodos gestionados basados en Linux mediante Patch Manager, una herramienta incluida. AWS Systems Manager El objetivo principal de este manual de procedimientos es identificar la causa raíz del error del comando de revisión y sugerir un plan de corrección.

¿Cómo funciona?

El `AWSSupport-TroubleshootPatchManagerLinux` manual tiene en cuenta el par de ID/Command identificadores de instancia proporcionados por usted para la solución de problemas. Si no se proporciona ningún identificador de comando, selecciona el último comando de parche fallido en los últimos 30 días en la instancia proporcionada. Tras comprobar el estado del comando, el cumplimiento de los requisitos previos y la distribución del sistema operativo, el runbook descarga y ejecuta un paquete analizador de registros. El resultado incluye la causa raíz del problema, así como las medidas necesarias para solucionarlo.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

- Amazon Linux 2 y AL2023
- Red Hat Enterprise Linux 8.X y 9.X
- Centos 8.X y 9.X
- SUSE 15.X

Parámetros

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Instrucciones

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootPatchManagerLinux](#) la AWS Systems Manager consola.
2. Elija `Execute automation` (Ejecutar automatización).
3. Para los parámetros de entrada, introduzca lo siguiente:
 - `InstanceId` (Obligatorio):

Usa el selector de instancias interactivo para elegir el ID del nodo gestionado por SSM basado en Linux (Amazon Elastic Compute Cloud (Amazon EC2) o servidor activado híbrido) contra el que falló el comando de parche, o introduce manualmente el ID de la instancia gestionada por SSM.

- `AutomationAssumeRole` (Opcional):

Introduzca el ARN del rol de IAM que permite a `Automation` realizar acciones en su nombre. Si no se especifica ningún rol, `Automation` usa los permisos del usuario que inicia este manual.

- `RunCommandId` (Opcional):

Introduzca el identificador del AWS-RunPatchBaseline documento con el comando de ejecución fallido. Si no proporciona un identificador de comando, el runbook buscará el último comando de parche fallido en los últimos 30 días en la instancia seleccionada.

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.

☒ Show interactive instance picker

i-0

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.

42e

4. Seleccione Ejecutar.

5. Se inicia la automatización.

6. Este documento realiza los siguientes pasos:

- CheckConcurrency:

Garantiza que solo haya una ejecución de este runbook dirigida a la misma instancia. Si el runbook encuentra otra ejecución en curso dirigida a la misma instancia, devuelve un error y finaliza.

- ValidateCommandID:

Valida si el ID de comando proporcionado, como parámetro de entrada, se ejecutó para el documento AWS-RunPatchBaseline SSM. Si no se proporciona ningún identificador de comando, el runbook considerará la última ejecución fallida de los AWS-RunPatchBaseline últimos 30 días en la instancia seleccionada.

- BranchOnCommandStatus:

Confirma que el estado del comando proporcionado ha fallado. De lo contrario, el manual finaliza la ejecución y genera un informe en el que se indica que el comando proporcionado se ejecutó correctamente.

- VerifyPrerequisites:

Confirma que se cumplen los requisitos previos mencionados anteriormente.

- GetPlatformDetails:

Recupera la distribución y la versión del sistema operativo (SO).

- **GetDownloadURL:**

Recupera la URL de descarga del paquete PatchManager Log Analyzer.

- **EvaluatePatchManagerLogs:**

Descarga y ejecuta el paquete python de PatchManager Log Analyzer en la instancia para evaluar el archivo de registro.

- **GenerateReport:**

Genera un informe final de la ejecución del manual de ejecución que incluye el problema identificado y la solución sugerida.

7. Una vez finalizada, revise la sección de resultados para ver los resultados detallados de la ejecución:

```

▼ Outputs

GenerateReportOutput
Starting 'python3 main.py i-0[REDACTED] 3e016680-82f4-45f4-845c-aa4685b4fab Ubuntu 22.04'

TROUBLESHOOTING RESULTS
-----
[PROBLEM] :
The error found in the log file at /var/lib/amazon/ssm/i-0[REDACTED]/document/orchestration/3e016680-82f4-45f4-845c-aa4685b4fab/awssrunShellScript/PatchLinux/stdout is :
Unable to download payload: https://s3.dualstack.eu-west-1.amazonaws.com/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

```

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWSsupport-TroubleshootSessionManager

Descripción

El manual de procedimientos `AWSSupport-TroubleshootSessionManager` le ayuda a solucionar problemas comunes que le impiden conectarse a instancias administradas de Amazon Elastic Compute Cloud (Amazon EC2) mediante Session Manager. El administrador de sesiones es una herramienta de AWS Systems Manager. Este manual de procedimientos comprueba lo siguiente:

- Comprueba si la instancia se está ejecutando e informando como gestionada por Systems Manager.
- Ejecuta el manual de procedimientos `AWSSupport-TroubleshootManagedInstance` si la instancia no informa como gestionada por Systems Manager.
- Comprueba la versión del agente SSM instalada en la instancia.
- Comprueba si un perfil de instancia que contiene una política de AWS Identity and Access Management (IAM) recomendada para Session Manager está adjunto a la instancia Amazon EC2.
- Recopila los registros del agente SSM de la instancia.
- Analiza sus preferencias de Session Manager.
- Ejecuta el `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook para analizar la conectividad de la instancia con los puntos de conexión de Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3) y CloudWatch Amazon Logs (Logs). CloudWatch

Consideraciones

- No se admiten los nodos gestionados híbridos.
- Este manual de procedimientos solo comprueba si hay una política de IAM administrada recomendada asociada al perfil de instancia. No analiza la IAM ni los permisos AWS KMS que se incluyen en su perfil de instancia.

Important

El manual de procedimientos `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` utiliza el [Analizador de accesibilidad de VPC](#) para analizar la conectividad de red entre una fuente y un punto de conexión de servicio. Se le cobrará por cada análisis realizado entre un origen y un destino. Para obtener más información, consulte [Precios de Amazon EFS](#).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- InstanceId

Tipo: cadena

Descripción: (obligatorio) el ID de la instancia de Amazon EC2 a la que no puede conectarse mediante Session Manager.

- SessionPreferenceDocument

Tipo: cadena

Predeterminado: SSM- SessionManagerRunShell

Descripción: (opcional) el nombre de su documento de preferencias de sesión. Si no especifica un documento de preferencias de sesión personalizado al iniciar las sesiones, utilice el valor predeterminado.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

1. `aws:waitForAwsResourceProperty`: espera hasta 6 minutos para que su instancia de destino supere las comprobaciones de estado.
2. `aws:executeScript`: analiza el documento de preferencias de sesión.
3. `aws:executeAwsApi`: obtiene el ARN del perfil de instancia asociado a su instancia.
4. `aws:executeAwsApi`: comprueba si su instancia informa como gestionada por Systems Manager.
5. `aws:branch`: se ramifica en función de si su instancia genera informes según la gestión de Systems Manager.
6. `aws:executeScript`: comprueba si el agente SSM instalado en su instancia es compatible con Session Manager.
7. `aws:branch`: se ramifican según la plataforma de su instancia para recopilar registros `ssm-cli`.
8. `aws:runCommand`: recopila la salida de los registros `ssm-cli` de una instancia Linux o macOS.
9. `aws:runCommand`: recopila la salida de los registros `ssm-cli` de una instancia Windows.
10. `aws:executeScript`: analiza los registros `ssm-cli`.
11. `aws:executeScript`: comprueba si hay una política de IAM recomendada asociada al perfil de instancia.
12. `aws:branch`: determina si se debe evaluar la conectividad del punto de conexión `ssmmessages` en función de los registros `ssm-cli`.
13. `aws:executeAutomation`: evalúa si la instancia se puede conectar a un punto de conexión `ssmmessages`.
14. `aws:branch`: determina si se debe evaluar la conectividad del punto de conexión de Amazon S3 en función de los registros `ssm-cli` y sus preferencias de sesión.
15. `aws:executeAutomation`: evalúa si la instancia se puede conectar a un punto de conexión de Amazon S3.
16. `aws:branch`: Determina si se debe evaluar la conectividad del AWS KMS punto final en función de `ssm-cli` los registros y las preferencias de la sesión.
17. `aws:executeAutomation`: Evalúa si la instancia se puede conectar a un AWS KMS punto final.

- 18aws:branch: Determina si se debe evaluar la conectividad de CloudWatch los puntos finales de ssm-cli Logs en función de los registros y de sus preferencias de sesión.
- 19aws:executeAutomation: Evalúa si la instancia se puede conectar a un punto final de CloudWatch Logs.
- 20aws:executeAutomation: ejecuta el manual de procedimientos AWSSupport-TroubleshootManagedInstance.
- 21aws:executeScript: compila el resultado de los pasos anteriores y genera un informe.

Salidas

- generateReport.EvalReport: los resultados de las comprobaciones realizadas por el manual de procedimientos en texto sin formato.

De terceros

AWS Systems Manager La automatización proporciona manuales predefinidos para productos y servicios de terceros. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-CreateJiraIssue](#)
- [AWS-CreateServiceNowIncident](#)
- [AWS-RunPacker](#)

AWS-CreateJiraIssue

Descripción

Cree un problema en Jira.

Note

Para un mejor control y validación, te recomendamos [clonar](#) el AWS-CreateJiraIssue manual para crear tu propia versión privada. En el runbook clonado, añade una [lógica de](#)

[validación](#) para el `JiraURL` parámetro para asegurarte de que coincide con las instancias de Jira aprobadas antes de la ejecución. A continuación, utilice el runbook clonado en lugar del gestionado por AWS y restrinja los permisos de ejecución de IAM. `AWS-CreateJiraIssue` Este enfoque le proporciona más flexibilidad y garantiza que el parámetro cumpla con los requisitos de seguridad y conformidad de su organización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AssigneeName`

Tipo: cadena

Descripción: (opcional) el nombre de usuario de la persona a la que debe asignarse el problema.

- `DueDate`

Tipo: cadena

Descripción: (opcional) La fecha de vencimiento de la emisión en yyyy-mm-dd formato.

- `IssueDescription`

Tipo: cadena

Descripción: (obligatorio) una descripción detallada del problema.

- `IssueSummary`

Tipo: cadena

Descripción: (obligatorio) un breve resumen del problema.

- IssueTypeName

Tipo: cadena

Descripción: (obligatorio) el nombre del tipo de problema que desea crear (por ejemplo, Task, Sub-task, Bug, etc.).

- JiraURL

Tipo: cadena

Descripción: (obligatorio) la URL de la instancia de Jira.

- JiraUsername

Tipo: cadena

Descripción: (obligatorio) el nombre del usuario con el que se creará el problema.

- PriorityName

Tipo: cadena

Descripción: (opcional) el nombre de la prioridad del problema.

- ProjectKey

Tipo: cadena

Descripción: (obligatorio) la clave del proyecto en el que se debe crear el problema.

- SSMPParameterNombre

Tipo: cadena

Descripción: (obligatorio) el nombre de un parámetro SSM cifrado que contiene la clave de API o la contraseña del usuario de Jira.

Pasos de documentos

`aws:createStack`- Cree una CloudFormation pila para crear el rol y la función de Lambda IAM.

`aws:invokeLambdaFunction`: invoca la función de Lambda para crear el problema de Jira

`aws:deleteStack`- Elimine la CloudFormation pila creada.

Salidas

Issueld: ID de la edición de Jira recién creada

AWS-CreateServiceNowIncident

Descripción

Cree un incidente en la tabla de ServiceNow incidentes.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Categoría

Tipo: cadena

Descripción: (opcional) la categoría del incidente.

Valores válidos: Ninguno | Software Inquiry/Help | Hardware | Red | Base de datos

Valor predeterminado: None

- Description (Descripción)

Tipo: cadena

Descripción: (obligatorio) una explicación detallada sobre el incidente.

- Impact

Tipo: cadena

Descripción: (opcional) el efecto que un incidente tiene en el negocio.

Valores válidos: Alto | Medio | Bajo

Valor predeterminado: bajo

- ServiceNowInstanceUsername

Tipo: cadena

Descripción: (obligatorio) el nombre del usuario con el que se creará el incidente.

- ServiceNowInstancePassword

Tipo: cadena

Descripción: (obligatorio) El nombre de un parámetro SSM cifrado que contiene la contraseña del ServiceNow usuario.

- ServiceNowInstanceURL

Tipo: cadena

Descripción: (Obligatorio) La URL de la ServiceNow instancia

- ShortDescription

Tipo: cadena

Descripción: (obligatorio) una breve descripción del incidente.

- Subcategory

Tipo: cadena

Descripción: (opcional) la subcategoría del incidente.

Valores válidos: Ninguno | Antivirus | Correo electrónico | Aplicación interna | Sistema operativo | CPU | Disco | Teclado | Hardware | Memoria | Monitor | Ratón | DHCP | DNS | Dirección IP | VPN | Inalámbrica | DB2 | MS SQL Server | Oracle

Valor predeterminado: None

Pasos de documentos

PUSH_incident: envía la información del incidente a. ServiceNow

Salidas

Push_incident.incidentID: el ID del incidente creado.

AWS-RunPacker

Descripción

Este manual utiliza la herramienta HashiCorp [Packer](#) para validar, corregir o crear plantillas de empaquetador que se utilizan para crear imágenes de máquinas. Este manual utiliza la versión 1.11.2 de Packer.

Note

Si especifica un valor `vpc_id`, también debe especificar el valor `subnet_id` de una subred pública. A menos que modifique el atributo de direccionamiento IPv4 público de la subred, también debe establecerlo en `true`. `associate_public_ip_address`

Important

Los aprovisionadores de Packer se ejecutan con privilegios de nivel raíz en la instancia EC2 temporal. Siga las prácticas de privilegios mínimos al crear plantillas de Packer. Evite conceder a los aprovisionadores acceso a los metadatos confidenciales de las instancias o a los archivos de credenciales locales. Si has agregado políticas adicionales a la función de IAM utilizada en la [configuración de administración de hosts predeterminada](#), ten en

cuenta que cualquier proceso que se ejecute como root en la instancia puede acceder a esos permisos ampliados. Revisa tus plantillas de Packer para asegurarte de que solo contengan comandos confiables.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Force

Tipo: Booleano

Descripción: una opción de Packer para forzar la ejecución de un generador cuando artefactos de una compilación anterior impiden la ejecución de una compilación.

- Mode

Tipo: cadena

Descripción: el modo, o comando, en el que utilizar Packer al realizar la validación respecto a la plantilla. Las opciones incluyen Build, Validate y Fix.

- **TemplateFileName**

Tipo: cadena

Descripción: el nombre, o clave, del archivo de plantilla en el bucket de S3.

- **Plantillas (3) BucketName**

Tipo: cadena

Descripción: el nombre del bucket de S3 que contiene la plantilla de empaquetador.

Pasos de documentos

RunPackerProcessTemplate — Ejecuta el modo seleccionado en la plantilla mediante la herramienta Packer.

Salidas

RunPackerProcessTemplate.output: la salida estándar de la herramienta Packer.

RunPackerProcessTemplate.fixed_template_key: el nombre de la plantilla almacenada en un bucket de S3 para usarla solo cuando se ejecuta en modo «Fix».

RunPackerProcessTemplate.s3_bucket: el nombre del bucket de S3 que contiene la plantilla fija para usarla solo cuando se ejecuta en modo «Fix».

Amazon VPC

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon Virtual Private Cloud. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [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

Descripción

Este manual elimina todas las reglas de entrada y salida del grupo de seguridad que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- SecurityGroupId

Tipo: cadena

Descripción: (obligatorio) El ID del grupo de seguridad que desea cerrar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

Pasos de documentos

- aws:executeScript- Elimina todas las reglas de entrada y salida del grupo de seguridad que especifique en el SecurityGroupId parámetro.

AWSSupport-ConfigureDNSQueryLogging

Descripción

El manual de procedimientos AWSSupport-ConfigureDNSQueryLogging configura el registro de las consultas de DNS que se originan en su nube privada virtual (VPC) o en las zonas alojadas de Amazon Route 53. Puede optar por publicar los registros de consultas en Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3) o Amazon Data Firehose. Para obtener más información sobre el registro de consultas y el solucionador de registros de consultas, consulte [Registro de consultas de DNS público](#) y [Solucionador de registro de consultas](#) .

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LogDestinationArn

Tipo: cadena

Descripción: (opcional) El ARN del grupo CloudWatch Logs, el bucket de Amazon S3 o la transmisión Firehose a los que desea enviar los registros de consultas. Tenga en cuenta que el

registro de consultas de DNS público de Route 53 solo admite grupos de CloudWatch registros. Si no especifica un valor para este parámetro, la automatización crea un grupo de CloudWatch registros con el formato `AWSSupport-ConfigureDNSQueryLogging-{automation:
EXECUTION_ID}` y una política de recursos de IAM para publicar los registros de consultas. El grupo de CloudWatch registros creado por la automatización tiene un período de retención de 14 días.

- `QueryLogType`

Tipo: cadena

Descripción: (opcional) los tipos de consultas que desea registrar.

Valores válidos: `Public` | `Resolver/Private`

Predeterminado: `Public`

- `ResourceId`

Tipo: cadena

Descripción: (obligatorio) el ID del recurso cuyas consultas desea registrar. Si especifica `Public` para el parámetro `QueryLogType`, el recurso debe ser el ID de una zona alojada privada de Route 53. Si especifica `Resolver/Private` para el parámetro `QueryLogType`, el recurso debe ser el ID de una VPC.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `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`

Pasos de documentos

- `aws:executeScript`: verifica que el recurso que especificó para el parámetro `ResourceId` existe y comprueba si el tipo de recurso coincide con la opción requerida `QueryLogType`.
- `aws:executeScript`: comprueba que el valor especificado para el parámetro `LogDestinationArn` coincide con el `QueryLogType` requerido.
- `aws:executeScript`- Verifica los permisos necesarios para que Route 53 publique registros en el grupo de CloudWatch registros y crea la política de recursos de IAM requerida si no existe.
- `aws:executeScript`: habilita el registro de consulta de DNS en el destino seleccionado.

AWSSupport-ConfigureTrafficMirroring

Descripción

El manual de procedimientos `AWSSupport-ConfigureTrafficMirroring` configura la duplicación de tráfico para ayudarle a resolver problemas de conectividad entre un equilibrador de carga e instancias de Amazon Elastic Compute Cloud (Amazon EC2). La duplicación del tráfico copia el tráfico entrante y saliente de las interfaces de red que están conectadas a sus instancias. Para configurar la duplicación de tráfico, este manual de procedimientos crea los destinos, filtros y sesiones necesarios. De forma predeterminada, el manual de procedimientos configura la duplicación de todo el tráfico entrante y saliente de todos los protocolos, excepto Amazon DNS. Si desea reflejar el tráfico de fuentes y destinos específicos, puede modificar las reglas de entrada y salida una vez finalizada la automatización.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- SourceENI

Tipo: cadena

Descripción: (obligatorio) la interfaz de red elástica para la que desea configurar la duplicación de tráfico.

- Target

Tipo: cadena

Descripción: (obligatorio) el destino del tráfico reflejado. Debe especificar el ID de una interfaz de red, un punto de conexión de equilibrador de carga de red o equilibrador de carga de puerta de enlace. Si especifica un equilibrador de carga de red, debe haber receptores UDP en el puerto 4789.

- SessionNumber

Tipo: cadena

Valores válidos: 1-32766

Descripción: (obligatorio) el número de la sesión duplicada que desea utilizar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ec2:CreateTrafficMirrorTarget`
- `ec2:CreateTrafficMirrorFilter`
- `ec2:CreateTrafficMirrorFilterRule`
- `ec2:CreateTrafficMirrorSession`
- `ec2>DeleteTrafficMirrorSession`

- `ec2:DeleteTrafficMirrorFilter`
- `ec2:DeleteTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorFilterRule`
- `iam:ListRoles`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`

Pasos de documentos

- `aws:executeScript`: ejecuta un script para crear un objetivo.
- `aws:executeAwsApi`: crea una regla de filtro.
- `aws:executeAwsApi`: crea una regla de filtro espejo para todo el tráfico entrante.
- `aws:executeAwsApi`: crea una regla de filtro espejo para todo el tráfico saliente.
- `aws:executeAwsApi`: crea una sesión de reflejo de tráfico.
- `aws:executeAwsApi`: elimina el filtro si se produce un error al crear el filtro o la sesión.
- `aws:executeAwsApi`: elimina el objetivo si se produce un error al crear el filtro o la sesión.

Salidas

`CreateFilter.FilterId`

`CreateSession.SessionId`

`CreateTarget.Target IDOutput`

AWSSupport-ConnectivityTroubleshooter

Descripción

El manual de procedimientos `AWSSupport-ConnectivityTroubleshooter` diagnostica los problemas de conectividad entre los siguientes:

- AWS recursos dentro de una Amazon Virtual Private Cloud (Amazon VPC)
- AWS recursos en diferentes Amazon VPCs dentro del mismo Región de AWS que están conectados mediante el emparejamiento de VPC

- AWS recursos en una Amazon VPC y un recurso de Internet mediante una puerta de enlace de Internet
- AWS recursos en una Amazon VPC y un recurso de Internet mediante una puerta de enlace de traducción de direcciones de red (NAT)

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DestinationIp

Tipo: cadena

Descripción: (Obligatorio) La IPv4 dirección del recurso al que desea conectarse.

- DestinationPort

Tipo: cadena

Predeterminado: true

Descripción: (obligatorio) el número de puerto al que desea conectarse en el recurso de destino.

- DestinationVpc

Tipo: cadena

Valor predeterminado: All

Descripción: (opcional) el ID de la Amazon VPC con la que desea probar la conectividad.

- SourceIp

Tipo: cadena

Descripción: (Obligatoria) La IPv4 dirección privada del AWS recurso de tu Amazon VPC desde el que quieres probar la conectividad.

- SourcePortRange

Tipo: cadena

Descripción: (opcional) El rango de puertos que utiliza el AWS recurso de tu Amazon VPC desde el que quieres probar la conectividad.

- SourceVpc

Tipo: cadena

Valor predeterminado: All

Descripción: (opcional) el ID de la Amazon VPC desde la que desea probar la conectividad.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcPeeringConnections

Pasos de documentos

- `aws:executeScript`- Recopila detalles sobre el AWS recurso que especifique en el `SourceIP` parámetro.
- `aws:executeScript`- Determina el destino del tráfico de red procedente del AWS recurso utilizando las rutas recopiladas en el paso anterior.
- `aws:branch`: se ramifican en función del destino del tráfico de la red.
- `aws:executeAwsApi`: recopila detalles sobre el recurso de destino.
- `aws:executeScript`: confirma que el ID regresado para la Amazon VPC de destino coincide con el valor especificado, si lo hubiera, en el parámetro `DestinationVpc`.
- `aws:executeAwsApi`: recopila las reglas del grupo de seguridad para los recursos de origen y destino.
- `aws:executeScript`: confirma si las reglas del grupo de seguridad permiten el tráfico necesario entre los recursos de origen y destino.
- `aws:executeAwsApi`- Recopila las listas de control de acceso a la red (NACLs) asociadas a las subredes de los recursos de origen y destino.
- `aws:executeScript`- Confirma si NACLs permite el tráfico necesario entre los recursos de origen y destino.
- `aws:executeScript`: confirma si la fuente tiene una dirección IP pública asociada al recurso, si el destino de la ruta es una puerta de enlace de Internet.
- `aws:executeAwsApi`: recopila las reglas del grupo de seguridad para el recurso fuente.
- `aws:executeScript`: confirma si las reglas del grupo de seguridad permiten el tráfico necesario desde el recurso de origen al de destino.
- `aws:executeAwsApi`- Recopila lo NACLs asociado a la subred del recurso de origen.
- `aws:executeScript`- Confirma si NACLs permite el tráfico necesario desde el recurso fuente.
- `aws:executeAwsApi`: recopila detalles sobre la puerta de enlace de NAT.
- `aws:executeAwsApi`- Recopila lo NACLs asociado a la subred de la puerta de enlace NAT.
- `aws:executeScript`- Confirma si NACLs permite el tráfico necesario desde la subred para la puerta de enlace NAT.
- `aws:executeScript`: recopila las rutas asociadas a la subred de la puerta de enlace NAT.
- `aws:executeScript`: confirma si la puerta de enlace NAT tiene una ruta hacia una puerta de enlace de Internet.

- `aws:executeAwsApi`: recopila detalles sobre la conexión de emparejamiento de VPC.
- `aws:executeScript`- Confirma que ambas VPCs se encuentran en la misma región y que el ID devuelto para la VPC de destino coincide con el valor especificado, si lo hubiera, en el `DestinationVpc` parámetro.
- `aws:executeAwsApi`: regresa la subred del recurso de destino.
- `aws:executeScript`: recopila las rutas asociadas a la subred de la VPC interconectada.
- `aws:executeScript`: confirma si la VPC interconectada tiene una ruta hacia la conexión de intercambio de tráfico.
- `aws:executeScript`: confirma si el tráfico está permitido desde el recurso de origen si la automatización no admite el destino.

AWSSupport-TroubleshootVPN

Descripción

El `AWSSupport-TroubleshootVPN` manual le ayuda a rastrear y resolver los errores de una AWS Site-to-Site VPN conexión. La automatización incluye varias comprobaciones automatizadas diseñadas para rastrear IKEv1 IKEv2 los errores relacionados con los túneles de AWS Site-to-Site VPN conexión. La automatización intenta hacer coincidir errores específicos y su correspondiente resolución para formar una lista de problemas comunes.

Nota: Esta automatización no corrige los errores. Se ejecuta durante el intervalo de tiempo mencionado y escanea el grupo de registros en busca de errores en el grupo de [CloudWatch registros de la VPN](#).

¿Cómo funciona?

El runbook ejecuta una validación de parámetros para confirmar si el grupo de CloudWatch registros de Amazon incluido en el parámetro de entrada existe, si hay algún flujo de registro en el grupo de registros que corresponda al registro del túnel VPN, si existe el identificador de conexión VPN y si existe la dirección IP del túnel. Realiza llamadas a la API de Logs Insights en su grupo de CloudWatch registros que está configurado para el registro de VPN.

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- LogGroupName

Tipo: cadena

Descripción: (obligatorio) El nombre del grupo de CloudWatch registros de Amazon configurado para el registro de AWS Site-to-Site VPN conexiones

Valor permitido: `^[\\.\-_/#A-Za-z0-9]{1,512}`

- VpnConnectionId

Tipo: cadena

Descripción: (Obligatorio) El identificador de AWS Site-to-Site VPN conexión que se va a solucionar.

Valor permitido: `^vpn-[0-9a-f]{8,17}$`

- Túnel AIPAddress

Tipo: cadena

Descripción: (Obligatoria) La IPv4 dirección número 1 del túnel asociada a su AWS Site-to-Site VPN.

Valor permitido: `^((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}$`

- Túnel BIPAddress

Tipo: cadena

Descripción: (Opcional) La IPv4 dirección número 2 del túnel asociada a su AWS Site-to-Site VPN.

Valor permitido: `^((25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)[.]){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?){1}|^$`

- IKEVersion

Tipo: cadena

Descripción: (obligatorio) seleccione la versión de IKE que está utilizando. Valores permitidos: IKEv1, IKEv2

Valores válidos: `['IKEv1', 'IKEv2']`

- StartTimeinEpoch

Tipo: cadena

Descripción: (opcional) hora de inicio para el análisis de registro. Puede utilizar StartTimeinEpoch/EndTimeinEpoch o LookBackPeriod para el análisis de registros

Valor permitido: `^\d{10}|^$`

- EndTimeinEpoch

Tipo: cadena

Descripción: (opcional) hora de finalización para el análisis de registro. Puede utilizar StartTimeinEpoch/EndTimeinEpoch o LookBackPeriod para el análisis de registros. Si se dan ambos StartTimeinEpoch/EndTimeinEpoch LookBackPeriod , entonces LookBackPeriod tiene prioridad

Valor permitido: `^\d{10}|^$`

- LookBackPeriod

Tipo: cadena

Descripción: (opcional) Tiempo de dos dígitos en horas para analizar el registro. Rango válido: 01 - 99. Este valor tiene prioridad si también se da y StartTimeinEpoch EndTime

Valor permitido: `^(\d?[1-9]|[1-9]0)|^$`

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`
- `ec2:DescribeVpnConnections`

Instrucciones

Nota: Esta automatización funciona en los grupos de CloudWatch registros que están configurados para el registro del túnel de la VPN, cuando el formato de salida del registro es JSON.

Siga estos pasos para configurar la automatización:

1. Navegue hasta [AWSSupport-TroubleshootVPN](#) la AWS Systems Manager consola.
2. Para los parámetros de entrada, introduzca lo siguiente:

- `AutomationAssumeRole` (Opcional):

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- `LogGroupName` (Obligatorio):

El nombre del grupo de CloudWatch registros de Amazon que se va a validar. Debe ser el grupo de CloudWatch registros que está configurado para que la VPN envíe los registros.

- `VpnConnectionId` (Obligatorio):

El identificador de AWS Site-to-Site VPN conexión cuyo grupo de registros se ha rastreado para detectar un error de VPN.

- **Túnel AIPAddress (obligatorio):**

La dirección IP del túnel A asociada a su AWS Site-to-Site VPN conexión.

- **Túnel BIPAddress (opcional):**

La dirección IP del túnel B asociada a su AWS Site-to-Site VPN conexión.

- **IKEVersion (Obligatorio):**

Selecciona lo IKEVersion que estás usando. Valores permitidos: IKEv1, IKEv2.

- **StartTimeinEpoch (Opcional):**

El comienzo del intervalo de tiempo para realizar la consulta en busca de errores. El rango es inclusivo, por lo que la hora de inicio especificada se incluye en la consulta. Se especifica como tiempo de época el número de segundos desde el 1 de enero de 1970 a las 00:00:00 UTC.

- **EndTimeinEpoch (Opcional):**

El final del intervalo de tiempo para buscar errores. El intervalo es inclusivo, por lo que la hora de finalización especificada se incluye en la consulta. Se especifica como tiempo de época el número de segundos desde el 1 de enero de 1970 a las 00:00:00 UTC.

- **LookBackPeriod (Obligatorio):**

Tiempo en horas para revisar la consulta en busca de errores.

Nota: Configure un StartTimeinEpoch EndTimeinEpoch, o LookBackPeriod para fijar el intervalo de tiempo para el análisis de registros. Indique un número de dos dígitos en horas para comprobar si hay errores en el pasado desde la hora de inicio de la automatización. O bien, si el error se produjo en el pasado dentro de un intervalo de tiempo específico, incluya StartTimeinEpoch y EndTimeinEpoch, en lugar de LookBackPeriod.

Input parameters	
AutomationAssumeRole (Optional) The ARN of the role that allows Automation to perform the actions on your behalf. Choose an option	LogGroupName (Required) The Amazon CloudWatch log group name to be validated. This must be the CloudWatch log group which is destined for VPN logs. vpnlog
VpnConnectionId (Required) The AWS Site-to-Site VPN connection id to be validated. vpn-123abc456zxc	TunnelAIPAddress (Required) The tunnel number 1 IP address associated with your AWS Site-to-Site VPN to be validated. 1.1.1.1
TunnelBIPAddress (Optional) The tunnel number 2 IP address associated with your AWS Site-to-Site VPN to be validated. String	IKEVersion (Required) Select what IKE Version you are using. Allowed values : IKEv1, IKEv2 or both IKEv1
StartTimeinEpoch (Optional) Start time for log analysis. You can either use StartTimeinEpoch/EndTimeinEpoch or LookBackPeriod for logs analysis. String	EndTimeinEpoch (Optional) End time for log analysis. You can either use StartTimeinEpoch/EndTimeinEpoch or LookBackPeriod for logs analysis. String
LookBackPeriod (Required) Time in hours to look back for log analysis. 05	

3. Seleccione Ejecutar.

4. Se inicia la automatización.

5. El manual de procedimientos de automatización realiza los siguientes pasos:

- `parameterValidation`:

Ejecuta una serie de validaciones de los parámetros de entrada incluidos en la automatización.

- `branchOnValidationOfLogGroup`:

Comprueba si el grupo de registro mencionado en el parámetro es válido. Si no es válido, detiene los siguientes pasos de la automatización.

- `branchOnValidationOfLogStream`:

Comprueba si el flujo de registros existe en el grupo de CloudWatch registros incluido. Si no es válido, detiene los siguientes pasos de la automatización.

- `branchOnValidationOfVpnConnectionId`:

Comprueba si el identificador de conexión VPN incluido en el parámetro es válido. Si no es válido, detiene los siguientes pasos de la automatización.

- `branchOnValidationOfVpnIp`:

Comprueba si la dirección IP del túnel mencionada en el parámetro es válida o no. Si no es válida, detiene la ejecución posterior de los pasos de automatización.

- `traceError`:

Realiza una llamada a la API de logs Insight en el grupo de registros incluido CloudWatch y busca el error relacionado con IKEv1/IKEv2 junto con una solución sugerida al respecto.

6. Una vez finalizada, consulte la sección de resultados para ver los resultados detallados de la ejecución.

▼ Outputs	
parameterValidation.LogGroupName LogGroupValid parameterValidation.VpnConnection validVpnConnection traceErrorTunnel1IKEv2 ("IKEv2ErrorCount":0) traceErrorTunnel2IKEv2 ("IKEv2ErrorCount":0) traceErrorTunnel1IKEv1 ["Error related to : AWS tunnel received DELETE for Phase 2 SA"] Please treat below as Potential resolution of this error : AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent Delete_SA message for Phase 2. When AWS receives Delete_SA for Phase 2 from CGW it deletes the Phase 2 of SPI mentioned in Delete_SA request. Possible reason of CGW sending Delete_SA message can be due to any configurational changes made in CGW side Next Steps: * Check IPsec Logs on the CGW Device to verify if you are able to see information pertaining to this issue. References: [1] Tunnel stability issues during a rekey: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-fix-ikev2-tunnel-instability-rekey/ [2] Phase 2 Troubleshooting: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-phase-2-ipsec/ ","Error related to : AWS tunnel received DELETE for IKE_SA from CGW"] Please treat below as Potential resolution of this error : AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent the Delete_SA message for Parent/IKE_SA. When AWS receives Delete_SA from CGW, it honours the message and brings down the VPN tunnel. There can be various reasons for CGW sending Delete_SA message like : * A reset to clear active SAs has been performed on the CGW side * IKE SA has been timed out * Configurational changes have been made on CGW Next Steps: * Review your VPN device idle timeout settings using information from your device vendor. When there is no traffic through a VPN tunnel for the duration of your vendor-specific VPN idle time, the IPsec session terminates. For more information on tunnel inactivity and instability refer to this documentation [1] * Check logs on your CGW device to verify if you are able to see information pertaining to this issue. References: [1] Tunnel inactivity or instability: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-instability-inactivity/ ","Error related to : No proposal chosen"] Please treat below as Potential resolution of this error : AWS CloudWatch monitoring has detected that IKE Phase 2 parameters (such as encryption algorithm, hashing algorithm and DH group) configured on Customer Gateway (CGW) device and AWS VPN endpoint do not match or the CGW is using parameters that are not supported by the AWS VPN. Next Steps: * Verify that the Phase 2 parameters (Integrity algorithm, Encryption algorithm and DH group) being proposed by CGW are matching with those configured on AWS side. If you are using default settings on AWS side then verify that parameters being proposed are supported by AWS VPN. To Find list of parameters supported by * If you want to modify the parameters on the AWS VPN side you can follow below steps: Step 1: Open the Amazon VPC console at https://console.aws.amazon.com/vpc/ Step 2: In the navigation pane, choose Site-to-Site VPN Connections. Step 3: Select the Site-to-Site VPN connection, and choose Actions, Modify VPN Tunnel Options. Step 4: For VPN Tunnel Outside IP Address, choose the tunnel endpoint IP of the VPN tunnel that you are modifying options for. Step 5: Choose or enter new values for the tunnel options. Step 6: Choose Save.	parameterValidation.LogStream validLogStream parameterValidation.VpnIpAddress validVpnIP traceErrorTunnel2IKEv1 ("IKEv1ErrorCount":0)

Referencias

Automatización de Systems Manager

- [Ejecuta esta automatización \(consola\)](#)
- [Ejecución de una automatización](#)
- [Configuración de Automatización](#)
- [Página de inicio de Support Automation Workflows](#)

AWS documentación de servicio

- [Contenido de los registros de la Site-to-Site VPN](#)

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Descripción

El manual de procedimientos de AWSConfigRemediation-DeleteEgressOnlyInternetGateway elimina la puerta de enlace de Internet de solo salida especificada.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- EgressOnlyInternetGatewayId

Tipo: cadena

Descripción: (obligatorio) el ID de la puerta de enlace de Internet de solo salida que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteEgressOnlyInternetGateway
- ec2:DescribeEgressOnlyInternetGateways

Pasos de documentos

- `aws:executeScript`: elimina la puerta de enlace de Internet de solo salida especificada en el parámetro `EgressOnlyInternetGatewayId`.
- `aws:executeScript`: verifica que se haya eliminado la puerta de enlace de Internet de solo salida.

AWSConfigRemediation-DeleteUnusedENI

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedENI` elimina una interfaz de red elástica (ENI) que tiene un estado de conexión de `detached`.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `NetworkInterfaceId`

Tipo: cadena

Descripción: (obligatorio) ID de la instancia de ENI que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

Pasos de documentos

- `aws:executeAwsApi`: elimina el ENI que especifique en el parámetro `NetworkInterfaceId`.
- `aws:executeScript`: verifica que se haya eliminado el ENI.

AWSConfigRemediation-DeleteUnusedSecurityGroup

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteUnusedSecurityGroup` elimina el grupo de seguridad que especifique en el parámetro `GroupId`. Si intenta eliminar un grupo de seguridad asociado a una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o si otro grupo de seguridad hace referencia a este, falla la automatización. Esta automatización no elimina un grupo de seguridad predeterminado.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- GroupId

Tipo: cadena

Descripción: (obligatorio) el ID del grupo de seguridad que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2>DeleteSecurityGroup

Pasos de documentos

- aws:executeAwsApi: regresa el nombre del grupo de seguridad utilizando el valor que haya proporcionado en el parámetro GroupId.
- aws:branch: confirma que el nombre del grupo no es “predeterminado”.
- aws:executeAwsApi: elimina el grupo de seguridad especificado en el parámetro GroupId.
- aws:executeScript: confirma que se ha eliminado el grupo de seguridad.

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

Descripción

El manual de procedimientos AWSConfigRemediation-DeleteUnusedVPCNetworkACL elimina una lista de control de acceso (ACL) de red que no está asociada a una subred.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- NetworkAclId

Tipo: cadena

Descripción: (obligatorio) el ID de la ACL de red que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2>DeleteNetworkAcl
- ec2:DescribeNetworkAcls

Pasos de documentos

- `aws:executeAwsApi`: elimina la ACL de red especificada en el parámetro `NetworkACLId`.
- `aws:executeScript`: confirma que se ha eliminado la ACL de red especificada en el parámetro `NetworkACLId`.

AWSConfigRemediation-DeleteVPCFlowLog

Descripción

El manual de procedimientos `AWSConfigRemediation-DeleteVPCFlowLog` elimina el registro de flujo de nube privada virtual (VPC) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `FlowLogId`

Tipo: cadena

Descripción: (obligatorio) ID del registro de flujo que desea eliminar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Pasos de documentos

- `aws:executeAwsApi`: elimina el registro de flujo que especifique en el parámetro `FlowLogId`.
- `aws:executeScript`: verifica que se haya eliminado el registro de flujo.

AWSConfigRemediation-DetachAndDeleteInternetGateway

Descripción

El manual de procedimientos `AWSConfigRemediation-DetachAndDeleteInternetGateway` separa y elimina la puerta de enlace de Internet que especifique. Si alguna instancia de Amazon EC2 de su nube privada virtual (VPC) tiene direcciones IP elásticas o IPv4 direcciones públicas asociadas, se produce un error en el runbook.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- InternetGatewayId

Tipo: cadena

Descripción: (obligatorio) el ID de la puerta de enlace de Internet que desea eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteInternetGateway
- ec2:DescribeInternetGateways
- ec2:DetachInternetGateway

Pasos de documentos

- aws:waitForAwsResourceProperty: acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad estatal de la puerta de enlace privada virtual cambie a `available` o se agote el tiempo de espera.
- aws:executeAwsApi: recupera una configuración de puerta de enlace privada virtual específica.
- aws:branch- Se ramifican según el valor del parámetro VpcAttachments .state.
- aws:waitForAwsResourceProperty- Acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad VpcAttachments .state de la puerta de enlace privada virtual cambie `attached` o se agote el tiempo de espera.
- aws:executeAwsApi: acepta el ID de la puerta de enlace virtual privada y el ID de Amazon VPC como entrada y separa la puerta de enlace virtual privada de la Amazon VPC.

- `aws:waitForAwsResourceProperty`- Acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad `VpcAttachments .state` de la puerta de enlace privada virtual cambie o se agote el tiempo de espera. `detached`
 - `aws:executeAwsApi`: acepta el ID de la puerta de enlace privada virtual como entrada y lo elimina.
 - `aws:waitForAwsResourceProperty`: acepta el ID de la puerta de enlace privada virtual como entrada y verifica su eliminación.
- `aws:executeAwsApi`: recopila el ID de VPC del ID de la puerta de enlace de Internet.
- `aws:executeAwsApi`: separa el ID de la puerta de enlace de Internet de la VPC.
 - `aws:executeAwsApi`: elimina la puerta de enlace de Internet.

AWSConfigRemediation- DetachAndDeleteVirtualPrivateGateway

Descripción

El manual de procedimientos `AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` separa y elimina una determinada puerta de enlace privada virtual de Amazon Elastic Compute Cloud (Amazon EC2) asociada a una nube privada virtual (VPC) creada con Amazon Virtual Private Cloud (Amazon VPC).

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- VpnGatewayId

Tipo: cadena

Descripción: (obligatorio) el ID de la puerta de enlace privada virtual que se va a eliminar.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteVpnGateway
- ec2:DetachVpnGateway
- ec2:DescribeVpnGateways

Pasos de documentos

- aws:waitForAwsResourceProperty: acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad estatal de la puerta de enlace privada virtual cambie a `available` o se agote el tiempo de espera.
- aws:executeAwsApi: recupera una configuración de puerta de enlace privada virtual específica.
- aws:branch- Se ramifica según el valor del parámetro VpcAttachments .state.
- aws:waitForAwsResourceProperty- Acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad VpcAttachments .state de la puerta de enlace privada virtual cambie `attached` o se agote el tiempo de espera.

- `aws:executeAwsApi`: acepta el ID de la puerta de enlace virtual privada y el ID de Amazon VPC como entrada y separa la puerta de enlace virtual privada de la Amazon VPC.
- `aws:waitForAwsResourceProperty`- Acepta el ID de la puerta de enlace privada virtual y espera a que la propiedad `VpcAttachments .state` de la puerta de enlace privada virtual cambie o se agote el tiempo de espera. `detached`
- `aws:executeAwsApi`: acepta el ID de la puerta de enlace privada virtual como entrada y lo elimina.
- `aws:waitForAwsResourceProperty`: acepta el ID de la puerta de enlace privada virtual como entrada y verifica su eliminación.

AWS-DisableIncomingSSHOnPort22

Descripción

El `AWS-DisableIncomingSSHOnPort22` manual elimina las reglas que permiten el tráfico SSH entrante sin restricciones en el puerto TCP 22 para los grupos de seguridad.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- SecurityGroupIds

Tipo: cadena

Descripción: (Obligatorio) Lista separada por comas de los IDs grupos de seguridad a los que desea restringir el tráfico SSH.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupIngress

Pasos de documentos

- aws:executeAwsApi- Elimina todas las reglas que permiten el tráfico SSH entrante en el puerto TCP 22 de los grupos de seguridad que especifique en el parámetro. SecurityGroupIds

Salidas

DisableIncomingSSTemplate. RestrictedSecurityGroupIds - Una lista de los grupos IDs de seguridad a los que se les han eliminado las reglas de SSH entrantes.

AWS-DisablePublicAccessForSecurityGroup

Descripción

Este manual de procedimientos deshabilita los puertos SSH y RDP predeterminados que se abren a todas las direcciones IP.

Important

Este manual falla con un». InvalidPermission NotFound«error para los grupos de seguridad que cumplen los dos criterios siguientes: 1) El grupo de seguridad está ubicado en una VPC

no predeterminada; y 2) Las reglas de entrada del grupo de seguridad no especifican los puertos abiertos mediante los cuatro patrones siguientes:

- 0.0.0.0/0
- ::/0
- SSH or RDP port + 0.0.0.0/0
- SSH or RDP port + ::/0

 Note

Este manual no está disponible en Regiones de AWS China.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- GroupId

Tipo: cadena

Descripción: (obligatorio) el ID del grupo de seguridad para el que los puertos deben estar deshabilitados.

- IpAddressToBlock

Tipo: cadena

Descripción: (opcional) IPv4 Direcciones adicionales desde las que se debe bloquear el acceso, en este formato 1.2.3.4/32.

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Descripción

El AWSConfigRemediation-DisableSubnetAutoAssignPublicIP manual desactiva el atributo de direccionamiento IPv4 público de la subred que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- SubnetId

Tipo: cadena

Descripción: (obligatorio) El ID de la subred en la que desea deshabilitar la asignación automática del atributo de IPv4 dirección pública.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

Pasos de documentos

- `aws:executeAwsApi`- Desactiva el atributo de IPv4 dirección pública de asignación automática para la subred que especificó en el parámetro. `SubnetId`
- `aws:assertAwsResourceProperty`: verifica que el atributo se ha desactivado.

AWSSupport-EnableVPCFlowLogs

Descripción

El `AWSSupport-EnableVPCFlowLogs` manual crea registros de flujo de Amazon Virtual Private Cloud (Amazon VPC) para subredes, VPCs interfaces de red y en su. Cuenta de AWS Si crea un log de flujo para una subred o VPC, se supervisará cada interfaz de red elástica de Amazon VPC o la subred. Los datos del registro de flujo se publican en el grupo de CloudWatch registros de Amazon Logs o en el depósito de Amazon Simple Storage Service (Amazon S3) que especifique. Para obtener más información sobre los registros de flujo, consulte [Registros de flujo de VPC](#) en la Guía del usuario de Amazon VPC.

⚠ Important

Los cargos por ingesta y archivado de datos para los registros vendidos se aplican cuando publica los CloudWatch registros de flujo en Logs o en Amazon S3. Para obtener más información, consulte [Registros de flujo de precios](#).

[Ejecuta esta automatización \(consola\)](#)**ℹ Note**

s3Al seleccionar el destino del registro, asegúrese de que la política de compartimentos permita al servicio de entrega de registros acceder al depósito. Para obtener más información, consulte [Permisos de bucket de Amazon S3 para registros de flujo](#).

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- DeliverLogsPermissionArn

Tipo: cadena

Descripción: (opcional) El ARN de la función de IAM que permite a Amazon Elastic Compute Cloud (Amazon EC2) publicar registros de flujo en CloudWatch el grupo de registros de su cuenta. Si especifica s3 para el parámetro LogDestinationType, no proporcione un valor para este parámetro. Para obtener más información, consulte [Publicar registros de flujo en CloudWatch registros](#) en la Guía del usuario de Amazon VPC.

- LogDestinationARN

Tipo: cadena

Descripción: (opcional) el ARN del recurso en el que se publican los datos del registro de flujo. Si cloud-watch-logs se especifica para el LogDestinationType parámetro, proporcione el ARN del grupo de CloudWatch registros en el que desea publicar los datos del registro de flujo. También puede utilizar LogGroupName en su lugar. Si se especifica s3 para el parámetro LogDestinationType, debe especificar el ARN del bucket de Amazon S3 en el que desea publicar los datos del registro de flujo para este parámetro. También puede especificar una carpeta de bucket.

 Important

s3Al elegir uno, LogDestinationType debe asegurarse de que el bucket seleccionado siga [las prácticas recomendadas de seguridad de Amazon S3 Bucket](#) y de que cumpla con las leyes de privacidad de datos de su organización y región geográfica.

- LogDestinationType

Tipo: cadena

Valores válidos: cloud-watch-logs | s3

Descripción: (obligatorio) determina dónde se publican los datos del registro de flujo. Si especifica LogDestinationType como s3, no especifique DeliverLogsPermissionArn ni LogGroupName.

- LogFormat

Tipo: cadena

Descripción: (opcional) los campos que se van a incluir en el registro de logs de flujo, en el orden en que deben aparecer. Para obtener una lista de los campos disponibles, consulte [Entradas de](#)

[registros de flujo](#) en la Guía del usuario de Amazon VPC. Si no proporciona un valor para este parámetro, el registro de flujo se crea con el formato predeterminado. Si especifica este parámetro, debe especificar al menos un campo.

- LogGroupName

Tipo: cadena

Descripción: (opcional) Nombre del grupo de CloudWatch registros donde se publican los datos del registro de flujo. Si especifica s3 para el parámetro LogDestinationType, no proporcione un valor para este parámetro.

- ResourceIds

Tipo: StringList

Descripción: (Obligatorio) Una lista separada IDs por comas de las subredes, interfaces de red elásticas o VPC para las que desea crear un registro de flujo.

- TrafficType

Tipo: cadena

Valores válidos: ACCEPT | REJECT | ALL

Descripción: (obligatorio) el tipo de tráfico que se va a registrar. Puede registrar el tráfico que el recurso acepta o rechaza, o todo el tráfico.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:CreateFlowLogs
- ec2>DeleteFlowLogs
- ec2:DescribeFlowLogs
- iam:AttachRolePolicy
- iam:CreateRole

- iam:CreatePolicy
- iam>DeletePolicy
- iam>DeleteRole
- iam>DeleteRolePolicy
- iam:GetPolicy
- iam:GetRole
- iam:TagRole
- iam:PassRole
- iam:PutRolePolicy
- iam:UpdateRole
- logs:CreateLogDelivery
- logs:CreateLogGroup
- logs>DeleteLogDelivery
- logs>DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- s3:GetBucketLocation
- s3:GetBucketAcl
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:ListBucket
- s3:PutObject

Ejemplo de política

JSON

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

```

        "Sid": "SSMExecutionPermissions",
        "Effect": "Allow",
        "Action": [
            "ssm:StartAutomationExecution",
            "ssm:GetAutomationExecution"
        ],
        "Resource": "*"
    },
    {
        "Sid": "EC2FlowLogsPermissions",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateFlowLogs",
            "ec2>DeleteFlowLogs",
            "ec2:DescribeFlowLogs"
        ],
        "Resource": [
            "arn:aws:ec2:us-east-1:111122223333:instance/resource-id",
            "arn:aws:ec2:us-east-1:111122223333:subnet/resource-id",
            "arn:aws:ec2:us-east-1:111122223333:vpc/resource-id",
            "arn:aws:ec2:us-east-1:111122223333:transit-gateway/resource-id",
            "arn:aws:ec2:us-east-1:111122223333:transit-gateway-
attachment/resource-id"
        ]
    },
    {
        "Sid": "IAMCreateRolePermissions",
        "Effect": "Allow",
        "Action": [
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:CreatePolicy",
            "iam>DeletePolicy",
            "iam>DeleteRole",
            "iam>DeleteRolePolicy",
            "iam:GetPolicy",
            "iam:GetRole",
            "iam:TagRole",
            "iam:PassRole",
            "iam:PutRolePolicy",
            "iam:UpdateRole"
        ],
        "Resource": [
            "arn:aws:iam:111122223333:role/role-name",

```

```

        "arn:aws:iam::111122223333:role/AWSSupportCreateFlowLogsRole"
    ],
    },
    {
        "Sid": "CloudWatchLogsPermissions",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogDelivery",
            "logs:CreateLogGroup",
            "logs>DeleteLogDelivery",
            "logs>DeleteLogGroup",
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams"
        ],
        "Resource": [
            "arn:aws:logs:us-east-1:111122223333:log-group:log-group-name",
            "arn:aws:logs:us-east-1:111122223333:log-group:log-group-name:*"
        ]
    },
    {
        "Sid": "S3Permissions",
        "Effect": "Allow",
        "Action": [
            "s3:GetBucketLocation",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketAcl",
            "s3:ListBucket",
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    }
]
}

```

Pasos de documentos

- `aws:branch`: se ramifica en función del valor especificado para el parámetro `LogDestinationType`.
- `aws:executeScript`- Comprueba si el Amazon Simple Storage Service (Amazon S3) de destino puede conceder acceso de lectura o public escritura a sus objetos.
- `aws:executeScript`: crea un grupo de registro si no se especifica ningún valor para el parámetro `LogDestinationARN`, y se especifica `cloud-watch-logs` para el parámetro `LogDestinationType`.
- `aws:executeScript`: crea registros de flujo en función de los valores especificados en los parámetros del manual de procedimientos.

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

Descripción

El `AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch` runbook reemplaza un registro de flujo de Amazon VPC existente que publica los datos del registro de flujo en Amazon Simple Storage Service (Amazon S3) por un registro de flujo que publica los datos del registro de flujo en el grupo de registros de CloudWatch Amazon Logs CloudWatch (Logs) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DestinationLogGroup

Tipo: cadena

Descripción: (obligatorio) El nombre del grupo de CloudWatch registros en el que desea publicar los datos de los registros de flujo.

- DeliverLogsPermissionArn

Tipo: cadena

Descripción: (obligatorio) El ARN del rol AWS Identity and Access Management (IAM) que desea utilizar y que proporciona a Amazon Elastic Compute Cloud (Amazon EC2) los permisos necesarios para publicar datos de registros de flujo en Logs. CloudWatch

- FlowLogId

Tipo: cadena

Descripción: (obligatorio) el ID del registro de flujo que publica en Amazon S3 que desea reemplazar.

- MaxAggregationInterval

Tipo: entero

Valores válidos: 60 | 600

Descripción: (opcional) el intervalo máximo de tiempo durante el cual se captura un flujo de paquetes y se agrega un registro de logs de flujo.

- TrafficType

Tipo: cadena

Valores válidos: ACCEPT | REJECT | ALL

Descripción: (obligatorio) el tipo de datos del registro de flujo que desea registrar y publicar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2>DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Pasos de documentos

- `aws:executeAwsApi`: recopila detalles sobre su VPC a partir del valor que especifique en el parámetro `FlowLogId`.
- `aws:executeAwsApi`: crea un registro de flujo en función de los valores que especifique para los parámetros del manual de procedimientos.
- `aws:assertAwsResourceProperty`- Verifica que el registro de flujo recién creado se publique en Logs. CloudWatch
- `aws:executeAwsApi`: elimina el registro de flujo que se publica en Amazon S3.
- `aws:executeScript`: confirma que se ha eliminado el registro de flujo publicado en Amazon S3.

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

Descripción

El `AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket` runbook reemplaza un registro de flujo de Amazon VPC existente que publica los datos del registro de flujo en CloudWatch Amazon Logs CloudWatch (Logs) por un registro de flujo que publica los datos del registro de flujo en el depósito de Amazon Simple Storage Service (Amazon S3) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- Destino S3 BucketArn

Tipo: cadena

Descripción: (obligatorio) el ARN del bucket de Amazon S3 en el que desea publicar los datos del registro de flujo.

- FlowLogId

Tipo: cadena

Descripción: (obligatorio) El ID del registro de flujo que se publica en los CloudWatch registros que desea reemplazar.

- MaxAggregationInterval

Tipo: entero

Valores válidos: 60 | 600

Descripción: (opcional) el intervalo máximo de tiempo durante el cual se captura un flujo de paquetes y se agrega un registro de logs de flujo.

- TrafficType

Tipo: cadena

Valores válidos: ACCEPT | REJECT | ALL

Descripción: (obligatorio) el tipo de datos del registro de flujo que desea registrar y publicar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2>DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Pasos de documentos

- `aws:executeAwsApi`: recopila detalles sobre su VPC a partir del valor que especifique en el parámetro `FlowLogId`.
- `aws:executeAwsApi`: crea un registro de flujo en función de los valores que especifique para los parámetros del manual de procedimientos.
- `aws:assertAwsResourceProperty`: verifica que el registro de flujo recién creado se publique en Amazon S3.
- `aws:executeAwsApi`- Elimina el registro de flujo que se publica en CloudWatch Logs.
- `aws:executeScript`- Confirma que se ha eliminado el registro de flujo publicado en CloudWatch Logs.

AWS-ReleaseElasticIP

Descripción

Libere la dirección IP elástica especificada utilizando el ID de asignación.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AllocationId

Tipo: cadena

Descripción: (obligatorio) el ID de asignación de la dirección IP elástica.

AWS-RemoveNetworkACLUnrestrictedSSHRDP

Descripción

El AWS-RemoveNetworkACLUnrestrictedSSHRDP manual elimina todas las reglas de la lista de control de acceso a la red (ACL) de la ACL de red especificada que permiten la entrada de tráfico desde todas las direcciones de origen a los puertos SSH y RDP predeterminados. No se eliminan las reglas que incluyen rangos de puertos que se superponen con los puertos SSH y RDP predeterminados.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- NetworkAclId

Tipo: cadena

Descripción: (obligatorio) El identificador de la ACL de red que desea eliminar, reglas sin restricciones que permiten la entrada de tráfico desde todas las direcciones de origen a los puertos SSH y RDP predeterminados.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkAclEntry
- ec2:DescribeNetworkAcls

Pasos de documentos

- aws:executeScript: elimina todas las reglas de entrada que permiten el tráfico de todas las direcciones de origen del grupo de seguridad que especificó en el parámetro SecurityGroupId.

Salidas

RemoveNACLEntriesAndVerify. VerificationMessage - Mensajes de verificación de las reglas de ACL de la red eliminadas correctamente.

RemoveNACLEntriesAndVerify. RulesDeletedAndApiResponse - Las reglas de ACL de la red que se eliminaron y las respuestas de la operación de la DeleteNetworkACLEntry API.

AWSConfigRemediation- RemoveUnrestrictedSourceIngressRules

Descripción

El manual de procedimientos AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules elimina todas las reglas de entrada del grupo de seguridad que especifique que permiten el tráfico desde todas las direcciones de origen.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- SecurityGroupId

Tipo: cadena

Descripción: (obligatorio) el ID del grupo de seguridad del que desea eliminar las reglas de entrada que permiten el tráfico desde todas las direcciones de origen.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Pasos de documentos

- `aws:executeScript`: elimina todas las reglas de entrada que permiten el tráfico de todas las direcciones de origen del grupo de seguridad que especificó en el parámetro `SecurityGroupId`.

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

Descripción

El manual de procedimientos `AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` elimina todas las reglas del grupo de seguridad predeterminado de la nube privada virtual (VPC) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- GroupId

Tipo: cadena

Descripción: (obligatorio) el ID del grupo de seguridad del que desea eliminar todas las reglas.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

Pasos de documentos

- aws:assertAwsResourceProperty: confirma que el grupo de seguridad que especificó en el parámetro GroupId se denomina predeterminado.
- aws:executeScript: elimina todas las reglas del grupo de seguridad que especificó en el parámetro GroupId.

AWSSupport-SetupIPMonitoringFromVPC

Descripción

AWSSupport-SetupIPMonitoringFromVPC crea una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en la subred especificada y monitorea el IPs objetivo IPv4 (IPv6o) seleccionado mediante la ejecución continua de pruebas de ping, MTR, traceroute y tracetcp. Los resultados se almacenan en los CloudWatch registros de Amazon Logs y se aplican filtros de métricas para visualizar rápidamente las estadísticas de latencia y pérdida de paquetes en un CloudWatch panel de control.

Información adicional

CloudWatch Los datos de los registros se pueden utilizar para solucionar problemas de red y analizar si la pattern/trends. Additionally, you can configure CloudWatch alarms with Amazon SNS notifications when packet loss and/or latencia alcanza un umbral. Los datos también se pueden usar al abrir un caso AWS Support, para ayudar a aislar un problema rápidamente y reducir el tiempo de resolución al investigar un problema de red.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- CloudWatchLogGroupNamePrefix

Tipo: cadena

Valor predeterminado: /AWSSupport-SetupIPMonitoringFromVPC

Descripción: Prefijo (opcional) utilizado para cada grupo de CloudWatch registros creado para los resultados de las pruebas.

- CloudWatchLogGroupRetentionInDays

Tipo: cadena

Valores válidos: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

Valor predeterminado: 7

Descripción: (opcional) número de días para los que desea conservar los resultados de monitorización de red.

- InstanceType

Tipo: cadena

Valores válidos: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

Valor predeterminado: t3.micro

Descripción: (opcional) El tipo de instancia EC2 de la instancia de EC2 Rescue. Tamaño recomendado: t3.micro.

- SubnetId

Tipo: cadena

Descripción: (opcional) ID de subred para la instancia de monitor. Tenga en cuenta que si especifica una subred privada, debe asegurarse de que haya acceso a Internet para permitir que la instancia del monitor configure la prueba (es decir, instale el agente CloudWatch Logs, interactúe con Systems Manager y CloudWatch).

- Destino IPs

Tipo: cadena

Descripción: (Obligatorio) Lista separada por comas de IPv4s y/o IPv6s para monitorear. No se permiten espacios. El tamaño máximo es de 255 caracteres. Tenga en cuenta que si proporciona una IP no válida, la Automation producirá un error y restaurará la configuración de prueba.

- `TestInstanceSecurityGroupId`

Tipo: cadena

Descripción: (opcional) El ID del grupo de seguridad de la instancia de prueba. Si no se especifica, la automatización crea uno durante la creación de la instancia. Asegúrese de que el grupo de seguridad permita el acceso saliente a la supervisión IPs.

- `TestInstanceProfileName`

Tipo: cadena

Descripción: (opcional) El nombre de un perfil de instancia de IAM existente para la instancia de prueba. Si no se especifica, la automatización crea uno durante la creación de la instancia. El rol debe tener los siguientes permisos: `logs:CreateLogStream`, `logs:DescribeLogGroups`, `logs:DescribeLogStreams`, y `logs:PutLogEvents` y la Política AWS gestionada `AmazonSSMManagedInstanceCore`.

- `TestInterval`

Tipo: cadena

Descripción: (opcional) El número de minutos entre los intervalos de prueba. El valor predeterminado es 1 minuto y el máximo 10 minutos.

- `RetainDashboardAndLogsOnDeletion`

Tipo: cadena

Descripción: (opcional) `False` Especifica que se eliminen el CloudWatch panel de control y los registros de Amazon al eliminar la AWS CloudFormation pila. El valor predeterminado es `True`. De forma predeterminada, el panel y los registros se conservan y deberán eliminarse manualmente cuando ya no se necesiten.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

⚠ Warning

Se recomienda introducir `TestInstanceProfileName` parámetros o garantizar la instalación de barreras de seguridad para evitar el uso indebido de los permisos de IAM mutables.

Se recomienda que el usuario que ejecuta la automatización tenga adjunta la política gestionada por Amazon SSMAutomation Role IAM. Además, el usuario debe tener la siguiente política asociada a su cuenta de usuario, grupo o rol:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "iam:AddRoleToInstanceProfile",
        "iam:GetRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam>DeleteInstanceProfile",
        "iam:PutRolePolicy",
        "iam:TagRole"
      ],
      "Resource": [
        "arn:aws:iam::111122223333:role/SetupIPMonitoringFromVPC*",
        "arn:aws:iam::111122223333:instance-profile/SetupIPMonitoringFromVPC*"
      ],
      "Effect": "Allow"
    }
  ],
}
```

```

{
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:CreateChangeSet",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudwatch:PutDashboard",
    "cloudwatch>DeleteDashboards",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:CreateSecurityGroup",
    "ec2:CreateLaunchTemplate",
    "ec2>DeleteSecurityGroup",
    "ec2:DescribeImages",
    "ec2:DescribeSubnets",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeVpcs",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteSecurityGroup",
    "ec2:RunInstances",
    "ec2:TerminateInstances",
    "ec2:DescribeInstanceStatus",
    "ec2:CreateTags",
    "ec2:AssignIpv6Addresses",
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeLaunchTemplates",
    "ec2:RevokeSecurityGroupEgress",
    "logs:CreateLogGroup",
    "logs>DeleteLogGroup",
    "logs:PutMetricFilter",
    "logs:PutRetentionPolicy",
    "logs:TagResource",
    "ssm:DescribeInstanceInformation",
    "ssm:GetParameter",
    "ssm:GetParameters",
    "ssm:SendCommand",
    "ssm:ListCommands",
    "ssm:ListCommandInvocations"
  ],
  "Resource": [
    "*"
  ],

```

```

    "Effect": "Allow"
  }
]
}

```

Si se proporciona el `TestInstanceProfileName` parámetro, no se requieren los siguientes permisos de IAM para ejecutar el runbook:

- iam: CreateRole
- objetivo: CreateInstanceProfile
- objetivo: DetachRolePolicy
- objetivo: AttachRolePolicy
- objetivo: AddRoleToInstanceProfile
- objetivo: RemoveRoleFromInstanceProfile
- objetivo: DeleteRole
- objetivo: DeleteRolePolicy
- objetivo: DeleteInstanceProfile

Pasos de documentos

1. **aws:executeAwsApi**- describa la subred proporcionada para obtener el ID de VPC IPv6 y el estado de asociación de bloques CIDR.
2. **aws:executeScript**- compruebe que el destino proporcionado es correcto desde el punto de vista sintáctico IPv4 o IPv6 las direcciones, obtenga la arquitectura del tipo de instancia seleccionado y compruebe que la subred tiene una asociación de grupos, si es que IPs hay alguna IP IPv6 de destino. IPv6
3. **aws:createStack**- cree una AWS CloudFormation pila que aprovisiona la instancia Amazon EC2 de prueba, el perfil de la instancia de IAM (si no se proporciona), el grupo de seguridad (si no se proporciona), los grupos de CloudWatch registros y el panel de control. CloudWatch

(Limpieza) Si el paso falla:

aws:executeScript- describa los eventos de la CloudFormation pila para identificar el motivo del error.

aws:deleteStack- eliminar la CloudFormation pila y todos los recursos asociados.

4. **aws:waitForAwsResourceProperty**- espere a que se complete la creación de la CloudFormation pila.

(Limpieza) Si el paso falla:

aws:executeScript- describa los eventos de la CloudFormation pila para identificar el motivo del error.

aws:deleteStack- eliminar la CloudFormation pila y todos los recursos asociados.

5. **aws:executeScript**- describa los recursos de la CloudFormation pila para obtener el ID de la instancia de prueba, el ID del grupo de seguridad, la función de IAM, el perfil de la instancia y el nombre del panel de control.

(Limpieza) Si el paso falla:

aws:executeScript- describa los eventos de la CloudFormation pila para identificar el motivo del error.

aws:deleteStack- eliminar la CloudFormation pila y todos los recursos asociados.

6. **aws:waitForAwsResourceProperty**: espera a que la instancia de prueba se convierta en una instancia gestionada.

(Limpieza) Si el paso falla:

aws:deleteStack- eliminar la CloudFormation pila y todos los recursos asociados.

7. **aws:runCommand**- instale el CloudWatch agente en la instancia de prueba.

(Limpieza) Si el paso falla:

aws:deleteStack- eliminar la CloudFormation pila y todos los recursos asociados.

8. **aws:runCommand**- defina los scripts de prueba de red (MTR, ping, tracepath y traceroute) para cada uno de los proporcionados. IPs

(Limpieza) Si el paso falla:

aws:deleteStack- elimine la pila y todos los CloudFormation recursos asociados.

9. **aws:runCommand**- inicie las pruebas de red y programe las ejecuciones posteriores mediante cronjobs que se ejecutan cada TestInterval minuto.

(Limpieza) Si el paso falla:

aws:deleteStack- eliminar la CloudFormation pila y todos los recursos asociados.

10**aws:runCommand**- configurar el CloudWatch agente para enviar los resultados de las pruebas / home/ec2-user/logs/ a CloudWatch los registros.

(Limpieza) Si el paso falla:

aws:deleteStack- eliminar la CloudFormation pila y todos los recursos asociados.

11**aws:runCommand**- configurar la rotación de registros para los resultados de las pruebas en/ home/ec2-user/logs/.

12**aws:executeScript**- establezca la política de retención para todos los grupos de CloudWatch registros creados por la CloudFormation pila.

13**aws:executeScript**- cree filtros métricos de grupos de CloudWatch registros para la latencia de ping y la pérdida de paquetes de ping.

(Limpieza) Si el paso falla:

aws:deleteStack- eliminar la CloudFormation pila y todos los recursos asociados.

14**aws:executeScript**- actualice el CloudWatch panel de control para incluir widgets con estadísticas de latencia de ping y pérdida de paquetes de ping.

(Limpieza) Si el paso falla:

aws:executeAwsApi- elimine el CloudWatch panel de control, si existe.

aws:deleteStack- eliminar la CloudFormation pila y todos los recursos asociados.

15**aws:branch**- evaluar el SleepTime parámetro. Si se establece en0, la automatización finaliza sin eliminar la pila.

16**aws:sleep**- espere el tiempo especificado SleepTime antes de eliminar la CloudFormation pila.

17**aws:deleteStack**- eliminar la CloudFormation pila. Según el RetainDashboardAndLogsOnDeletion parámetro, el CloudWatch panel de control y los grupos de registros se conservan o se eliminan.

(Limpieza) Si se produce un error al eliminar la pila:

aws:executeScript- describa los eventos de la CloudFormation pila para identificar el motivo del error de eliminación.

Salidas

updateCloudWatchPanel de control. StackUrl - la URL de la CloudFormation pila.

updateCloudWatchPanel de control. DashboardUrl - la URL del CloudWatch panel de control.

updateCloudWatchPanel de control. DashboardName - el nombre del CloudWatch panel de control.

updateCloudWatchCuadro de mandos. LogGroups - la lista de grupos de CloudWatch registros creados.

describeStackResources. HelperInstanceId - el ID de la instancia de prueba.

describeStackResources. StackName - el nombre de la CloudFormation pila.

AWSSupport-TerminateIPMonitoringFromVPC

Descripción

AWSSupport-TerminateIPMonitoringFromVPC finaliza una prueba de supervisión de IP iniciada previamente por AWSSupport-SetupIPMonitoringFromVPC. Se eliminarán los datos relacionados con el ID de prueba especificado.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en

su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- AutomationExecutionId

Tipo: cadena

Descripción: (obligatorio) el ID de ejecución de la automatización de cuando ejecutó anteriormente el manual de procedimientos `AWSSupport-SetupIPMonitoringFromVPC`. Se eliminan todos los recursos asociados a este ID de ejecución.

- InstanceId

Tipo: cadena

Descripción: (opcional) ID de instancia para la instancia de monitor.

- SubnetId

Tipo: cadena

Descripción: (opcional) ID de subred para la instancia de monitor.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

Se recomienda que el usuario que ejecuta la automatización tenga adjunta la política gestionada por Amazon SSMAutomation Role IAM. Además, el usuario debe tener la siguiente política asociada a su usuario, grupo o rol:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:DetachRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteInstanceProfile",
```

```

        "iam:DeleteRolePolicy"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/AWSSupport/
SetupIPMonitoringFromVPC_*",
        "arn:aws:iam::111122223333:instance-profile/AWSSupport/
SetupIPMonitoringFromVPC_*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "iam:DetachRolePolicy"
    ],
    "Resource": [
        "arn:aws:iam::aws:policy/service-role/
AmazonSSMManagedInstanceCore"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "cloudwatch:DeleteDashboards"
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow"
},
{
    "Action": [
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2>DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus"
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow"
}
]

```

```
}
```

Pasos de documentos

1. `aws:assertAwsResourceProperty`- comprueban `AutomationExecutionId` y `InstanceId` están relacionados con la misma prueba.
2. `aws:assertAwsResourceProperty`- comprueban `SubnetId` y `InstanceId` están relacionados con la misma prueba.
3. `aws:executeAwsApi`: recupera el grupo de seguridad de prueba.
4. `aws:executeAwsApi`- eliminar el CloudWatch panel de control.
5. `aws:changeInstanceState`: termina la instancia de prueba.
6. `aws:executeAwsApi`: quita el perfil de instancia de IAM del rol.
7. `aws:executeAwsApi`: elimina el perfil de instancia de IAM creado por la automatización.
8. `aws:executeAwsApi`- elimine la política CloudWatch en línea del rol creado por la automatización.
9. `aws:executeAwsApi`- separar la política `SSMManged InstanceCore` gestionada por Amazon del rol creado por la automatización.
10. `aws:executeAwsApi`: elimina el rol de IAM creado por la automatización.
11. `aws:executeAwsApi`: elimina el grupo de seguridad creado por la automatización, en caso de que exista.

Salidas

Ninguno

AWS WAF

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS WAF Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-AddWAFRegionalRuleToRuleGroup](#)

- [AWS-AddWAFRegionalRuleToWebAcl](#)
- [AWSConfigRemediation-EnableWAFClassicLogging](#)
- [AWSConfigRemediation-EnableWAFClassicRegionalLogging](#)
- [AWSConfigRemediation-EnableWAFV2Logging](#)

AWS-AddWAFRegionalRuleToRuleGroup

Descripción

El AWS-AddWAFRegionalRuleToRuleGroup manual agrega una regla AWS WAF regional existente a un grupo de reglas AWS WAF regionales. Solo se admiten los grupos de reglas regionales AWS WAF clásicos. AWS WAF Los grupos de reglas regionales clásicos pueden tener un máximo de 10 reglas.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- RuleGroupId

Tipo: cadena

Descripción: (obligatorio) El identificador del grupo de reglas que desea actualizar.

- RulePriority

Tipo: entero

Descripción: (Obligatorio) La prioridad de la nueva regla. La prioridad de las reglas determina el orden en que se evalúan las reglas de un grupo regional. Las reglas con un valor más bajo tienen mayor prioridad que las reglas con un valor más alto. El valor debe ser un número entero. Si agrega varias reglas a un grupo de reglas regional, los valores no tienen que ser consecutivos.

- RuleId

Tipo: cadena

Descripción: (obligatorio) El identificador de la regla que desea agregar a su grupo de reglas regional.

- RuleAction

Tipo: cadena

Descripción: (Obligatorio) Especifica la acción que AWS WAF se lleva a cabo cuando una solicitud web cumple las condiciones de la regla.

Valores válidos: ALLOW | BLOCK | COUNT

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- waf-regional:GetChangeToken
- waf-regional:GetChangeTokenStatus
- waf-regional:ListActivatedRulesInRuleGroup
- waf-regional:UpdateRuleGroup

Pasos de documentos

- **Get WAFChange Token (aws:executeAwsApi):** recupera un token de AWS WAF cambio para garantizar que el runbook no envíe solicitudes contradictorias al servicio.
- **Añadir WAFRule a WAFRegional RuleGroup (AWS:Executescript):** añade la regla especificada al grupo de reglas regional. AWS WAF
- **VerifyChangeTokenPropagating (aws: waitForAwsResourceProperty)** - Comprueba que el estado del token de cambio es o. PENDING INSYNC
- **VerifyRuleAddedToRuleGroup (AWS:Executescript)** - Verifica que la AWS WAF regla especificada se haya agregado al grupo de reglas regional de destino.

Salidas

- **VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse** - Resultado del paso que verifica que la nueva regla se agregó al grupo de reglas regional.
- **VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse** - Resultado de la operación de la `ListActivatedRulesInRuleGroup` API.

AWS-AddWAFRegionalRuleToWebAcl

Descripción

El `AWS-AddWAFRegionalRuleToWebAcl` manual agrega una regla AWS WAF regional, un grupo de reglas o una regla basada en tasas existentes a una lista de control de acceso web (ACL) regional AWS WAF clásica. Este manual no actualiza las ACL web regionales AWS WAF clásicas existentes administradas por. AWS Firewall Manager

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Web ACLId

Tipo: cadena

Descripción: (obligatorio) El ID de la ACL web que desea actualizar.

- ActivatedRulePriority

Tipo: entero

Descripción: (Obligatorio) La prioridad de la nueva regla. La prioridad de las reglas determina el orden en que se evalúan las reglas de una ACL web. Las reglas con un valor más bajo tienen mayor prioridad que las reglas con un valor más alto. El valor debe ser un número entero. Si agrega varias reglas a una ACL web regional, los valores no tienen que ser consecutivos.

- ActivatedRuleRuleId

Tipo: cadena

Descripción: (Obligatorio) El ID de la regla normal, la regla basada en tasas o el grupo que desea agregar a la ACL web.

- ActivatedRuleAction

Tipo: cadena

Valores válidos: ALLOW | BLOCK | COUNT

Descripción: (opcional) Especifica la acción que AWS WAF se realiza cuando una solicitud web cumple las condiciones de la regla.

- ActivatedRuleType

Tipo: cadena

Valores válidos: REGULAR | RATE_BASED | GROUP

Predeterminado: REGULAR

Descripción: (opcional) El tipo de regla que va a agregar a la ACL web. Aunque este campo es opcional, tenga en cuenta que si intenta agregar una RATE_BASED regla a una ACL web sin establecer el tipo, la solicitud fallará porque la solicitud utiliza una REGULAR regla de forma predeterminada.

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

Pasos de documentos

- `DetermineWebACLNotEn FMSAnd RulePriority` (AWS:ExecuteScript): verifica si la ACL AWS WAF web está en una política de seguridad de Firewall Manager y verifica que el ID de prioridad no entre en conflicto con una ACL existente.
- `AddRuleOrRuleGroupToWebACL` (AWS:Executescript): agrega la regla especificada a la ACL web. AWS WAF
- `VerifyRuleOrRuleGroupAddedToWebAcl` (AWS:Executescript): verifica que la regla especificada AWS WAF se haya agregado a la ACL web de destino.

Salidas

- `DetermineWebACLNotEn. FMSAnd RulePriority PrereqResponse`: Salida del `DetermineWebACLNotInFMSAndRulePriority` paso.

- VerifyRuleOrRuleGroupAddedToWebAcl. VerifyRuleOrRuleGroupAddedToWebACLResponse: Resultado del AddRuleOrRuleGroupToWebACL paso.
- VerifyRuleOrRuleGroupAddedToWebAcl. ListActivatedRulesOrRuleGroupsInWebACLResponse: Resultado del VerifyRuleOrRuleGroupAddedToWebAcl paso.

AWSConfigRemediation-EnableWAFClassicLogging

Descripción

El AWSConfigRemediation-EnableWAFClassicLogging runbook permite iniciar sesión en Amazon Data Firehose (Firehose) para obtener AWS WAF la lista de control de acceso web (ACL web) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- DeliveryStreamName

Tipo: cadena

Descripción: (Obligatorio) El nombre de la transmisión de entrega de Firehose a la que desea enviar los registros.

- Web ACLId

Tipo: cadena

Descripción: (obligatorio) El ID de la ACL AWS WAF web en la que desea habilitar el inicio de sesión.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

Pasos de documentos

- `aws:executeAwsApi`: confirma que existe el flujo de entrega que especifique en `DeliveryStreamName`.
- `aws:executeAwsApi`- Recopila el ARN de la ACL web especificada en AWS WAF `WebACLId` el parámetro.
- `aws:executeAwsApi`: permite el registro para la web ACL.
- `aws:assertAwsResourceProperty`- Verifica que el registro esté habilitado en la AWS WAF ACL web.

AWSConfigRemediation-EnableWAFClassicRegionalLogging

Descripción

El `AWSConfigRemediation-EnableWAFClassicRegionalLogging` runbook permite iniciar sesión en Amazon Data Firehose (Firehose) para AWS WAF la lista de control de acceso web (ACL) que especifique.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- `AutomationAssumeRole`

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- `LogDestinationConfigs`

Tipo: cadena

Descripción: (obligatorio) El nombre del recurso de Amazon (ARN) de la transmisión de entrega de Firehose a la que desea enviar los registros.

- `Web ACLId`

Tipo: cadena

Descripción: (obligatorio) El ID de la ACL AWS WAF web en la que desea habilitar el inicio de sesión.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

Pasos de documentos

- `aws:executeAwsApi`- Recopila el ARN de la ACL web especificada en AWS WAF `WebACLId` el parámetro.
- `aws:executeAwsApi`: permite el registro para la web ACL.
- `aws:assertAwsResourceProperty`- Verifica que el registro esté habilitado en la AWS WAF ACL web.

AWSConfigRemediation-EnableWAFV2Logging

Descripción

El `AWSConfigRemediation-EnableWAFV2Logging` runbook permite registrar una lista de control de acceso web AWS WAF (ACL web) (AWS WAF V2) con el flujo de entrega de Amazon Data Firehose (Firehose) especificado.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- LogDestinationConfigs

Tipo: cadena

Descripción: (Obligatorio) El ARN del flujo de entrega de Firehose que desea asociar a la ACL web.

Note

El ARN de la transmisión de entrega de Firehose debe empezar por el prefijo. `aws-waf-logs-` Por ejemplo, `aws-waf-logs-us-east-2-analytics`. Para obtener más información, consulte [Amazon Data Firehose](#).

- WebAclArn

Tipo: cadena

Descripción: (obligatorio) el ARN de la web ACL para la que se habilitará el registro.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`

- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

Pasos de documentos

- `aws:executeScript`- Habilita el registro para la ACL web AWS WAF V2 y verifica que el registro tenga la configuración especificada.

Amazon WorkSpaces

AWS Systems Manager La automatización proporciona manuales predefinidos para Amazon WorkSpaces. Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWS-CreateWorkSpace](#)
- [AWSSupport-RecoverWorkSpace](#)

AWS-CreateWorkSpace

Descripción

El `AWS-CreateWorkSpace` runbook crea un nuevo escritorio WorkSpaces virtual de Amazon, conocido como a Workspace, en función de los valores que especifique para los parámetros de entrada. Para obtener más información WorkSpaces, consulta [¿Qué es Amazon WorkSpaces?](#) en la Guía de WorkSpaces administración de Amazon.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- BundleId

Tipo: cadena

Descripción: (Obligatorio) El identificador del paquete que se utilizará en WorkSpace.

- ComputeTypeName

Tipo: cadena

Valores válidos: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

Descripción: (opcional) El tipo de cálculo para su WorkSpace.

- DirectoryId

Tipo: cadena

Descripción: (obligatorio) El ID del directorio al que quieres WorkSpace añadirlo.

- RootVolumeEncryptionEnabled

Tipo: Booleano

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) Determina si el volumen raíz del WorkSpace está cifrado.

- **RootVolumeSizeGib**

Tipo: entero

Descripción: (obligatorio) El tamaño del volumen raíz del Workspace.

- **RunningMode**

Tipo: cadena

Valores válidos: ALWAYS_ON | AUTO_STOP

Descripción: (Obligatorio) El modo de ejecución del Workspace.

- **RunningModeAutoStopTimeoutInMinutes**

Tipo: entero

Descripción: (opcional) El tiempo transcurrido desde que un usuario cierra sesión y se WorkSpaces detiene. Especifique un valor en intervalos de 60 minutos.

- **Tags**

Tipo: cadena

Descripción: (opcional) Etiquetas que desea aplicar a Workspace.

- **UserName**

Tipo: cadena

Descripción: (obligatorio) El nombre de usuario que se va a asociar a Workspace.

- **UserVolumeEncryptionEnabled**

Tipo: Booleano

Valores válidos: true | false

Predeterminado: false

Descripción: (opcional) Determina si el volumen de usuarios del Workspace está cifrado.

- **UserVolumeSizeGib**

Tipo: entero

Descripción: (obligatorio) El tamaño del volumen de usuarios del Workspace.

- VolumeEncryptionKey

Tipo: cadena

Descripción: (opcional) La AWS Key Management Service clave simétrica que desea utilizar para cifrar los datos almacenados en su Workspace

Permisos de IAM necesarios

El parámetro AutomationAssumeRole requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- workspaces:CreateWorkspaces
- workspaces:DescribeWorkspaces

Pasos de documentos

- aws:executeScript- Crea una Workspace basada en los valores que especifique para los parámetros de entrada.
- aws:waitForAwsResourceProperty- Verifica el estado del Workspace esAVAILABLE.

Salidas

CreateWorkspace.WorkspaceId

AWSSupport-RecoverWorkspace

Descripción

El AWSSupport-RecoverWorkspace runbook lleva a cabo los pasos de recuperación en el escritorio WorkSpaces virtual de Amazon, conocido como a Workspace, que usted especifique. El runbook lo reinicia y Workspace, si el estado se mantieneUNHEALTHY, lo restaura o reconstruye en Workspace función de los valores que especifique para los parámetros de entrada. Antes de utilizar este manual, te recomendamos que consultes la sección [Solución de WorkSpaces problemas](#) en la Guía de WorkSpaces administración de Amazon.

⚠ Important

Restaurar o reconstruir un WorkSpace es una acción potencialmente destructiva que puede provocar la pérdida de datos. Esto se debe a que WorkSpace se restaura a partir de la última instantánea disponible y los datos recuperados de las instantáneas pueden tener una antigüedad de hasta 12 horas.

La opción de restauración recrea tanto el volumen raíz como el volumen de usuarios en función de las instantáneas más recientes. La opción de reconstrucción recrea el volumen de usuario a partir de la instantánea más reciente y recrea el volumen de usuario a WorkSpace a partir de la imagen asociada al paquete desde el que WorkSpace se creó. Se pierden las aplicaciones que se instalaron o la configuración del sistema que se modificó después de WorkSpace su creación. Para obtener más información sobre la restauración y la reconstrucción WorkSpaces, consulte [Restore a Workspace](#) and [Rebuild a Workspace](#) en la Amazon WorkSpaces Administration Guide.

Ejecuta esta automatización (consola)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (opcional) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre. Si no se especifica ningún rol, Systems Manager Automation utiliza los permisos del usuario que comienza este manual de procedimientos.

- Acknowledge

Tipo: cadena

Valores válidos: Yes

Descripción: (Obligatorio) Si introduce sí, entiende que las acciones de restauración y reconstrucción intentarán recuperar la WorkSpace instantánea más reciente y que los datos restaurados a partir de estas instantáneas pueden tener una antigüedad de hasta 12 horas.

- Reboot

Tipo: cadena

Valores válidos: Yes | No

Valor predeterminado: Yes

Descripción: (Obligatorio) Determina si WorkSpace se reinicia.

- Reconstruir

Tipo: cadena

Valores válidos: Yes | No

Valor predeterminado: No

Descripción: (Obligatoria) Determina si WorkSpace se reconstruye.

- Restore

Tipo: cadena

Valores válidos: Yes | No

Valor predeterminado: No

Descripción: (Obligatoria) Determina si WorkSpace se restaura.

- Workspaceld

Tipo: cadena

Descripción: (Obligatorio) El identificador del WorkSpace objeto que desea recuperar.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

Pasos de documentos

- `aws:executeAwsApi`- Recopila el estado del `WorkSpace` que especifique en el `WorkspaceId` parámetro.
- `aws:assertAwsResourceProperty`- Verifica el estado de `WorkSpace` `isAVAILABLE`, `ERRORIMPAIREDSTOPPED`, o `UNHEALTHY`
- `aws:branch`- Sucursales en función del estado del `WorkSpace`.
- `aws:executeAwsApi`- Inicia el `WorkSpace`.
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Action`.
- `aws:waitForAwsResourceProperty`- Espera el `WorkSpace` estado una vez iniciado.
- `aws:waitForAwsResourceProperty`- Espera a que el `WorkSpace` estado cambie a `AVAILABLE`, `ERRORIMPAIRED`, o `UNHEALTHY` después de su inicio.
- `aws:executeAwsApi`- Recopila el estado de una `WorkSpace` vez iniciado.
- `aws:branch`- Las ramas se basan en el estado en el que se encuentran `WorkSpace` después de su puesta en marcha.
- `aws:executeAwsApi`- Reúne las instantáneas disponibles para restaurarlas o reconstruirlas. `WorkSpace`
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Reboot`.
- `aws:executeAwsApi`- Reinicia el `WorkSpace`

- `aws:executeAwsApi`- Recopila el estado de una `WorkSpace` vez iniciado.
- `aws:waitForAwsResourceProperty`- Espera a que cambie el `WorkSpace` estado de. `REBOOTING`
- `aws:waitForAwsResourceProperty`- Espera a que el `WorkSpace` estado cambie a `AVAILABLE` o `UNHEALTHY` después `ERROR` de reiniciarse.
- `aws:executeAwsApi`- Recopila el estado de después de reiniciarse. `WorkSpace`
- `aws:branch`- Las ramas se basan en el estado en el que se encuentren tras el reinicio `WorkSpace` .
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Restore`.
- `aws:executeAwsApi`- Restaura el. `WorkSpace` Si se produce un error en la restauración, el `runbook` intentará reconstruirlo. `WorkSpace`
- `aws:waitForAwsResourceProperty`- Espera a que cambie el `WorkSpace` estado de. `RESTORING`
- `aws:waitForAwsResourceProperty`- Espera a que el `WorkSpace` estado cambie a `AVAILABLEERROR`, o `UNHEALTHY` después de ser restaurado.
- `aws:executeAwsApi`- Recopila el estado del `WorkSpace` tras su restauración.
- `aws:branch`- Las ramas se basan en el estado de la restauración `WorkSpace` posterior.
- `aws:branch`: se ramifica en función del valor que especifique para el parámetro `Rebuild`.
- `aws:executeAwsApi`- Reconstruye el `WorkSpace`.
- `aws:waitForAwsResourceProperty`- Espera a que cambie el `WorkSpace` estado de. `REBUILDING`
- `aws:waitForAwsResourceProperty`- Espera a que el `WorkSpace` estado cambie a o `UNHEALTHY` después `AVAILABLE` de `ERROR` ser reconstruido.
- `aws:executeAwsApi`- Recopila el estado del `WorkSpace` tras su reconstrucción.
- `aws:assertAwsResourceProperty`- Confirma el estado del sistema `WorkSpace` . `AVAILABLE`

X-Ray

AWS Systems Manager La automatización proporciona manuales de ejecución predefinidos para. AWS X-Ray Para obtener información acerca de los manuales de procedimientos, consulte [Trabajar con manuales de procedimientos](#). Para obtener información acerca de cómo ver el contenido del manual de procedimientos, consulte [Cómo ver contenido del manual de procedimientos](#).

Temas

- [AWSConfigRemediation-UpdateXRayKMSKey](#)

AWSConfigRemediation-UpdateXRayKMSKey

Descripción

El AWSConfigRemediation-UpdateXRayKMSKey manual permite el cifrado de sus AWS X-Ray datos mediante una clave AWS Key Management Service (AWS KMS). Este manual solo debe usarse como referencia para garantizar que sus AWS X-Ray datos estén cifrados de acuerdo con las mejores prácticas de seguridad mínimas recomendadas. Recomendamos cifrar varios conjuntos de datos con diferentes claves de KMS.

[Ejecuta esta automatización \(consola\)](#)

Tipo de documento

Automatización

Propietario

Amazon

Plataformas

Linux, macOS, Windows

Parámetros

- AutomationAssumeRole

Tipo: cadena

Descripción: (obligatorio) el Nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que permite a Systems Manager Automation realizar las acciones en su nombre.

- KeyId

Tipo: cadena

Descripción: (obligatorio) El nombre del recurso de Amazon (ARN), el ID de clave o el alias de clave de la clave de KMS que desea utilizar AWS X-Ray para cifrar los datos.

Permisos de IAM necesarios

El parámetro `AutomationAssumeRole` requiere las siguientes acciones para utilizar el manual de procedimientos correctamente.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

Pasos de documentos

- `aws:executeAwsApi`: permite el cifrado de sus datos X-Ray mediante la clave de KMS que especifique en el parámetro `KeyId`.
- `aws:waitForAwsResourceProperty`: espera a que el estado de la configuración de cifrado de su X-Ray sea `ACTIVE`.
- `aws:executeAwsApi`: recopila el ARN de la clave que especifique en el parámetro `KeyId`.
- `aws:assertAwsResourceProperty`: verifica que el cifrado esté habilitado en su X-Ray.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.