Guia do usuário

AWS Systems Manager Referência do runbook de automação

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

AWS Systems Manager Referência do runbook de automação: Guia do usuário

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

Referência do runbook do Automation 1
Exibir conteúdo do runbook 3
API Gateway 4
AWSConfigRemediation-DeleteAPIGatewayStage 4
AWSConfigRemediation-EnableAPIGatewayTracing 6
AWSConfigRemediation-UpdateAPIGatewayMethodCaching 7
AWS Batch 8
AWSSupport-TroubleshootAWSBatchJob 9
AWS CloudFormation 14
AWS-DeleteCloudFormationStack 15
AWS-EnableCloudFormationSNSNotification 16
AWS-RunCfnLint 18
AWSSupport-TroubleshootCFNCustomResource 20
AWS-UpdateCloudFormationStack 22
CloudFront 23
AWSConfigRemediation-EnableCloudFrontDefaultRootObject 23
AWSConfigRemediation-EnableCloudFrontAccessLogs 25
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity 27
AWSConfigRemediation-EnableCloudFrontOriginFailover 29
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS 30
CloudTrail 32
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail 32
AWS-EnableCloudTrail 34
AWS-EnableCloudTrailCloudWatchLogs 35
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS 37
AWS-EnableCloudTrailKmsEncryption 38
AWSConfigRemediation-EnableCloudTrailLogFileValidation 40
AWS-EnableCloudTrailLogFileValidation 41
AWS-QueryCloudTrailLogs 42
CloudWatch 45
AWS-ConfigureCloudWatchOnEC2Instance 45
AWS-EnableCWAlarm 46
AWSSupport-TroubleshootCloudWatchAlarm 49
Amazon DocumentDB 56

AWS-EnableDocDbClusterBackupRetentionPeriod 56
CodeBuild 59
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK 59
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject 61
AWS CodeDeploy 62
AWSSupport-TroubleshootCodeDeploy 62
AWS Config 64
AWSSupport-SetupConfig 65
Amazon Connect 67
AWSSupport-AssociatePhoneNumbersToConnectContactFlows 68
AWSSupport-CollectAmazonConnectContactFlowLog 76
AWS Directory Service 81
AWS-CreateDSManagementInstance 82
AWSSupport-TroubleshootADConnectorConnectivity 86
AWSSupport-TroubleshootDirectoryTrust 90
AWS AppSync 93
AWS-EnableAppSyncGraphQLApiLogging 94
Amazon Athena 96
AWS-EnableAthenaWorkGroupEncryptionAtRest 96
DynamoDB 99
AWS-ChangeDDBRWCapacityMode 99
AWS-CreateDynamoDBBackup 101
AWS-DeleteDynamoDbBackup 102
AWSConfigRemediation-DeleteDynamoDbTable 103
AWS-DeleteDynamoDbTableBackups 104
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable 106
AWSConfigRemediation-EnablePITRForDynamoDbTable 107
AWS-EnableDynamoDbAutoscaling 109
AWS-RestoreDynamoDBTable 112
AWS Database Migration Service 115
AWSSupport-TroubleshootDMSTableErrors 115
Amazon EBS 121
AWSSupport-AnalyzeEBSResourceUsage 121
AWS-ArchiveEBSSnapshots 128
AWS-AttachEBSVolume 130
AWSSupport-CalculateEBSPerformanceMetrics 131

AWS-CopySnapshot 138
AWS-CreateSnapshot 139
AWS-DeleteSnapshot 140
AWSConfigRemediation-DeleteUnusedEBSVolume 141
AWS-DeregisterAMIs 143
AWS-DetachEBSVolume 144
AWSConfigRemediation-EnableEbsEncryptionByDefault 145
AWS-ExtendEbsVolume 147
AWSSupport-ModifyEBSSnapshotPermission 149
AWSConfigRemediation-ModifyEBSVolumeType 151
Amazon EC2 153
AWS-ASGEnterStandby 155
AWS-ASGExitStandby 156
AWS-CreateImage 157
AWS-DeleteImage 158
AWS-PatchAsgInstance 160
AWS-PatchInstanceWithRollback 162
AWS-QuarantineEC2Instance 165
AWS-ResizeInstance 167
AWS-RestartEC2Instance 168
AWS-SetupJupyter 169
AWS-StartEC2Instance 172
AWS-StopEC2Instance 173
AWS-TerminateEC2Instance 174
AWS-UpdateLinuxAmi 175
AWS-UpdateWindowsAmi 177
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck 181
AWSConfigRemediation-EnforceEC2InstanceIMDSv2 183
AWSEC2-CloneInstanceAndUpgradeSQLServer 185
AWSEC2-CloneInstanceAndUpgradeWindows 188
AWSEC2-ConfigureSTIG 192
AWSEC2-PatchLoadBalancerInstance 229
AWSEC2-SQLServerDBRestore 230
AWSSupport-ActivateWindowsWithAmazonLicense 236
AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 239
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD 244

AWSSupport-CheckXenToNitroMigrationRequirements 250
AWSSupport-ConfigureEC2Metadata 253
AWSSupport-ContainEC2Instance 256
AWSSupport-CopyEC2Instance 267
AWSSupport-EnableWindowsEC2SerialConsole 273
AWSSupport-ExecuteEC2Rescue 281
AWSSupport-ListEC2Resources 284
AWSSupport-ManageRDPSettings 287
AWSSupport-ManageWindowsService 289
AWSSupport-MigrateEC2ClassicToVPC 291
AWSSupport-MigrateXenToNitroLinux 298
AWSSupport-ResetAccess 310
AWSSupport-ResetLinuxUserPassword 312
AWSPremiumSupport-ResizeNitroInstance 319
AWSSupport-RestoreEC2InstanceFromSnapshot 326
AWSSupport-SendLogBundleToS3Bucket 331
AWSSupport-StartEC2RescueWorkflow 333
AWSPremiumSupport-TroubleshootEC2DiskUsage 343
AWSSupport-TroubleshootEC2InstanceConnect 348
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs 354
AWSSupport-TroubleshootRDP 357
AWSSupport-TroubleshootSSH 363
AWSSupport-TroubleshootSUSERegistration 367
AWSSupport-TroubleshootWindowsPerformance 369
AWSSupport-TroubleshootWindowsUpdate 376
AWSSupport-UpgradeWindowsAWSDrivers 383
Amazon ECS 387
AWSSupport-CollectECSInstanceLogs 388
AWS-InstallAmazonECSAgent 390
AWS-ECSRunTask 392
AWSSupport-TroubleshootECSContainerInstance 396
AWSSupport-TroubleshootECSTaskFailedToStart 398
AWS-UpdateAmazonECSAgent 402
Amazon EFS 404
AWSSupport-CheckAndMountEFS 404
Amazon EKS 407

AWSSupport-CollectEKSInstanceLogs 408
AWS-CreateEKSClusterWithFargateProfile 410
AWS-CreateEKSClusterWithNodegroup 414
AWS-DeleteEKSCluster 417
AWS-MigrateToNewEKSSelfManagedNodeGroup 420
AWSPremiumSupport-TroubleshootEKSCluster 426
AWSSupport-TroubleshootEKSWorkerNode 430
AWS-UpdateEKSCluster 433
AWS-UpdateEKSManagedNodeGroup 434
AWS-UpdateEKSSelfManagedLinuxNodeGroups 438
AWSSupport-SetupK8sApiProxyForEKS 442
AWSSupport-TroubleshootEbsCsiDriversForEks 453
Elastic Beanstalk 462
AWSSupport-CollectElasticBeanstalkLogs 462
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming .. 466
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications 467
AWSSupport-TroubleshootElasticBeanstalk 469
Elastic Load Balancing 472
AWSConfigRemediation-DropInvalidHeadersForALB 472
AWS-EnableCLBAccessLogs 473
AWS-EnableCLBConnectionDraining 475
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing 477
AWSConfigRemediation-EnableELBDeletionProtection 478
AWSConfigRemediation-EnableLoggingForALBAndCLB 480
AWSSupport-TroubleshootCLBConnectivity 481
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing 485
AWS-UpdateALBDesyncMitigationMode 486
AWS-UpdateCLBDesyncMitigationMode 488
Amazon EMR 490
AWSSupport-AnalyzeEMRLogs 490
AWSSupport-DiagnoseEMRLogsWithAthena 496
OpenSearch Serviço Amazon 505
AWSConfigRemediation-DeleteOpenSearchDomain 505
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain 507
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups 508
AWSSupport-TroubleshootOpenSearchRedYellowCluster 510

AWSSupport-TroubleshootOpenSearchHighCPU 516
EventBridge 522
AWS-AddOpsItemDedupStringToEventBridgeRule 522
AWS-DisableEventBridgeRule 523
AWS Glue 525
AWSSupport-TroubleshootGlueConnection 525
Amazon FSx 536
AWSSupport-ValidateFSxWindowsADConfig 537
GuardDuty 551
AWSConfigRemediation-CreateGuardDutyDetector 551
IAM 552
AWSSupport-TroubleshootIAMAccessDeniedEvents 553
AWS-AttachIAMToInstance 559
AWS-DeleteIAMInlinePolicy 562
AWSConfigRemediation-DeleteIAMRole 563
AWSConfigRemediation-DeleteIAMUser 565
AWSConfigRemediation-DeleteUnusedIAMGroup 567
AWSConfigRemediation-DeleteUnusedIAMPolicy 568
AWSConfigRemediation-DetachIAMPolicy 570
AWSConfigRemediation-EnableAccountAccessAnalyzer 571
AWSSupport-GrantPermissionsToIAMUser 573
AWSConfigRemediation-RemoveUserPolicies 578
AWSConfigRemediation-ReplaceIAMInlinePolicy 579
AWSConfigRemediation-RevokeUnusedIAMUserCredentials 581
AWSConfigRemediation-SetIAMPasswordPolicy 583
AWSSupport-ContainIAMPrincipal 586
Amazon Kinesis Data Streams 601
AWS-EnableKinesisStreamEncryption 601
AWS KMS 603
AWSConfigRemediation-CancelKeyDeletion 603
AWSConfigRemediation-EnableKeyRotation 604
Lambda 606
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing 606
AWSConfigRemediation-DeleteLambdaFunction 607
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK 609
AWSConfigRemediation-MoveLambdaToVPC 611

AWSSupport-RemediateLambdaS3Event ... 612
AWSSupport-TroubleshootLambdaInternetAccess ... 615
AWSSupport-TroubleshootLambdaS3Event ... 619
Amazon Managed Workflows for Apache Airflow ... 621
AWSSupport-TroubleshootMWAAEnvironmentCreation ... 621
Neptune ... 627
AWS-EnableNeptuneDbAuditLogsToCloudWatch ... 627
AWS-EnableNeptuneDbBackupRetentionPeriod ... 629
AWS-EnableNeptuneClusterDeletionProtection ... 631
Amazon RDS ... 632
AWS-CreateEncryptedRdsSnapshot ... 633
AWS-CreateRdsSnapshot ... 636
AWSConfigRemediation-DeleteRDSCluster ... 637
AWSConfigRemediation-DeleteRDSClusterSnapshot ... 639
AWSConfigRemediation-DeleteRDSInstance ... 640
AWSConfigRemediation-DeleteRDSInstanceSnapshot ... 642
AWSConfigRemediation-DisablePublicAccessToRDSInstance ... 643
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster ... 645
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance ... 647
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance ... 648
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS ... 650
AWSConfigRemediation-EnableMultiAZOnRDSInstance ... 652
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance ... 654
AWSConfigRemediation-EnableRDSClusterDeletionProtection ... 656
AWSConfigRemediation-EnableRDSInstanceBackup ... 657
AWSConfigRemediation-EnableRDSInstanceDeletionProtection ... 659
AWSConfigRemediation-ModifyRDSInstancePortNumber ... 661
AWSSupport-ModifyRDSSnapshotPermission ... 663
AWSPremiumSupport-PostgreSQLWorkloadReview ... 665
AWS-RebootRdsInstance ... 681
AWSSupport-ShareRDSSnapshot ... 683
AWS-StartRdsInstance ... 687
AWS-StartStopAuroraCluster ... 688
AWS-StopRdsInstance ... 689
AWSSupport-TroubleshootConnectivityToRDS ... 690
AWSSupport-TroubleshootRDSIAMAuthentication ... 693

AWSSupport-ValidateRdsNetworkConfiguration 701
Amazon Redshift 706
AWSConfigRemediation-DeleteRedshiftCluster 706
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster 708
AWSConfigRemediation-EnableRedshiftClusterAuditLogging 709
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot 711
AWSConfigRemediation-EnableRedshiftClusterEncryption 712
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting 714
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster 715
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings 717
AWSConfigRemediation-ModifyRedshiftClusterNodeType 719
Amazon S3 721
AWS-ArchiveS3BucketToIntelligentTiering 721
AWS-ConfigureS3BucketLogging 724
AWS-ConfigureS3BucketVersioning 726
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock 727
AWSConfigRemediation-ConfigureS3PublicAccessBlock 729
AWS-CreateS3PolicyToExpireMultipartUploads 731
AWS-DisableS3BucketPublicReadWrite 733
AWS-EnableS3BucketEncryption 734
AWS-EnableS3BucketKeys 735
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy 737
AWSConfigRemediation-RestrictBucketSSLRequestsOnly 739
AWSSupport-TroubleshootS3PublicRead 740
AWSSupport-EmptyS3Bucket 746
AWSSupport-TroubleshootS3EventNotifications 753
AWSSupport-ContainS3Resource 760
Amazon SES 769
AWSSupport-AnalyzeSESMessageSendingStatus 769
SageMaker IA 773
AWS-DisableSageMakerNotebookRootAccess 773
Secrets Manager 776
AWSConfigRemediation-DeleteSecret 776
AWSConfigRemediation-RotateSecret 777
Security Hub 779
AWSConfigRemediation-EnableSecurityHub 779

AWS Shield 781
AWSPremiumSupport-DDoSResiliencyAssessment 781
Amazon SNS 790
AWS-EnableSNSTopicDeliveryStatusLogging 790
AWSConfigRemediation-EncryptSNSTopic 793
AWS-PublishSNSNotification 794
Amazon SQS 795
AWS-EnableSQSEncryption 796
Step Functions 798
AWS-EnableStepFunctionsStateMachineLogging 798
Systems Manager 800
AWS-BulkDeleteAssociation 801
AWS-BulkEditOpsItems 802
AWS-BulkResolveOpsItems 805
AWS-ConfigureMaintenanceWindows 808
AWS-CreateManagedLinuxInstance 809
AWS-CreateManagedWindowsInstance 812
AWSConfigRemediation-EnableCWLoggingForSessionManager 814
AWS-ExportOpsDataToS3 816
AWS-ExportPatchReportToS3 818
AWS-SetupInventory 819
AWS-SetupManagedInstance 824
AWS-SetupManagedRoleOnEC2Instance 825
AWSSupport-TroubleshootManagedInstance 826
AWSSupport-TroubleshootPatchManagerLinux 829
AWSSupport-TroubleshootSessionManager 832
Terceiros 838
AWS-CreateJiraIssue 838
AWS-CreateServiceNowIncident 840
AWS-RunPacker 842
Amazon VPC 844
AWS-CloseSecurityGroup 845
AWSSupport-ConfigureDNSQueryLogging 847
AWSSupport-ConfigureTrafficMirroring 850
AWSSupport-ConnectivityTroubleshooter 852
AWSSupport-TroubleshootVPN 856

AWSConfigRemediation-DeleteEgressOnlyInternetGateway 862
AWSConfigRemediation-DeleteUnusedENI 864
AWSConfigRemediation-DeleteUnusedSecurityGroup 865
AWSConfigRemediation-DeleteUnusedVPCNetworkACL 866
AWSConfigRemediation-DeleteVPCFlowLog 868
AWSConfigRemediation-DetachAndDeleteInternetGateway 869
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway 871
AWS-DisableIncomingSSHOnPort22 872
AWS-DisablePublicAccessForSecurityGroup 874
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP 875
AWSSupport-EnableVPCFlowLogs 877
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch 883
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket 885
AWS-ReleaseElasticIP 887
AWS-RemoveNetworkACLUnrestrictedSSHRDP 888
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules 890
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules 891
AWSSupport-SetupIPMonitoringFromVPC 892
AWSSupport-TerminateIPMonitoringFromVPC 906
AWS WAF 909
AWS-AddWAFRegionalRuleToRuleGroup 909
AWS-AddWAFRegionalRuleToWebAcl 912
AWSConfigRemediation-EnableWAFClassicLogging 914
AWSConfigRemediation-EnableWAFClassicRegionalLogging 916
AWSConfigRemediation-EnableWAFV2Logging 917
Amazon WorkSpaces 919
AWS-CreateWorkSpace 919
AWSSupport-RecoverWorkSpace 922
X-Ray 926
AWSConfigRemediation-UpdateXRayKMSKey 927
..... cmxxix

Referência do runbook do Systems Manager Automation

Para ajudar você a começar rapidamente, AWS Systems Manager fornece runbooks predefinidos. Esses runbooks são mantidos pela Amazon Web Services AWS Support, e. AWS Config A referência do runbook descreve cada um dos runbooks predefinidos fornecidos pelo Systems Manager, e. Suporte AWS Config

> **Important**
>
> Se você executar um fluxo de trabalho de automação que invoca outros serviços usando um perfil AWS Identity and Access Management de serviço (IAM), esteja ciente de que esta função deve ser configurada com permissão para invocar esses serviços. Esse requisito aplica-se a todos os runbooks do Automation da AWS (runbooks da `AWS-*`), como os runbooks `AWS-ConfigureS3BucketLogging`, `AWS-CreateDynamoDBBackup` e `AWS-RestartEC2Instance`, entre outros. Esse requisito também se aplica a todos os runbooks de automação personalizados que você criar e que invocam outros AWS serviços usando ações que chamam outros serviços. Por exemplo, se você usar as ações `aws:executeAwsApi`, `aws:createStack` ou `aws:copyImage`, então você deve configurar um perfil de serviço com permissão para invocar esses serviços. Você pode habilitar permissões para outros AWS serviços adicionando uma política embutida do IAM à função. Para obter mais informações, consulte Adicionar uma política embutida de automação para invocar outros AWS serviços.

Essa referência inclui tópicos que descrevem cada um dos runbooks do Systems Manager que são de propriedade de AWS AWS Support, e. AWS Config Os runbooks são organizados por pessoas relevantes AWS service (Serviço da AWS). Cada página fornece uma explicação dos parâmetros obrigatórios e opcionais que você pode especificar ao usar o runbook. Cada página também lista as etapas no runbook e a saída da execução, se houver.

Essa referência não inclui uma página separada para runbooks que exigem aprovação, como o runbook `AWS-CreateManagedLinuxInstanceWithApproval` ou `AWS-StopEC2InstanceWithApproval`. Qualquer nome do runbook que inclua `WithApproval`, significa que o runbook inclui a ação `aws:approve`. Essa ação pausa temporariamente uma automação até que as entidades principais designadas aprovem ou rejeitem a ação. Depois que o número necessário de aprovações for atingido, a execução da automação será retomada.

Para obter informações sobre como executar automações, consulte Como executar uma automação simples. Para obter informações sobre a execução de automações em vários destinos, consulte Execução de automações que usam destinos e controles de taxa.

Tópicos

- Exibir conteúdo do runbook
- API Gateway
- AWS Batch
- AWS CloudFormation
- CloudFront
- CloudTrail
- CloudWatch
- Amazon DocumentDB
- CodeBuild
- AWS CodeDeploy
- AWS Config
- Amazon Connect
- AWS Directory Service
- AWS AppSync
- Amazon Athena
- DynamoDB
- AWS Database Migration Service
- Amazon EBS
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Elastic Beanstalk
- Elastic Load Balancing
- Amazon EMR
- OpenSearch Serviço Amazon

- EventBridge
- AWS Glue
- Amazon FSx
- GuardDuty
- IAM
- Amazon Kinesis Data Streams
- AWS KMS
- Lambda
- Amazon Managed Workflows for Apache Airflow
- Neptune
- Amazon RDS
- Amazon Redshift
- Amazon S3
- Amazon SES
- SageMaker IA
- Secrets Manager
- Security Hub
- AWS Shield
- Amazon SNS
- Amazon SQS
- Step Functions
- Systems Manager
- Terceiros
- Amazon VPC
- AWS WAF
- Amazon WorkSpaces
- X-Ray

Exibir conteúdo do runbook

Você pode visualizar o conteúdo dos runbooks no console do Systems Manager.

Para ver o conteúdo do runbook

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, escolha Documents.

   - ou -

   Se a página AWS Systems Manager inicial abrir primeiro, escolha o ícone do menu (☰) para abrir o painel de navegação e, em seguida, escolha Documentos no painel de navegação.
3. Na seção Categorias, escolha Documentos de Automação.
4. Selecione um runbook e, em seguida, selecione Visualizar detalhes.
5. Escolha a guia Conteúdo.

API Gateway

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon API Gateway. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-DeleteAPIGatewayStage
- AWSConfigRemediation-EnableAPIGatewayTracing
- AWSConfigRemediation-UpdateAPIGatewayMethodCaching

`AWSConfigRemediation-DeleteAPIGatewayStage`

Descrição

O `AWSConfigRemediation-DeleteAPIGatewayStage` runbook exclui um estágio do Amazon API Gateway (API Gateway). AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- StageArn

  Tipo: string

  Descrição: (obrigatório) o nome do recurso da Amazon (ARN) do estágio do API Gateway que você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: exclui o estágio do API Gateway especificado no parâmetro `StageArn`.

AWSConfigRemediation-EnableAPIGatewayTracing

Descrição

O `AWSConfigRemediation-EnableAPIGatewayTracing` runbook permite o rastreamento em um estágio do Amazon API Gateway (API Gateway). AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- StageArn

  Tipo: string

  Descrição: (obrigatório) o nome do recurso da Amazon (ARN) do estágio do API Gateway no qual você deseja ativar o rastreamento.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`

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

Etapas do documento

- `aws:executeScript`: permite o rastreamento no estágio do API Gateway especificado no parâmetro `StageArn`.

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

Descrição

O runbook `AWSConfigRemediation-UpdateAPIGatewayMethodCaching` atualiza a configuração do método de cache para um recurso de estágio do Amazon API Gateway.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- CachingAuthorizedMethods

Tipo: StringList

Descrição: (obrigatório) os métodos autorizados a ter o armazenamento em cache ativado. A lista deve ser uma combinação de `DELETE` , `GET` , `HEAD` , `OPTIONS` , `PATCH` , `POST` e `PUT` . O armazenamento em cache está ativado para métodos selecionados e desativado para métodos não selecionados. O armazenamento em cache está habilitado para todos os métodos se `ANY` estiver selecionado e desabilitado para todos os métodos se `NONE` estiver selecionado.

- StageArn

  Tipo: string

  Descrição: (obrigatório) o ARN de estágio do API Gateway para a API `REST`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: aceita o ID do recurso do estágio como entrada, atualiza a configuração do método de cache para um estágio do API Gateway usando a ação da API `UpdateStage` e verifica a atualização.

AWS Batch

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Batch Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-TroubleshootAWSBatchJob

AWSSupport-TroubleshootAWSBatchJob

Descrição

O AWSSupport-TroubleshootAWSBatchJob runbook ajuda você a solucionar problemas que impedem que um AWS Batch trabalho passe do status para o status. RUNNABLE STARTING

Como funciona?

Esse runbook executa as seguintes verificações:

- Se o ambiente computacional estiver em um DISABLED estado INVALID ou.
- Se o Max vCPU parâmetro do ambiente computacional for grande o suficiente para acomodar o volume de trabalhos na fila de trabalhos.
- Se os trabalhos exigirem mais recursos de v CPUs ou memória do que os tipos de instância do ambiente computacional podem fornecer.
- Se os trabalhos precisarem ser executados em instâncias baseadas em GPU, mas o ambiente computacional não estiver configurado para usar instâncias baseadas em GPU.
- Se o grupo de Auto Scaling do ambiente computacional falhar ao iniciar as instâncias.
- Se as instâncias lançadas puderem se juntar ao cluster subjacente do Amazon Elastic Container Service (Amazon ECS); caso contrário, ele executará o runbook. AWSSupport-TroubleshootECSContainerInstance
- Se algum problema de permissão estiver bloqueando ações específicas necessárias para executar o trabalho.

Important

- Esse runbook deve ser iniciado na mesma AWS região do seu trabalho que está preso no RUNNABLE status.
- Esse runbook pode ser iniciado para AWS Batch trabalhos agendados em instâncias do Amazon ECS ou do AWS Fargate Amazon Elastic Compute Cloud (Amazon EC2). Se a automação for iniciada para um AWS Batch trabalho no Amazon Elastic Kubernetes Service (Amazon EKS), a iniciação será interrompida.
- Se as instâncias estiverem disponíveis para executar o trabalho, mas não conseguirem registrar o cluster do Amazon ECS, esse runbook iniciará o runbook de AWSSupport-TroubleshootECSContainerInstance automação para

tentar determinar o motivo. Para obter mais informações, consulte o AWSSupport-TroubleshootECSContainerInstancerunbook.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- JobId

  Tipo: string

  Descrição: (Obrigatório) O ID do AWS Batch Job que está preso no `RUNNABLE` status.

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

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

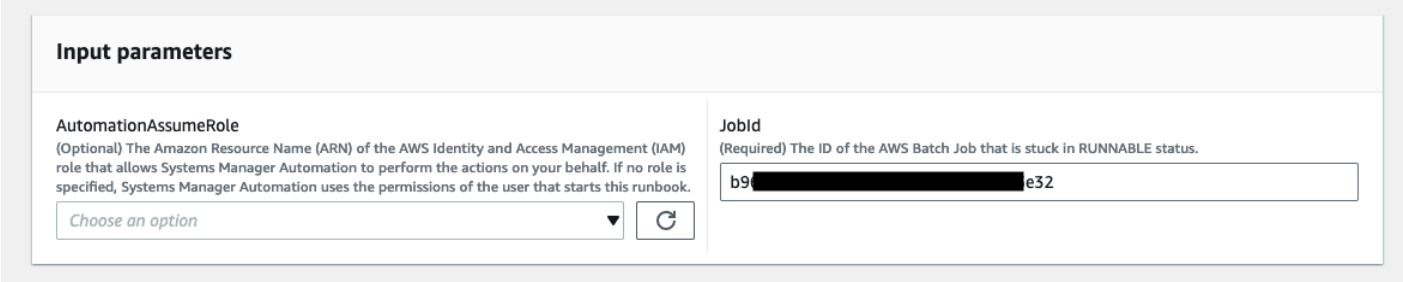
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sts:GetCallerIdentity`

Instruções

1. Navegue até o AWSSupport-TroubleshootAWSBatchJobno AWS Systems Manager console.
2. Selecione Executar automação.
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole(Opcional):

     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - JobId(Obrigatório):

     O ID do AWS Batch Job que está preso no `RUNNABLE` status.



4. Selecione Executar.
5. Observe que a automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - PreflightPermissionChecks:

     Executa verificações prévias de permissão do IAM em relação ao usuário/função inicial. Se houver alguma permissão ausente, essa etapa fornece as ações de API ausentes na seção de saída global.

- ProceedOnlyIfUserHasPermission:

  Ramifica com base em se você tem permissões para todas as ações necessárias para o runbook.

- AWSBatchJobEvaluation:

  Executa verificações em relação ao AWS Batch Job, verificando se ele existe e está no `RUNNABLE` status.

- ProceedOnlyIfBatchJobExistsAndIsinRunnableEstado:

  Ramifica com base na existência e no `RUNNABLE` status dos trabalhos.

- BatchComputeEnvironmentEvaluation:

  Executa verificações em relação ao ambiente AWS Batch de computação.

- ProceedOnlyIfComputeEnvironmentChecksAreOK:

  Ramificações com base no sucesso das verificações do ambiente computacional.

- UnderlyingInfraEvaluation:

  Executa verificações em relação ao Grupo de Auto Scaling ou à Solicitação de Frota Spot subjacente.

- ProceedOnlyIfInstancesNotJoiningEcsCluster:

  Ramificações com base na existência de instâncias que não estão ingressando no cluster do Amazon ECS.

- EcsAutomationRunner:

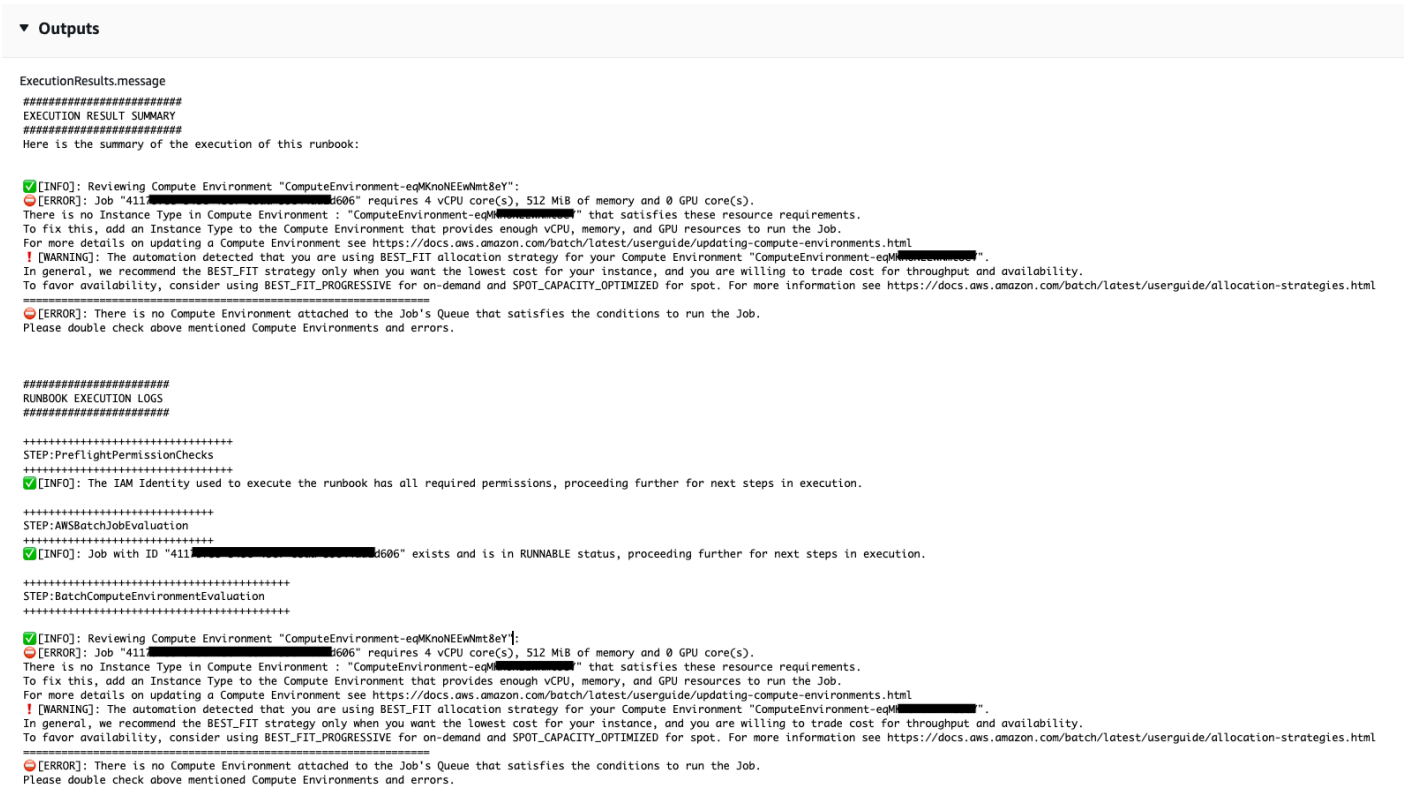
  Executa a automação do Amazon ECS para as instâncias que não se juntam ao cluster.

- ExecutionResults:

  Gera saída com base nas etapas anteriores.

7. Depois de concluído, o URI do arquivo HTML do relatório de avaliação é fornecido:

   Link do console S3 e URI do Amazon S3 para o relatório sobre a execução bem-sucedida do runbook



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS CloudFormation

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS CloudFormation Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-DeleteCloudFormationStack
- AWS-EnableCloudFormationSNSNotification

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

AWS-DeleteCloudFormationStack

Descrição

Exclua uma AWS CloudFormation pilha.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- StackNameOrId

  Tipo: string

  Descrição: (Obrigatório) Nome ou ID exclusivo da CloudFormation pilha a ser excluída

AWS-EnableCloudFormationSNSNotification

Descrição

O AWS-EnableCloudFormationSNSNotification runbook habilita notificações do Amazon Simple Notification Service (Amazon SNS) para a pilha AWS CloudFormation (AWS CloudFormation) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- StackArn

  Tipo: string

  Descrição: (Obrigatório) O ARN ou o nome da AWS CloudFormation pilha para a qual você deseja habilitar as notificações do Amazon SNS.
- NotificationArn

  Tipo: string

Descrição: (Obrigatório) O ARN do tópico do Amazon SNS que você deseja associar à pilha. AWS CloudFormation

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- sms: GetAutomationExecution
- sms: StartAutomationExecution
- formação de nuvens: DescribeStacks
- formação de nuvens: UpdateStack
- kms:Decrypt
- kms:GenerateDataKey
- sns:Publish
- metros quadrados: GetQueueAttributes

Etapas do documento

- CheckCfnSnsLimits (`aws:executeScript`) - Verifica se o número máximo de tópicos do Amazon SNS ainda não foi associado AWS CloudFormation à pilha especificada.
- EnableCfnSnsNotification (`aws:executeAwsApi`) - Ativa notificações do Amazon SNS para a AWS CloudFormation pilha.
- VerificationCfnSnsNotification (`aws:executeScript`) - Verifica se as notificações do Amazon SNS foram habilitadas para AWS CloudFormation a pilha.

Saídas

CheckCfnSnsLimits. NotificationArnList - Uma lista dos ARNs que recebem notificações do Amazon SNS para a AWS CloudFormation pilha.

VerificationCfnSnsNotification. VerifySnsTopicsResponse - Resposta da operação da API confirmando que as notificações do Amazon SNS foram habilitadas para AWS CloudFormation a pilha.

AWS-RunCfnLint

Descrição

Esse runbook usa um AWS CloudFormation Linter (`cfn-python-lint`) para validar os modelos YAML e JSON em relação à especificação do recurso. AWS CloudFormation O runbook do `AWS-RunCfnLint` realiza verificações adicionais, como garantir que valores válidos foram inseridos para as propriedades do recurso. Se a validação não for bem-sucedida, a etapa `RunCfnLintAgainstTemplate` falhará e a saída da ferramenta de linter será fornecida em uma mensagem de erro. Este runbook está usando cfn-lint v0.24.4.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ConfigureRuleFlag

  Tipo: string

  Descrição: (Opcional) opções de configuração para uma regra a ser passado para o parâmetro `--configure-rule`.

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

- FormatFlag

  Tipo: string

  Descrição: (Opcional) valor a ser passado ao parâmetro `--format` para especificar o formato de saída.

  Valores válidos: Default | quiet | parseable | json

  Padrão: Default

- IgnoreChecksFlag

  Tipo: string

  Descrição: (Opcional) IDs das regras a serem passadas para o parâmetro --ignore-checks. Essas regras não são verificadas.

  Exemplo: E1001,E1003,W7001

- IncludeChecksFlag

  Tipo: string

  Descrição: (Opcional) IDs das regras a serem passadas para o `--include-checks` parâmetro. Essas regras são verificadas.

  Exemplo: E1001,E1003,W7001

- InfoFlag

  Tipo: string

  Descrição: (Opcional) opção para o parâmetro `--info`. Inclua a opção para habilitar informações adicionais de registro em log sobre o processamento do modelo.

  Padrão: False

- TemplateFileName

  Tipo: string

  Descrição: o nome ou a chave do arquivo de modelo no bucket do S3.

- Templates3 BucketName

  Tipo: string

  Descrição: o nome do bucket do S3 que contém o modelo do empacotador.
- RegionsFlag

  Tipo: string

  Descrição: (Opcional) Valores a serem passados para o `--regions` parâmetro for para testar o modelo em relação ao especificado Regiões da AWS.

  Exemplo: us-east-1,us-west-1

Etapas do documento

RunCfnLintAgainstTemplate — Executa a `cfn-python-lint` ferramenta em relação ao AWS CloudFormation modelo especificado.

Saídas

RunCfnLintAgainstTemplate.output — O stdout da ferramenta. `cfn-python-lint`

AWSSupport-TroubleshootCFNCustomResource

Descrição

O runbook `AWSSupport-TroubleshootCFNCustomResource` ajuda a diagnosticar por que uma pilha do AWS CloudFormation falhou ao criar, atualizar ou excluir um recurso personalizado. O runbook verifica o token de serviço usado para o recurso personalizado e a mensagem de erro que foi retornada. Depois de analisar os detalhes do recurso personalizado, a saída do runbook fornece uma explicação sobre o comportamento da pilha e as etapas de solução de problemas do recurso personalizado.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- StackName

  Tipo: string

  Descrição: (Obrigatório) O nome da AWS CloudFormation pilha em que o recurso personalizado falhou.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `validateCloudFormationStack`- Verifica se a AWS CloudFormation pilha existe na mesma e. Conta da AWS Região da AWS
- `checkCustomResource`- Analisa a AWS CloudFormation pilha, verifica o recurso personalizado com falha e gera informações sobre como solucionar o problema do recurso personalizado com falha.

AWS-UpdateCloudFormationStack

Descrição

Atualize uma AWS CloudFormation pilha usando um AWS CloudFormation modelo armazenado em um bucket do Amazon S3.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LambdaAssumeRole

Tipo: string

Descrição: (obrigatório) O ARN da função assumida pelo Lambda

- StackNameOrId

  Tipo: string

  Descrição: (Obrigatório) Nome ou ID exclusivo da AWS CloudFormation pilha a ser atualizada

- TemplateUrl

  Tipo: string

  Descrição: (Obrigatório) Local do bucket do S3 que contém o CloudFormation modelo atualizado (por exemplo, `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`)

CloudFront

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. CloudFront Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

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

`AWSConfigRemediation-EnableCloudFrontDefaultRootObject`

Descrição

O `AWSConfigRemediation-EnableCloudFrontDefaultRootObject` runbook configura o objeto raiz padrão para a distribuição Amazon CloudFront (CloudFront) especificada por você.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- CloudFrontDistributionId

  Tipo: string

  Descrição: (Obrigatório) O ID da CloudFront distribuição para a qual você deseja configurar o objeto raiz padrão.
- DefaultRootObject

  Tipo: string

  Descrição: (Obrigatório) O objeto que você deseja CloudFront retornar quando uma solicitação do visualizador aponta para sua URL raiz.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

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

Etapas do documento

- `aws:executeScript`- Configura o objeto raiz padrão para a CloudFront distribuição que você especifica no `CloudFrontDistributionId` parâmetro.

AWSConfigRemediation-EnableCloudFrontAccessLogs

Descrição

O `AWSConfigRemediation-EnableCloudFrontAccessLogs` runbook permite o registro de acesso para a distribuição Amazon CloudFront (CloudFront) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- BucketName

Tipo: string

Descrição: (Obrigatório) O nome do bucket do Amazon Simple Storage Service (Amazon S3) em que você deseja armazenar logs de acesso. Não há suporte para buckets da Região da AWS af-south-1, ap-east-1, eu-south-1 e me-south-1.

- CloudFrontId

  Tipo: string

  Descrição: (Obrigatório) O ID da CloudFront distribuição na qual você deseja ativar o login de acesso.

- IncludeCookies

  Tipo: booliano

  Valores válidos: True | False

  Descrição: (Obrigatório) Defina esse parâmetro como`true`, se quiser que os cookies sejam incluídos nos registros de acesso.

- Prefixo

  Tipo: string

  Descrição: (Opcional) Uma string opcional que você CloudFront deseja prefixar no log `filenames` de acesso da sua distribuição, por exemplo,my`prefix/`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `s3:PutBucketAcl`

> **Note**
>
> A `s3:GetBucketLocation` API só pode ser usada para buckets do S3 na mesma conta. Você não pode usá-lo para buckets S3 entre contas.

Etapas do documento

- `aws:executeScript`- Ativa o registro de acesso para a CloudFront distribuição que você especifica no `CloudFrontDistributionId` parâmetro.

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

Descrição

O `AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity` runbook habilita a identidade de acesso de origem para a distribuição Amazon CloudFront (CloudFront) que você especificar. Essa automação atribui a mesma identidade de acesso de CloudFront origem para todas as origens do tipo de origem do Amazon Simple Storage Service (Amazon S3) sem identidade de acesso de origem para a distribuição que você especificar. CloudFront Essa automação não concede permissão de leitura à identidade de acesso de origem CloudFront para acessar objetos em seu bucket do Amazon S3. Você deve atualizar suas permissões de bucket do Amazon S3 para permitir o acesso.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- CloudFrontDistributionId

  Tipo: string

  Descrição: (Obrigatório) O ID da CloudFront distribuição na qual você deseja ativar o failover de origem.

- OriginAccessIdentityId

  Tipo: string

  Descrição: (Obrigatório) O ID da identidade de acesso de CloudFront origem a ser associada à origem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Ativa a identidade de acesso de origem para a CloudFront distribuição especificada no `CloudFrontDistributionId` parâmetro e verifica se a identidade de acesso de origem foi atribuída.

AWSConfigRemediation-EnableCloudFrontOriginFailover

Descrição

O AWSConfigRemediation-EnableCloudFrontOriginFailover runbook permite o failover de origem para a distribuição Amazon CloudFront (CloudFront) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- CloudFrontDistributionId

  Tipo: string

  Descrição: (Obrigatório) O ID da CloudFront distribuição na qual você deseja ativar o failover de origem.
- OriginGroupId

  Tipo: string

  Descrição: (obrigatório) o ID do grupo de origem.
- PrimaryOriginId

Tipo: string

Descrição: (obrigatório) o ID da origem primária no grupo de origem.

- SecondaryOriginId

  Tipo: string

  Descrição: (obrigatório) o ID da origem secundária no grupo de origem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Ativa o failover de origem para a CloudFront distribuição especificada no `CloudFrontDistributionId` parâmetro e verifica se o failover foi ativado.

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

Descrição

O `AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS` runbook ativa a política de protocolo do visualizador para a distribuição Amazon CloudFront (CloudFront) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- CloudFrontDistributionId

  Tipo: string

  Descrição: (Obrigatório) O ID da CloudFront distribuição na qual você deseja habilitar a política de protocolo do visualizador.
- ViewerProtocolPolicy

  Tipo: string

  Valores válidos: somente https, redirect-to-https

  Descrição: (obrigatório) o protocolo que os visualizadores podem usar para acessar os arquivos na origem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Ativa a política de protocolo do visualizador para a CloudFront distribuição especificada no `CloudFrontDistributionId` parâmetro e verifica se a política foi atribuída.

CloudTrail

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS CloudTrail Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

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

`AWSConfigRemediation-CreateCloudTrailMultiRegionTrail`

Descrição

O `AWSConfigRemediation-CreateCloudTrailMultiRegionTrail` runbook cria uma trilha AWS CloudTrail (CloudTrail) que entrega arquivos de log de vários Regiões da AWS para o bucket do Amazon Simple Storage Service (Amazon S3) de sua escolha.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- BucketName

  Tipo: string

  Descrição: (obrigatório) o nome do bucket do Amazon S3 no qual você deseja fazer o upload de logs.
- KeyPrefix

  Tipo: string

  Descrição: (opcional) o prefixo da chave do Amazon S3 que é fornecida após o nome do bucket que você designou para a entrega de arquivos de log.
- TrailName

  Tipo: string

  Descrição: (Obrigatório) O nome da CloudTrail trilha a ser criada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `cloudtrail:CreateTrail`
- `cloudtrail:StartLogging`

- `cloudtrail:GetTrail`
- `s3:PutObject`
- `s3:GetBucketAcl`
- `s3:PutBucketLogging`
- `s3:ListBucket`

Etapas do documento

- `aws:executeAwsApi`- Aceita o nome da trilha e o nome do bucket do Amazon S3 como entrada e cria uma CloudTrail trilha.
- `aws:executeAwsApi`: ativa o registro na trilha criada e inicia a entrega do log para o bucket do Amazon S3 que você especificou.
- `aws:assertAwsResourceProperty`- Verifica se a CloudTrail trilha foi criada.

AWS-EnableCloudTrail

Descrição

Crie uma AWS CloudTrail trilha e configure o registro em um bucket do S3.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- S3 BucketName

  Tipo: string

  Descrição: (obrigatória) o nome do bucket do S3 designado para a publicação de arquivos de log.

  > **Note**
  >
  > O bucket do S3 deve existir, e a política do bucket precisa conceder permissão ao CloudTrail para gravar nele. Para obter informações, consulte a Política de bucket do Amazon S3 para. CloudTrail

- TrailName

  Tipo: string

  Descrição: (obrigatório) o nome da nova trilha.

AWS-EnableCloudTrailCloudWatchLogs

Descrição

Esse runbook atualiza a configuração de uma ou mais AWS CloudTrail trilhas para enviar eventos para um grupo de CloudWatch logs do Amazon Logs.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- CloudWatchLogsLogGroupArn

  Tipo: string

  Descrição: (Obrigatório) O ARN do grupo de registros de CloudWatch registros em que os CloudTrail registros serão entregues.
- CloudWatchLogsRoleArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função do IAM CloudWatch Logs Logs presume para gravar no grupo de registros especificado.
- TrailNames

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos nomes das CloudTrail trilhas cujos eventos você deseja enviar para o CloudWatch Logs.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Atualiza as CloudTrail trilhas especificadas para entregar eventos ao grupo de CloudWatch registros de registros especificado.

`AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS`

Descrição

O `AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS` runbook criptografa uma trilha AWS CloudTrail (CloudTrail) usando a chave gerenciada pelo cliente AWS Key Management Service (AWS KMS) que você especifica. Esse runbook só deve ser usado como base para garantir que suas CloudTrail trilhas sejam criptografadas de acordo com as melhores práticas mínimas de segurança recomendadas. Recomendamos criptografar várias trilhas com chaves KMS diferentes. CloudTrail os arquivos de resumo não são criptografados. Se você definiu anteriormente o `EnableLogFileValidation` parâmetro como `true` para a trilha, consulte a seção “Usar criptografia do lado do servidor com chaves AWS KMS gerenciadas” do tópico Práticas recomendadas de segurança CloudTrail preventiva no Guia do AWS CloudTrail usuário para obter mais informações.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- KMSKeyIdentificação

  Tipo: string

  Descrição: (obrigatório) O ARN, o ID da chave ou o alias da chave gerenciada pelo cliente que você deseja usar para criptografar a trilha especificada no parâmetro `TrailName`.

- TrailName

  Tipo: string

  Descrição: (obrigatório) o ARN ou o nome da trilha que você deseja atualizar para ser criptografada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: ativa a criptografia na trilha que você especifica no parâmetro `TrailName`.
- `aws:executeAwsApi`: reúne o ARN da chave gerenciada pelo cliente que você especifica no parâmetro `KMSKeyId`.
- `aws:assertAwsResourceProperty`- Verifica se a criptografia foi ativada na CloudTrail trilha.

AWS-EnableCloudTrailKmsEncryption

Descrição

Este runbook atualiza a configuração de uma ou mais AWS CloudTrail trilhas para usar a criptografia AWS Key Management Service (AWS KMS).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- KMSKeyIdentificação

  Tipo: string

  Descrição: (Obrigatório) O ID da chave gerenciada pelo cliente que você deseja usar para criptografar a trilha especificada no `TrailName` parâmetro. O valor pode ser um nome de alias prefixado por “alias/”, um ARN totalmente especificado para um alias ou um ARN totalmente especificado para uma chave.
- TrailNames

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas das trilhas que você deseja atualizar para serem criptografadas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Ativa a AWS KMS criptografia nas trilhas que você especifica no `TrailName` parâmetro.

AWSConfigRemediation-EnableCloudTrailLogFileValidation

Descrição

O `AWSConfigRemediation-EnableCloudTrailLogFileValidation` runbook permite a validação do arquivo de log para sua AWS CloudTrail trilha.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- TrailName

  Tipo: string

  Descrição: (obrigatório) o nome ou o nome do recurso da Amazon (ARN) da trilha para a qual você deseja ativar a validação do log.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: ativa a validação do log para a trilha do AWS CloudTrail que você especifica no parâmetro `TrailName`.
- `aws:assertAwsResourceProperty`: verifica se a validação do log está ativada para sua trilha.

AWS-EnableCloudTrailLogFileValidation

Descrição

O `AWS-EnableCloudTrailLogFileValidation` runbook permite a validação do arquivo de log para as AWS CloudTrail trilhas que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- TrailNames

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos nomes das CloudTrail trilhas para as quais você deseja habilitar a validação de registros.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Permite a validação do registro para as AWS CloudTrail trilhas que você especifica no `TrailNames` parâmetro.

AWS-QueryCloudTrailLogs

Descrição

O `AWS-QueryCloudTrailLogs` runbook cria uma tabela do Amazon Athena a partir do bucket do Amazon Simple Storage Service (Amazon S3) de sua escolha contendo () logs. AWS CloudTrail

CloudTrail Depois de criar a tabela, a automação executa as consultas SQL que você especifica e, em seguida, exclui a tabela.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Consulta

  Tipo: string

  Descrição: (obrigatório) a consulta SQL que você deseja executar.
- SourceBucketPath

  Tipo: string

  Descrição: (Obrigatório) O nome do bucket do Amazon S3 contendo os arquivos de CloudTrail log que você deseja consultar.
- TableName

  Tipo: string

Descrição: (opcional) o nome da tabela do Athena criada pela automação.

Padrão: cloudtrail_logs

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:executeAwsApi`: cria uma tabela do Athena.
- `aws:executeAwsApi` : executa a sequência de caracteres de consulta que você especifica no parâmetro`Query`.
- `aws:executeScript`: pesquisa e aguarda a conclusão da consulta.
- `aws:executeAwsApi`: obtém os resultados da consulta.

- `aws:executeAwsApi`: exclui a tabela criada pela automação.

CloudWatch

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. CloudWatch Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

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

`AWS-ConfigureCloudWatchOnEC2Instance`

Descrição

Ative ou desative o monitoramento CloudWatch detalhado da Amazon em instâncias gerenciadas.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon na qual você deseja ativar o CloudWatch monitoramento.

- propriedades

  Tipo: string

  Descrição: (opcional) esse parâmetro não é compatível. Ele está listado aqui pela compatibilidade com versões anteriores.

- status

  Valores válidos: Enabled | Disabled

  Descrição: (opcional) Especifica se você deseja habilitar ou desabilitar o CloudWatch.

  Padrão: Habilitado

Etapas do documento

configureCloudWatch - Configura CloudWatch na EC2 instância da Amazon com o status fornecido.

Saídas

Esta automação não tem saída.

AWS-EnableCWAlarm

Descrição

O `AWS-EnableCWAlarm` runbook cria alarmes da Amazon CloudWatch (CloudWatch) para AWS recursos em seu computador Conta da AWS que ainda não têm um. CloudWatch os alarmes são criados para os seguintes AWS recursos:

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

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ComparisonOperator

  Tipo: string

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

  Descrição: (Obrigatório) A operação aritmética a ser usada ao comparar a estatística e o limite especificados.
- MetricName

Tipo: string

Descrição: (Obrigatório) O nome da métrica associada ao alarme.

- Período

  Tipo: inteiro

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

  Descrição: (Obrigatório) O período, em segundos, durante o qual a estatística é aplicada.

- Recurso ARNs

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas ARNs dos recursos para os quais criar um CloudWatch alarme

- Estatística

  Tipo: string

  Valores válidos: Média | Máximo | Mínimo | SampleCount | Soma

  Descrição: (Obrigatório) A estatística da métrica associada ao alarme.

- Limite

  Tipo: inteiro

  Descrição: (Obrigatório) O valor a ser comparado com a estatística especificada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `cloudwatch:PutMetricAlarm`

Etapas do documento

- `aws:executeScript`- Cria um CloudWatch alarme de acordo com os valores especificados nos parâmetros do runbook para os recursos que você especifica no `ResourceARNs` parâmetro.

Saídas

HabilitarCWAlarm. FailedResources: uma lista de mapas de recursos ARNs para os quais um CloudWatch alarme não foi criado e o motivo da falha.

HabilitarCWAlarm. SuccessfulResources: uma lista de recursos ARNs para os quais um CloudWatch alarme foi criado com sucesso.

AWSSupport-TroubleshootCloudWatchAlarm

Descrição

O `AWSSupport-TroubleshootCloudWatchAlarm` runbook ajuda a identificar e solucionar problemas com alarmes Amazon CloudWatch () mal configurados ou problemáticos. CloudWatch Ele aproveita a lógica pública AWS APIs e conhecida de avaliação de alarmes para detectar pontos de dados atrasados ou ausentes nas métricas monitoradas, o que pode levar a ações de alarme perdidas ou atrasadas. Este runbook fornece uma abordagem estruturada para investigar e resolver problemas relacionados ao Amazon CloudWatch (CloudWatch) Alarm.

Como funciona?

O runbook `AWSSupport-TroubleshootCloudWatchAlarm` executa as seguintes etapas:

- Verifica os detalhes do alarme Amazon CloudWatch (CloudWatch) e o valor do `AlarmTriggerTimestamp` parâmetro para verificar se está dentro de 2.592.000 segundos (30 dias).
- Verifica se um alarme é baseado em uma métrica ou matemática métrica ou se é um alarme detector de anomalias.
- Verifica se um alarme está em estado de dados insuficiente.
- Verifica se as métricas usadas no alarme coincidem com o `ListMetrics` valor.
- Verifica se faltavam pontos de dados em uma métrica em um determinado timestamp.
- Obtém o histórico mais recente de um determinado carimbo de data/hora.
- Verifica se um alarme não foi acionado devido a uma métrica atrasada ou perdida.
- Verifica se a (s) ação (ões) ativada (s) de um alarme was/were foi executada.
- Gera um relatório de solução de problemas combinando todos os resultados do diagnóstico.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

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

```
        }
    ]
}
```

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-TroubleshootCloudWatchAlarmem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):
     - Tipo: `String`
     - Descrição: (Opcional) O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - CloudWatchMetricAlarmName (Obrigatório):
     - Tipo: `String`
     - Descrição: (Obrigatório) O nome do alarme métrico Amazon CloudWatch (CloudWatch) para solucionar o problema.
     - Allowed-pattern: `^[a-zA-Z0-9.:;,\\-_&() ]{1,255}$`
   - AlarmTriggerTimestamp (Obrigatório):
     - Tipo: `String`
     - Descrição: (Obrigatório) A data e hora UTC de quando ocorreu o problema do alarme. Essas informações são cruciais para solucionar o problema e entender o contexto em que ele aconteceu. O valor do carimbo de data/hora deve ser um horário nos últimos 30 dias a partir de hoje e no formato. `YYYY-MM-DDTHH:mm:ssZ` Example: `2024-10-29T09:04:00Z`
     - Allowed-pattern: `^(\\d{4})-(\\d{2})-(\\d{2})T(\\d{2}):(\\d{2}):(\\d{2})Z$`
4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - **`VerifyRunbookInputs`**

Verifica os detalhes do alarme Amazon CloudWatch (CloudWatch) e o valor do `AlarmTriggerTimestamp` parâmetro para verificar se está dentro de 2.592.000 segundos (30 dias).

- **`UpdateSSMDocumentInputChecksVariable`**

  Atualiza a variável `SSMDocumentInputChecks` com o valor `SSMDocumentInputChecks` da `VerifyRunbookInputs` etapa.

- **`BranchOnAlarmIsVerified`**

  Ramificações na verificação `AlarmTriggerTimestamp` de entradas do Runbook e. `CloudWatchAlarmName`

- **`CheckMetricAlarmType`**

  Verifica se um alarme é baseado em uma métrica ou matemática métrica ou se é um alarme detector de anomalias.

- **`CheckAlarmInInsufficientDataState`**

  Verifica se um alarme está em estado de dados insuficiente.

- **`UpdateInsufficientDataChecksVariable`**

  Atualiza a variável `InsufficientDataChecks` com o valor `InsufficientDataChecks` da `CheckAlarmInInsufficientDataState` etapa.

- **`BranchOnAlarmHasInsufficientData`**

  Ramifica o `AlarmHasInsufficientData` valor da `CheckAlarmInInsufficientDataState` etapa, a etapa padrão é`CheckMetricMismatch`.

- **`CheckMetricMismatch`**

  Verifica se as métricas usadas no alarme coincidem com o `ListMetrics` valor.

- **`UpdateMetricMismatchChecksVariable`**

  Atualiza a variável `MetricMismatchChecks` com o valor `MetricMismatchChecks` da `CheckMetricMismatch` etapa.

- **`BranchOnMetricsMatched`**

  Ramifica o `MetricsMatched` valor da `CheckMetricMismatch` etapa, a etapa padrão é`CheckMissingDatapoint`.

- **CheckMissingDatapoint**

  Verifica se faltavam pontos de dados em uma métrica em um determinado timestamp.

- **UpdateMetricMissingDatapointsChecksVariable**

  Atualiza a variável `MetricMissingDatapointsChecks` com o valor `MetricMissingDatapointsChecks` da `CheckMissingDatapoint` etapa.

- **BranchOnMetricMissingDatapoint**

  Ramifica o `MetricMissingDatapoint` valor da `CheckMissingDatapoint` etapa, a etapa padrão é`GetAlarmHistoryDetails`.

- **GetAlarmHistoryDetails**

  Obtém o histórico mais recente de um determinado carimbo de data/hora.

- **UpdateAlarmHistoryChecksVariable**

  Atualiza a variável `AlarmHistoryChecks` com o valor `AlarmHistoryChecks` da `GetAlarmHistoryDetails` etapa.

- **BranchOnAlarmHistoryFound**

  Ramifica o `AlarmHistoryFound` valor da `GetAlarmHistoryDetails` etapa, a etapa padrão é`CheckDelayedMetric`.

- **CheckDelayedMetric**

  Verifica se um alarme não foi acionado devido a uma métrica atrasada ou perdida.

- **UpdateDelayedMetricChecksVariable**

  Atualiza a variável `DelayedMetricChecks` com o valor `DelayedMetricChecks` da `CheckDelayedMetric` etapa.

- **BranchOnMetricDelayedAndDatapointsMeetThreshold**

  Ramifica `DatapointsMeetThreshold` os valores `MetricDelayed` e da `CheckDelayedMetric` etapa, a etapa padrão é`GenerateReport`.

- **CheckActionDelivered**

  Verifica se a (s) ação (ões) ativada (s) de um alarme was/were foi executada.

- **UpdateActionDeliveredChecksVariable**

Atualiza a variável `ActionDeliveredChecks` com `ActionDeliveredChecks` a saída da `CheckActionDelivered` etapa.

- **`GenerateReport`**

  Compila a saída das etapas anteriores e gera um relatório.

7. Após a conclusão da execução, revise a seção Saídas para obter os resultados detalhados da execução:
   - GenerateReport.Relatório

     Um relatório do alarme métrico Amazon CloudWatch (CloudWatch) fornecido.

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

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

Amazon DocumentDB

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon DocumentDB (com compatibilidade com o MongoDB). Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableDocDbClusterBackupRetentionPeriod

AWS-EnableDocDbClusterBackupRetentionPeriod

Descrição

O `AWS-EnableDocDbClusterBackupRetentionPeriod` runbook permite um período de retenção de backup para o cluster Amazon DocumentDB que você especificar. Esse recurso define o número total de dias durante os quais um backup automatizado é retido. Para modificar um cluster, o cluster deve estar no estado disponível com um tipo de mecanismo de`docdb`.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DBClusterResourceId

  Tipo: string

  Descrição: (Obrigatório) O ID do recurso para o cluster Amazon DocumentDB para o qual você deseja habilitar o período de retenção de backup.
- BackupRetentionPeriod

  Tipo: inteiro

  Descrição: (Obrigatório) O número de dias durante os quais os backups automatizados são retidos. Deve ser um valor de 7 a 35 dias.

- PreferredBackupWindow

  Tipo: string

  Descrição: (Opcional) Um intervalo de tempo diário em Tempo Universal Coordenado (UTC) no formato hh24:mm-hh24:mm, por exemplo, 07:14-07:44. O valor deve ser de pelo menos 30 minutos e não pode entrar em conflito com a janela de manutenção preferida.

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

Etapas do documento

- GetDocDbClusterIdentifier (`aws:executeAwsApi`) - Retorna o identificador do cluster Amazon DocumentDB usando o ID do recurso fornecido.
- VerifyDocDbEngine (`aws:assertAwsResourceProperty`) - Verifica se o tipo de mecanismo Amazon DocumentDB `docdb` é para evitar alterações inadvertidas em outros tipos de mecanismo do Amazon RDS.
- VerifyDocDbStatus (`aws:waitAwsResourceProperty`) - Verifica se o status do cluster Amazon DocumentDB é. `available`
- ModifyDocDbRetentionPeriod (`aws:executeAwsApi`) - Define o período de retenção usando os valores fornecidos para o cluster Amazon DocumentDB especificado.
- VerifyDocDbBackupsEnabled (`aws:executeScript`) - Verifica se o período de retenção do cluster Amazon DocumentDB e a janela de backup preferencial, se especificada, foram configurados com sucesso.

Saídas

ModifyDocDbRetentionPeriod. ModifyDbClusterResponse - Resposta da operação `ModifyDBCluster` da API.

VerifyDocDbBackupsEnabled. VerifyDbClusterBackupsEnabledResponse - Saída da `VerifyDocDbBackupsEnabled` etapa que confirma a modificação bem-sucedida do cluster Amazon DocumentDB.

CodeBuild

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS CodeBuild Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK
- AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

`AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK`

Descrição

O `AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK` runbook criptografa os artefatos de construção de um projeto AWS CodeBuild (CodeBuild) usando a chave gerenciada pelo cliente AWS Key Management Service (AWS KMS) que você especifica. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- KMSKeyIdentificação

  Tipo: string

  Descrição: (Obrigatório) O nome de recurso da Amazon (ARN) da chave gerenciada pelo AWS KMS cliente que você deseja usar para criptografar o CodeBuild projeto especificado no parâmetro. `ProjectId`

- ProjectId

  Tipo: string

  Descrição: (Obrigatório) O ID do CodeBuild projeto cujos artefatos de construção você deseja criptografar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`- Reúne o nome do CodeBuild projeto a partir do ID do projeto.
- `aws:executeAwsApi`- Ativa a criptografia no CodeBuild projeto que você especifica no `ProjectId` parâmetro.
- `aws:assertAwsResourceProperty`- Verifica se a criptografia foi ativada no CodeBuild projeto.

Saídas

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Resposta da chamada `UpdateFunctionConfiguration` da API.

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

Descrição

O `AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject` runbook exclui as variáveis de `AWS_SECRET_ACCESS_KEY` ambiente `AWS_ACCESS_KEY_ID` e do projeto AWS CodeBuild (CodeBuild) que você especificar. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ResourceId

  Tipo: string

Descrição: (Obrigatório) O ID do CodeBuild projeto cujas variáveis de ambiente da chave de acesso você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Exclui as variáveis de ambiente da chave de acesso para o CodeBuild projeto especificado no `ResourceId` parâmetro.

AWS CodeDeploy

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS CodeDeploy Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-TroubleshootCodeDeploy

`AWSSupport-TroubleshootCodeDeploy`

Descrição

O `AWSSupport-TroubleshootCodeDeploy` runbook ajuda a diagnosticar por que uma AWS CodeDeploy implantação falhou em uma instância do Amazon Elastic Compute Cloud (Amazon EC2). O runbook fornece etapas para ajudar você a resolver o problema ou resolver problemas

adicionais. As melhores práticas para também CodeDeploy são fornecidas para ajudá-lo a evitar problemas semelhantes no futuro.

Este runbook pode ajudá-lo a resolver os seguintes problemas:

- O CodeDeploy agente não está instalado ou não está em execução na EC2 instância da Amazon
- A EC2 instância da Amazon não tem um perfil de instância AWS Identity and Access Management (IAM) anexado
- O perfil da instância do IAM anexado à EC2 instância da Amazon não tem as permissões necessárias do Amazon Simple Storage Service (Amazon S3)
- Uma revisão armazenada no Amazon S3 está ausente ou o bucket do Amazon S3 usado está em Região da AWS uma que é diferente da instância da Amazon EC2
- Problemas com o arquivo de especificação do aplicativo (AppSpec)
- Erros “O arquivo já existe no local”
- Ganchos de eventos de ciclo de vida CodeDeploy gerenciado com falha
- Falha nos hooks de eventos do ciclo de vida gerenciado do cliente
- Eventos de escalonamento durante a implantação

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DeploymentId

  Tipo: string

  Descrição: (obrigatório) o ID da implantação que falhou.

- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon em que a implantação falhou.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: verifica os valores fornecidos para os parâmetros `DeploymentId` e `InstanceId`.
- `aws:executeScript`- Coleta informações da EC2 instância da Amazon, como o estado da instância e detalhes do perfil da instância do IAM.
- `aws:executeScript`: analisa a implantação especificada e retorna uma análise sobre por que a implantação falhou.

AWS Config

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Config Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-SetupConfig

AWSSupport-SetupConfig

Descrição

O AWSSupport-SetupConfig runbook cria uma função vinculada ao serviço AWS Identity and Access Management (IAM), um gravador de configuração alimentado por AWS Config e um canal de entrega com um bucket do Amazon Simple Storage Service (Amazon S3) AWS Config que envia snapshots de configuração e arquivos de histórico de configuração. Se você especificar valores para os AggregatorAccountRegion parâmetros AggregatorAccountId e, o runbook também cria autorizações para agregação de dados para coletar dados de AWS Config configuração e conformidade de vários e vários Contas da AWS . Regiões da AWS Para saber mais sobre como agregar dados de várias contas e regiões, consulte Agregação de dados de várias regiões e várias contas no Guia do desenvolvedor do AWS Config .

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AggregatorAccountId

Tipo: string

Descrição: (Opcional) O ID do Conta da AWS local em que um agregador será adicionado aos dados agregados de AWS Config configuração e conformidade de várias contas e. Regiões da AWS Essa conta também é usada pelo agregador para autorizar as contas de origem.

- AggregatorAccountRegion

  Tipo: string

  Descrição: (Opcional) A região em que um agregador será adicionado para agregar dados de AWS Config configuração e conformidade de várias contas e regiões.

- IncludeGlobalResourcesRegion

  Tipo: string

  Padrão: us-east-1

  Descrição: (obrigatório) para evitar o registro de dados de recursos globais em cada região, especifique uma região da qual registrar dados de recursos globais.

- Partition

  Tipo: string

  Padrão: `aws`

  Descrição: (obrigatório) a partição da qual você deseja coletar dados de configuração e conformidade do AWS Config .

- S3 BucketName

  Tipo: string

  Padrão: `aws-config-delivery-channel`

  Descrição: (opcional) o nome que você deseja aplicar ao bucket do Amazon S3 criado para o canal de entrega. O ID da conta é anexado ao final do nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- 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

Etapas do documento

- aws:executeScript: cria um perfil do IAM vinculado ao serviço para o AWS Config , caso ainda não exista.
- aws:executeScript: cria um gravador de configuração, caso ainda não exista.
- aws:executeScript: cria um bucket do Amazon S3 para ser usado pelo canal de entrega, caso ainda não exista.
- aws:executeScript: cria um canal de entrega usando os recursos criados pelo runbook.
- aws:executeAwsApi: parar ou iniciar o gravador de configuração.
- aws:executeScript: se você especificou valores para os parâmetros AggregatorAccountId e AggregatorAccountRegion, as autorizações para agregação de dados de várias contas e várias regiões serão configuradas.

Amazon Connect

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Connect. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-AssociatePhoneNumbersToConnectContactFlows
- AWSSupport-CollectAmazonConnectContactFlowLog

AWSSupport-AssociatePhoneNumbersToConnectContactFlows

Descrição

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows`Isso ajuda você a associar números de telefone aos fluxos de contato na sua instância do Amazon Connect. Ao fornecer os mapeamentos de números de telefone e fluxos de contato em um arquivo de entrada de valores separados por vírgula (CSV), o runbook associa o maior número possível de números de telefone aos fluxos de contato em 14,5 minutos. O runbook produz um arquivo CSV de todos os pares de números de telefone e fluxo de contatos que ele não pôde associar dentro do limite de tempo para que você possa inseri-los na próxima execução.

Como funciona?

O runbook `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` ajuda você a associar números de telefone aos fluxos de contato em sua instância do Amazon Connect usando um arquivo CSV de dados de mapeamento que é armazenado em um bucket do Amazon Simple Storage Service (Amazon S3). O arquivo CSV de entrada deve estar alinhado ao seguinte formato, com `PhoneNumber` valores no formato E.164.

Exemplo do arquivo CSV de entrada

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

O runbook de automação também cria os seguintes arquivos no local de destino especificado no `DestinationFileBucket` e. `DestinationFilePath`

- **`automation:EXECUTION_ID/ResourceIdList.csv`**: um arquivo temporário que contém os `ContactFlowId` pares `PhoneNumberId` e que são necessários para a `AssociatePhoneNumberContactFlow` API.
- **`automation:EXECUTION_ID/ErrorResourceList.csv`**: um arquivo que contém o número de telefone e os pares de fluxo de contatos que não puderam ser

processados devido a um erro, como `ResourceNotFoundException` no formato de`PhoneNumber,ContactFlowName,ErrorMessage`.

- **`automation:EXECUTION_ID/NonProcessedResourceList.csv`**: um arquivo que contém o número de telefone e os pares de fluxo de contatos que não foram processados. O runbook tenta processar o maior número possível de números de telefone e fluxos de contato em 14,5 minutos (15 minutos de tempo limite da AWS Lambda função - 30 segundos de buffer). Se houver alguns números de telefone/fluxos de contato que não puderam ser processados devido à restrição de tempo, o runbook os incluirá em um arquivo CSV para usar como entrada para a próxima execução do runbook.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-AssociatePhoneNumbersToConnectContactFlowsem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional)

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - ConnectInstanceId (Obrigatório)

     O ID da sua instância do Amazon Connect.
   - SourceFileBucket (Obrigatório)

     O bucket do Amazon S3 que armazena o arquivo CSV que contém o número de telefone e os pares de fluxo de contato.
   - SourceFilePath (Obrigatório)

     A chave de objeto do Amazon S3 do arquivo CSV que contém o número de telefone e os pares de fluxo de contato. Por exemplo, `path/to/input.csv`.

- DestinationFileBucket (Obrigatório)

  O bucket do Amazon S3 no qual a automação colocará um arquivo intermediário e um relatório de resultados.

- DestinationFilePath (Opcional)

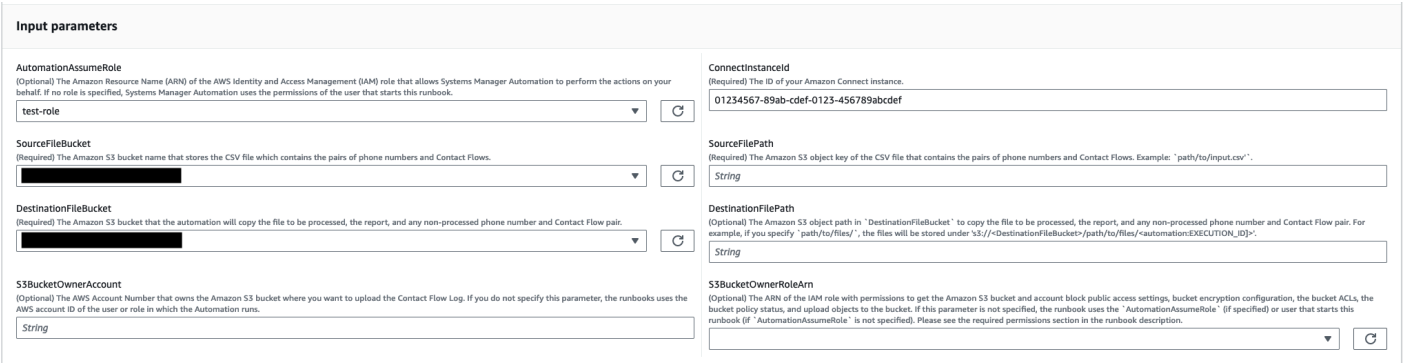
  O caminho do objeto Amazon S3 no `DestinationFileBucket` qual um arquivo intermediário e um relatório de resultados devem ser armazenados. Por exemplo, se você especificar`path/to/files/`, os arquivos serão armazenados em`s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`.

- S3 BucketOwnerAccount (opcional)

  O número da AWS conta que possui o bucket do Amazon S3 em que você deseja fazer o upload do registro de fluxo de contatos. Se você não especificar esse parâmetro, os runbooks usarão o ID da AWS conta do usuário ou da função na qual a automação é executada.

- S3 BucketOwnerRoleArn (opcional)

  O ARN da função do IAM com permissões para obter o bucket e a conta do Amazon S3 bloqueia as configurações de acesso público, a configuração da criptografia do bucket, o bucket, o ACLs status da política do bucket e o upload de objetos para o bucket. Se esse parâmetro não for especificado, o runbook usa o `AutomationAssumeRole` (se especificado) ou o usuário que inicia esse runbook (se não `AutomationAssumeRole` for especificado). Consulte a seção de permissões necessárias na descrição do runbook.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - CheckConnectInstanceExistance

Verifica se a instância do Amazon Connect fornecida em `ConnectInstanceId` existe.

- Verificações 3 BucketPublicStatus

  Verifica se os buckets do Amazon S3 especificados no `SourceFileBucket` e `DestinationFileBucket` permitem permissões de acesso anônimas ou públicas de leitura ou gravação.

- CheckSourceFileExistenceAndSize

  Verifica se o arquivo CSV de origem especificado no `SourceFilePath` existe e se o tamanho do arquivo excede o limite de 25 MiB.

- GenerateResourceIdMap

  Faz o download do arquivo CSV de origem especificado na identificação `SourceFilePath` `PhoneNumberId` e `ContactFlowId` para cada recurso. Depois de concluído, ele carrega um arquivo CSV que contém`PhoneNumber`,, `PhoneNumberId``ContactFlowName`, e `ContactFlowId` para o bucket de destino do Amazon S3 especificado em. `DestinationFileBucket` Se `PhoneNumberId` não puder ser identificado por um determinado número, o campo ficará vazio no arquivo CSV.

- AssociatePhoneNumbersToContactFlows

  Cria uma AWS Lambda função na sua conta usando uma AWS CloudFormation pilha. A AWS Lambda função associa cada número a um fluxo de contato listado no arquivo CSV de origem especificado em `SourceFileBucket` e `SourceFilePath` e a AWS CloudFormation pilha invoca a função. A AWS Lambda função mapeia o maior número possível de números de telefone para fluxos de contato antes que o tempo limite atinja o tempo limite (15 minutos). A lista de números de telefone e fluxos de contato que não puderam ser processados devido a um erro é carregada em`[automation:EXECUTION_ID]/ErrorResourceList.csv`. Aqueles que não puderam ser processados devido ao excesso do número máximo de números de telefone que podem ser processados em uma única execução são enviados`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. Se essa etapa falhar, ela vai para a `DescribeCloudFormationErrorFromStackEvents` etapa para mostrar por que ela falhou nos eventos da AWS CloudFormation pilha.

- WaitForPhoneNumberContactFlowAssociationCompletion

  Espera até que a AWS Lambda função que mapeia números de telefone para fluxos de contato seja criada e a AWS CloudFormation pilha conclua sua invocação.

- GenerateReport

  Gera o relatório que contém o número de números de telefone mapeados para fluxos de contato, aqueles que não puderam ser processados devido a um erro e aqueles que não puderam ser processados devido ao excesso do número máximo de números de telefone que podem ser processados em uma única execução. O relatório também mostra a localização (URI do Amazon S3 e URL do console do Amazon S3) `[automation:EXECUTION_ID]/ErrorResourceList.csv` para `[automation:EXECUTION_ID]/NonProcessedResourceList.csv` ou, se aplicável.

- **`DeleteCloudFormationStack`**

  Exclui a AWS CloudFormation pilha, incluindo a função Lambda para mapeamento.

- **`DescribeCloudFormationErrorFromStackEvent`**

  Descreve os erros da AWS CloudFormation pilha da `AssociatePhoneNumbersToContactFlows` etapa.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

   - GenerateReport.OutputPayload

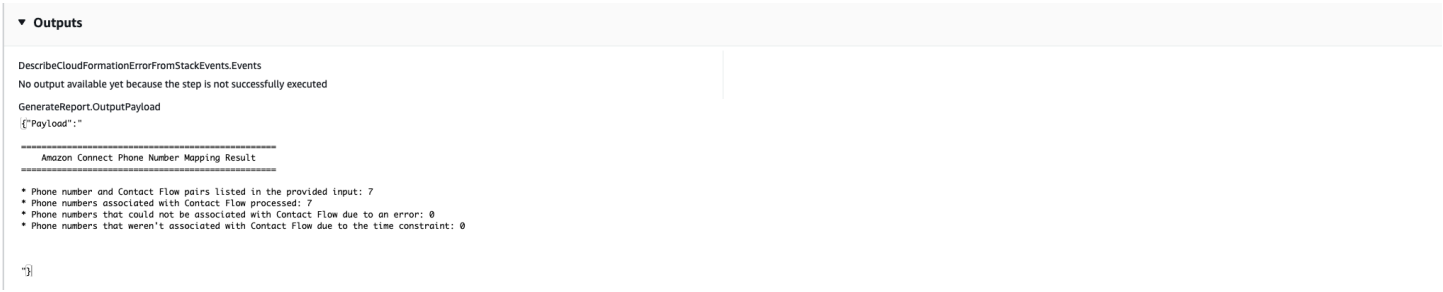
     Saída de associações de número de telefone e fluxo de contatos. Esse relatório contém as seguintes informações:

     - O número de pares de números de telefone e fluxo de contatos listados no arquivo CSV de entrada
     - O número de números de telefone associados aos fluxos de contato, conforme especificado no arquivo CSV de entrada
     - O número de números de telefone que não puderam ser associados aos fluxos de contato devido a um erro
     - O número de números de telefone que não estavam associados aos fluxos de contato devido à restrição de tempo
     - A localização (URI do Amazon S3 e URL do console do Amazon S3) do arquivo CSV que contém o número de telefone e os pares de fluxo de contato que não puderam ser associados devido a um erro
     - A localização (URI do Amazon S3 e URL do console do Amazon S3) do arquivo CSV que contém o número de telefone e os pares de fluxo de contato que não foram associados devido à restrição de tempo

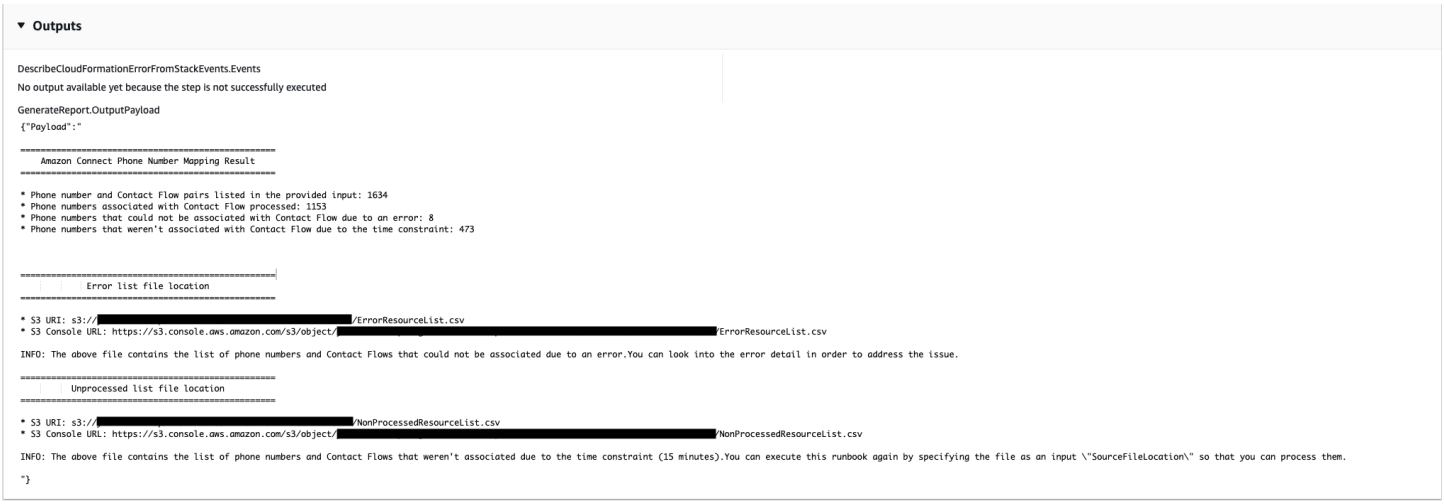
- DescribeCloudFormationErrorFromStackEvents.Eventos

  Saída que mostra os eventos da AWS CloudFormation pilha se a `AssociatePhoneNumbersToContactFlows` etapa falhar.

Saída de execução com um pequeno número de números de telefone e fluxos de contato



Saída de execução com um grande número de números de telefone e fluxos de contato e números de telefone que não foram associados devido a erro ou restrição de tempo



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSSupport-CollectAmazonConnectContactFlowLog

Descrição

O runbook de `AWSSupport-CollectAmazonConnectContactFlowLog` automação é usado para coletar os registros de fluxo de contatos do Amazon Connect para uma ID de contato específica. Ao fornecer seu ID de instância e ID de contato do Amazon Connect, o runbook pesquisa os registros de fluxo de contatos do grupo de CloudWatch registros da Amazon e os carrega no bucket do Amazon Simple Storage Service (Amazon S3) especificado no parâmetro de solicitação. O runbook gera uma saída que fornece o URL do console Amazon S3 e o comando AWS CLI para você baixar os registros.

Como funciona?

O runbook de `AWSSupport-CollectAmazonConnectContactFlowLog` automação ajuda a coletar os registros de fluxo de contatos do Amazon Connect para um ID de contato específico armazenado no grupo de CloudWatch registros configurado e os carrega em um bucket específico do Amazon S3. Para ajudar na segurança dos registros coletados do seu fluxo de contatos do Amazon Connect, a automação avalia a configuração do bucket do Amazon S3 para determinar se o bucket concede permissões `read` públicas `write` ou de acesso e é de propriedade AWS da conta especificada no `S3BucketOwnerAccountId` parâmetro. Se seu bucket do Amazon S3 usa criptografia do lado do servidor com AWS Key Management Service chaves (SSE-KMS), certifique-se de que o usuário ou a função AWS Identity and Access Management (IAM) que está executando essa automação tenha as permissões na chave. `kms:GenerateDataKey` AWS KMS Para obter mais informações sobre os registros gerados pela sua instância do Amazon Connect, consulte Registros de fluxo armazenados em um grupo de CloudWatch registros da Amazon.

> **Important**
>
> As consultas do CloudWatch Logs Insights incorrem em cobranças com base na quantidade de dados consultados. Os clientes do nível gratuito são cobrados apenas pelo uso que ultrapassar as cotas de serviço. Para obter mais informações, consulte Definição de preço do Amazon CloudWatch.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-CollectAmazonConnectContactFlowLogem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - ConnectInstanceId (Obrigatório):

     O ID da sua instância do Amazon Connect.
   - ContactId (Obrigatório):

     A ID do contato para o qual você deseja coletar o registro do fluxo de contatos.
   - S3 BucketName (obrigatório):

     O nome do bucket do Amazon S3 na sua conta em que você deseja fazer o upload do log de fluxo de contatos. Certifique-se de que a política de bucket não conceda permissões desnecessárias de leitura/gravação a partes que não precisam acessar os registros coletados.
   - S3 ObjectPrefix (opcional):

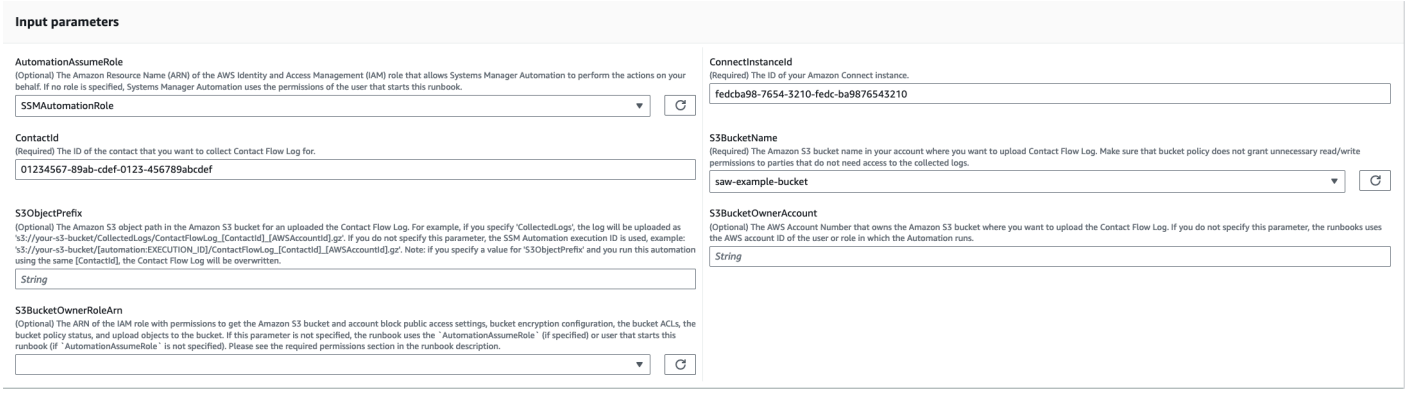
O caminho do objeto do Amazon S3 no bucket do Amazon S3 para um log de fluxo de contatos carregado. Por exemplo, se você especificar`CollectedLogs`, o registro será carregado como`s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId]_[AWSAccountId].gz`. Se você não especificar esse parâmetro, o ID de execução do Systems Manager Automation será usado, por exemplo:`s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz`. Observação: se você especificar um valor `S3ObjectPrefix` e executar essa automação usando o mesmo [ContactId], o registro do fluxo de contatos será sobrescrito.

- S3 BucketOwnerAccount (opcional):

  O número da AWS conta que possui o bucket do Amazon S3 em que você deseja fazer o upload do log de fluxo de contatos. Se você não especificar esse parâmetro, o runbook usará o ID da AWS conta do usuário ou da função na qual a automação é executada.

- S3 BucketOwnerRoleArn (opcional):

  O ARN da função do IAM com permissões para obter o bucket e a conta do Amazon S3 bloqueia as configurações de acesso público, a configuração da criptografia do bucket, o ACLs bucket, o status da política do bucket e carrega objetos no bucket. Se esse parâmetro não for especificado, o runbook usa o `AutomationAssumeRole` (se especificado) ou o usuário que inicia esse runbook (se não `AutomationAssumeRole` for especificado). Veja a seção de permissões necessárias na descrição do runbook.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - CheckConnectInstanceExistance

     Verifica se a instância do Amazon Connect fornecida no `ConnectInstanceId` é`ACTIVE`.

- Verificações 3 BucketPublicStatus

  Verifica se o bucket do Amazon S3 especificado em `S3BucketName` permite permissões de acesso anônimas ou públicas de leitura ou gravação.

- GenerateLogSearchTimeRange

  Gera `StartTime` e `EndTime` para a `StartQuery` etapa com base na `InitiationTimestamp` e `LastUpdateTimestamp` retornada pela `DescribeContact` API. `StartTime`será uma hora antes `InitiationTimestamp` e `EndTime` será uma hora depois`LastUpdateTimestamp`.

- StartQuery

  Inicia um registro de consulta para o fornecido `ContactId` no grupo de CloudWatch registros de registros associado à instância do Amazon Connect fornecida em`ConnectInstanceId`. As consultas atingem o tempo limite após 60 minutos de tempo de execução. Se sua consulta atingir o tempo limite, reduza o intervalo de tempo pesquisado. Você pode ver as consultas atualmente em andamento, bem como seu histórico de consultas recentes no CloudWatch console. Para obter mais informações, consulte Exibir consultas em execução ou histórico de consultas.

- WaitForQueryCompletion

  Aguarda a conclusão do registro de consultas de CloudWatch registros para que o fornecido seja `ContactId` concluído. Observe que a consulta expira após 60 minutos de tempo de execução. Se sua consulta atingir o tempo limite, reduza o intervalo de tempo pesquisado. Você pode visualizar as consultas atualmente em andamento, bem como seu histórico de consultas recentes no console do Amazon Connect. Para obter mais informações, consulte Exibir consultas em execução ou histórico de consultas.

- UploadContactFlowLog

  Obtém o resultado da consulta e carrega o log do fluxo de contatos para o bucket do Amazon S3 especificado em. `S3BucketName`

- GenerateReport

  Retorna a URL do console Amazon S3 em que o log do fluxo de contatos foi carregado e um exemplo de comando AWS CLI que você pode usar para baixar o arquivo de log.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

- GenerateReport.OutputPayload

Saída que informa que o runbook recuperou com sucesso os registros de fluxo de contato do contato especificado. Esse relatório também contém a URL do console Amazon S3 e um exemplo de comando da AWS CLI para que você possa baixar o arquivo de log.

Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS Directory Service

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Directory Service Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

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

AWS-CreateDSManagementInstance

Descrição

O `AWS-CreateDSManagementInstance` runbook cria uma instância Windows da Amazon Elastic Compute Cloud EC2 (Amazon) que você pode usar para gerenciar seu AWS Directory Service diretório. A instância de gerenciamento não pode ser usada para gerenciar diretórios do AD Connector.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AmiID

  Tipo: string

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

  Descrição: (Obrigatório) O ID do Amazon Machine Image (AMI) que você deseja usar para iniciar a instância de gerenciamento.

- DirectoryId

  Tipo: string

  Descrição: (Obrigatório) O ID do AWS Directory Service diretório que você deseja gerenciar. A instância é ligada ao diretório especificado.

- IamInstanceProfileName

  Tipo: string

  Descrição: (obrigatório) o nome que você especifica é aplicado ao perfil de instância do IAM que é criado pela automação e anexado à instância de gerenciamento.

- InstanceType

  Tipo: string

  Padrão: 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

  Descrição: (obrigatório) tipo de instância a ser executada.

- KeyPairName

Tipo: string

Descrição: (opcional) o par de chaves a ser usado ao criar a instância. Se você não especificar um valor, nenhum par de chaves será associado à instância.

- RemoteAccessCidr

  Tipo: string

  Descrição: (obrigatório) o bloco CIDR do qual você deseja permitir o tráfego RDP (porta 3389). O bloco CIDR que você especifica é aplicado a uma regra de entrada que é adicionada ao grupo de segurança criado pela automação.

- SecurityGroupName

  Tipo: string

  Descrição: (obrigatório) o nome que você especifica é aplicado ao grupo de segurança criado pela automação e associado à instância de gerenciamento.

- Tags

  Tipo: MapList

  Descrição: (opcional) um par de chave-valor que você deseja aplicar aos recursos criados pela automação.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeAwsApi: reúne detalhes sobre o diretório que você especifica no parâmetro DirectoryId.
- aws:executeAwsApi: obtém o bloco CIDR da nuvem privada virtual (VPC) em que o diretório foi iniciado.
- aws:executeAwsApi: cria um grupo de segurança usando o valor especificado no parâmetro SecurityGroupName.
- aws:executeAwsApi: cria uma regra de entrada para o grupo de segurança recém-criado que permite o tráfego RDP do CIDR que você especifica no parâmetro RemoteAccessCidr.
- aws:executeAwsApi: cria um perfil do IAM e um perfil de instância usando o valor especificado no parâmetro IamInstanceProfileName.
- aws:executeAwsApi- Lança uma EC2 instância da Amazon com base nos valores que você especifica nos parâmetros do runbook.
- aws:executeAwsApi- Cria um AWS Systems Manager documento para unir a instância recém-lançada ao seu diretório.
- aws:runCommand: liga a nova instância ao seu diretório.
- aws:runCommand: instala ferramentas de administração de servidor remoto na nova instância.

AWSSupport-TroubleshootADConnectorConnectivity

Descrição

O runbook AWSSupport-TroubleshootADConnectorConnectivity verifica os seguintes pré-requisitos para um AD Connector:

- Verifica se o tráfego necessário é permitido pelo grupo de segurança e pelas regras da lista de controle de acesso (ACL) à rede associadas ao seu AD Connector.
- Verifica se os endpoints VPC da CloudWatch interface AWS Systems Manager AWS Security Token Service, e da Amazon existem na mesma nuvem privada virtual (VPC) do AD Connector.

Quando as verificações de pré-requisitos são concluídas com sucesso, o runbook inicia duas instâncias Linux t2.micro do Amazon Elastic Compute Cloud (Amazon EC2) nas mesmas sub-redes

do seu AD Connector. Os testes de conectividade de rede são então realizados usando os utilitários `netcat` e `nslookup`.

Executar esta automação (console)

> **Important**
>
> O uso desse runbook pode gerar cobranças extras Conta da AWS para você pelas EC2 instâncias da Amazon, volumes do Amazon Elastic Block Store e Amazon Machine Image (AMI) criado durante a automação. Para obter mais informações, consulte Amazon Elastic Compute Cloud Pricing e Amazon Elastic Block Store Pricing.
>
> Se a `aws:deletestack` etapa falhar, acesse o AWS CloudFormation console para excluir manualmente a pilha. O nome da pilha criada por esse runbook começa com `AWSSupport-TroubleshootADConnectorConnectivity`. Para obter informações sobre como excluir AWS CloudFormation pilhas, consulte Excluindo uma pilha no Guia do usuário.AWS CloudFormation

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DirectoryId

  Tipo: string

  Descrição: (obrigatório) o ID do diretório do AD Connector no qual você deseja solucionar problemas de conectividade.

- Ec2 InstanceProfile

  Tipo: string

  Máximo de caracteres: 128

  Descrição: (obrigatório) o nome do perfil de instância que você deseja atribuir às instâncias que são iniciadas para realizar testes de conectividade. O perfil de instância que você especificar deve ter a política `AmazonSSMManagedInstanceCore` ou as permissões equivalentes anexadas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:assertAwsResourceProperty: confirma que o diretório especificado no parâmetro DirectoryId é um AD Connector.
- aws:executeAwsApi: reúne informações sobre o AD Connector.
- aws:executeAwsApi: reúne informações sobre os grupos de segurança associados ao AD Connector.
- aws:executeAwsApi: reúne informações sobre as regras de ACL de rede associadas às sub-redes do AD Connector.
- aws:executeScript: avalia as regras do grupo de segurança do AD Connector para verificar se o tráfego de saída necessário é permitido.
- aws:executeScript: avalia as regras de ACL de rede do AD Connector para verificar se o tráfego de rede de saída e entrada necessário é permitido.
- aws:executeScript- Verifica se os endpoints da CloudWatch interface AWS Systems Manager, AWS Security Token Service e da Amazon, existem na mesma VPC que o AD Connector.
- aws:executeScript: compila as saídas das verificações realizadas nas etapas anteriores.
- aws:branch: ramifica a automação dependendo da saída das etapas anteriores. A automação é interrompida aqui se as regras de saída e entrada necessárias estiverem ausentes para os grupos de segurança e a rede. ACLs
- aws:createStack- Cria uma AWS CloudFormation pilha para iniciar EC2 instâncias da Amazon e realizar testes de conectividade.
- aws:executeAwsApi- Reúne as IDs EC2 instâncias recém-lançadas da Amazon.
- aws:waitForAwsResourceProperty- Espera que a primeira EC2 instância recém-lançada da Amazon seja reportada como gerenciada por AWS Systems Manager.
- aws:waitForAwsResourceProperty- Espera que a segunda EC2 instância recém-lançada da Amazon seja reportada como gerenciada por AWS Systems Manager.

- `aws:runCommand`- Executa testes de conectividade de rede com os endereços IP do servidor DNS local da primeira instância da Amazon EC2 .
- `aws:runCommand`- Executa testes de conectividade de rede com os endereços IP do servidor DNS local da segunda instância da Amazon EC2 .
- `aws:changeInstanceState`- Interrompe as EC2 instâncias da Amazon usadas para os testes de conectividade.
- `aws:deleteStack`- Exclui a AWS CloudFormation pilha.
- `aws:executeScript`- Produz instruções sobre como excluir manualmente a AWS CloudFormation pilha se a automação falhar em excluir a pilha.

`AWSSupport-TroubleshootDirectoryTrust`

Descrição

O `AWSSupport-TroubleshootDirectoryTrust` runbook diagnostica problemas de criação de confiança entre um AWS Managed Microsoft AD e um Microsoft Active Directory. A automação garante que o tipo de diretório ofereça suporte a relações de confiança e, em seguida, verifica as regras do grupo de segurança, as listas de controle de acesso à rede (rede ACLs) e as tabelas de rotas associadas em busca de possíveis problemas de conectividade.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DirectoryId

  Tipo: string

  Padrão permitido: ^d-[a-z0-9]\{10\}$

  Descrição: (Obrigatório) O ID do AWS Managed Microsoft AD para solucionar o problema.

- RemoteDomainCidrs

  Tipo: StringList

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

  Descrição: (obrigatória) os CIDRs do domínio remoto com o qual você está tentando estabelecer uma relação de confiança. Você pode adicionar vários CIDRs usando valores separados por vírgula. Por exemplo, 172.31.48.0/20, 192.168.1.10/32.

- RemoteDomainName

  Tipo: string

  Descrição: (obrigatória) o nome totalmente qualificado do domínio remoto com o qual você está estabelecendo uma relação de confiança.

- RequiredTrafficACL

  Tipo: string

  Descrição: (Obrigatório) Os requisitos de porta padrão para AWS Managed Microsoft AD. Na maioria dos casos, não modifique o valor padrão.

  Padrão: {"entrada":{"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]]},"saída":{"-1":[[0,65535]]}}

- RequiredTrafficSG

Tipo: string

Descrição: (Obrigatório) Os requisitos de porta padrão para AWS Managed Microsoft AD. Na maioria dos casos, não modifique o valor padrão.

Padrão: {"entrada":{"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]]},"saída":{"-1":[[0,65535]]}}

- TrustId

  Tipo: string

  Descrição: (opcional) o ID do relacionamento de confiança a ser solucionado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:assertAwsResourceProperty`: confirma que o tipo de diretório é AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Obtém informações sobre AWS Managed Microsoft AD o.
- `aws:branch`: ramifica a automação se um valor for fornecido para o parâmetro de entrada `TrustId`.
- `aws:executeAwsApi`: obtém informações sobre o relacionamento de confiança.

- `aws:executeAwsApi`: obtém os endereços IP DNS de encaminhador condicional para o `RemoteDomainName`.
- `aws:executeAwsApi`: obtém informações sobre rotas IP adicionadas ao AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Obtém CIDRs as AWS Managed Microsoft AD sub-redes.
- `aws:executeAwsApi`: obtém informações sobre os grupos de segurança associados a AWS Managed Microsoft AD.
- `aws:executeAwsApi`- Obtém informações sobre a rede ACLs associada ao AWS Managed Microsoft AD.
- `aws:executeScript`: confirma que os `RemoteDomainCidrs` são valores válidos. Confirma que AWS Managed Microsoft AD tem encaminhadores condicionais para o e que as rotas IP necessárias foram adicionadas ao`RemoteDomainCidrs`, AWS Managed Microsoft AD se não `RemoteDomainCidrs` forem endereços IP RFC 1918.
- `aws:executeScript`: avalia as regras do grupo de segurança.
- `aws:executeScript`- Avalia a rede ACLs.

Saídas

evalDirectorySecurityGroup.output - Resulta da avaliação de se as regras do grupo de segurança associadas ao AWS Managed Microsoft AD permitem o tráfego necessário para a criação de confiança.

evalAclEntries.output - Resulta da avaliação de se a rede ACLs associada ao AWS Managed Microsoft AD permite o tráfego necessário para a criação de confiança.

evaluateRemoteDomainCIDR.Output - Resulta da avaliação de se os valores são válidos`RemoteDomainCidrs`. Confirma que AWS Managed Microsoft AD tem encaminhadores condicionais para o e que as rotas IP necessárias foram adicionadas ao`RemoteDomainCidrs`, AWS Managed Microsoft AD se não `RemoteDomainCidrs` forem endereços IP RFC 1918.

AWS AppSync

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS AppSync Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableAppSyncGraphQLApiLogging

AWS-EnableAppSyncGraphQLApiLogging

Descrição

O `AWS-EnableAppSyncGraphQLApiLogging` runbook permite o registro em nível de campo e registro em nível de solicitação para a API AWS AppSync GraphQL que você especificar. O runbook aplicará as alterações na API GraphQL especificada, mesmo que o registro já tenha sido habilitado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ApiId

  Tipo: string

  Descrição: (Obrigatório) O ID da API para a qual você deseja ativar o registro.
- FieldLogLevel

Tipo: string

Valores válidos: ERROR | ALL

Descrição: (Obrigatório) O nível de registro do campo.

- CloudWatchLogsRoleArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da função de serviço que AWS AppSync pressupõe publicar no Amazon Logs. CloudWatch

- ExcludeVerboseContent

  Tipo: booliano

  Padrão: False

  Descrição: (Opcional) Defina como `True` para excluir informações como cabeçalhos, contexto e modelos de mapeamento avaliados, independentemente do nível de registro.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- aws: executeAwsApi - Reúne o tipo de autenticação e as informações de configuração relevantes para o tipo de autenticação principal.
- aws:branch - Ramificações com base no tipo de autenticação.
- aws: executeAwsApi - Atualiza a configuração de registro da API AWS AppSync GraphQL com base nos valores especificados para os parâmetros de entrada do runbook.

Saídas

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: Resposta da `UpdateGraphqlApi` chamada.
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: Resposta da `UpdateGraphqlApi` chamada.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: Resposta da `UpdateGraphqlApi` chamada.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: Resposta da `UpdateGraphqlApi` chamada.

Amazon Athena

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Athena. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableAthenaWorkGroupEncryptionAtRest

`AWS-EnableAthenaWorkGroupEncryptionAtRest`

Descrição

O `AWS-EnableAthenaWorkGroupEncryptionAtRest` runbook permite a criptografia em repouso para o grupo de trabalho do Amazon Athena que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- WorkGroup

  Tipo: string

  Descrição: (Obrigatório) O grupo de trabalho para o qual você deseja habilitar a criptografia em repouso.

- EncryptionOption

  Tipo: string

  Valores válidos: SSE_S3 | SSE_KMS | CSE_KMS

  Descrição: (Obrigatório) Especifica qual opção de criptografia é usada. Você pode escolher criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE_S3), criptografia do lado do servidor com chaves gerenciadas (SSE_KMS) ou criptografia do lado do cliente com chaves AWS KMS gerenciadas (CSE_KMS). AWS KMS

- KmsKeyId

  Tipo: string

  Descrição: (Opcional) Se você estiver usando uma opção de AWS KMS criptografia, especifique o ARN da chave, o ID da chave ou o alias da chave que você deseja usar.

- EnableMinimumEncryptionConfiguration

  Tipo: booleano

  Padrão: verdadeiro

Descrição: (Opcional) Impõe um nível mínimo de criptografia para o grupo de trabalho para resultados de consulta e cálculo que são gravados no Amazon S3. Quando ativada, os usuários do grupo de trabalho podem definir a criptografia somente no nível mínimo definido pelo administrador ou superior ao enviarem consultas. Essa configuração não se aplica aos grupos de trabalho habilitados para Spark.

- EnforceWorkGroupConfiguration

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Se definido como`True`, as configurações do grupo de trabalho substituem as configurações do lado do cliente. Se definido como`False`, as configurações do lado do cliente serão usadas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- aws:branch - Ramificações com base na opção de criptografia especificada no `EncryptionOption` parâmetro.
- aws: executeAwsApi - Esta etapa atualiza o Athena Work Group com a configuração de criptografia especificada.
- aws: executeAwsApi - Atualiza o Athena Work Group com a configuração de criptografia especificada.
- aws: assertAwsResource Propriedade - Verifica se a criptografia para o grupo de trabalho foi ativada.

DynamoDB

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon DynamoDB. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

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

AWS-ChangeDDBRWCapacityMode

Descrição

O `AWS-ChangeDDBRWCapacityMode` runbook altera o modo de capacidade de leitura/gravação de uma ou mais tabelas do Amazon DynamoDB (DynamoDB) para o modo sob demanda ou para o modo provisionado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- CapacityMode

  Tipo: string

  Valores válidos: PROVISIONED | PAY_PER_REQUEST

  Descrição: (Obrigatório) O modo de capacidade de leitura/gravação desejado. Ao mudar da capacidade sob demanda (pay-per-request) para a capacidade provisionada, os valores iniciais da capacidade provisionada devem ser definidos. Os valores iniciais da capacidade provisionada são estimados com base na capacidade de leitura e gravação consumida da sua tabela e dos índices secundários globais nos últimos 30 minutos.

- ReadCapacityUnits

  Tipo: inteiro

  Padrão: 0

  Descrição: (Opcional) O número máximo de leituras altamente consistentes consumidas por segundo antes que o DynamoDB retorne uma exceção de limitação.

- TableNames

  Tipo: string

  Descrição: (Obrigatório) Lista separada por vírgula de nomes de tabelas do DynamoDB para alterar o modo de capacidade de leitura/gravação para..

- WriteCapacityUnits

  Tipo: inteiro

  Padrão: 0

Descrição: (Opcional) O número máximo de gravações consumidas por segundo antes que o DynamoDB retorne uma exceção de limitação.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Altera o modo de capacidade de leitura/gravação das tabelas do DynamoDB especificadas no parâmetro. `TableNames`

Saídas

DDBRWCapacityModo de mudança. SuccessesTables - Lista de nomes de tabelas do DynamoDB em que o modo de capacidade foi alterado com sucesso

DDBRWCapacityModo de mudança. FailedTables - Lista mapeada dos nomes das tabelas do DynamoDB em que a alteração do modo de capacidade falhou e o motivo da falha.

AWS-CreateDynamoDBBackup

Descrição

Criar um backup da tabela do Amazon DynamoDB.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BackupName

  Tipo: string

  Descrição: (obrigatório) Nome do backup a ser criado.
- LambdaAssumeRole

  Tipo: string

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.
- TableName

  Tipo: string

  Descrição: (obrigatório) nome da tabela do DynamoDB.

AWS-DeleteDynamoDbBackup

Descrição

Excluir o backup de uma tabela do Amazon DynamoDB.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BackupArn

  Tipo: string

  Descrição: (obrigatório) ARN do backup da tabela do DynamoDB a ser excluído.

AWSConfigRemediation-DeleteDynamoDbTable

Descrição

O runbook `AWSConfigRemediation-DeleteDynamoDbTable` exclui a tabela do Amazon DynamoDB (DynamoDB) que você especificar.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- TableName

  Tipo: string

  Descrição: (obrigatório) nome da tabela do DynamoDB que você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: exclui a tabela do DynamoDB especificada no parâmetro `TableName`.
- `aws:executeScript`: verifica se a tabela do DynamoDB foi excluída.

AWS-DeleteDynamoDbTableBackups

Descrição

Excluir backups de tabelas do DynamoDB com base em dias ou contagem de retenção.

Execute esta Automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LambdaAssumeRole

  Tipo: string

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.
- RetentionCount

  Tipo: string

  Padrão: 10

  Descrição: (opcional) o número de backups a serem retidos para a tabela. Se existir mais backups do que o número especificado, os backups mais antigos além desse número são excluídos. Um RetentionCount ou RetentionDays pode ser usado, não os dois.
- RetentionDays

  Tipo: string

Descrição: (opcional) o número de dias a reter backups para a tabela. Os backups mais antigos que o número especificado de dias são excluídos. Um RetentionCount ou RetentionDays pode ser usado, não os dois.

- TableName

  Tipo: string

  Descrição: (obrigatório) nome da tabela do DynamoDB.

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

Descrição

O `AWSConfigRemediation-EnableEncryptionOnDynamoDbTable` runbook criptografa uma tabela do Amazon DynamoDB (DynamoDB) usando a chave gerenciada pelo cliente AWS KMS() que você especifica para AWS Key Management Service o parâmetro. `KMSKeyId`

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- KMSKeyIdentificação

Tipo: string

Descrição: (obrigatório) o ARN da chave gerenciada pelo cliente que você deseja usar para criptografar a tabela do DynamoDB especificada no parâmetro `TableName`.

- TableName

  Tipo: string

  Descrição: (obrigatório) nome da tabela do DynamoDB que você deseja criptografar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: criptografa a tabela do DynamoDB que você especifica no parâmetro `TableName`.
- `aws:waitForAwsResourceProperty`: verifica se a propriedade `Enabled` do `SSESpecification` da tabela do DynamoDB está definida como `true`.
- `aws:assertAwsResourceProperty`: verifica se a tabela do DynamoDB está criptografada com a chave gerenciada pelo cliente especificada no parâmetro `KMSKeyId`.

AWSConfigRemediation-EnablePITRForDynamoDbTable

Descrição

O `AWSConfigRemediation-EnablePITRForDynamoDbTable` runbook permite a point-in-time recuperação (PITR) na tabela do Amazon DynamoDB que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- TableName

  Tipo: string

  Descrição: (Obrigatório) O nome da tabela do DynamoDB para ativar a point-in-time recuperação.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`- Permite a point-in-time recuperação na tabela do DynamoDB que você especifica no parâmetro. `TableName`

- `aws:assertAwsResourceProperty`- Confirma que a point-in-time recuperação está ativada na tabela do DynamoDB.

`AWS-EnableDynamoDbAutoscaling`

Descrição

O `AWS-EnableDynamoDbAutoscaling` runbook habilita o Application Auto Scaling para a tabela de capacidade provisionada do Amazon DynamoDB que você especificar. O Application Auto Scaling ajusta dinamicamente a capacidade de transferência provisionada em resposta aos padrões de tráfego. Para obter mais informações, consulte Gerenciamento automático da capacidade de transferência com o auto scaling do DynamoDB no Amazon DynamoDB Developer Guide.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- TableName

  Tipo: string

  Descrição: (Obrigatório) O nome da tabela do DynamoDB na qual você deseja ativar o Application Auto Scaling.

- MinReadCapacity

  Tipo: inteiro

  Descrição: (Obrigatório) O número mínimo de unidades de capacidade de leitura de throughput provisionadas para a tabela do DynamoDB.
- MaxReadCapacity

  Tipo: inteiro

  Descrição: (Obrigatório) O número máximo de unidades de capacidade de leitura de throughput provisionadas para a tabela do DynamoDB.
- TargetReadCapacityUtilization

  Tipo: inteiro

  Descrição: (Obrigatório) A meta de utilização da capacidade de leitura desejada. A meta de utilização é a porcentagem da taxa de transferência provisionada consumida em um determinado momento. Você pode definir os valores de utilização alvo do auto scaling entre 20 e 90 por cento.
- ReadScaleOutCooldown

  Tipo: inteiro

  Descrição: (Obrigatório) A quantidade de tempo, em segundos, de espera até que uma atividade anterior de expansão da capacidade de leitura entre em vigor.
- ReadScaleInCooldown

  Tipo: inteiro

  Descrição: (Obrigatório) A quantidade de tempo em segundos após a conclusão de uma atividade de expansão da capacidade de leitura antes que outra atividade de expansão possa ser iniciada.
- MinWriteCapacity

  Tipo: inteiro

  Descrição: (Obrigatório) O número mínimo de unidades de gravação de taxa de transferência provisionadas para a tabela do DynamoDB.
- MaxWriteCapacity

  Tipo: inteiro

Descrição: (Obrigatório) O número máximo de unidades de gravação de taxa de transferência provisionadas para a tabela do DynamoDB.

- TargetWriteCapacityUtilization

  Tipo: inteiro

  Descrição: (Obrigatório) A utilização desejada da capacidade de gravação. A meta de utilização é a porcentagem da taxa de transferência provisionada consumida em um determinado momento. Você pode definir os valores de utilização alvo do auto scaling entre 20 e 90 por cento.

- WriteScaleOutCooldown

  Tipo: inteiro

  Descrição: (Obrigatório) A quantidade de tempo, em segundos, de espera até que uma atividade anterior de expansão da capacidade de gravação entre em vigor.

- WriteScaleInCooldown

  Tipo: inteiro

  Descrição: (Obrigatório) A quantidade de tempo em segundos após a conclusão de uma atividade de expansão da capacidade de gravação antes que outra atividade de expansão possa ser iniciada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- RegisterAppAutoscalingTargetWrite (`aws:executeAwsApi`) - Configura o Application Auto Scaling na tabela do DynamoDB que você especificar.

- RegisterAppAutoscalingTargetWriteDelay (`aws:sleep`) - Dorme para evitar a limitação da API.
- PutScalingPolicyWrite (`aws:executeAwsApi`) - Configura a meta de utilização da capacidade de gravação para a tabela do DynamoDB.
- PutScalingPolicyWriteDelay (`aws:sleep`) - Dorme para evitar a limitação da API.
- RegisterAppAutoscalingTargetRead (`aws:executeAwsApi`) - Configura as unidades de capacidade mínima e máxima de leitura para a tabela do DynamoDB.
- RegisterAppAutoscalingTargetReadDelay (`aws:sleep`) - Dorme para evitar a limitação da API.
- PutScalingPolicyRead (`aws:executeAwsApi`) - Configura a meta de utilização da capacidade de leitura para a tabela do DynamoDB.
- VerifyDynamoDbAutoscalingEnabled (`aws:executeScript`) - Verifica se o Application Auto Scaling está habilitado para a tabela do DynamoDB de acordo com os valores que você especificar.

Saídas

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

AWS-RestoreDynamoDBTable

Descrição

O `AWS-RestoreDynamoDBTable` runbook restaura a tabela do Amazon DynamoDB que você especifica point-in-time usando a recuperação (PITR).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EnablePointInTimeRecoverAsNeeded

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Determina se a automação ativa a point-in-time recuperação conforme necessário para restaurar a tabela.
- GlobalSecondaryIndexOverride

  Tipo: string

  Descrição: (opcional) os novos índices secundários globais para substituir os índices secundários existentes na nova tabela.
- LocalSecondaryIndexOverride

  Tipo: string

  Descrição: (opcional) os novos índices secundários locais para substituir os índices secundários existentes na nova tabela.
- RestoreDateTime

  Tipo: string

  Descrição: (Obrigatório) A point-in-time recuperação para a qual você deseja restaurar sua tabela nos últimos 35 dias. Especifique a data e a hora no seguinte formato: `DD/MM/YYYY HH:MM:SS`

- SourceTableArn

  Tipo: string

  Descrição: (obrigatório) o ARN da tabela que deseja restaurar.

- SseSpecificationOverride

  Tipo: string

  Descrição: (opcional) as configurações de criptografia do lado do servidor a serem usadas na nova tabela.

- TargetTableName

  Tipo: string

  Descrição: (obrigatório) o nome da tabela a ser restaurada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Restaura a tabela do DynamoDB que você especifica no `TargetTableName` parâmetro usando a recuperação. point-in-time

AWS Database Migration Service

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Database Migration Service Para obter mais informações sobre runbooks, consulte Trabalhando com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-TroubleshootDMSTableErrors

AWSSupport-TroubleshootDMSTableErrors

Descrição

O runbook de AWS Systems Manager `AWSSuport-TroubleshootDMSTabelErrors` automação ajuda você a automatizar o processo de solução de problemas `Table errors` encontrado na tarefa de migração do banco de dados ou na replicação sem servidor do. AWS Database Migration Service Esses erros ocorrem quando as tabelas não conseguem migrar do endpoint de origem (banco de dados de origem) para o endpoint de destino (banco de dados de destino) pela tarefa de migração do banco de dados ou pela replicação sem servidor criada no serviço. AWS DMS Este runbook analisa as mensagens de erro de assinatura dos CloudWatch registros, focando especificamente nos registros de tarefas para tarefas tradicionais de migração de banco de dados e nos registros sem servidor para replicação sem servidor. Ele também fornece sugestões específicas e etapas de correção para mensagens de erro comuns encontradas `Table error` durante as AWS DMS migrações.

Como funciona?

O runbook executa as seguintes etapas:

- Busca informações sobre o AWS DMS ARN fornecido, que pode ser uma tarefa de migração de banco de dados ou uma replicação sem servidor.
- Verifica se o AWS DMS recurso fornecido foi iniciado pelo menos uma vez, verificando o `FreshStartDate` valor na resposta da DescribeReplicationTasks API (para tarefa de migração de banco de dados) e DescribeReplications da API (para replicação sem servidor). Se o recurso não tiver sido iniciado, a automação gerará um erro.
- Se o recurso foi iniciado, a automação verifica as tabelas nos `TableError` estados usando `TableStatistics` informações. Se nenhum erro for encontrado, a automação encerrará o fluxo

de trabalho após exibir uma mensagem confirmando que nenhum erro de tabela foi encontrado na tarefa de migração do banco de dados ou na replicação sem servidor especificada.

- Se forem encontradas tabelas com `TableError` estado, a automação verificará se o CloudWatch registro está habilitado para o AWS DMS recurso especificado. Se o registro não estiver ativado, a automação encerrará o fluxo de trabalho após exibir uma mensagem indicando que o registro não está ativado.

  Observação: espera-se que o CloudWatch registro seja ativado, pois a automação depende desses registros para analisar e identificar os problemas com as tabelas em `TableError` estado.
- Se o registro estiver ativado, a automação analisa os CloudWatch registros e gera um relatório para cada tabela que está em `TableError` estado. O relatório inclui sugestões para mensagens de erro comuns e fornece registros de erros relevantes para ajudar a identificar e resolver problemas que impedem a migração bem-sucedida da tabela do endpoint de AWS DMS origem para o endpoint de AWS DMS destino.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DMSArn

Tipo: String

Descrição: (Obrigatório) ARN da tarefa de migração do banco de dados ou replicação sem servidor

Allowed-pattern: `^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: String

  Descrição: (Opcional) Esse parâmetro define o início do intervalo de tempo para análise de CloudWatch registros de determinada tarefa de migração de banco de dados ou replicação sem servidor. Quando fornecidos, somente os registros gerados a partir desse momento específico serão coletados e analisados. Observe que existe a possibilidade de o fluxo de trabalho atingir o tempo limite se o intervalo de tempo entre `startDate` e `endDate` for muito longo. O valor deve ser fornecido no formato de data e hora ISO 6081.

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

- EndTimeRange

  Tipo: String

  Descrição: (Opcional) Esse parâmetro define o final do intervalo de tempo para análise de CloudWatch log da determinada tarefa de migração de banco de dados ou replicação sem servidor. Quando fornecidos, somente os registros gerados até esse momento específico serão coletados e analisados. Observe que existe a possibilidade de o fluxo de trabalho atingir o tempo limite se o intervalo de tempo entre `startDate` e `endDate` for muito longo. O valor deve ser fornecido no formato de data e hora ISO 6081.

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

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `dms:DescribeReplicationTasks`

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

Exemplo de política do IAM para a função Automation Assume

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

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-TroubleshootDMSTableErrorsem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:

- AutomationAssumeRole (Opcional):

  O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.

- DMSArn

  ARN da tarefa de migração do banco de dados ou replicação sem servidor que tem erros de tabela.

- StartTimeRange

  (Opcional) Formato de data e hora ISO 6081 que define o início do intervalo de tempo para analisar CloudWatch os registros de determinada tarefa de migração de banco de dados ou replicação sem servidor.

- EndTimeRange

  (Opcional) Formato de data e hora ISO 6081 que define o final do intervalo de tempo para analisar CloudWatch os registros da determinada tarefa de migração do banco de dados ou replicação sem servidor.

4. Selecione o botão Executar na parte inferior da página.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - validar DMSInput TypeAndGatherDetails

     Valida a entrada AWS DMS ARN fornecida e reúne os detalhes básicos da tarefa de migração do banco de dados ou da replicação sem servidor, que são necessários nas próximas etapas.

   - branchOnTableErros

     Ramifica o fluxo de trabalho com base no número de erros de tabela encontrados na etapa acima. Se a contagem for maior que 0, vá para a `branchOnCWLoggingStatus` etapa -. Caso contrário, vá para a `outputNoTableErrors` etapa -.

   - outputNoTableErros

     Exiba uma mensagem informando que os erros da tabela não foram encontrados na tarefa de migração do banco de dados ou na replicação sem servidor especificada.

   - Status do BranchOn CWLogging

Ramifica o fluxo de trabalho com base no status de CloudWatch registro encontrado na etapa acima. Se ativado, prossiga para a `gatherTableDetails` etapa -. Caso contrário, vá para a `outputNoCWLoggingEnabled` etapa -.

- Saída: Não ativada CWLogging

  Produz uma mensagem informando que o CloudWatch registro não está habilitado na tarefa de migração do banco de dados ou na replicação sem servidor especificada.

- gatherTableDetails

  Reúne os registros de `FullLoadEndTime` data e hora das tabelas com falha e calcula os valores do intervalo de tempo para analisar os registros. CloudWatch

- analyzeCloudWatchLogs

  Analisa os registros encontrados no grupo de CloudWatch registros com base nas mensagens de erro da assinatura e retorna o relatório ao usuário.

7. Após a conclusão da execução, revise a seção Saídas para obter os resultados detalhados da execução.

   - Saída de nenhum erro de tabela encontrado

     Se não houver erros de tabela encontrados na tarefa de migração do banco de dados fornecida ou na replicação sem servidor, a automação mostrará a saída informando o mesmo.

   - Saída de Sem CloudWatch login ativado

     Se o CloudWatch registro não estiver habilitado na tarefa de migração de banco de dados fornecida ou na replicação sem servidor, a automação mostrará a saída informando a mesma e fornecerá as etapas para habilitar o registro.

   - Relatório de análise de log

     Produz um relatório que identifica as tabelas no `Table error` estado da tarefa de migração do banco de dados fornecida ou da replicação sem servidor, diferenciando os tipos de erro, listando as mensagens de erro encontradas e fornecendo etapas e sugestões de remediação direcionadas para cada tabela identificada.

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

Amazon EBS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic Block Store. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- 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`

Descrição

O runbook de `AWSSupport-AnalyzeEBSResourceUsage` automação é usado para analisar o uso de recursos no Amazon Elastic Block Store (Amazon EBS). Ele analisa o uso do volume e identifica volumes, imagens e instantâneos abandonados em uma determinada região. AWS

Como funciona?

O runbook executa as quatro tarefas a seguir:

1. Verifica se existe um bucket do Amazon Simple Storage Service (Amazon S3) ou cria um novo bucket do Amazon S3.
2. Reúne todos os volumes do Amazon EBS no estado disponível.
3. Reúne todos os snapshots do Amazon EBS cujo volume de origem foi excluído.
4. Reúne todas as Amazon Machine Images (AMIs) que não estão em uso por nenhuma instância não encerrada do Amazon Elastic Compute Cloud (Amazon EC2).

O runbook gera relatórios CSV e os armazena em um bucket Amazon S3 fornecido pelo usuário. O bucket fornecido deve ser protegido seguindo as melhores práticas de AWS segurança, conforme descrito no final. Se o bucket do Amazon S3 fornecido pelo usuário não existir na conta, o runbook cria um novo bucket do Amazon S3 com o formato do nome`<User-provided-name>-awssupport-YYYY-MM-DD`, criptografado com uma chave personalizada AWS Key Management Service (AWS KMS), com o controle de versão do objeto ativado, acesso público bloqueado e exige solicitações para usar SSL/TLS.

Se você quiser especificar seu próprio bucket do Amazon S3, certifique-se de que ele esteja configurado de acordo com estas melhores práticas:

- Bloqueie o acesso público `IsPublic` ao bucket (definido como`False`).
- Ative o registro de acesso ao Amazon S3.
- Permita somente solicitações SSL em seu bucket.
- Ative o controle de versão de objetos.
- Use uma chave AWS Key Management Service (AWS KMS) para criptografar seu bucket.

> **Important**
>
> O uso desse runbook pode gerar cobranças adicionais em sua conta pela criação de buckets e objetos do Amazon S3. Consulte os preços do Amazon S3 para obter mais detalhes sobre as cobranças que podem ser incorridas.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- S3 BucketName

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

  Descrição: (Obrigatório) O bucket do Amazon S3 em sua conta para fazer o upload do relatório. Certifique-se de que a política de bucket não conceda permissões desnecessárias de leitura/gravação a partes que não precisam acessar os registros coletados. Se o intervalo especificado não existir na conta, a automação cria um novo intervalo na região em que a automação é iniciada com o formato do nome`<User-provided-name>-awssupport-YYYY-MM-DD`, criptografado com uma AWS KMS chave personalizada.

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

- CustomerManagedKmsKeyArn

  Tipo: string

  Descrição: (Opcional) A AWS KMS chave personalizada Amazon Resource Name (ARN) para criptografar o novo bucket do Amazon S3 que será criado se o bucket especificado não existir na conta. A automação falhará se a criação do bucket for tentada sem especificar um ARN de AWS KMS chave personalizada.

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

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Exemplo de política com permissões mínimas exigidas do IAM para executar este runbook:

```
        {
            "Version": "2012-10-17",
            "Statement": [{
                "Sid": "Read_Only_Permissions",
                "Effect": "Allow",
                "Action": [
                    "ec2:DescribeImages",
                    "ec2:DescribeInstances",
                    "ec2:DescribeSnapshots",
                    "ec2:DescribeVolumes",
                    "ssm:DescribeAutomationExecutions"
                ],
                "Resource": ""
            }, {
                "Sid": "KMS_Generate_Permissions",
                "Effect": "Allow",
                "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
                "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            }, {
                "Sid": "S3_Read_Only_Permissions",
                "Effect": "Allow",
                "Action": [
                    "s3:GetBucketAcl",
                    "s3:GetBucketPolicyStatus",
                    "s3:GetBucketPublicAccessBlock",
                    "s3:ListBucket"
                ],
                "Resource": [
                    "arn:aws:s3:::amzn-s3-demo-bucket1",
                    "arn:aws:s3:::amzn-s3-demo-bucket2/"
                ]
            }, {
                "Sid": "S3_Create_Permissions",
                "Effect": "Allow",
```

```
                "Action": [
                    "s3:CreateBucket",
                    "s3:PutObject",
                    "s3:PutBucketLogging",
                    "s3:PutBucketPolicy",
                    "s3:PutBucketPublicAccessBlock",
                    "s3:PutBucketTagging",
                    "s3:PutBucketVersioning",
                    "s3:PutEncryptionConfiguration"
                ],
                "Resource": "*"
            }]
        }
```

Instruções

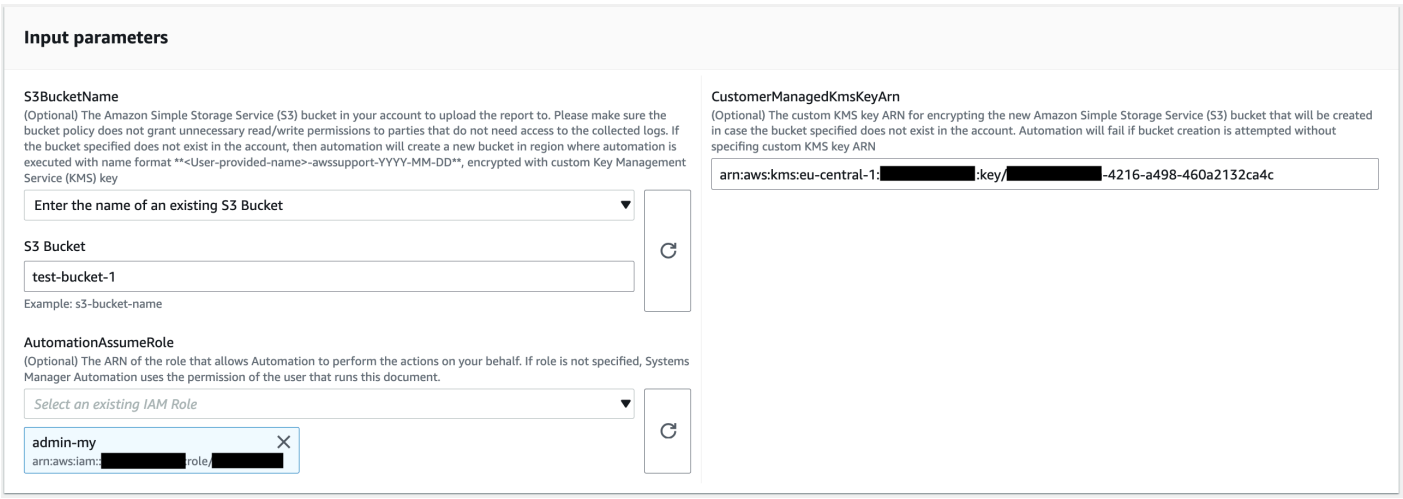
Siga estas etapas para configurar a automação:

1. Navegue até o AWSSupport-AnalyzeEBSResourceUsageno AWS Systems Manager console.
2. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - S3 BucketName (obrigatório):

     O bucket do Amazon S3 em sua conta para fazer o upload do relatório.
   - CustomerManagedKmsKeyArn(Opcional):

     A AWS KMS chave personalizada Amazon Resource Name (ARN) para criptografar o novo bucket do Amazon S3 que será criado se o bucket especificado não existir na conta.



3. Selecione Executar.
4. A automação é iniciada.
5. O runbook de automação realiza as seguintes etapas:
   - Verifique a simultaneidade:

     Garante que haja apenas uma iniciação desse runbook na região. Se o runbook encontrar outra execução em andamento, ele retornará um erro e terminará.
   - verifyOrCreateCaçamba S3:

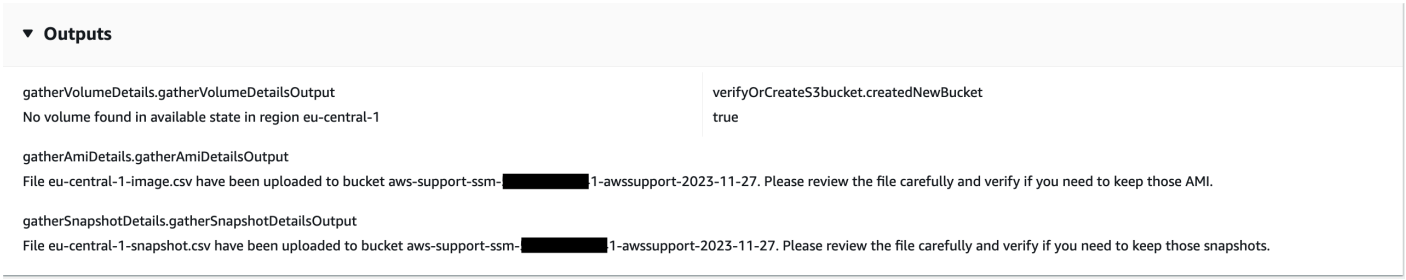
     Verifica se o bucket do Amazon S3 existe. Caso contrário, ele cria um novo bucket do Amazon S3 na região em que a automação é iniciada com o formato de nome`<User-provided-name>-awssupport-YYYY-MM-DD`, criptografado com uma chave personalizada AWS KMS .
   - gatherAmiDetails:

     As pesquisas por AMIs, que não estão em uso por nenhuma EC2 instância da Amazon, geram o relatório com o formato `<region>-images.csv` do nome e o carregam no bucket do Amazon S3.
   - gatherVolumeDetails:

     Verifica os volumes do Amazon EBS no estado disponível, gera o relatório com o formato `<region>-volume.csv` do nome e o carrega em um bucket do Amazon S3.
   - gatherSnapshotDetails:

     Procura os snapshots do Amazon EBS dos volumes do Amazon EBS que já foram excluídos, gera o relatório com o formato `<region>-snapshot.csv` do nome e o carrega no bucket do Amazon S3.

6. Depois de concluído, revise a seção Outputs para obter os resultados detalhados da execução.



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS-ArchiveEBSSnapshots

Descrição

O runbook da `AWS-ArchiveEBSSnapshots` ajuda a arquivar snapshots para volumes do Amazon Elastic Block Store (Amazon EBS), especificando a tag que foi aplicada aos snapshots. Como alternativa, você pode fornecer o ID de um volume se os snapshots estiverem sem tags.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Descrição

  Tipo: String

  Descrição: (opcional) uma descrição para o snapshot da Amazon EBS.

- DryRun

  Tipo: String

  Valores válidos: sim | não

  Descrição: (obrigatório) verifica se você tem as permissões necessárias para a ação, sem realmente fazer a solicitação, e fornece uma resposta de erro.

- RetentionCount

  Tipo: String

  Descrição: (opcional) o número de snapshots que você deseja arquivar. Não especifique um valor para esse parâmetro se foi especificado um valor para `RetentionDays`.

- RetentionDays

  Tipo: String

  Descrição: (opcional) o número de dias anteriores de snapshots que você deseja arquivar. Não especifique um valor para esse parâmetro se foi especificado um valor para `RetentionCount`.

- SnapshotWithTag

  Tipo: String

  Valores válidos: sim | não

  Descrição: (obrigatório) especifica se os snapshots que deseja arquivar estão marcados.

- TagKey

  Tipo: String

  Descrição: (opcional) a chave da tag atribuída aos snapshots que deseja arquivar.
- TagValue

  Tipo: String

  Descrição: (opcional) o valor da tag atribuída aos snapshots que deseja arquivar.
- VolumeId

  Tipo: String

  Descrição: (opcional) o ID do volume cujos snapshots deseja arquivar. Use esse parâmetro se os snapshots não estiverem marcados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

`aws:executeScript`: arquiva os snapshots usando a tag especificada usando os parâmetros `TagKey` e `TagValue` ou o parâmetro do `VolumeId`.

AWS-AttachEBSVolume

Descrição

Anexe um volume do Amazon Elastic Block Store (Amazon EBS) a uma instância do Amazon Elastic Compute Cloud (EC2Amazon).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Dispositivo

  Tipo: String

  Descrição: (obrigatório) o nome do dispositivo (por exemplo, /dev/sdh ou xvdh).
- InstanceId

  Tipo: String

  Descrição: (obrigatório) o ID da instância à qual você deseja associar o volume.
- VolumeId

  Tipo: String

  Descrição: (obrigatório) o ID do volume do Amazon EBS. O volume e a instância devem estar na mesma zona de disponibilidade.

AWSSupport-CalculateEBSPerformanceMetrics

Descrição

O `AWSSupport-CalculateEBSPerformanceMetrics` runbook ajuda a diagnosticar problemas de desempenho do Amazon EBS calculando e publicando métricas de desempenho em um

painel. CloudWatch O painel exibe a média estimada de IOPS e taxa de transferência para um volume alvo do Amazon EBS ou todos os volumes anexados à instância de destino do Amazon Elastic Compute Cloud (Amazon). EC2 Para EC2 instâncias da Amazon, ele também mostra a média de IOPS e a taxa de transferência da instância. O runbook gera o link para o CloudWatch painel recém-criado que exibe as métricas calculadas CloudWatch relevantes. O CloudWatch painel é criado em sua conta com o nome:`AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>`.

Como funciona?

O runbook executa as seguintes etapas:

- Garante que os carimbos de data/hora especificados sejam válidos.
- Valida se o ID do recurso (volume do Amazon EBS ou EC2 instância da Amazon) é válido.
- Quando você fornece um Amazon EC2 como ResourceID, ele cria CloudWatch um painel com o gráfico do IOPS/Throughput for that Amazon EC2 instance and Estimated Average IOPS/ Throughput total real para todos os volumes do Amazon EBS anexados a uma instância da Amazon. EC2
- Quando você fornece um volume do Amazon EBS como um ResourceID, ele cria CloudWatch um painel com gráfico de IOPS/taxa de transferência média estimada para esse volume.
- Depois que o CloudWatch painel for gerado, se a média estimada de IOPS ou a taxa de transferência média estimada for maior que a IOPS máxima ou a taxa de transferência máxima, respectivamente, o microbursting será possível para o volume ou volumes anexados a uma instância da Amazon. EC2

> **Note**
>
> Para volumes intermitentes (gp2, sc2 e st1), as métricas máximas. IOPS/throughput should be consider, until you have burst balance. After burst balance is completely utilized i.e. it becomes zero, consider baseline IOPS/throughput

> **Important**
>
> A criação CloudWatch do painel pode resultar em cobranças extras em sua conta. Para obter mais informações, consulte o guia de CloudWatch preços da Amazon.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Política de amostra

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

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

Instruções

Siga estas etapas para configurar a automação:

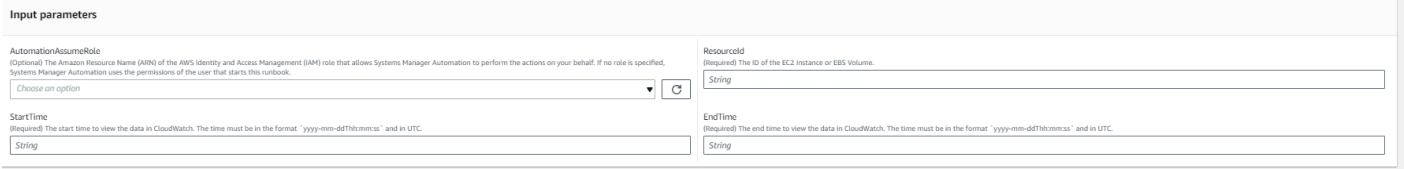
1. Navegue até AWSSupport-CalculateEBSPerformanceMetricsem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - ResourceID (obrigatório):

     O ID da EC2 instância da Amazon ou do volume do Amazon EBS.
   - Hora de início (obrigatório):

     A hora de início para visualizar os dados CloudWatch. A hora deve estar no formato `yyyy-mm-ddThh:mm:ss` e em UTC.
   - Hora de término (obrigatório):

     A hora de término para visualizar os dados CloudWatch. A hora deve estar no formato `yyyy-mm-ddThh:mm:ss` e em UTC.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - CheckResourceIdAndTimeStamps:

     Verifica se a hora de término é maior que a hora de início em pelo menos um minuto e se o recurso fornecido existe.
   - CreateCloudWatchDashboard:

     Calcula o desempenho do Amazon EBS e exibe um gráfico com base no seu ID de recurso. Se você fornecer um ID de volume do Amazon EBS para o parâmetro Resource ID, esse runbook cria um CloudWatch painel com IOPS médio estimado e taxa de transferência média estimada para o volume do Amazon EBS. Se você fornecer uma ID de EC2 instância da Amazon para o parâmetro Resource ID, esse runbook cria um CloudWatch painel com média total de IOPS e taxa de transferência total média para a EC2 instância da Amazon e com média estimada de IOPS e taxa de transferência média estimada para todos os volumes do Amazon EBS anexados à instância da Amazon. EC2
7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

Exemplo de CloudWatch painel para ID de recurso como EC2 instância da Amazon

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

Autosave: Off

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

Aggregated Metrics for EC2 Instance i-[redacted]

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

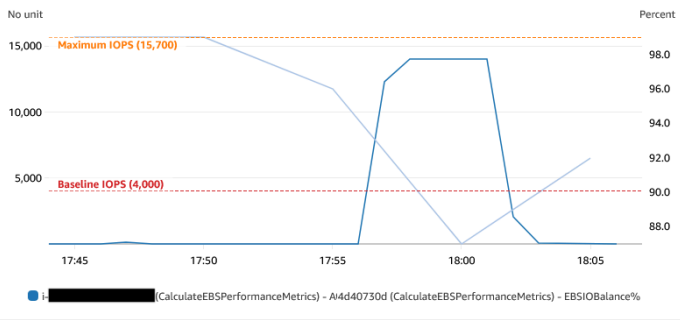
More details on EBS Optimized instances | More details on EBS Volume Types

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

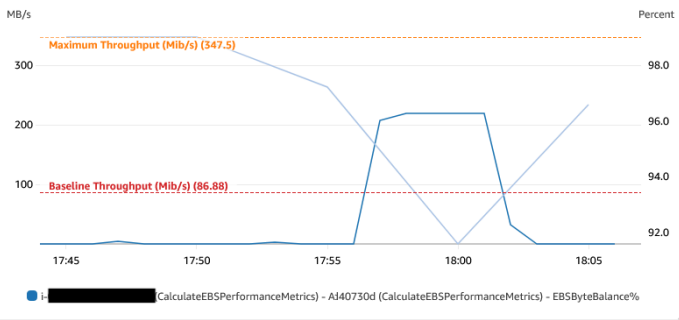
Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	SUM(For All Volumes[(SUM(VolumeReadOps) + SUM(VolumeWriteOps))]) / Period	IOPS
Average Total Throughput	SUM(For All Volumes[(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes))]) / Period / 1024 / 1024	MiB/s

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

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



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



EBS Volume(s) Metrics

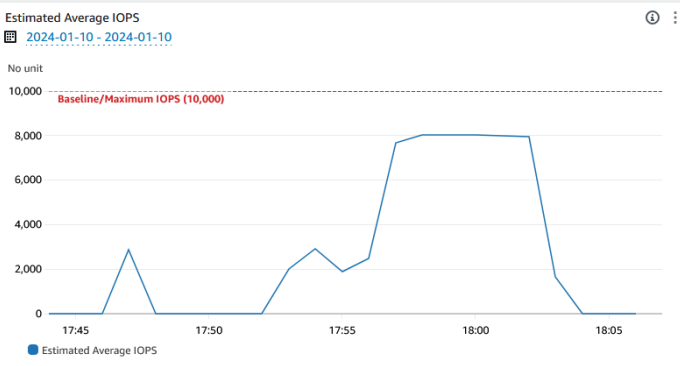
Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	(SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime))	IOPS
Estimated Average Throughput	(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024 / 1024	MiB/s

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

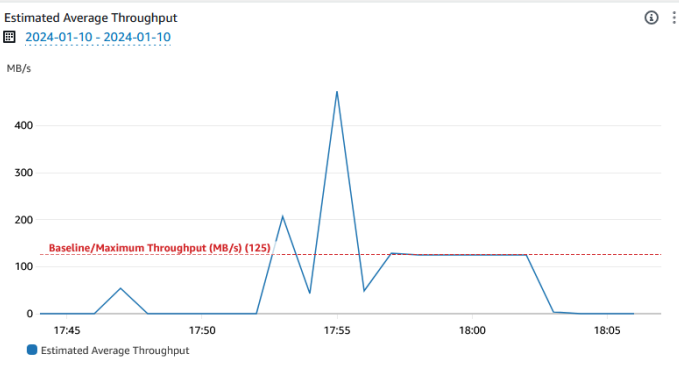
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

Volume: vol[redacted] Type: gp3

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

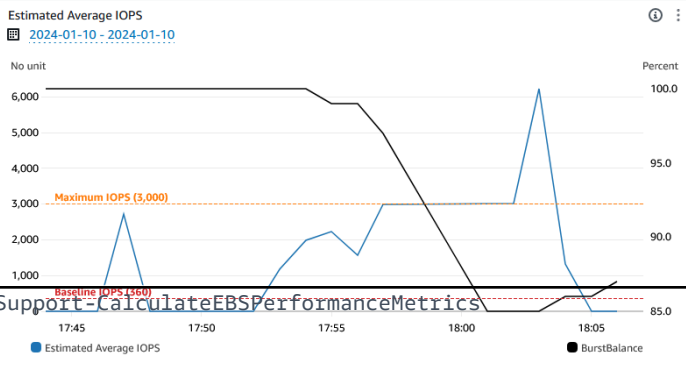


Estimated Average Throughput
2024-01-10 - 2024-01-10

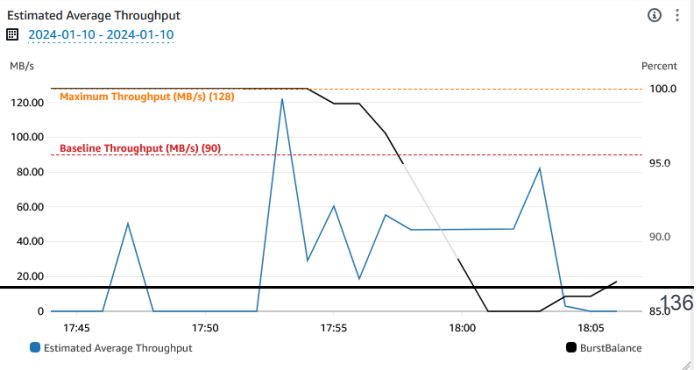


Volume: vol[redacted] | Type: gp2

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



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

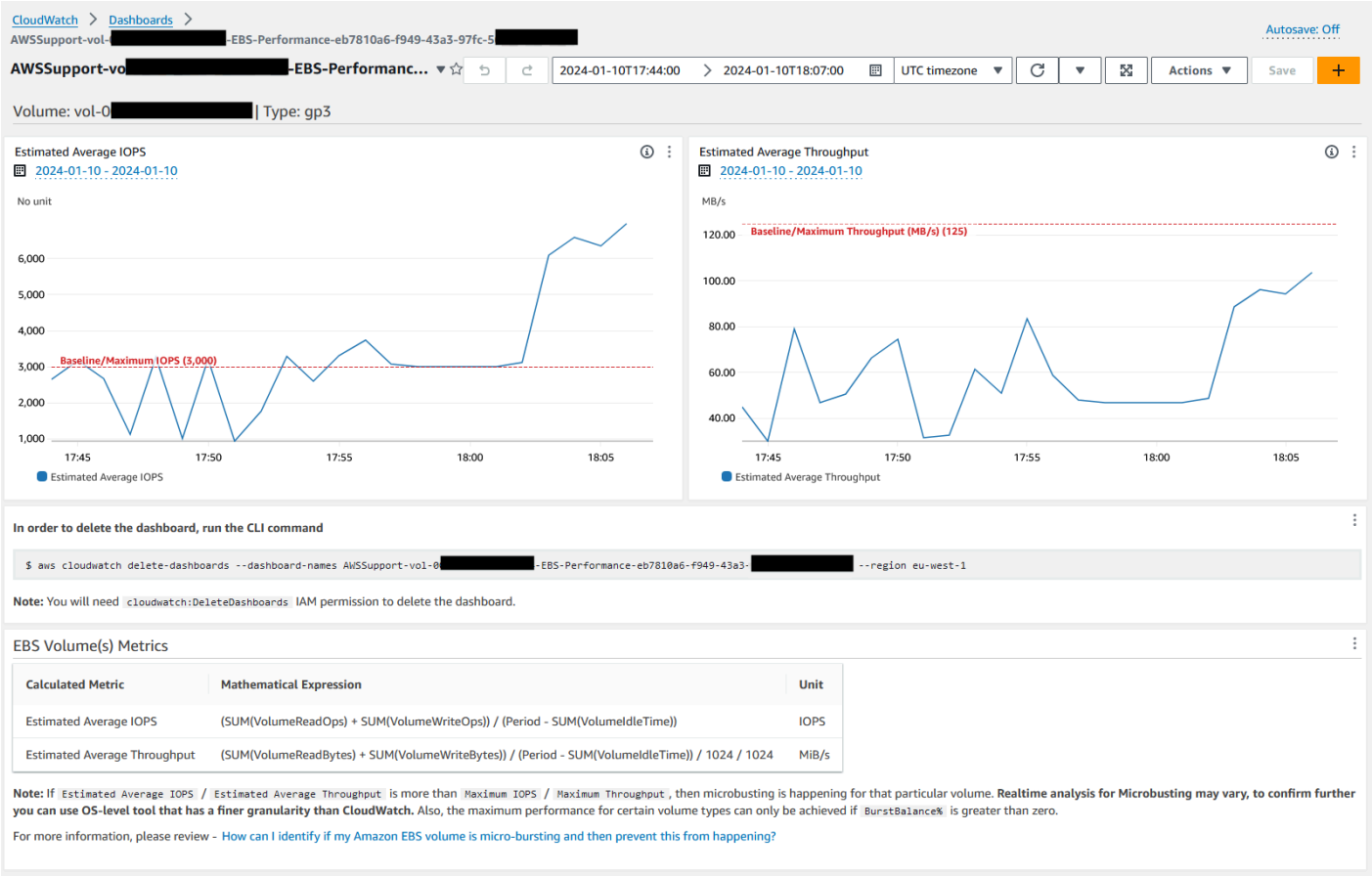


Volume: vol[redacted] | Type: gp3

Estimated Average IOPS

Estimated Average Throughput

Exemplo de CloudWatch painel para ID de recurso como ID de volume do Amazon EBS



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- Como posso identificar se meu volume do Amazon EBS está microestourando e evitar que isso aconteça?
- Como faço CloudWatch para visualizar as métricas agregadas de desempenho do Amazon EBS para uma EC2 instância?

AWS-CopySnapshot

Descrição

Copia um point-in-time snapshot de um volume do Amazon Elastic Block Store (Amazon EBS). Você pode copiar o instantâneo dentro da mesma região Região da AWS ou de uma região para outra. Cópias de snapshots criptografados do Amazon EBS permanecem criptografadas. Cópias de snapshots não criptografados permanecem não criptografadas. Para copiar um snapshot criptografado que foi compartilhado de outra conta, é necessário ter permissões para a chave KMS usada para criptografar o snapshot. Os snapshots criados ao copiar outro snapshot têm um ID arbitrário de volume que não deve ser usado para nenhuma outra finalidade.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Descrição

  Tipo: String

  Descrição: (opcional) uma descrição para o snapshot da Amazon EBS.
- SnapshotId

Tipo: String

Descrição: (obrigatório) o ID do snapshot do Amazon EBS a ser copiado.

- SourceRegion

  Tipo: String

  Descrição: (obrigatório) a região em que o snapshot de origem existe atualmente.

Etapas do documento

copySnapshot: Copia um snapshot de um volume do Amazon EBS.

Saídas

Copiar Snapshot. SnapshotId - O ID do novo instantâneo.

AWS-CreateSnapshot

Descrição

Criar um snapshot de um volume do Amazon EBS.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Descrição

  Tipo: String

  Description: (opcional) uma descrição para o snapshot

- VolumeId

  Tipo: String

  Descrição: (obrigatório) o ID do volume.

AWS-DeleteSnapshot

Descrição

Excluir um snapshot de um volume do Amazon EBS.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- SnapshotId

  Tipo: String

  Descrição: (obrigatório) o ID do snapshot do EBS.

AWSConfigRemediation-DeleteUnusedEBSVolume

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedEBSVolume` exclui um volume não utilizado do Amazon Elastic Block Store (Amazon EBS).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- CreateSnapshot

  Tipo: booliano

  Descrição: (opcional) se configurada como `true`, a automação cria um snapshot do volume do Amazon EBS antes de ser excluído.

- VolumeId

  Tipo: String

  Descrição: (obrigatório) o ID do volume do Amazon EBS que você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: verifica se o volume do Amazon EBS especificado no parâmetro `VolumeId` não está em uso e cria um snapshot dependendo do valor escolhido para o parâmetro `CreateSnapshot`.
- `aws:branch`: ramifica com base no valor escolhido para o parâmetro `CreateSnapshot`.
- `aws:waitForAwsResourceProperty`: aguarda a conclusão do snapshot.
- `aws:executeAwsApi`: exclui o snapshot se a criação do snapshot falhar.
- `aws:executeAwsApi`: exclui o volume do Amazon EBS que foi especificado no parâmetro `VolumeId`.
- `aws:executeScript`: verifica se o volume do Amazon EBS foi excluído.

AWS-DeregisterAMIs

Descrição

O runbook `AWS-DeregisterAMIs` ajuda a cancelar o registro de Amazon Machine Images (AMIs) especificando a tag que foi aplicada ao AMIs.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DryRun

  Tipo: String

  Valores válidos: sim | não

  Descrição: (obrigatório) verifica se você tem as permissões necessárias para a ação, sem realmente fazer a solicitação, e fornece uma resposta de erro.
- RetainNumber

  Tipo: String

Descrição: (opcional) o número de AMIs que você deseja reter. Não especifique um valor para esse parâmetro se foi especificado um valor para `Age`.

- Idade

  Tipo: String

  Descrição: (opcional) o número de dias anteriores de AMIs que você deseja reter. Não especifique um valor para esse parâmetro se foi especificado um valor para `RetainNumber`.

- TagKey

  Tipo: String

  Descrição: (obrigatório) a chave da tag atribuída às AMIs cujo registro você deseja cancelar.

- TagValue

  Tipo: String

  Descrição: (obrigatório) o valor da tag atribuída às AMIs cujo registro você deseja cancelar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: valida os valores especificados para os parâmetros de entrada do runbook.
- `aws:executeAwsApi` :cancela o log de AMIs usando a tag que foi especificada usando os parâmetros `TagKey` e `TagValue`.

AWS-DetachEBSVolume

Descrição

Separe um volume do Amazon EBS de uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LambdaAssumeRole

  Tipo: String

  Descrição: (opcional) o ARN da função assumida pelo lambda
- VolumeId

  Tipo: String

  Descrição: (obrigatório) o ID do volume do EBS. O volume e a instância devem estar na mesma zona de disponibilidade

AWSConfigRemediation-EnableEbsEncryptionByDefault

Descrição

O `AWSConfigRemediation-EnableEbsEncryptionByDefault` runbook permite a criptografia em todos os novos volumes do Amazon Elastic Block Store (Amazon EBS) no Amazon Elastic Block Store (Amazon EBS) Conta da AWS e Região da AWS onde você executa a automação. Os volumes criados antes de executar a automação não são criptografados.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeAwsApi`: habilita a definição padrão de criptografia do Amazon EBS na conta atual e na região.
- `aws:assertAwsResourceProperty`: verifica se a definição padrão de criptografia do Amazon EBS foi habilitada.

AWS-ExtendEbsVolume

Descrição

O runbook `AWS-ExtendEbsVolume` aumenta o tamanho de um volume do Amazon EBS e estende o sistema de arquivos. Essa automação oferece suporte aos sistemas de arquivos `xfs` e `ext4`.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DriveLetter

  Tipo: String

  Descrição: (opcional) a letra da unidade cujo sistema de arquivos você deseja estender. Esse parâmetro é obrigatório para instâncias do Windows.

- InstanceId

  Tipo: String

  Descrição: (Opcional) O ID da EC2 instância da Amazon à qual o volume do Amazon EBS que você deseja estender está anexado.

- KeepSnapshot

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (opcional) define se o snapshot criado deve ser mantido antes de aumentar o tamanho do volume do Amazon EBS.

- MountPoint

  Tipo: String

  Descrição: (opcional) O ponto de montagem da unidade cujo sistema de arquivos você deseja estender. Esse parâmetro é necessário para instâncias do Linux.

- SizeGib

  Tipo: String

  Descrição: (obrigatório) O tamanho em GiB para o qual deseja modificar seu volume do Amazon EBS.

- VolumeId

  Tipo: String

  Descrição: (obrigatório) O ID do volume do EBS que você deseja estender.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

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

Etapas do documento

- `aws:executeScript` :Aumenta o tamanho do volume até o valor especificado no parâmetro do `VolumeId` e estende o sistema de arquivos.

AWSSupport-ModifyEBSSnapshotPermission

Descrição

O runbook `AWSSupport-ModifyEBSSnapshotPermission` ajuda a modificar permissões para vários snapshots do Amazon Elastic Block Store (Amazon EBS). Usando este runbook, você pode criar snapshots `Public` ou `Private` e compartilhá-los com outras Contas da AWS. Os snapshots criptografados com uma chave KMS padrão não podem ser compartilhados com outras contas usando este runbook.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- AccountIds

  Tipo: StringList

  Padrão: nenhum

  Descrição: (Opcional) A IDs das contas com as quais você deseja compartilhar instantâneos. Esse parâmetro será necessário se um valor `No` for especificado para o parâmetro `Private`.

- AccountPermissionOperation

  Tipo: String

  Valores válidos: add | remove

  Padrão: nenhum

  Descrição: (opcional) O tipo de operação a ser executada.

- Privado

  Tipo: String

  Valores válidos: sim | não

  Descrição: (obrigatório) Insira o valor `No` se quiser compartilhar snapshots com contas específicas.

- SnapshotIds

  Tipo: StringList

  Descrição: (Obrigatório) Os snapshots IDs do Amazon EBS cuja permissão você deseja modificar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`

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

Etapas do documento

1. `aws:executeScript`- Verifica IDs os instantâneos fornecidos no `SnapshotIds` parâmetro. Depois de verificar o IDs, o script verifica se há instantâneos criptografados e gera uma lista, se alguma for encontrada.
2. `aws:branch` :Ramifica a automação com base no valor inserido para o parâmetro `Private`.
3. `aws:executeScript` :Modifica as permissões dos snapshots especificados para compartilhá-los com as contas especificadas.
4. `aws:executeScript` :Modifica as permissões dos snapshots para alterá-los de `Public` para `Private`.

Saídas

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Resultado

MakePrivate.Resultado

MakePrivate.Comandos

`AWSConfigRemediation-ModifyEBSVolumeType`

Descrição

O runbook `AWSConfigRemediation-ModifyEBSVolumeType` modifica o tipo de volume do Amazon Elastic Block Store (Amazon EBS). Depois que o tipo de volume é modificado, o volume entra no estado `optimizing`. Para obter informações sobre o monitoramento do progresso das modificações de volume, consulte Monitorar o progresso das modificações de volume no Guia EC2 do usuário da Amazon.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- EbsVolumeId

  Tipo: String

  Descrição: (obrigatório) O ID do volume do Amazon EBS que deseja modificar.
- EbsVolumeType

  Tipo: String

  Valores válidos: standart | io1 | io2 | gp2 | gp3 | sc1 | st1

  Descrição: O tipo de volume para o qual deseja alterar o volume do Amazon EBS. Para obter informações sobre os tipos de volume do Amazon EBS, consulte os tipos de volume do Amazon EBS no Guia EC2 do usuário da Amazon.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `ec2:ModifyVolume`

Etapas do documento

- `aws:waitForAwsResourceProperty` :Verifica se o estado do volume é `available` ou `in-use`.
- `aws:executeAwsApi` :Modifica o volume do Amazon EBS especificado no parâmetro de `EbsVolumeId`.
- `aws:waitForAwsResourceProperty` :Verifica se o tipo do volume foi alterado para o valor especificado no parâmetro de `EbsVolumeType`.

Amazon EC2

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic Compute Cloud. Os runbooks do Amazon Elastic Block Store estão localizados na seção Amazon EBS de referência do runbook. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-ASGEnterStandby
- AWS-ASGExitStandby
- AWS-CreateImage
- AWS-DeleteImage
- AWS-PatchAsgInstance
- AWS-PatchInstanceWithRollback
- AWS-QuarantineEC2Instance
- AWS-ResizeInstance
- AWS-RestartEC2Instance
- AWS-SetupJupyter
- AWS-StartEC2Instance
- AWS-StopEC2Instance
- AWS-TerminateEC2Instance

- AWS-UpdateLinuxAmi
- AWS-UpdateWindowsAmi
- AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck
- AWSConfigRemediation-EnforceEC2InstanceIMDSv2
- AWSEC2-CloneInstanceAndUpgradeSQLServer
- AWSEC2-CloneInstanceAndUpgradeWindows
- AWSEC2-ConfigureSTIG
- AWSEC2-PatchLoadBalancerInstance
- AWSEC2-SQLServerDBRestore
- AWSSupport-ActivateWindowsWithAmazonLicense
- AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2
- AWSPremiumSupport-ChangeInstanceTypeIntelToAMD
- AWSSupport-CheckXenToNitroMigrationRequirements
- AWSSupport-ConfigureEC2Metadata
- AWSSupport-ContainEC2Instance
- AWSSupport-CopyEC2Instance
- AWSSupport-EnableWindowsEC2SerialConsole
- AWSSupport-ExecuteEC2Rescue
- AWSSupport-ListEC2Resources
- AWSSupport-ManageRDPSettings
- AWSSupport-ManageWindowsService
- AWSSupport-MigrateEC2ClassicToVPC
- AWSSupport-MigrateXenToNitroLinux
- AWSSupport-ResetAccess
- AWSSupport-ResetLinuxUserPassword
- AWSPremiumSupport-ResizeNitroInstance
- AWSSupport-RestoreEC2InstanceFromSnapshot
- AWSSupport-SendLogBundleToS3Bucket
- AWSSupport-StartEC2RescueWorkflow
- AWSPremiumSupport-TroubleshootEC2DiskUsage

- AWSSupport-TroubleshootEC2InstanceConnect
- AWSSupport-TroubleshootLinuxMGNDRSAgentLogs
- AWSSupport-TroubleshootRDP
- AWSSupport-TroubleshootSSH
- AWSSupport-TroubleshootSUSERegistration
- AWSSupport-TroubleshootWindowsPerformance
- AWSSupport-TroubleshootWindowsUpdate
- AWSSupport-UpgradeWindowsAWSDrivers

AWS-ASGEnterStandby

Descrição

Altere o estado de espera de uma instância do Amazon Elastic Compute Cloud EC2 (Amazon) em um grupo de Auto Scaling.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: string

  Descrição: ID (obrigatório) de uma EC2 instância da Amazon para a qual você deseja alterar o estado de espera em um grupo de Auto Scaling.

- LambdaRoleArn

  Tipo: string

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.

AWS-ASGExitStandby

Descrição

Altere o estado de espera de uma instância do Amazon Elastic Compute Cloud EC2 (Amazon) em um grupo de Auto Scaling.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: string

  Descrição: (Obrigatório) ID de uma EC2 instância para a qual você deseja alterar o estado de espera em um grupo de Auto Scaling.

- LambdaRoleArn

  Tipo: string

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.

AWS-CreateImage

Descrição

Crie um novo Amazon Machine Image (AMI) de uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância.

- NoReboot

  Tipo: booliano

  Descrição: (opcional) Não reinicialize a instância antes de criar a imagem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage",
                "ec2:DescribeImages"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS-DeleteImage

Descrição

Excluir um Amazon Machine Image (AMI) e todos os instantâneos associados.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ImageId

  Tipo: string

  Descrição: (obrigatório) O ID do AMI.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

```
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeImages",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeregisterImage",
            "Resource": "*"
        }
    ]
}
```

AWS-PatchAsgInstance

Descrição

Corrija instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um grupo de Auto Scaling.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: string

  Descrição: (obrigatório) o ID da instância onde o patch será aplicado. Não especifique um ID de instância que está configurado para ser executado durante uma janela de manutenção.

- LambdaRoleArn

  Tipo: string

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função do Lambda.

- WaitForInstance

  Tipo: string

  Padrão: PT2 M

  Descrição: (opcional) duração que a Automação deve dormir para permitir que a instância volte ao serviço.

- WaitForReboot

  Tipo: string

  Padrão: PT5 M

  Descrição: (opcional) duração que a Automação deve dormir para permitir que uma instância com patch reinicialize.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Descrição

Coloca uma EC2 instância em conformidade com a linha de base do patch aplicável. Reverte o volume raiz em caso de falha.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (Obrigatório) EC2 InstanceId à qual aplicamos a linha de base do patch.
- LambdaAssumeRole

  Tipo: string

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.
- ReportS3Bucket

  Tipo: string

  Descrição: (opcional) destino de bucket do Amazon S3 para o relatório de conformidade gerado durante o processo.

Etapas do documento

Número da etapa	Nome da etapa	Ação de Automação
1	createDocumentStack	`aws:createStack`

Número da etapa	Nome da etapa	Ação de Automação
2	IdentifyRootVolume	`aws:invokeLambdaFunction`
3	PrePatchSnapshot	`aws:executeAutomation`
4	installMissingUpdates	`aws:runCommand`
5	SleepThruInstallation	`aws:invokeLambdaFunction`
6	CheckCompliance	`aws:invokeLambdaFunction`
7	SaveComplianceReportToS3	`aws:invokeLambdaFunction`
8	ReportSuccessOrFailure	`aws:invokeLambdaFunction`
9	RestoreFromSnapshot	`aws:invokeLambdaFunction`
10	DeleteSnapshot	`aws:invokeLambdaFunction`
11	deleteCloudFormationModelo	`aws:deleteStack`

Saídas

IdentifyRootVolume.Carga útil

PrePatchSnapshot.Saída

SaveComplianceReportToS3. Carga útil

RestoreFromSnapshot.Carga útil

CheckCompliance.Carga útil

AWS-QuarantineEC2Instance

Descrição

Com o `AWS-QuarantineEC2Instance` runbook, você pode atribuir um grupo de segurança a uma instância do Amazon Elastic Compute Cloud EC2 (Amazon) que não permite nenhum tráfego de entrada ou saída.

> **Important**
>
> As alterações nas configurações do RDP devem ser cuidadosamente analisadas antes de executar este runbook.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

Descrição: (Obrigatório) O ID da instância gerenciada para gerenciar as configurações de RDP.

- IsolationSecurityGroup

  Tipo: string

  Descrição: (obrigatório) o nome do grupo de segurança que você deseja atribuir à instância para evitar tráfego de entrada ou saída.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `autoscaling:DescribeAutoScalingInstances`
- `autoscaling:DetachInstances`
- `ec2:CreateSecurityGroup`
- `ec2:CreateSnapshot`
- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSnapshots`
- `ec2:ModifyInstanceAttribute`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Etapas do documento

- `aws:executeAwsApi`: reúne detalhes sobre a instância.
- `aws:executeScript`: verifica se a instância não faz parte de um grupo do Auto Scaling.
- `aws:executeAwsApi`: cria um snapshot do novo volume raiz anexado à instância.
- `aws:waitForAwsResourceProperty`: espera que o estado do instantâneo seja `completed`.
- `aws:executeAwsApi`: atribui o grupo de segurança especificado no parâmetro `IsolationSecurityGroup` à sua instância.

Saídas

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

AWS-ResizeInstance

Descrição

Altere o tipo de instância de uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: String

  Descrição: (obrigatório) O ID da instância.

- InstanceType

  Tipo: String

  Descrição: (obrigatório) O tipo de instância.

AWS-RestartEC2Instance

Descrição

Reinicie uma ou mais instâncias do Amazon Elastic Compute Cloud (Amazon EC2).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: StringList

  Descrição: (Obrigatório) A IDs das EC2 instâncias da Amazon a serem reiniciadas.

AWS-SetupJupyter

Descrição

O `AWS-SetupJupyter` runbook ajuda você a configurar o Jupyter Notebook em uma instância do Amazon Elastic Compute Cloud (Amazon). EC2 Você pode especificar uma instância existente ou fornecer uma Amazon Machine Image (AMI) ID da automação para iniciar e configurar uma nova instância. Antes de começar, é necessário criar um parâmetro `SecureString` no repositório de parâmetros para usar como senha do caderno Jupyter. O Parameter Store é uma ferramenta em AWS Systems Manager. Para obter mais informações sobre criação de parâmetro, consulte Criação de parâmetros no Guia do usuário do AWS Systems Manager .

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AmiId

  Tipo: string

  Descrição: (Opcional) O ID do AMI que você deseja usar para iniciar uma nova instância e configurar o Jupyter Notebook.

- InstanceId

  Tipo: string

  Descrição: (obrigatório) o ID da instância do caderno Jupyter que você deseja reinicializar.

- InstanceType

  Tipo: string

  Padrão: t3.medium

  Descrição: (opcional) se você estiver iniciando uma nova instância para configurar o caderno Jupyter, especifique o tipo de instância que deseja usar.

- JupyterPasswordSSMKey

  Tipo: string

  Descrição: (obrigatório) o nome do parâmetro `SecureString` no repositório de parâmetros que você deseja usar como senha para o caderno Jupyter.

- KeyPairName

  Tipo: string

  Descrição: (opcional) o par de chaves que você deseja associar à instância recém-iniciada.

- RemoteAccessCidr

  Tipo: string

  Padrão: 0.0.0.0/0

  Descrição: (opcional) o intervalo CIDR do qual você deseja permitir o tráfego SSH.

- RoleName

  Tipo: string

  Padrão: SSMManaged InstanceProfileRole

  Descrição: (opcional) o nome do perfil da instância recém-iniciada.

- StackName

  Tipo: string

Padrão: CreateManagedInstanceStack {{automation:execution_id}}

Descrição: (Opcional) O nome da AWS CloudFormation pilha que você deseja que a automação use.

- SubnetId

  Tipo: string

  Padrão: Default

  Descrição: (opcional) a sub-rede na qual você deseja iniciar a nova instância para usar.

- VpcId

  Tipo: string

  Padrão: Default

  Descrição: (opcional) o ID da nuvem privada virtual (VPC) na qual você deseja iniciar a nova instância.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:executeScript`: configura o caderno Jupyter na instância especificada ou em uma instância recém-lançada, usando os valores que você especifica para os parâmetros de entrada do runbook.

AWS-StartEC2Instance

Descrição

Inicie uma ou mais instâncias do Amazon Elastic Compute Cloud (Amazon EC2).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: StringList

  Descrição: EC2 instâncias (obrigatórias) para iniciar.

AWS-StopEC2Instance

Descrição

Interrompe uma ou mais instâncias do Amazon Elastic Compute Cloud (Amazon EC2).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: StringList

  Descrição: EC2 instâncias (obrigatórias) a serem interrompidas.

AWS-TerminateEC2Instance

Descrição

Encerre uma ou mais instâncias do Amazon Elastic Compute Cloud EC2 (Amazon).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: StringList

  Descrição: (Obrigatório) IDs de uma ou mais EC2 instâncias a serem encerradas.

AWS-UpdateLinuxAmi

Descrição

Atualizar um Amazon Machine Image (AMI) com pacotes de distribuição Linux e software Amazon.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ExcludePackages

  Tipo: string

  Padrão: nenhum

Descrição: (Opcional) Nomes de pacotes para evitar atualizações, em todas as condições. Por padrão ("none"), nenhum pacote é excluído.

- IamInstanceProfileName

  Tipo: string

  Padrão: ManagedInstanceProfile

  Descrição: (obrigatório) o nome do perfil de instância que permite que o Systems Manager gerencie a instância.

- IncludePackages

  Tipo: string

  Padrão: all

  Descrição: (Opcional) Somente atualiza esses pacotes nomeados. Por padrão ("all"), todas as atualizações disponíveis são aplicadas.

- InstanceType

  Tipo: string

  Padrão: t2.micro

  Descrição: (Opcional) O tipo de instância a ser executada como o host do espaço de trabalho. Os tipos de instância variam de acordo com a região.

- MetadataOptions

  Tipo: StringMap

  Padrão: {” HttpEndpoint “: “ativado”, "HttpTokens“: “opcional"}

  Descrição: (opcional) as opções de metadados para a instância. Para obter mais informações, consulte InstanceMetadataOptionsRequest.

- PostUpdateScript

  Tipo: string

  Padrão: nenhum

Descrição: (Opcional) URL de um script a ser executado depois de as atualizações de pacote serem aplicadas. O padrão ("none") é não executar um script.

- PreUpdateScript

  Tipo: string

  Padrão: nenhum

  Descrição: (Opcional) A URL de um script a ser executado antes de as atualizações serem aplicadas. O padrão ("none") é não executar um script.

- SecurityGroupIds

  Tipo: string

  Descrição: (Obrigatório) Uma lista separada por vírgulas IDs dos grupos de segurança que você deseja aplicar ao AMI.

- SourceAmiId

  Tipo: string

  Descrição: (Obrigatório) O ID de Imagem de máquina da Amazon de origem.

- SubnetId

  Tipo: string

  Descrição: (opcional) o ID da sub-rede na qual você deseja iniciar a instância. Se você excluiu sua VPC padrão, esse parâmetro é obrigatório.

- TargetAmiName

  Tipo: string

  Padrão: UpdateLinuxAmi _from_ {{SourceAmiId}} _on_ {{global:date_time}}

  Descrição: (Opcional) O nome da nova AMI que será criada. O padrão é uma string gerada pelo sistema que inclui o ID da AMI de origem, bem como a data e a hora de criação.

AWS-UpdateWindowsAmi

Descrição

Atualizar um Microsoft Windows Amazon Machine Image (AMI). Por padrão, esse runbook instala todas as atualizações do Windows, o software da Amazon e os drivers da Amazon. Depois, ele executa o Sysprep para criar uma nova AMI. Compatível com Windows Server 2008 R2 ou posterior.

> **Important**
>
> Se suas instâncias se conectarem AWS Systems Manager usando VPC endpoints, esse runbook falhará, a menos que seja usado na região us-east-1. As instâncias devem ter o TLS 1.2 ativado para usar esse runbook.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Categorias

  Tipo: string

  Descrição: (opcional) especifique uma ou mais categorias de atualização. Você pode filtrar categorias usando valores separados por vírgulas. Opções: Aplicativo, Conectores, CriticalUpdates, DefinitionUpdates DeveloperKits, Drivers, OrientaçãoFeaturePacks, Microsoft,,

SecurityUpdates ServicePacks, FerramentasUpdateRollups, Atualizações. Os formatos válidos incluem uma única entrada, por exemplo:CriticalUpdates. Ou você pode especificar uma lista separada por vírgulas:CriticalUpdates,SecurityUpdates. NOTA: Não pode haver nenhum espaço em torno do vírgulas.

- ExcludeKbs

  Tipo: string

  Descrição: (Opcional) Especifique um ou mais artigos da Base de Conhecimento da Microsoft (KB) IDs a serem excluídos. Você pode excluir vários IDs usando valores separados por vírgula. Formatos válidos: KB9876543 ou 9876543.

- IamInstanceProfileName

  Tipo: string

  Padrão: ManagedInstanceProfile

  Descrição: (obrigatório) o nome da função que permite que o Systems Manager gerencie a instância.

- IncludeKbs

  Tipo: string

  Descrição: (Opcional) Especifique um ou mais artigos da Base de Conhecimento da Microsoft (KB) IDs a serem incluídos. Você pode instalar vários IDs usando valores separados por vírgula. Formatos válidos: KB9876543 ou 9876543.

- InstanceType

  Tipo: string

  Padrão: t2.medium

  Descrição: (Opcional) O tipo de instância a ser executada como o host do espaço de trabalho. Os tipos de instância variam de acordo com a região. O padrão é t2.medium.

- MetadataOptions

  Tipo: StringMap

  Padrão: {” HttpEndpoint “: “ativado”, "HttpTokens“: “opcional"}

Descrição: (opcional) as opções de metadados para a instância. Para obter mais informações, consulte InstanceMetadataOptionsRequest.

- PostUpdateScript

  Tipo: string

  Descrição: (Opcional) Um script fornecido como string. Ele será executado após a instalação das atualizações do sistema operacional.

- PreUpdateScript

  Tipo: string

  Descrição: (Opcional) Um script fornecido como string. Ele será executado antes da instalação de atualizações do sistema operacional.

- PublishedDateAfter

  Tipo: string

  Descrição: (Opcional) Especifique a data depois da qual as atualizações devem ser publicadas. Por exemplo, se 01/01/2017 for especificado, todas as atualizações que foram encontrados durante a pesquisa do Windows Update que foram publicadas em ou depois de 01/01/2017 será retornado.

- PublishedDateBefore

  Tipo: string

  Descrição: (Opcional) Especifique a data antes da qual as atualizações devem ser publicadas. Por exemplo, se 01/01/2017 for especificado, todas as atualizações que foram encontradas durante a pesquisa do Windows Update que foram publicadas em ou antes de 01/01/2017 serão retornadas.

- PublishedDaysOld

  Tipo: string

  Descrição: (Opcional) Especifique a quantidade de dias que as atualizações devem ter a partir da data publicada. Por exemplo, se 10 for especificado, todas as atualizações que foram encontradas durante a pesquisa do Windows Update que foram publicadas 10 ou mais dias atrás serão retornadas.

- SecurityGroupIds

Tipo: string

Descrição: (Obrigatório) Uma lista separada por vírgulas IDs dos grupos de segurança que você deseja aplicar ao AMI.

- SeverityLevels

  Tipo: string

  Descrição: (Opcional) Especifique um ou mais níveis de gravidade MSRC associados a uma atualização. Você pode filtrar os níveis de gravidade usando valores separados por vírgulas. Por padrão, patches para todos os níveis de segurança são selecionados. Se o valor for fornecido, a lista de atualização será filtrada por esses valores. Opções: Crítica, Importante, Baixa, Moderada ou Não especificada. Os formatos válidos incluem uma única entrada, por exemplo: Crítica. Como alternativa, você pode especificar uma lista separada por vírgulas: Crítica, Importante, Baixa.

- SourceAmiId

  Tipo: string

  Descrição: (Obrigatório) A fonte AMI IDENTIFICAÇÃO.

- SubnetId

  Tipo: string

  Descrição: (opcional) o ID da sub-rede na qual você deseja iniciar a instância. Se você excluiu sua VPC padrão, esse parâmetro é obrigatório.

- TargetAmiName

  Tipo: string

  Padrão: UpdateWindowsAmi _from_ {{SourceAmiId}} _on_ {{global:date_time}}

  Descrição: (Opcional) O nome da nova AMI que será criada. O padrão é uma string gerada pelo sistema que inclui o ID da AMI de origem, bem como a data e a hora de criação.

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

Descrição

O `AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck` runbook permite verificações de saúde para o grupo Amazon EC2 Auto Scaling (Auto Scaling) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- AutoScalingGroupARN

  Tipo: string

  Descrição: (obrigatório) o nome do recurso da Amazon (ARN) do grupo do Auto Scaling em que você deseja ativar as verificações de integridade.
- HealthCheckGracePeriod

  Tipo: inteiro

  Padrão: 300

  Descrição: (Opcional) A quantidade de tempo, em segundos, que o Auto Scaling espera antes de verificar o status de saúde de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que entrou em serviço.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`: ativa verificações de integridade no grupo do Auto Scaling que você especifica no parâmetro `AutoScalingGroupARN`.

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

Descrição

O `AWSConfigRemediation-EnforceEC2InstanceIMDSv2` runbook exige que a instância do Amazon Elastic Compute Cloud EC2 (Amazon) especificada por você use o Instance Metadata Service versão 2 (). IMDSv2

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- InstanceId

Tipo: string

Descrição: (Obrigatório) O ID da EC2 instância da Amazon que você deseja usar IMDSv2.

- AutomationAssumeRole

  Tipo: string

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- HttpPutResponseHopLimit

  Tipo: inteiro

  Descrição: (Opcional) O limite de resposta do Hop do serviço IMDS de volta ao solicitante. Defina como 2 ou mais para EC2 instâncias que hospedam contêineres. Defina como 0 para não mudar (Padrão).

  Padrão permitido: `^([1-5]?\d|6[0-4])$`

  Padrão: 0

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Define a `HttpTokens` opção como `required` na EC2 instância da Amazon que você especifica no `InstanceId` parâmetro.
- `aws:assertAwsResourceProperty`- Verifica se IMDSv2 é necessário na EC2 instância da Amazon.

AWSEC2-CloneInstanceAndUpgradeSQLServer

Descrição

Crie um AMI de uma EC2 instância para Windows Server executando o SQL Server 2008 ou posterior e, em seguida, atualize a AMI para uma versão posterior do SQL Server. Somente as versões em inglês do SQL Server são suportadas.

Os caminhos de atualização com suporte são os seguintes:

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

Se você estiver usando uma versão anterior do Windows Server que é incompatível com o SQL Server 2019, o documento de automação deve atualizar sua versão do Windows Server para 2016.

A atualização é um processo de várias etapas que pode levar 2 horas para ser concluído. A automação cria a AMI a partir da instância e, em seguida, executa uma instância temporária a partir da nova AMI no especificado`SubnetID`. Os grupos de segurança associados à instância original são aplicados à instância temporária. O automação executa uma atualização in-loco para a `TargetSQLVersion` na instância temporária. Após a atualização, a automação cria um novo AMI da instância temporária e, em seguida, encerra a instância temporária.

Você pode testar a funcionalidade do aplicativo lançando o novo AMI na sua VPC. Depois de concluir o teste e antes de executar outra atualização, programe o tempo de inatividade do aplicativo antes de mudar completamente para a instância atualizada.

> **Note**
>
> Se você quiser modificar o nome do computador da EC2 instância executada a partir do novo AMI , consulte Renomear um computador que hospeda uma instância autônoma do SQL Server.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Pré-requisitos

- TLS versão 1.2.
- Somente as versões em inglês do SQL Server são suportadas.
- A EC2 instância deve usar uma versão do Windows Server isso é Windows Server 2008 R2 (ou posterior) e SQL Server 2008 (ou posterior).
- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Instalação e configuração do SSM Agent em EC2 instâncias do Windows Server.
- Configure a instância para usar uma função de perfil de instância AWS Identity and Access Management (IAM). Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager.
- Verifique se a instância tem 20 GB de espaço livre em disco no disco de inicialização da instância.
- Para instâncias que usam uma versão Traga sua própria licença (BYOL) do SQL Server, os seguintes pré-requisitos adicionais se aplicam:
  - Forneça um ID de snapshot do EBS que inclua a mídia de instalação do SQL Server. Para fazer isso:

    1. Verifique se a EC2 instância está executando o Windows Server 2008 R2 ou posterior.
    2. Crie um volume do EBS de 6 GB na mesma zona de disponibilidade em que a instância está sendo executada. Associe o volume à instância. Instale-a, por exemplo, como unidade D.
    3. Clique com o botão direito do mouse no ISO e instale-o a uma instância como, por exemplo, unidade E.
    4. Copie o conteúdo do ISO da unidade E:\ para a unidade D:\

5. Crie um snapshot do EBS do volume de 6 GB criado na etapa 2.

Limitações

- A atualização só pode ser realizada em um SQL Server usando a autenticação do Windows.
- Verifique se há atualizações de patch de segurança pendentes nas instâncias. Abra Control Panel (Painel de controle) e, em seguida, escolha Check for updates (Verificar atualizações).
- Implantações do SQL Server no modo HA e espelhamento não são compatíveis.

Parâmetros

- IamInstanceProfile

  Tipo: string

  Descrição: (obrigatório) o perfil de instância do IAM.
- InstanceId

  Tipo: string

  Descrição: (Obrigatório) A instância em execução Windows Server 2008 R2 (ou posterior) e SQL Server 2008 (ou posterior).
- KeepPreUpgradeImageBackUp

  Tipo: string

  Descrição: (opcional) se definido como `true`, a automação não excluirá a AMI criada da instância antes da atualização. Se definida como `true`, você deverá excluir a AMI. Por padrão, a AMI é excluída.
- SubnetId

  Tipo: string

  Descrição: (obrigatório) Forneça uma sub-rede para o processo de atualização. Verifique se a sub-rede tem conectividade de saída com AWS serviços, Amazon S3 e Microsoft (para baixar patches).
- SQLServerSnapshotId

  Tipo: string

Descrição: (condicional) ID do snapshot da mídia de instalação do SQL Server. Esse parâmetro é necessário para instâncias que usam uma versão BYOL do SQL Server. Esse parâmetro é opcional para instâncias incluídas na licença do SQL Server (instâncias lançadas usando uma AWS Amazon Machine Image fornecida para Windows Server com Microsoft SQL Server).

- RebootInstanceBeforeTakingImage

  Tipo: string

  Descrição: (opcional) se definido como `true`, a automação reinicializará a instância antes de criar uma AMI de pré-atualização. Por padrão, a automação não reinicializa antes da atualização.

- Alvo SQLVersion

  Tipo: string

  Descrição: (opcional) selecione a versão do servidor SQL de destino.

  Destinos possíveis:

  - SQL Server 2019
  - SQL Server 2017
  - SQL Server 2016
  - SQL Server 2014

  Destino padrão: SQL Server 2016

Saídas

AMIId: o ID da AMI criada a partir da instância que foi atualizada para uma versão posterior do SQL Server.

AWSEC2-CloneInstanceAndUpgradeWindows

Descrição

Crie um Amazon Machine Image (AMI) de um Windows Server Instância 2008 R2, 2012 R2, 2016 ou 2019 e, em seguida, atualize a AMI com Windows Server 2016, 2019 ou 2022. Os caminhos de atualização com suporte são os seguintes.

- Windows Server 2008 R2 a Windows Server 2016.

- Windows Server 2012 R2 até Windows Server 2016.
- Windows Server 2012 R2 até Windows Server 2019.
- Windows Server 2012 R2 até Windows Server 2022.
- Windows Server 2016 a Windows Server 2019.
- Windows Server 2016 a Windows Server 2022.
- Windows Server 2019 a Windows Server 2022.

A operação de atualização é um processo de várias etapas que pode levar 2 horas para ser concluído. Recomendamos realizar uma atualização do sistema operacional em instâncias com pelo menos 2 v CPUs e 4 GB de RAM. A automação cria uma AMI a partir da instância e depois executa uma instância temporária na AMI recém-criada no `SubnetId` especificado. Os grupos de segurança associados à instância original são aplicados à instância temporária. O automação executa uma atualização in-loco para a `TargetWindowsVersion` na instância temporária. Para atualizar seu Windows Server Instância 2008 R2 para Windows Server Em 2016, 2019 ou 2022, uma atualização no local é realizada duas vezes devido à atualização direta Windows Server 2008 R2 a Windows Server 2016, 2019 ou 2022 não são compatíveis. A automação também atualiza ou instala os drivers da AWS exigidos pela instância temporária. Após a atualização, a automação cria uma nova AMI na instância temporária e encerra a instância temporária.

Você pode testar a funcionalidade do aplicativo iniciando uma instância de teste na AMI atualizada em sua Amazon Virtual Private Cloud (Amazon VPC). Depois de concluir o teste e antes de executar outra atualização, programe o tempo de inatividade do aplicativo antes de mudar completamente para a AMI atualizada.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows Server 2008 R2, 2012 R2, 2016 ou 2019 edições Standard e Datacenter

Pré-requisitos

- TLS versão 1.2.
- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Instalação e configuração do SSM Agent em EC2 instâncias do Windows Server.
- O Windows PowerShell 3.0 ou posterior deve estar instalado na sua instância.
- Para instâncias ingressadas em um domínio do Microsoft Active Directory, é recomendável especificar um `SubnetId` que não tenha conectividade com seus controladores de domínio para ajudar a evitar conflitos de nome de host.
- A sub-rede da instância deve ter conectividade de saída com a Internet, que fornece acesso ao Serviços da AWS Amazon S3 e acesso ao download de patches da Microsoft. Esse requisito será atendido se a sub-rede for pública e a instância tiver um endereço IP público ou se a sub-rede for uma sub-rede privada com uma rota que envie o tráfego da Internet para um dispositivo NAT público.
- Essa automação funciona somente com Windows Server Instâncias 2008 R2, 2012 R2, 2016 e 2019.
- Configurar o Windows Server instância com um perfil de instância AWS Identity and Access Management (IAM) que fornece as permissões necessárias para o Systems Manager. Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager.
- Verifique se a instância tem 20 GB de espaço livre em disco no disco de inicialização.
- Se a instância não usar uma licença do Windows AWS fornecida, especifique um ID de snapshot do Amazon EBS que inclua Windows Server Mídia de instalação 2012 R2. Para fazer isso:
  - Verifique se a EC2 instância está em execução Windows Server 2012 ou mais tarde.
  - Crie um volume do EBS de 6 GB na mesma zona de disponibilidade em que a instância está sendo executada. Associe o volume à instância. Instale-a, por exemplo, como unidade D.
  - Clique com o botão direito do mouse no ISO e instale-o a uma instância como, por exemplo, unidade E.
  - Copie o conteúdo do ISO da unidade E:\ para a unidade D:\
  - Crie um snapshot do EBS do volume de 6 GB criado na etapa 2 acima.

Limitações

Essa automação não é compatível com a atualização de controladores de domínio do Windows, clusters ou sistemas operacionais de desktop do Windows. Essa automação também não oferece suporte a EC2 instâncias para Windows Server com as seguintes funções instaladas.

- Host de sessão de área de trabalho remota (RDSH)
- Agente de conexão de área de trabalho remota (RDCB)
- Host de virtualização de área de trabalho remota (RDVH)
- Acesso via Web à Área de Trabalho Remota (RDWA)

Parâmetros

- AlternativeKeyPairName

  Tipo: string

  Descrição: (opcional) o nome de um par de chaves alternativo a ser usado durante o processo de atualização. Isso é útil em situações em que o par de chaves atribuído à instância original não está disponível. Se a instância original não tiver sido atribuída a um par de chaves, você deverá especificar um valor para esse parâmetro.
- BYOLWindowsMediaSnapshotId

  Tipo: string

  Descrição: (opcional) o ID do snapshot do Amazon EBS a ser copiado que inclui a mídia de instalação do Windows Server 2012R2. Obrigatória somente se você estiver atualizando uma instância BYOL.
- IamInstanceProfile

  Tipo: string

  Descrição: (obrigatório) o nome do perfil da instância do IAM que permite que o Systems Manager gerencie a instância.
- InstanceId

  Tipo: string

  Descrição: (Obrigatório) A EC2 instância em execução Windows Server 2008 R2, 2012 R2, 2016 ou 2019.
- KeepPreUpgradeImageBackUp

  Tipo: string

Descrição: (Opcional) Se definida como True, a automação não exclui a AMI criada da EC2 instância antes da atualização. Se definida como Verdadeiro, você deverá excluir a AMI. Por padrão, a AMI é excluída.

- SubnetId

  Tipo: string

  Descrição: (Obrigatório) Essa é a sub-rede do processo de atualização e onde sua EC2 instância de origem reside. Verifique se a sub-rede tem conectividade de saída com AWS serviços, Amazon S3 e Microsoft (para baixar patches).

- TargetWindowsVersion

  Tipo: string

  Descrição: (obrigatória) selecione a versão de destino do Windows.

  Padrão: 2022

- RebootInstanceBeforeTakingImage

  Tipo: string

  Descrição: (opcional) Se definida como Verdadeiro, a Automação reinicializa a instância antes de criar uma AMI pré-atualização. Por padrão, a Automação não reinicializa antes da atualização.

AWSEC2-ConfigureSTIG

Os Guias de Implementação Técnica de Segurança (STIGs) são os padrões de fortalecimento da configuração criados pela Agência de Sistemas de Informação de Defesa (DISA) para proteger sistemas de informação e software. Para que seus sistemas estejam em conformidade com os padrões STIG, você deve instalar, definir e testar uma variedade de configurações de segurança.

EC2 A Amazon fornece um documento de comando do Systems ManagerAWSEC2-ConfigureSTIG, que você pode usar para aplicar as configurações do STIG a uma instância. Este documento ajuda você a criar rapidamente imagens compatíveis com os padrões do STIG. O documento do STIG Systems Manager verifica se há configurações incorretas e executa um script de correção. Ele também é instalado InstallRoot do Departamento de Defesa (DoD) no AMIs Windows para instalar e atualizar os certificados do DoD e remover certificados desnecessários para manter a conformidade com o STIG. Não há cobranças adicionais pelo uso do documento do STIG Systems Manager.

> **Note**
>
> AWSEC2-ConfigureSTIGé um documento de comando. Para pesquisar AWSEC2-ConfigureSTIG no AWS Systems Manager console, selecione a categoria Documentos de comando.

Esta página lista tudo o STIGs que a Amazon EC2 suporta para que os componentes de fortalecimento do STIG se apliquem à sua instância. EC2

Você pode escolher qual categoria de conformidade do STIG deseja aplicar.

Níveis de conformidade

- Alto (categoria I)

  O risco mais grave. Inclui qualquer vulnerabilidade que possa resultar em perda de confidencialidade, disponibilidade ou integridade.
- Médio (categoria II)

  Inclui qualquer vulnerabilidade que possa resultar em perda de confidencialidade, disponibilidade ou integridade, mas os riscos podem ser mitigados.
- Baixo (categoria III)

  Inclui qualquer vulnerabilidade que degrade medidas de proteção contra perda de confidencialidade, disponibilidade ou integridade.

Tópicos

- Downloads de componentes de fortelecimento do STIG
- Configurações do STIG no Windows
- Histórico de versões do Windows STIG
- Configurações de STIG no Linux
- Histórico de versões do STIG do Linux

Downloads de componentes de fortelecimento do STIG

A Amazon agrupa os componentes de fortalecimento do STIG em pacotes relacionados ao sistema operacional para cada versão. Os pacotes são arquivos de arquivamento apropriados para o sistema operacional de destino em que são baixados e executados. Os pacotes de componentes Linux são armazenados como arquivos TAR (extensão de arquivo .tgz). Os pacotes de componentes do Windows são armazenados como arquivos ZIP (extensão de arquivo .zip).

A Amazon armazena os pacotes de componentes no bucket `STIG` do S3 do Image Builder em cada Região da AWS. Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.

> **Important**
>
> Com poucas exceções, os componentes de fortalecimento do STIG que o documento do Systems Manager baixa não instalam pacotes de terceiros. Se pacotes de terceiros já estiverem instalados na instância e se houver algo relacionado ao STIGs EC2 suporte da Amazon para esse pacote, eles STIGs serão aplicados.

Os padrões e exemplos de caminhos de armazenamento de componentes e nomes de arquivos de pacotes são os seguintes:

Caminho de armazenamento de componentes

`s3://aws-windows-downloads-`*`<region>`*`/STIG/`*`<bundle file name>`*

Variáveis do caminho do componente

region

Região da AWS (Cada região tem seu próprio bucket de componentes.)

bundle file name

O formato é *`<os bundle name>`* _ *`<YYYY>`* _Q *`<quarter>`* [_*`<release>`*]. *`<file extension>`*. Observe que o nome tem sublinhados entre os nós, não pontos.

os bundle name

O prefixo do nome padrão para o pacote do sistema operacional é `LinuxAWSConfigureSTIG` ou `AWSConfigureSTIG`. Para manter a compatibilidade com versões anteriores, o download para Windows não inclui um prefixo de plataforma.

YYYY

O ano de quatro dígitos do lançamento.

quarter

Identifica o trimestre do ano: 1, 2, 3 ou 4.

release

Número incremental que começa em um e aumenta em um para cada nova versão. A versão não está incluída na primeira versão em um trimestre e só é adicionada nas versões subsequentes.

file extension

Formato de arquivo compactado `tgz` (Linux) ou `zip` (Windows).

Exemplos de nomes de arquivos de pacotes

- `LinuxAWSConfigureSTIG_2023_Q1_2.tgz`
- `AWSConfigureSTIG_2022_Q4.zip`

Configurações do STIG no Windows

Os componentes STIG AMIs e de proteção EC2 do Amazon Windows foram projetados para servidores autônomos e aplicam a Política de Grupo Local. Componentes compatíveis com STIG são instalados InstallRoot do Departamento de Defesa (DoD) no Windows AMIs para baixar, instalar e atualizar os certificados do DoD. Eles também removem certificados desnecessários para manter a conformidade com o STIG. Atualmente, a Amazon EC2 oferece suporte às linhas de base STIG para as seguintes versões do Windows Server: 2012 R2, 2016, 2019 e 2022.

Esta seção lista as configurações atuais do STIG que a Amazon EC2 suporta para sua infraestrutura Windows, seguidas por um registro do histórico de versões.

Você pode aplicar configurações de STIG baixas, médias ou altas.

STIG do Windows baixa (categoria III)

A lista a seguir contém as configurações STIG que a Amazon EC2 oferece suporte à sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, a Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento

do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa do Windows STIGs, consulte a Biblioteca de STIGs Documentos. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

- Windows Server 2022 STIG versão 2 versão 2

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 e V-254481
- Windows Server 2019 STIG versão 3 versão 2

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 e V-205923
- Windows Server 2016 STIG versão 2 versão 9

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 e V-225060
- Windows Server 2012 R2 MS STIG Versão 3 Release 5

  V-225537, V-225536, V-225526, V-225525, V-225514, V-225511, V-225490, V-225489, V-225488, V-225487, V-225485, V-225484, V-225483, V-225482, V-225481, V-225480, V-225479, V-225476, V-225473, V-225468, V-225462, V-225460, V-225459, V-225412, V-225394, V-225392, V-225376, V-225363, V-225362, V-225360, V-225359, V-225358, V-225357, V-225355, V-225343, V-225342, V-225336, V-225335, V-225334, V-225333, V-225332, V-225331, V-225330, V-225328, V-225327, V-225324, V-225319, V-225318 e V-225250
- Microsoft .NET Framework 4,0 STIG Versão 2 Release 2

  Nenhuma configuração STIG é aplicada ao Microsoft .NET Framework para vulnerabilidades de Categoria III.
- Firewall do Windows STIG versão 2 versão 2

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 e V-242008
- Internet Explorer 11 STIG Versão 2 Versão 5

  V-223016, V-223056 e V-223078
- Microsoft Edge STIG versão 2 versão 2 (somente Windows Server 2022)

  V-235727, V-235731, V-235751, V-235752 e V-235765

Windows STIG Medium (categoria III)

A lista a seguir contém as configurações STIG que a Amazon EC2 oferece suporte à sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, a Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa do Windows STIGs, consulte a Biblioteca de STIGs Documentos. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Windows STIG Medium inclui todas as configurações de proteção STIG listadas que se aplicam ao Windows STIG low (Categoria III), além das configurações de fortalecimento STIG que a Amazon suporta para vulnerabilidades da Categoria II. EC2

- Windows Server 2022 STIG versão 2 versão 2

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

  V-254247, V-254265, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254289, V-254290, V-254291, V-254292, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V-254310, V-254311, V-254312, V-254313, V-254314, V-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254330, V-254331, V-254332 V-254333, V-254334, V-254339, V-254341, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254356, V-254358, V-254359, V-254360, V-254361, V-254362, V-254364, V-254364, V-254364 365, V-254366, V-254367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254382, V-254383, V-254384, V-254431, V-254432, V-254433, V-254435, V-254436, V-254438, V-254439, V-254442, V-254443, V-254444, V-254445, V-254449, V-254450, V-254451, V-254452, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254484, V-254485, V-254485 254486, V-254487, V-254489, V-254490,

V-254493, V-254494, V-254495, V-254497, V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254507, V-254507, V-254508, V-254509, V-254510, V-254511 e V-254512

- Windows Server 2019 STIG versão 3 versão 2

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

  V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205643, V-205644, V-205648, V-205649, V-205650, V-205651, V-205651, V-205651 2, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205679, V-205680, V-205681, V-205682, V-205683, V-205683 5684, V-205685, V-205686, V-205687, V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205722, V-205729, V-205730, V-205733, V-205747, V-205751, V-205752, V-205754, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205764, V-205765, V-205766, V-205767, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205781, V-205782, V-205783, V-205784, V-205795, V-205795, V-205796, V-205797, V-205798, V-205801, V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205824 25, V-205826, V-205827, V-205828, V-205830, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838, V-205839, V-205840, V-205841, V-205842, V-205861, V-205863, V-205865, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205924, V-205925, V-236001 e V-257503

- Windows Server 2016 STIG versão 2 versão 9

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

  V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224869, V-224870, V-224871, V-224872, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224895, V-224896, V-224897, V-224898, V-224899, V-224900, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936,

V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224947, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225015, V-225015, V-2225015, V-222V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040, V-225040, V-225040 25041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225058, V-225059, V-225061, V-225062, V-225063, V-225064, V-225065, V-225066, V-225067, V-225068, V-225069, V-225072, V-225073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093, V-236000 e V-257502

- Windows Server 2012 R2 MS STIG Versão 3 Release 5

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

  V-225574, V-225573, V-225572, V-225571, V-225570, V-225569, V-225568, V-225567, V-225566, V-225565, V-225564, V-225563, V-225562, V-225561, V-225560, V-225559, V-225558, V-225557, V-225555, V-225554, V-225553, V-225551, V-225550, V-225549, V-225548, V-225546, V-225545, V-225544, V-225543, V-225542, V-225541, V-225540, V-225539, V-225538, V-225535, V-225534, V-225533, V-225532, V-225531, V-225530, V-225529, V-225528, V-225527, V-225524, V-225523, V-225522, V-225521, V-225520, V-225519, V-225518, V-225517, V-225516, V-225515, V-225513, V-225510, V-225509, V-225508, V-225506, V-225504, V-225503, V-225502, V-225501, V-225500, V-225494, V-225486, V-225478, V-225477, V-225475, V-225474, V-225472, V-225471, V-225470, V-225469, V-225464, V-225463, V-225461, V-225458, V-225457, V-225456, V-225455, V-225454, V-225453, V-225452, V-225448, V-225443, V-225442, V-225441, V-225415, V-225414, V-225413, V-225411, V-225410, V-225409, V-225408, V-225407, V-225406, V-225405, V-225404, V-225402, V-225401, V-225400, V-225398, V-225397, V-225395, V-225393, V-225391, V-225389, V-225386, V-225385, V-225384, V-225383, V-225382, V-225381, V-225380, V-225379, V-225378, V-225377, V-225375, V-225374, V-225373, V-225372, V-225371, V-225370, V-225369, V-225368, V-225367, V-225356, V-225353, V-225352, V-225351, V-225350, V-225349, V-225348, V-225347, V-225346, V-225345, V-225344, V-225341, V-225340, V-225339, V-225338, V-225337, V-225329, V-225326, V-225325, V-225317, V-225316, V-225315, V-225314, V-225305, V-225304, V-225303, V-225302, V-225301, V-225300, V-225299, V-225298, V-225297, V-225296, V-225295, V-225294, V-225293, V-225292, V-225291, V-225290, V-225289, V-225288, V-225287, V-225286, V-225285, V-225284, V-225283, V-225282, V-225281, V-225280, V-225279, V-225278, V-225277, V-225276, V-225275,

V-225273, V-225272, V-225271, V-225270, V-225269, V-225268, V-225267, V-225266, V-225265, V-225264, V-225263, V-225261, V-225260, V-225259 e V-225239

- Microsoft .NET Framework 4,0 STIG Versão 2 Release 2

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

  V-225238

- Firewall do Windows STIG versão 2 versão 2

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

  V-241989, V-241990, V-241991, V-241993, V-241993, V-241998, V-241998, V-242003 e V-242003

- Internet Explorer 11 STIG Versão 2 Versão 5

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

  V-223015, V-223017, V-223018, V-223019, V-223020, V-223021, V-223022, V-223023, V-223024, V-223025, V-223026, V-223027, V-223028, V-223029, V-223030, V-223031, V-223032, V-223033, V-223034, V-223035, V-223036, V-223037, V-223038, V-223039, V-223040, V-223041, V-223042, V-223043, V-223044, V-223045, V-223046, V-223048, V-223049, V-223050, V-223051, V-223052, V-223053, V-223054, V-223055, V-223057, V-223058, V-223059, V-223060, V-223061, V-223062, V-223063, V-223064, V-223065, V-223066, V-223067, V-223068, V-223069, V-223070, V-223071, V-223072, V-223073, V-227430, V-223075, V-223076, V-223077, V-223079, V-223080, V-223081, V-223082, V-223083, V-223084, V-223085, V-223086, V-223087, V-223088, V-223089, V-223090, V-223091, V-223092, V-223093, V-223094, V-223095, V-223096, V-223097, V-223098, V-223099, V-223100, V-223101, V-223102, V-223103, V-223104, V-223105, V-223106, V-223107, V-223108, V-223109, V-223110, V-223111, V-223112, V-223113, V-223113, V-223113, V-223113, V-223114, V-223115, V-223116, V-223117, V-223118, V-223119, V-223120, V-223121, V-223122, V-223123, V-223124, V-223125, V-223126, V-223127, V-223128, V-223129, V-223130, V-223131, V-223131, V-223131 23132, V-223133, V-223134, V-223135, V-223136, V-223137, V-223138, V-223139, V-223140, V-223141, V-223142, V-223143, V-223144, V-223145, V-223146, V-223147, V-223148, V-223148, V-223148, V-223148 149, V-250540 e V-250541

- Microsoft Edge STIG versão 2 versão 2 (somente Windows Server 2022)

V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774 e V-246736

- Microsoft Defender STIG Versão 2 Versão 4

  V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465 e V-213466

STIG do Windows High (categoria I)

A lista a seguir contém as configurações STIG que a Amazon EC2 oferece suporte à sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, a Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa do Windows STIGs, consulte a Biblioteca de STIGs Documentos. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Windows STIG High inclui todas as configurações de proteção STIG listadas que se aplicam às categorias Windows STIG Medium e Low, além das configurações de fortalecimento STIG que a Amazon suporta para vulnerabilidades da Categoria I. EC2

- Windows Server 2022 STIG versão 2 versão 2

  V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475 e V-254500

- Windows Server 2019 STIG versão 3 versão 2

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914 e V-205919

- Windows Server 2016 STIG versão 2 versão 9

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054 e V-225079

- Windows Server 2012 R2 MS STIG Versão 3 Release 5

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-225556, V-225552, V-225547, V-225507, V-225505, V-225498, V-225497, V-225496, V-225493, V-225492, V-225491, V-225449, V-225444, V-225399, V-225396, V-225390, V-225366, V-225365, V-225364, V-225354 e V-225274

- Microsoft .NET Framework 4,0 STIG Versão 2 Release 2

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa) do Microsoft.NET Framework. Nenhuma configuração adicional do STIG se aplica a vulnerabilidades da Categoria I.

- Firewall do Windows STIG versão 2 versão 2

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-241992, V-241997 e V-242002

- Internet Explorer 11 STIG Versão 2 Versão 5

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-252910

- Microsoft Edge STIG versão 2 versão 2 (somente Windows Server 2022)

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-235758 e V-235759

- Microsoft Defender STIG Versão 2 Versão 4

  Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

  V-213426, V-213426, V-213452, V-213452, V-213452, V-213453, V-213453 e V-213453

Histórico de versões do Windows STIG

Esta seção registra o histórico de versões do componente do Windows para as atualizações trimestrais do STIG. Para ver as alterações e as versões publicadas de um trimestre, escolha o título para expandir as informações.

Alterações no primeiro trimestre de 2025 - 05/04/2025:

STIGS atualizado para Internet Explorer 11 STIG versão 2 versão 5 para todos os componentes do STIG para a versão do primeiro trimestre de 2025.

- STIG-Build-Windows-Low versão 2025.1.x
- STIG-Build-Windows-Medium versão 2025.1.x
- STIG-Build-Windows-High versão 2025.1.x

Alterações no quarto trimestre de 2024 - 12/10/2024:

Versões atualizadas do STIG e aplicou STIGS para a versão do quarto trimestre de 2024 da seguinte forma:

STIG-Build-Windows-Low versão 2024.4.0

- Windows Server 2022 STIG versão 2 versão 2
- Windows Server 2019 STIG versão 3 versão 2
- Windows Server 2016 STIG versão 2 versão 9
- Windows Server 2012 R2 MS STIG Versão 3 Release 5

- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Firewall do Windows STIG versão 2 versão 2
- Internet Explorer 11 STIG Versão 2 Versão 5
- Microsoft Edge STIG versão 2 versão 2 (somente Windows Server 2022)

STIG-Build-Windows-Medium versão 2024.4.0

- Windows Server 2022 STIG versão 2 versão 2
- Windows Server 2019 STIG versão 3 versão 2
- Windows Server 2016 STIG versão 2 versão 9
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Firewall do Windows STIG versão 2 versão 2
- Internet Explorer 11 STIG Versão 2 Versão 5
- Microsoft Edge STIG versão 2 versão 2 (somente Windows Server 2022)
- Defender STIG Versão 2, Versão 4

STIG-Build-Windows-High versão 2024.4.0

- Windows Server 2022 STIG versão 2 versão 2
- Windows Server 2019 STIG versão 3 versão 2
- Windows Server 2016 STIG versão 2 versão 9
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Firewall do Windows STIG versão 2 versão 2
- Internet Explorer 11 STIG Versão 2 Versão 5
- Microsoft Edge STIG versão 2 versão 2 (somente Windows Server 2022)
- Defender STIG Versão 2, Versão 4

Alterações no terceiro trimestre de 2024 - 10/04/2024 (sem alterações):

Não houve alterações no componente STIGS do Windows para a versão do terceiro trimestre de 2024.

Alterações no segundo trimestre de 2024 (10/5/2024; sem alterações):

Não houve alterações no componente STIGS do Windows para o lançamento do segundo trimestre de 2024.

Alterações no primeiro trimestre de 2024 - 23/02/2024 (sem alterações):

Não houve alterações no componente STIGS do Windows para o lançamento do primeiro trimestre de 2024.

Alterações no quarto trimestre de 2023 - 12/07/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o lançamento do quarto trimestre de 2023.

Alterações no terceiro trimestre de 2023 - 04/10/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do terceiro trimestre de 2023.

Alterações no segundo trimestre de 2023 - 03/05/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do segundo trimestre de 2023.

Alterações no primeiro trimestre de 2023 - 27/03/2023 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do primeiro trimestre de 2023.

Alterações no quarto trimestre de 2022 - 01/02/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2022 da seguinte forma:

STIG-Build-Windows-Low versão 2022.4.0

- Windows Server 2022 STIG versão 1 release 1
- Windows Server 2019 STIG Versão 2 Release 5
- Windows Server 2016 STIG Versão 2 Release 5
- Windows Server 2012 R2 MS STIG Versão 3 Release 5

- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 2 Release 3
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)

STIG-Build-Windows-Medium versão 2022.4.0

- Windows Server 2022 STIG versão 1 release 1
- Windows Server 2019 STIG Versão 2 Release 5
- Windows Server 2016 STIG Versão 2 Release 5
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 2 Release 3
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)
- Defender STIG Versão 2 Release 4 (somente Windows Server 2022)

STIG-Build-Windows-High versão 2022.4.0

- Windows Server 2022 STIG versão 1 release 1
- Windows Server 2019 STIG Versão 2 Release 5
- Windows Server 2016 STIG Versão 2 Release 5
- Windows Server 2012 R2 MS STIG Versão 3 Release 5
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 2
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 2 Release 3
- Microsoft Edge STIG Versão 1 Release 6 (somente Windows Server 2022)
- Defender STIG Versão 2 Release 4 (somente Windows Server 2022)

Alterações no terceiro trimestre de 2022 - 30/09/2022 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do terceiro trimestre de 2022.

Alterações no segundo trimestre de 2022 - 02/08/2022:

Versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2022.

STIG-Build-Windows-Low versão 1.5.0

- Windows Server 2019 STIG Versão 2 Release 4
- Windows Server 2016 STIG Versão 2 Release 4
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

STIG-Build-Windows-Medium versão 1.5.0

- Windows Server 2019 STIG Versão 2 Release 4
- Windows Server 2016 STIG Versão 2 Release 4
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

STIG-Build-Windows-High versão 1.5.0

- Windows Server 2019 STIG Versão 2 Release 4
- Windows Server 2016 STIG Versão 2 Release 4
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

Alterações no primeiro trimestre de 2022 - 02/08/2022 (sem alterações):

Não houve alterações no componente STIGS do Windows para o release do primeiro trimestre de 2022.

Alterações no quarto trimestre de 2021 - 20/12/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2021.

STIG-Build-Windows-Low versão 1.5.0

- Windows Server 2019 STIG Versão 2 Release 3
- Windows Server 2016 STIG Versão 2 Release 3
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

STIG-Build-Windows-Medium versão 1.5.0

- Windows Server 2019 STIG Versão 2 Release 3
- Windows Server 2016 STIG Versão 2 Release 3
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

STIG-Build-Windows-High versão 1.5.0

- Windows Server 2019 STIG Versão 2 Release 3
- Windows Server 2016 STIG Versão 2 Release 3
- Windows Server 2012 R2 MS STIG Versão 3 Release 3
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 2 Release 1
- Internet Explorer 11 STIG Versão 1 Release 19

Alterações no terceiro trimestre de 2021 - 30/09/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do terceiro trimestre de 2021.

STIG-Build-Windows-Low versão 1.4.0

- Windows Server 2019 STIG Versão 2 Release 2
- Windows Server 2016 STIG Versão 2 Release 2
- Windows Server 2012 R2 MS STIG Versão 3 Release 2
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 1 Release 7
- Internet Explorer 11 STIG Versão 1 Release 19

STIG-Build-Windows-Medium versão 1.4.0

- Windows Server 2019 STIG Versão 2 Release 2
- Windows Server 2016 STIG Versão 2 Release 2
- Windows Server 2012 R2 MS STIG Versão 3 Release 2
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 1 Release 7
- Internet Explorer 11 STIG Versão 1 Release 19

STIG-Build-Windows-High versão 1.4.0

- Windows Server 2019 STIG Versão 2 Release 2
- Windows Server 2016 STIG Versão 2 Release 2
- Windows Server 2012 R2 MS STIG Versão 3 Release 2
- Microsoft .NET Framework 4.0 STIG Versão 2 Release 1
- Windows Firewall STIG Versão 1 Release 7
- Internet Explorer 11 STIG Versão 1 Release 19

Configurações de STIG no Linux

Esta seção contém informações sobre as configurações de fortalecimento do Linux STIG suportadas pela Amazon EC2 , seguidas por um registro do histórico de versões. Se a distribuição Linux não tiver configurações próprias de proteção STIG, a Amazon EC2 usará as configurações do RHEL. As configurações de fortalecimento do STIG suportadas se aplicam ao Amazon EC2 Linux AMIs e aos componentes baseados na distribuição Linux, da seguinte forma:

- Configurações do Red Hat Enterprise Linux (RHEL) 7 STIG
  - RHEL 7
  - CentOS 7
  - Amazon Linux (2AL2)
- Configurações do RHEL 8 STIG
  - RHEL 8
  - CentOS 8
  - Amazon Linux 2023 (AL 2023)
- Configurações do RHEL 9 STIG
  - RHEL 9
  - CentOS Stream 9

Linux STIG Low (categoria III)

A lista a seguir contém as configurações STIG que a Amazon EC2 oferece suporte à sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, a Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa, consulte a Biblioteca de STIGs documentos. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

RHEL 7 STIG Versão 3 Release 14

- RHEL 7/CentOS 7/ AL2

  V-204452, V-204576 e V-204605

RHEL 8 STIG Versão 2 Versão 2

- RHEL 8/CentOS 8/AL 2023

  V-230241, V-230281, V-244527, V-230269, V-230270, V-230285, V-230346, V-230381, V-230395, V-230491, V-230468, V-230469, V-230485, V-230486, V-230494, V-230495, V-230496, V-230497,

V-230497, V-230498, V-230498, V-230496, V-230497, V-230498, V-230496, V-230497, V-230498, V-230498, V-230496 230499 e V-230253

RHEL 9 STIG Versão 2 Versão 3

- RHEL 9/CentOS Stream 9

  V-257782, V-257824, V-258138, V-258037, V-257880, V-257795, V-257796, V-258173, V-258069, V-258076, V-258067, V-257946 e V-257947

Ubuntu 18.04 STIG versão 2 versão 15

V-219163, V-219164, V-219165, V-219172, V-219173, V-219174, V-219175, V-219178, V-219180, V-219210, V-219301, V-219327, V-219332 e V-219333

Ubuntu 20.04 STIG Versão 2 Versão 2

V-238203, V-238202, V-238234, V-238235, V-238237, V-238323, V-238373, V-238221, V-238222, V-238223, V-238224, V-238226, V-238362, V-238357 e V-238308

Ubuntu 22.04 STIG Versão 2 Versão 3

V-260479, V-260480, V-260481, V-260521, V-260520, V-260476, V-260472, V-260549, V-260550, V-260551, V-260552, V-260581 e V-260596

Ubuntu 24.04 STIG Versão 1 Versão 1

V-270645, V-270646, V-270664, V-270820, V-270677, V-270690, V-270706, V-270710, V-270695, V-270749, V-270752 e V-270818

Linux STIG Medium (categoria II)

A lista a seguir contém as configurações STIG que a Amazon EC2 oferece suporte à sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, a Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa, consulte a Biblioteca de STIGs documentos. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Linux STIG Medium inclui todas as configurações de fortalecimento STIG listadas que se aplicam ao Linux STIG Low (Categoria III), além das configurações de fortalecimento STIG que a Amazon suporta para vulnerabilidades de Categoria II. EC2

RHEL 7 STIG Versão 3 Versão 15

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

- RHEL 7/CentOS 7/ AL2

  V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204416, V-204417, V-204418, V-204422, V-204423, V-204426, V-204427, V-204427, V-204426, V-204427, V-204427, V-204431, V-204434, V-204435, V-204437, V-204449, V-204450, V-204451, V-204457, V-204466, V-204490, V-204491, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204512, V-204512, V-204512 14, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204546, V-204547, V-204547, V-204547, V-204547, V-204547 48, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204567, V-204568, V-204572, V-204578, V-204578, V-204579, V-204584, V-204585, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204595, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204602 609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204619, V-204622, V-204625, V-204630, V-204631, V-204633, V-233307, V-237634, V-237635, V-251703, V-251703, V-255925, V-255927, V-255928 e V-256970

RHEL 8 STIG Versão 2 Versão 2

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

- RHEL 8/CentOS 8/AL 2023

  V-230238, V-230239, V-230257, V-230258, V-230259, V-230262, V-230273, V-230275, V-230316, V-230325, V-230366, V-230478, V-230488, V-230489, V-230505, V-230523, V-230550, V-230559,

V-230560 230561, V-237640, V-244547, V-256974, V-230525, V-244544, V-230248, V-230249, V-230250, V-230245, V-230246, V-230247, V-230397, V-230399, V-230400, V-230401, V-244543, V-230228, V-230298, V-230298 387, V-230482, V-230231, V-230233, V-230324, V-230365, V-230370, V-230373, V-230378, V-230383, V-230236, V-230314, V-230315, V-244523, V-257258, V-230266, V-230267, V-230268, V-230280, V-230310, V-230311, V-230312, V-230502, V-230532, V-230535, V-230536, V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230549, V-244550, V-244551, V-244552, V-244553, V-244554, V-250317, V-251718, V-230237, V-230313, V-230356, V-230357, V-230358, V-230359, V-230360, V-230361, V-230362, V-230363, V-230363, V-230363, V-230368, V-230368, V-230363, V-230368, V-230363, V-230368, V-230363, V-230368, V-230363, V-230368, V-230363, V-230368, V-230363, V-230368, V-230363, V-230368, V-230363, V-230368, V-230230369, V-230375, V-230376, V-230377, V-244524, V-244533, V-251713, V-251717, V-251714, V-251715, V-251716, V-230332, V-230333, V-230335, V-230337, V-230339, V-230341, V-230343, V-230345, V-230240, V-230282, V-250315, V-250316, V-230255, V-230277, V-230278, V-230348, V-230353, V-230386, V-230390, V-230392, V-230394, V-230396, V-230393, V-230398, V-230402, V-230403, V-230403, V-230404, V-230403, V-230402, V-230403, V-230403, V-230402, V-230403, V-230403, V-230404, V-230403, V-230404 230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, V-230418, V-230419, V-230421, V-230422, V-230423, V-230424, V-230425, V-230426, V-230427, V-230427, V-230428, V-230428, V-230426, V-230427, V-230428, V-230428 230429, V-230430, V-230431, V-230432, V-230433, V-230434, V-230435, V-230436, V-230437, V-230438, V-230439, V-230444, V-230446, V-230447, V-230448, V-230449, V-230455, V-230456, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V-230471, V-230472, V-230473, V-230474, V-230480, V-230483, V-244542, V-230503, V-230507, V-244525, V-230244, V-230286, V-230287, V-230288, V-230288, V-230288 230290, V-230291, V-230296, V-230330, V-230382, V-230526, V-230527, V-230555, V-230556, V-244526, V-244528, V-237642, V-237643 e V-251711

RHEL 9 STIG Versão 2 Versão 3

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

- RHEL 9/CentOS Stream 9

  V-257981, V-257780, V-257825, V-257827, V-257828, V-257829, V-257830, V-257831, V-257832, V-257833, V-257834, V-257836, V-257838, V-257839, V-257840, V-257841, V-257842, V-257882, V-257882, V-257882 883, V-257884, V-257885, V-257889, V-257890, V-257891, V-257892,

V-257893, V-257894, V-257895, V-257896, V-257897, V-257898, V-257899, V-257900, V-257901, V-257902, V-257903, V-257903, V-257903, V-257904, V-257905, V-257906, V-257907, V-257908, V-257909, V-257910, V-257912, V-257913, V-257914, V-257915, V-257918, V-257919, V-257920, V-257921, V-257922, V-257923, V-257923, V-257928, V-257929, V-257930, V-257934, V-257935, V-257943, V-257948, V-257954, V-257978, V-257980, V-258035, V-258041, V-258046, V-258052, V-258063, V-258068, V-258081, V-258082, V-258083, V-258089, V-258120, V-258124, V-258126, V-258140, V-258141, V-258151, V-258234, V-257886, V-257916, V-257917, V-257924, V-257939, V-257940, V-258036, V-258038, V-257887, V-257924, V-257925, V-258145, V-258152, V-258153, V-258154, V-258156, V-258157, V-258158, V-258159, V-258161, V-258162, V-258163, V-258164, V-258165, V-258166, V-258167, V-258168, V-258169, V-258170, V-258171, V-258172, V-258176, V-258177, V-258178, V-258179, V-258180, V-258181, V-258182, V-258183, V-258184, V-258185, V-258186, V-258187, V-258188, V-258189, V-258190, V-258191, V-258191, V-258191, V-258192, V-258193, V-258194, V-258195, V-258196, V-258197, V-258198, V-258199, V-258200, V-258201, V-258202, V-258203, V-258204, V-258205, V-258206, V-258207, V-258207 8208, V-258209, V-258210, V-258211, V-258212, V-258213, V-258214, V-258215, V-258217, V-258218, V-258219, V-258220, V-258221, V-258222, V-258223, V-258224, V-258225, V-258226, V-258227, V-258228, V-258229, V-257781, V-257783, V-257786, V-257797, V-257798, V-257799, V-257800, V-257801, V-257802, V-257803, V-257809, V-257810, V-257811, V-257812, V-257813, V-257815, V-257816, V-257942, V-257957, V-257958, V-257959, V-257959, V-257959 257960, V-257961, V-257962, V-257963, V-257964, V-257965, V-257966, V-257967, V-257968, V-257969, V-257970, V-257971, V-257972, V-257973, V-257974, V-257975, V-257976, V-257977, V-258077, V-258128, V-258129, V-258043, V-258049, V-258071, V-258072, V-258073, V-258074, V-258075, V-258104, V-258105, V-258107, V-258108, V-258109, V-258110, V-258111, V-258117, V-258117 19, V-257979, V-257982, V-257983, V-257985, V-257987, V-257988, V-257992, V-257993, V-257994, V-257995, V-257996, V-257997, V-257998, V-257999, V-258000, V-258001, V-258002, V-258003, V-258004, V-258005, V-258006, V-258007, V-258008, V-258009, V-258010, V-258011, V-258130, V-257814, V-258054, V-258055, V-258056, V-258057, V-258060, V-258070, V-258080, V-258088, V-258091, V-258092, V-258093, V-258095, V-258097, V-258098, V-258099, V-258100, V-258101, V-258102, V-258103, V-258112, V-258113, V-258114, V-258115, V-258116, V-258118, V-258233, V-257951, V-257953, V-25853 142, V-258144, V-258146, V-258147, V-258148, V-258150, V-258064, V-258065, V-258066, V-258232, V-258237, V-258239, V-258240, V-257788, V-257790, V-257791, V-257792, V-257793, V-257794, V-257817, V-258175, V-257804, V-257805, V-257806, V-257808, V-258034, V-258039, V-257888, V-257926, V-257927, V-257933, V-258084, V-258085, V-257949, V-258040, V-257818, V-257849, V-258122, V-258123, V-258133, V-257944, V-258028, V-258079, V-258125 e V-258137

Ubuntu 18.04 STIG versão 2 versão 15

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

V-219149, V-219155, V-219156, V-219160, V-219166, V-219168, V-219176, V-219181, V-219184, V-219186, V-219188, V-219189, V-219190, V-219191, V-219192, V-219193, V-2193, V-22219194, V-219195, V-219196, V-219197, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219209, V-219209 213, V-219214, V-219215, V-219216, V-219217, V-219218, V-219219, V-219221, V-219222, V-219223, V-219224, V-219225, V-219226, V-219227, V-219228, V-219228, V-219228, V-219228 29, V-219230, V-219231, V-219232, V-219233, V-219234, V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243, V-219244, V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267, V-219268, V-219269, V-219269, V-219270, V-219271, V-219272, V-219273, V-219274, V-219275, V-219276, V-219279, V-219281, V-219287, V-219291, V-219291, V-219297, V-219298, V-219299, V-219300, V-222300, V-22219303, V-219304, V-219306, V-219309, V-219310, V-219311, V-219312, V-219315, V-219318, V-219319, V-219323, V-219326, V-219328, V-219330, V-219331, V-219335, V-219335, V-219335, V-219335, V-22235 336, V-219337, V-219338, V-219339, V-219342, V-219344, V-233779, V-233780 e V- 255906

Ubuntu 20.04 STIG Versão 2 Versão 2

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

V-238200, V-238205, V-238207, V-238231, V-238329, V-238337, V-238339, V-238340, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238350, V-238351, V-238352, V-238352, V-238352, V-238352, V-238371, V-238376, V-238377, V-238378, V-238209, V-238325, V-238330, V-238333, V-238369, V-238230, V-238338, V-238341, V-238342, V-238343, V-238324, V-238353, V-238228, V-238228, V-238225, V-238227, V-238299, V-238238, V-238239, V-238240, V-238241, V-238242, V-238244, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238251, V-238251 2, V-238253, V-238254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238290, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238300, V-238301, V-238302, V-238304, V-238309, V-238310, V-238315, V-238316, V-238317, V-238318, V-238318, V-238319, V-238320, V-251505, V-238360, V-238210, V-238211, V-238212, V-238213, V-238220, V-255912, V-238355, V-238236, V-238303, V-238356, V-238359, V-238370, V-238334 e V-238232

Ubuntu 22.04 STIG Versão 2 Versão 3

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

V-260546, V-260473, V-260474, V-260478, V-260485, V-260486, V-260487, V-260488, V-260489, V-260490, V-260495, V-260496, V-260497, V-260498, V-260499, V-260500, V-260508, V-260513, V-260522, V-260540, V-260542, V-260543, V-260547, V-260554, V-260572, V-260590, V-260475, V-260491, V-260510, V-260511, V-260492, V-260493, V-260494, V-260507, V-260591, V-260594, V-260597, V-260598, V-260599, V-260600, V-260601, V-260602, V-260603, V-260604, V-260605, V-260606, V-260607, V-260608, V-260609, V-260610, V-260611, V-260612, V-260613, V-260614, V-260615, V-260616, V-260617, V-260618, V-260619, V-260620, V-260621, V-260622, V-260623, V-260624, V-260625, V-260626, V-260627, V-260628, V-260629, V-260630, V-260631, V-260632, V-260633, V-260634, V-260635, V-260636, V-260637, V-260638, V-260639, V-260640, V-260641, V-260642, V-260643, V-260644, V-260645, V-260646, V-260647, V-260648, V-260648, V-260648, V-260648 49, V-260471, V-260514, V-260553, V-260573, V-260576, V-260574, V-260560, V-260561, V-260562, V-260563, V-260564, V-260565, V-260566, V-260567, V-260569, V-260569, V-260569, V-260569 527, V-260528, V-260530, V-260533, V-260534, V-260575, V-260505, V-260506, V-260512, V-260582, V-260584, V-260585, V-260586, V-260477, V-260545, V-260555, V-260556, V-260557, V-260509, V-260588, V-260589, V-260537, V-260538 e V-260535

Ubuntu 24.04 STIG Versão 1 Versão 1

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades de categoria III (baixa), além de:

V-270649, V-270651, V-270652, V-270653, V-270654, V-270656, V-270657, V-270659, V-270660, V-270661, V-270662, V-270663, V-270669, V-270672, V-270673, V-270674, V-270676, V-270678, V-270679, V-270680, V-270681, V-270683, V-270684, V-270685, V-270686, V-270687, V-270688, V-270689, V-270692, V-270693, V-270696, V-270697, V-270698, V-270699, V-270700, V-270701, V-270702, V-270703, V-270704, V-270705, V-270715, V-270716, V-270718, V-270720, V-270721, V-270722, V-270723, V-270724, V-270725, V-270725, V-270725 26, V-270727, V-270728, V-270729, V-270730, V-270731, V-270732, V-270733, V-270737, V-270739, V-270740, V-270741, V-270742, V-270743, V-270746, V-270750, V-270753, V-270755, V-270756, V-270757, V-270758, V-270759, V-270760, V-270765, V-270766, V-270766, V-270766, V-270767, V-270768, V-270769, V-270770, V-270771, V-270772, V-270773, V-270775, V-270776, V-270777, V-270778, V-270779, V-270780, V-270781, V-270782, V-270783, V-270784, V-270785, V-270786, V-270787, V-270788, V-270789, V-270790, V-270791, V-270792, V-270793, V-270794, V-270795, V-270796, V-270797, V-270798, V-270799, V-270800, V-270801, V-270801, V-270801 2, V-270803, V-270804, V-270805,

V-270806, V-270807, V-270808, V-270809, V-270810, V-270811, V-270812, V-270813, V-270814, V-270821, V-270822, V-270823, V-270824, V-270825, V-270826, V-270827, V-270828, V-270829, V-270829 0830, V-270831 e V-270832

Linux STIG High (categoria I)

A lista a seguir contém as configurações STIG que a Amazon EC2 oferece suporte à sua infraestrutura. Se uma configuração compatível não for aplicável à sua infraestrutura, a Amazon EC2 ignora essa configuração e segue em frente. Por exemplo, algumas configurações de fortalecimento do STIG podem não se aplicar a servidores autônomos. Políticas específicas da organização também podem afetar as configurações aplicáveis, como um requisito para que os administradores revisem as configurações do documento.

Para obter uma lista completa, consulte a Biblioteca de STIGs documentos. Para obter informações sobre como visualizar a lista completa, consulte STIG Viewing Tools.

> **Note**
>
> A categoria Linux STIG High inclui todas as configurações de fortalecimento STIG listadas que se aplicam às categorias Linux STIG Medium e Low, além das configurações de fortalecimento STIG que a Amazon suporta para vulnerabilidades de Categoria I. EC2

RHEL 7 STIG Versão 3 Versão 15

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

- RHEL 7/CentOS 7/ AL2

  V-204424, V-204425, V-204442, V-204443, V-204447, V-204448, V-204455, V-204497, V-204502, V-204594, V-204620 e V-204621

RHEL 8 STIG Versão 2 Versão 2

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

- RHEL 8/CentOS 8/AL 2023

V-230223, V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533, V-230558 e V-244540

RHEL 9 STIG Versão 2 Versão 3

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

- RHEL 9/CentOS Stream 9

  V-257820, V-257821, V-257826, V-257835, V-257955, V-257956, V-258059, V-258230, V-258238, V-257784, V-257785, V-257984, V-257986, V-258078, V-258094 e V-258235

Ubuntu 18.04 STIG versão 2 versão 15

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-219157, V-219158, V-219177, V-219212, V-219308, V-219314, V-219316, V-251507 e V-264388

Ubuntu 20.04 STIG Versão 2 Versão 2

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-238218, V-238219, V-238201, V-251504, V-238326, V-238327 e V-238380

Ubuntu 22.04 STIG Versão 2 Versão 3

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-260482, V-260483, V-260523, V-260524, V-260469, V-260526, V-260529, V-260570, V-260571, V-260579 e V-260539

Ubuntu 24.04 STIG Versão 1 Versão 1

Inclui todas as configurações de fortalecimento do STIG que a Amazon EC2 suporta para vulnerabilidades das categorias II e III (média e baixa), além de:

V-270647, V-270648, V-270665, V-270666, V-270708, V-270717, V-270711, V-270712, V-270713 e V-270714

Histórico de versões do STIG do Linux

Esta seção registra o histórico de versões do componente do Linux para as atualizações trimestrais do STIG. Para ver as alterações e as versões publicadas de um trimestre, escolha o título para expandir as informações.

Alterações no primeiro trimestre de 2025 - 11/04/2025:

Atualizou as seguintes versões do STIG, aplicou o STIGS na versão do primeiro trimestre de 2025 e adicionou suporte ao Ubuntu 24.04:

STIG-Build-Linux-Low versão 2025.1.x

- RHEL 7 STIG Versão 3 Versão 15
- RHEL 8 STIG Versão 2 Versão 2
- RHEL 9 STIG Versão 2 Versão 3
- Ubuntu 18.04 STIG versão 2 versão 15
- Ubuntu 20.04 STIG Versão 2 Versão 2
- Ubuntu 22.04 STIG Versão 2 Versão 3
- Ubuntu 24.04 STIG Versão 1 Versão 1

STIG-Build-Linux-Medium versão 2025.1.x

- RHEL 7 STIG Versão 3 Versão 15
- RHEL 8 STIG Versão 2 Versão 2
- RHEL 9 STIG Versão 2 Versão 3
- Ubuntu 18.04 STIG versão 2 versão 15
- Ubuntu 20.04 STIG Versão 2 Versão 2
- Ubuntu 22.04 STIG Versão 2 Versão 3
- Ubuntu 24.04 STIG Versão 1 Versão 1

STIG-Build-Linux-High versão 2025.1.x

- RHEL 7 STIG Versão 3 Versão 15

- RHEL 8 STIG Versão 2 Versão 2
- RHEL 9 STIG Versão 2 Versão 3
- Ubuntu 18.04 STIG versão 2 versão 15
- Ubuntu 20.04 STIG Versão 2 Versão 2
- Ubuntu 22.04 STIG Versão 2 Versão 3
- Ubuntu 24.04 STIG Versão 1 Versão 1

Alterações no quarto trimestre de 2024 - 12/10/2024:

Atualizou as seguintes versões do STIG, aplicou o STIGS para a versão do quarto trimestre de 2024 e adicionou informações sobre dois novos parâmetros de entrada para os componentes Linux:

STIG-Build-Linux-Low versão 2024.4.x

- RHEL 7 STIG Versão 3 Versão 15
- RHEL 8 STIG Versão 2 Versão 1
- RHEL 9 STIG Versão 2 Versão 2
- Ubuntu 18.04 STIG versão 2 versão 15
- Ubuntu 20.04 STIG versão 2, versão 1
- Ubuntu 22.04 STIG Versão 2 Versão 2

STIG-Build-Linux-Medium versão 2024.4.x

- RHEL 7 STIG Versão 3 Versão 15
- RHEL 8 STIG Versão 2 Versão 1
- RHEL 9 STIG Versão 2 Versão 2
- Ubuntu 18.04 STIG versão 2 versão 15
- Ubuntu 20.04 STIG versão 2, versão 1
- Ubuntu 22.04 STIG Versão 2 Versão 2

STIG-Build-Linux-High versão 2024.4.x

- RHEL 7 STIG Versão 3 Versão 15
- RHEL 8 STIG Versão 2 Versão 1

- RHEL 9 STIG Versão 2 Versão 2
- Ubuntu 18.04 STIG versão 2 versão 15
- Ubuntu 20.04 STIG versão 2, versão 1
- Ubuntu 22.04 STIG Versão 2 Versão 2

Alterações no terceiro trimestre de 2024 - 10/04/2024 (sem alterações):

Não houve alterações no componente Linux STIGS para a versão do terceiro trimestre de 2024.

Alterações no segundo trimestre de 2024 (10/5/2024):

Versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2024. Compatibilidade com RHEL 9, CentOS Stream 9 e Ubuntu 22.04 adicionada, conforme a seguir:

STIG-Build-Linux-Low versão 2024.2.x

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 14
- RHEL 9 STIG Versão 1 Release 3
- Ubuntu 18.04 STIG Versão 2 Release 14
- Ubuntu 20.04 STIG Versão 1 Release 12
- Ubuntu 22.04 STIG Versão 1 Release 1

STIG-Build-Linux-Medium versão 2024.2.x

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 14
- RHEL 9 STIG Versão 1 Release 3
- Ubuntu 18.04 STIG Versão 2 Release 14
- Ubuntu 20.04 STIG Versão 1 Release 12
- Ubuntu 22.04 STIG Versão 1 Release 1

STIG-Build-Linux-High versão 2024.2.x

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 14

- RHEL 9 STIG Versão 1 Release 3
- Ubuntu 18.04 STIG Versão 2 Release 14
- Ubuntu 20.04 STIG Versão 1 Release 12
- Ubuntu 22.04 STIG Versão 1 Release 1

Alterações no primeiro trimestre de 2024 (6/2/2024):

Versões do STIG atualizadas e STIGS aplicados para o lançamento do primeiro trimestre de 2024 da seguinte forma:

STIG-Build-Linux-Low versão 2024.1.x

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 13
- Ubuntu 18.04 STIG Versão 2 Release 13
- Ubuntu 20.04 STIG Versão 1 Release 11

STIG-Build-Linux-Medium versão 2024.1.x

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 13
- Ubuntu 18.04 STIG Versão 2 Release 13
- Ubuntu 20.04 STIG Versão 1 Release 11

STIG-Build-Linux-High versão 2024.1.x

- RHEL 7 STIG Versão 3 Release 14
- RHEL 8 STIG Versão 1 Release 13
- Ubuntu 18.04 STIG Versão 2 Release 13
- Ubuntu 20.04 STIG Versão 1 Release 11

Alterações no quarto trimestre de 2023 (7/12/2023):

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2023 da seguinte forma:

STIG-Build-Linux-Low versão 2023.4.x

- RHEL 7 STIG Versão 3 Release 13
- RHEL 8 STIG Versão 1 Release 12
- Ubuntu 18.04 STIG Versão 2 Release 12
- Ubuntu 20.04 STIG Versão 1 Release 10

STIG-Build-Linux-Medium versão 2023.4.x

- RHEL 7 STIG Versão 3 Release 13
- RHEL 8 STIG Versão 1 Release 12
- Ubuntu 18.04 STIG Versão 2 Release 12
- Ubuntu 20.04 STIG Versão 1 Release 10

STIG-Build-Linux-High versão 2023.4.x

- RHEL 7 STIG Versão 3 Release 13
- RHEL 8 STIG Versão 1 Release 12
- Ubuntu 18.04 STIG Versão 2 Release 12
- Ubuntu 20.04 STIG Versão 1 Release 10

Alterações no terceiro trimestre de 2023 - 04/10/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do terceiro trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 12
- RHEL 8 STIG Versão 1 Release 11
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 9

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 12
- RHEL 8 STIG Versão 1 Release 11
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 9

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 12
- RHEL 8 STIG Versão 1 Release 11
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 9

Alterações no segundo trimestre de 2023 - 03/05/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 11
- RHEL 8 STIG Versão 1 Release 10
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 8

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 11
- RHEL 8 STIG Versão 1 Release 10
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 8

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 11
- RHEL 8 STIG Versão 1 Release 10
- Ubuntu 18.04 STIG Versão 2 Release 11
- Ubuntu 20.04 STIG Versão 1 Release 8

Alterações no primeiro trimestre de 2023 - 27/03/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do primeiro trimestre de 2023 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 10
- RHEL 8 STIG Versão 1 Release 9
- Ubuntu 18.04 STIG Versão 2 Release 10
- Ubuntu 20.04 STIG Versão 1 Release 7

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 10
- RHEL 8 STIG Versão 1 Release 9
- Ubuntu 18.04 STIG Versão 2 Release 10
- Ubuntu 20.04 STIG Versão 1 Release 7

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 10
- RHEL 8 STIG Versão 1 Release 9
- Ubuntu 18.04 STIG Versão 2 Release 10
- Ubuntu 20.04 STIG Versão 1 Release 7

Alterações no quarto trimestre de 2022 - 01/02/2023:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2022 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 9
- RHEL 8 STIG Versão 1 Release 8
- Ubuntu 18.04 STIG Versão 2 Release 9
- Ubuntu 20.04 STIG Versão 1 Release 6

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 9
- RHEL 8 STIG Versão 1 Release 8
- Ubuntu 18.04 STIG Versão 2 Release 9
- Ubuntu 20.04 STIG Versão 1 Release 6

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 9
- RHEL 8 STIG Versão 1 Release 8
- Ubuntu 18.04 STIG Versão 2 Release 9
- Ubuntu 20.04 STIG Versão 1 Release 6

Alterações no terceiro trimestre de 2022 - 30/09/2022 (sem alterações):

Não houve alterações no componente STIGS do Linux para o release do terceiro trimestre de 2022.

Alterações no segundo trimestre de 2022 - 02/08/2022:

Suporte do Ubuntu introduzido, versões do STIG atualizadas e STIGS aplicados para o release do segundo trimestre de 2022 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 7

- RHEL 8 STIG Versão 1 Release 6
- Ubuntu 18.04 STIG Versão 2 Release 6 (novo)
- Ubuntu 20.04 STIG Versão 1 Release 4 (novo)

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 7
- RHEL 8 STIG Versão 1 Release 6
- Ubuntu 18.04 STIG Versão 2 Release 6 (novo)
- Ubuntu 20.04 STIG Versão 1 Release 4 (novo)

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 7
- RHEL 8 STIG Versão 1 Release 6
- Ubuntu 18.04 STIG Versão 2 Release 6 (novo)
- Ubuntu 20.04 STIG Versão 1 Release 4 (novo)

Alterações no primeiro trimestre de 2022 - 26/04/2022:

Refatorado para incluir melhor suporte para contêineres. Combinou o AL2 script anterior com o RHEL 7. Versões do STIG atualizadas e STIGS aplicados para o release do primeiro trimestre de 2022 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 6
- RHEL 8 STIG Versão 1 Release 5

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 6
- RHEL 8 STIG Versão 1 Release 5

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 6
- RHEL 8 STIG Versão 1 Release 5

Alterações no quarto trimestre de 2021 - 20/12/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do quarto trimestre de 2021 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 5
- RHEL 8 STIG Versão 1 Release 4

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 5
- RHEL 8 STIG Versão 1 Release 4

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 5
- RHEL 8 STIG Versão 1 Release 4

Alterações no terceiro trimestre de 2021 - 30/09/2021:

Versões do STIG atualizadas e STIGS aplicados para o release do terceiro trimestre de 2021 da seguinte forma:

Linux STIG Low (categoria III)

- RHEL 7 STIG Versão 3 Release 4
- RHEL 8 STIG Versão 1 Release 3

Linux STIG Medium (categoria II)

- RHEL 7 STIG Versão 3 Release 4

- RHEL 8 STIG Versão 1 Release 3

Linux STIG High (categoria I)

- RHEL 7 STIG Versão 3 Release 4
- RHEL 8 STIG Versão 1 Release 3

AWSEC2-PatchLoadBalancerInstance

Descrição

Atualize e corrija uma versão secundária de uma EC2 instância da Amazon (Windows ou Linux) conectada a qualquer balanceador de carga (clássico, ALB ou NLB). O tempo padrão de drenagem da conexão é aplicado antes que a instância seja corrigida. Você pode substituir o tempo de espera inserindo seu tempo de drenagem personalizado em minutos (1-59) para o ConnectionDrainTimeparâmetro.

O workflow da automação é o seguinte:

1. O balanceador de carga ou o grupo de destino ao qual a instância está vinculada é determinado e a instância é verificada como íntegra.
2. A instância é removida do balanceador de carga ou do grupo de destino.
3. A automação aguarda o período de tempo especificado para o tempo de drenagem da conexão.
4. A RunPatchBaseline automação da AWS é chamada para corrigir a instância.
5. A instância é reanexada ao balanceador de carga ou ao grupo de destino.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Pré-requisitos

- Verifique se o SSM Agent está instalado na sua instância. Para obter mais informações, consulte Trabalhando com o SSM Agent em EC2 instâncias para Windows Server.

Parâmetros

- InstanceId

  Tipo: string

  Descrição: (obrigatório) ID da instância a ser corrigida associada a um balanceador de carga (clássico, ALB ou NLB).

- ConnectionDrainTime

  Tipo: string

  Descrição: (opcional) o tempo de drenagem da conexão do balanceador de carga, em minutos (1-59).

- S3BucketLog

  Tipo: string

  Descrição: (Opcional) O nome do bucket do Amazon S3 a ser usado para armazenar as respostas de saída do comando. Você pode especificar um bucket que você possui ou um bucket que é compartilhado com você. Se você fornecer esse parâmetro, também deverá fornecer runCommandAssumeRole.

- runCommandAssumeFunção

  Tipo: string

  Descrição: (Opcional) O ARN da função do IAM a ser usado para executar o comando na instância. A função deve ter uma relação de confiança com o responsável pelo **ssm.amazonaws.com** serviço, deve ter a SSMManaged InstanceCore política da Amazon anexada e deve ter permissões de gravação para o bucket do Amazon S3 especificado para o S3. BucketLog

AWSEC2-SQLServerDBRestore

Descrição

O `AWSEC2-SQLServerDBRestore` runbook restaura os backups do banco de dados do Microsoft SQL Server armazenados no Amazon S3 para o SQL Server 2017 executado em uma instância Linux do Amazon Elastic Compute Cloud EC2 (). Você pode fornecer sua própria EC2 instância executando o SQL Server 2017 Linux. Se uma EC2 instância não for fornecida, a automação inicia e configura uma nova EC2 instância do Ubuntu 16.04 com o SQL Server 2017. A automação oferece suporte à restauração de backups de logs completos, diferenciais e transacionais. Essa automação aceita vários arquivos de backup de banco de dados e restaura automaticamente o backup válido mais recente de cada banco de dados nos arquivos fornecidos.

Para automatizar o backup e a restauração de um banco de dados SQL Server local em uma EC2 instância executando o SQL Server 2017 Linux, você pode usar o script AWS PowerShell -signed. `MigrateSQLServerToEC2Linux`

> **Important**
>
> Esse runbook redefine a senha do usuário SA do SQL Server sempre que o fluxo de trabalho é executado. Depois que a automação estiver concluída, você deverá definir sua própria senha de usuário SA novamente antes de se conectar à instância do SQL Server.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Pré-requisitos

Para executar esta automação, você deve cumprir os seguintes pré-requisitos:

- O usuário ou a função do IAM que executa esta automação deve ter uma política embutida anexada às permissões descritas em Permissões obrigatórias do IAM.

- Se você fornecer sua própria EC2 instância:
  - A EC2 instância que você fornece deve ser uma instância Linux executando o Microsoft SQL Server 2017.
  - A EC2 instância que você fornece deve ser configurada com um perfil de instância AWS Identity and Access Management (IAM) que tenha a política `AmazonSSMManagedInstanceCore` gerenciada anexada. Para obter mais informações, consulte Criar um perfil de instância do IAM para o Systems Manager.
  - O agente SSM deve estar instalado na sua EC2 instância. Para obter mais informações, consulte Instalação e configuração do SSM Agent em EC2 instâncias para Linux.
  - A EC2 instância deve ter espaço livre em disco suficiente para baixar e restaurar os backups do SQL Server.

Limitações

Essa automação não oferece suporte à restauração para o SQL Server em execução em EC2 instâncias de Windows Server. Essa automação restaura somente backups de banco de dados compatíveis com o SQL Server Linux 2017. Para obter mais informações, consulte Edições e recursos compatíveis do SQL Server 2017 no Linux.

Parâmetros

Essa automação tem os seguintes parâmetros:

- DatabaseNames

  Tipo: string

  Descrição: (opcional) Uma lista separada por vírgulas dos nomes de bancos de dados a serem restaurados.
- DataDirectorySize

  Tipo: string

  Descrição: (Opcional) Tamanho de volume desejado (GiB) do diretório de dados do SQL Server para a nova EC2 instância.

  Valor padrão: 100
- KeyPair

Tipo: string

Descrição: (Opcional) Par de chaves a ser usado ao criar a nova EC2 instância.

- IamInstanceProfileName

  Tipo: string

  Descrição: (Opcional) O perfil da instância do IAM a ser anexado à nova EC2 instância. O perfil de instância do IAM deve ter a política gerenciada pelo `AmazonSSMManagedInstanceCore` anexada.

- InstanceId

  Tipo: string

  Descrição: (opcional) A instância executando o SQL Server 2017 no Linux. Se nenhum InstanceId for fornecido, a automação iniciará uma nova EC2 instância usando a SQLServer edição InstanceType e fornecida.

- InstanceType

  Tipo: string

  Descrição: (Opcional) O tipo de instância da EC2 instância a ser executada.

- ISS3 PresignedUrl

  Tipo: string

  Descrição: (opcional) Se S3Input for um URL do S3 pré-assinado, indique `yes`.

  Valor padrão: Não

  Valores válidos: sim | não

- LogDirectorySize

  Tipo: string

  Descrição: (Opcional) Tamanho de volume desejado (GiB) do diretório de log do SQL Server para a nova EC2 instância.

  Valor padrão: 100

- S3Input

  Tipo: string

  Descrição: (Obrigatório) Nome do bucket do S3, lista separada por vírgula das chaves de objeto do S3 ou lista separada por vírgula do S3 pré-assinado URLs contendo os arquivos de backup SQL a serem restaurados.

- SQLServerEdição

  Tipo: string

  Descrição: (Opcional) A edição do SQL Server 2017 a ser instalada na EC2 instância recém-criada.

  Valores permitidos: Standard | Enterprise | Web | Express

- SubnetId

  Tipo: string

  Descrição: (Opcional) A sub-rede na qual executar a nova EC2 instância. A sub-rede deve ter conectividade de saída com os serviços. AWS Se um valor para não SubnetId for fornecido, a automação usará a sub-rede padrão.

- TempDbDirectorySize

  Tipo: string

  Descrição: (Opcional) Tamanho de volume desejado (GiB) do diretório TempDB do SQL Server para a nova instância. EC2

  Valor padrão: 100

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

```
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstances",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ssm:DescribeInstanceInformation",
                "ssm:GetAutomationExecution",
                "ssm:ListCommandInvocations",
                "ssm:ListCommands",
                "ssm:SendCommand",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::ACCOUNTID:role/ROLENAME"
        }
    ]
}
```

Etapas do documento

Para usar esta automação, siga as etapas que se aplicam ao seu tipo de instância:

Para novas EC2 instâncias:

1. `aws:executeAwsApi`: recupera o ID da AMI para o SQL Server 2017 no Ubuntu 16.04.
2. `aws:runInstances`- Inicie uma nova EC2 instância para Linux.
3. `aws:waitForAwsResourceProperty`- Aguarde até que a EC2 instância recém-criada esteja pronta.
4. `aws:executeAwsApi`: reinicializa a instância se ela não estiver pronta.
5. `aws:assertAwsResourceProperty`: verifica se o SSM Agent está instalado.
6. `aws:runCommand`- Execute o script de restauração do SQL Server em PowerShell.

Para EC2 instâncias existentes:

1. `aws:waitForAwsResourceProperty`- Verifique se a EC2 instância está pronta.
2. `aws:executeAwsApi`: reinicializa a instância se ela não estiver pronta.
3. `aws:assertAwsResourceProperty`: verifica se o SSM Agent está instalado.
4. `aws:runCommand`- Execute o script de restauração do SQL Server em PowerShell.

Saídas

getInstance. InstanceId

restoreToNewInstância.Saída

restoreToExistingInstância.Saída

AWSSupport-ActivateWindowsWithAmazonLicense

Descrição

O `AWSSupport-ActivateWindowsWithAmazonLicense` runbook ativa uma instância do Amazon Elastic Compute Cloud (Amazon EC2) para Windows Server com uma licença fornecida pela Amazon. A automação verifica e define as configurações necessárias do sistema operacional do serviço de gerenciamento de chaves e tenta a ativação. Isso inclui rotas do sistema operacional para os servidores de gerenciamento de chaves do Amazon e configurações do sistema operacional do serviço de gerenciamento de chaves. Definir o `AllowOffline` parâmetro para `true` permitir que a automação atinja com sucesso instâncias que não são gerenciadas por AWS Systems Manager, mas exigem uma parada e início da instância.

> **Note**
>
> Este runbook não pode ser usado no modelo Bring Your Own License (BYOL) Windows Server instâncias. Para obter informações sobre como usar sua própria licença, consulte Licenciamento da Microsoft na AWS.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AllowOffline

  Tipo: string

  Valores válidos: True | False

  Padrão: False

  Descrição: (opcional) defina como `true` se você permitir a correção da ativação do Windows offline caso houver falha na correção de problemas online ou caso a instância fornecida não seja uma instância gerenciada.

  > **Important**
  >
  > O método off-line exige que a EC2 instância fornecida seja interrompida e depois iniciada. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um IP elástico.

- AutomationAssumeRole

  Tipo: string

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ForceActivation

  Tipo: string

  Valores válidos: True | False

Padrão: False

Descrição: (opcional) defina como `true` se você deseja continuar, mesmo se o Windows já estiver ativado.

- InstanceId

  Tipo: string

  Descrição: ID (obrigatório) da sua EC2 instância gerenciada para Windows Server.

- SubnetId

  Tipo: string

  Padrão: CreateNew VPC

  Descrição: (Opcional) Somente off-line - O ID de sub-rede da instância do EC2 Rescue usado para realizar a solução de problemas off-line. Use `SelectedInstanceSubnet` para usar a mesma sub-rede como sua instância, ou `CreateNewVPC` para criar uma nova VPC. IMPORTANTE: A sub-rede deve estar na mesma InstanceId zona de disponibilidade e permitir o acesso aos endpoints do SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Recomendamos que a EC2 instância que recebe o comando tenha uma função do IAM com a política gerenciada SSMManaged InstanceCore da Amazon Amazon anexada. Você deve ter pelo menos ssm: StartAutomationExecution e ssm: SendCommand para executar a automação e enviar o comando para a instância, além de ssm: GetAutomationExecution para poder ler a saída da automação. Para a correção offline, consulte as permissões exigidas pelo `AWSSupport-StartEC2RescueWorkflow`.

Etapas do documento

1. `aws:assertAwsResourceProperty`: verifique se a plataforma da instância fornecida é Windows.
2. `aws:assertAwsResourceProperty`: confirme se a instância fornecida é uma instância gerenciada:

a. (Correção de ativação online) Se a instância de entrada for uma instância gerenciada, execute `aws:runCommand` para executar o PowerShell script para tentar corrigir a ativação do Windows.

b. (Correção de ativação offline) Se a instância de entrada não for uma instância gerenciada:

   i. `aws:assertAwsResourceProperty`: verifica se o sinalizador `AllowOffline` está definido como `true`. Se esse for o caso, a correção offline é iniciada; caso contrário, o fluxo de trabalho termina.

   ii. `aws:executeAutomation`: invocar `AWSSupport-StartEC2RescueWorkflow` com o script de correção offline de ativação do Windows. O script usa EC2 Config ou EC2 Launch, dependendo da versão do sistema operacional.

   iii. `aws:executeAwsApi`: lê o resultado de `AWSSupport-StartEC2RescueWorkflow`.

Saídas

activateWindows.Output

getActivateWindowsOfflineResult.Saída

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

Descrição

O `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook analisa a conectividade de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou interface de rede elástica com um endpoint. AWS service (Serviço da AWS) IPv6 não é suportado. O runbook usa o valor que você especifica para o parâmetro `ServiceEndpoint` para analisar a conectividade com um endpoint. Se não for possível encontrar um endpoint do AWS PrivateLink em sua VPC, o runbook usa um endereço IP público para o serviço na Região da AWS atual. Esta automação usa o Reachability Analyzer da Amazon Virtual Private Cloud. Para obter mais informações, consulte O que é o Reachability Analyzer?, no Reachability Analyzer.

Esta automação verifica o seguinte:

- Verifica se sua nuvem privada virtual (VPC) está configurada para usar o servidor DNS fornecido pela Amazon.
- Verifica se existe um AWS PrivateLink endpoint na VPC para AWS service (Serviço da AWS) o que você especifica. Se um endpoint for encontrado, a automação verifica se o atributo `privateDns` está ativado.

- Verifica se o AWS PrivateLink endpoint está usando a política de endpoint padrão.

Considerações

- Você é cobrado por análise executada entre a origem e o destino. Para obter mais informações, consulte Precificação da Amazon VPC.
- Durante a automação, um caminho de insights de rede e uma análise de insights de rede são criados. Se a automação for concluída com êxito, o runbook excluirá esses recursos. Se a etapa de limpeza falhar, o caminho de insights de rede não será excluído pelo runbook e você precisará excluí-lo manualmente. Se você não excluir o caminho de insights de rede manualmente, ele continuará contando para a cota da sua Conta da AWS. Para obter mais informações sobre cotas para o Reachability Analyzer, consulte Cotas para o Reachability Analyzer no Reachability Analyzer.
- Configurações em nível de sistema operacional, como o uso de um proxy, resolvedor de DNS local ou arquivo de hosts, podem afetar a conectividade mesmo se o Reachability Analyzer retornar `PASS`.
- Revise a avaliação de todas as verificações realizadas pelo Reachability Analyzer. Se alguma das verificações retornar com um status de `FAIL`, isso poderá afetar a conectividade, mesmo que a verificação geral de acessibilidade retorne um status de `PASS`.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Origem

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon ou da interface de rede a partir da qual você deseja analisar a acessibilidade.

- ServiceEndpoint

  Tipo: string

  Descrição: (obrigatório) o nome do host do endpoint do serviço ao qual você deseja analisar a acessibilidade.

- RetainVpcReachabilityAnalysis

  Tipo: string

  Padrão: False

  Descrição: (opcional) determina se o caminho de insight de rede e a análise relacionada criada são retidos. Por padrão, os recursos usados para analisar a acessibilidade são excluídos após uma análise bem-sucedida. Se você optar por reter a análise, o runbook não excluirá a análise e você poderá visualizá-la no console do Amazon VPC. Um link do console está disponível na saída de automação.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

1. aws:executeScript: valida o endpoint do serviço ao tentar resolver o nome do host.
2. aws:executeScript: reúne detalhes sobre a VPC e a sub-rede.
3. aws:executeScript: avalia a configuração de DNS da VPC.
4. aws:executeScript: avalia as verificações do endpoint da VPC.
5. aws:executeScript: localiza um gateway da Internet para se conectar ao endpoint de serviço público.
6. aws:executeScript: determina o destino a ser usado para análise de acessibilidade.
7. aws:executeScript: analisa a acessibilidade da origem ao endpoint usando o Reachability Analyzer e limpa os recursos se a análise for bem-sucedida.
8. aws:executeScript: gera um relatório de avaliação de acessibilidade.
9. aws:executeScript: gera a saída em JSON.

Saídas

- generateReport.EvalReport: os resultados das verificações realizadas pela automação em formato de texto.
- generateJsonOutput.Output: uma versão mínima dos resultados no formato JSON.

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

Descrição

O AWSPremiumSupport-ChangeInstanceTypeIntelToAMD runbook automatiza as migrações de instâncias da Amazon Elastic Compute Cloud (Amazon EC2) com tecnologia Intel para os tipos de instância equivalentes com tecnologia AMD. Este runbook oferece suporte a instâncias de uso geral (M), de uso geral intermitente (T), otimizadas para computação (C) e otimizadas para memória (R) criadas no sistema Nitro. Este runbook pode ser usado em instâncias que não são gerenciadas pelo Systems Manager.

Para reduzir o risco potencial de perda de dados e tempo de inatividade, o runbook verifica o comportamento de parada da instância, se a instância está em um grupo do Amazon EC2 Auto Scaling, a integridade da instância e se o tipo de instância equivalente com tecnologia AMD está disponível na mesma zona de disponibilidade. Por padrão, esse runbook não alterará o tipo de instância se os volumes de armazenamento de instâncias estiverem anexados ou se a instância fizer parte de uma AWS CloudFormation pilha. Se você quiser alterar esse comportamento, especifique yes para um dos parâmetros AllowInstanceStoreInstances e AllowCloudFormationInstances.

> **Important**
>
> O acesso aos runbooks da AWSPremiumSupport-* requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Comparar Suporte planos.

Considerações

- Recomendamos fazer backup da sua instância antes de usar este runbook.
- A alteração do tipo de instância exige que o runbook interrompa sua instância. Quando uma instância é interrompida, todos os dados armazenados na RAM ou nos volumes de armazenamento da instância são perdidos e o IPv4 endereço público automático é liberado. Para obter mais informações, consulte Interromper e iniciar sua instância.
- Se você não especificar um valor para o TargetInstanceType parâmetro, o runbook tentará identificar a instância AMD equivalente em termos de memória CPUs e virtual dentro da mesma família de instâncias. O runbook termina se não for capaz de identificar um tipo de instância AMD equivalente.

- Ao usar a opção `DryRun`, você pode capturar o tipo de instância AMD equivalente e validar os requisitos sem realmente alterar o tipo de instância.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Reconhecer

  Tipo: string

  Descrição: (obrigatório) digite `yes` para confirmar que sua instância de destino será interrompida se estiver em execução.
- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon cujo tipo você deseja alterar.
- TargetInstanceType

  Tipo: string

Padrão: automático

Descrição: (opcional) o tipo de instância AMD para a qual você deseja alterar sua instância. O `automatic` valor padrão usa o tipo de instância equivalente em termos de memória CPUs e virtual. Por exemplo, um m5.large seria alterado para m5a.large.

- AllowInstanceStoreInstances

  Tipo: string

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se você especificar `yes`, o runbook é executado em instâncias que têm volumes de armazenamento de instâncias anexados.

- AllowCloudFormationInstances

  Tipo: string

  Valores válidos: não | sim

  Padrão: não

  Descrição: (Opcional) Se definido como`yes`, o runbook é executado em instâncias que fazem parte de uma AWS CloudFormation pilha.

- AllowCrossGeneration

  Tipo: string

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se definido como `yes`, o runbook tenta encontrar o tipo de instância AMD equivalente mais recente dentro da mesma família de instâncias.

- DryRun

  Tipo: string

  Valores válidos: não | sim

Padrão: não

Descrição: (opcional) se definido como `yes`, o runbook retorna o tipo de instância AMD equivalente e valida os requisitos de migração sem fazer alterações no tipo de instância.

- SleepWait

  Tipo: string

  Padrão: PT3 S

  Descrição: (opcional) o tempo que o runbook deve esperar antes de iniciar uma nova automação. O valor fornecido para esse parâmetro deve corresponder ao padrão ISO 8601. Para obter mais informações sobre a criação de sequências de caracteres ISO 8601, consulte Formatar strings de data e hora para o Systems Manager.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

1. `aws:assertAwsResourceProperty`: confirma que o status da EC2 instância de destino da Amazon é`running`,, `pending``stopped`, ou`stopping`. Caso contrário, a automação termina.
2. `aws:executeAwsApi`: reúne propriedades da EC2 instância de destino da Amazon.
3. `aws:branch`: ramifica a automação com base no estado da EC2 instância da Amazon.
   a. Em caso `stopped` `stopping` afirmativo, a automação será executada `aws:waitForAwsResourceProperty` até que a EC2 instância da Amazon seja totalmente interrompida.
   b. Em caso `running` afirmativo`pending`, a automação será executada `aws:waitForAwsResourceProperty` até que a EC2 instância da Amazon passe nas verificações de status.
4. `aws:assertAwsResourceProperty`: confirma que a EC2 instância da Amazon não faz parte de um grupo de Auto Scaling verificando se `aws:autoscaling:groupName` a tag foi aplicada.
5. `aws:executeAwsApi`: reúne as propriedades do tipo de instância atual para encontrar o tipo de instância AMD equivalente.
6. `aws:assertAwsResourceProperty`: confirma que o código AWS Marketplace do produto não está associado à EC2 instância da Amazon. Alguns produtos não estão disponíveis em todos os tipos de instâncias.
7. `aws:branch`: ramifica a automação dependendo se você deseja que a automação verifique se a EC2 instância da Amazon faz parte de uma AWS CloudFormation pilha
   a. Se a `aws:cloudformation:stack-name` tag for aplicada à instância, a automação será executada `aws:assertAwsResourceProperty` para confirmar que a instância não faz parte de uma AWS CloudFormation pilha.
8. `aws:branch`: ramifica a automação com base no fato de o tipo de volume raiz da instância ser Amazon Elastic Block Store (Amazon EBS).
9. `aws:assertAwsResourceProperty`: confirma se o comportamento de desligamento da instância é `stop`, e não `terminate`.
10. `aws:executeScript`: confirma que há apenas uma automação desse runbook direcionada à instância atual. Se outra automação já estiver em andamento visando a mesma instância, ela retornará um erro e terminará.
11. `aws:executeAwsApi`: retorna uma lista dos tipos de instância da AMD com a mesma quantidade de memória e CPUs v.
12. `aws:executeScript`: verifica se o tipo de instância atual é compatível e retorna o tipo de instância AMD equivalente. Se não houver equivalente, a automação termina.

13. `aws:executeScript`: confirma que o tipo de instância AMD está disponível na mesma zona de disponibilidade e verifica as permissões do IAM fornecidas.
14. `aws:branch`: ramifica a automação com base no valor do parâmetro `DryRun` ser `yes`.
15. `aws:branch`: verifica se o tipo de instância original e de destino são iguais. Se forem iguais, a automação termina.
16. `aws:executeAwsApi`: obtém o estado atual da instância.
17. `aws:changeInstanceState`: interrompe a EC2 instância da Amazon.
18. `aws:changeInstanceState`: força a instância a parar se ela estiver presa no estado de parada.
19. `aws:executeAwsApi`: altera o tipo de instância para o tipo de instância AMD de destino.
20. `aws:sleep`: espera três segundos após alterar o tipo de instância para uma eventual consistência.
21. `aws:branch`: ramifica a automação com base no estado anterior da instância. Se foi `running`, a instância é iniciada.
    a. `aws:changeInstanceState`: inicia a EC2 instância da Amazon se ela estava em execução antes de alterar o tipo de instância.
    b. `aws:waitForAwsResourceProperty`: espera que a EC2 instância da Amazon passe pelas verificações de status. Se a instância não passar nas verificações de status, altere-a de volta para seu tipo original.
        i. `aws:changeInstanceState`: interrompe a EC2 instância da Amazon antes de alterá-la para o tipo de instância original.
        ii. `aws:changeInstanceState`: força a EC2 instância da Amazon a parar antes de alterá-la para o tipo de instância original, caso ela fique presa em um estado de parada.
        iii. `aws:executeAwsApi`: altera a EC2 instância da Amazon para seu tipo original.
        iv. `aws:sleep`: espera três segundos após alterar o tipo de instância para uma eventual consistência.
        v. `aws:changeInstanceState`: inicia a EC2 instância da Amazon se ela estava em execução antes de alterar o tipo de instância.
        vi. `aws:waitForAwsResourceProperty`: espera que a EC2 instância da Amazon passe pelas verificações de status.
22. `aws:sleep`: espera antes de terminar o runbook.

AWSSupport-CheckXenToNitroMigrationRequirements

Descrição

O `AWSSupport-CheckXenToNitroMigrationRequirements` runbook verifica se uma instância do Amazon Elastic Compute Cloud (Amazon EC2) atende aos pré-requisitos para alterar com sucesso o tipo de instância de uma instância do tipo Xen para um tipo de instância baseada em Nitro. Esta automação verifica o seguinte:

- O dispositivo raiz é um volume do Amazon Elastic Block Store (Amazon EBS).
- O atributo `enaSupport` está ativado.
- O módulo ENA está instalado na instância.
- O NVMe módulo está instalado na instância. Se sim, o módulo é instalado e um script verifica se o módulo está carregado na imagem `initramfs`.
- Analisa `/etc/fstab` e procura dispositivos de blocos que estão sendo montados usando nomes de dispositivos.
- Determina se o sistema operacional (SO) usa nomes previsíveis de interface de rede por padrão.

Este runbook é compatível com os seguintes sistemas operacionais:

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Debian Server
- Ubuntu Server
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Padrão: False

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon que você deseja verificar os pré-requisitos antes de migrar para um tipo de instância baseado em Nitro.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeAwsApi: reúne detalhes sobre a instância.
- aws:executeAwsApi: coleta informações sobre o hipervisor da instância.
- aws:branch: ramifica com base no fato de a instância de destino já estar executando um tipo de instância baseado em Nitro.
- aws:branch: verifica se o SO da instância é compatível com instâncias baseadas em Nitro.
- aws:assertAwsResourceProperty: verifica se a instância especificada é gerenciada pelo Systems Manager e se o status é Online.
- aws:branch: ramifica com base no fato de o dispositivo raiz da instância ser um volume do Amazon EBS.
- aws:branch: ramifica considerando se o atributo ENA está ativado para a instância.
- aws:runCommand: verifica se há drivers do ENA na instância.
- aws:runCommand- Verifica se há NVMe motoristas na instância.
- aws:runCommand: verifica o arquivo fstab em busca de formatos não reconhecidos.
- aws:runCommand: verifica a configuração previsível do nome da interface na instância.
- aws:executeScript: gera saída com base nas etapas anteriores.

Saídas

finalOutput.output - os resultados das verificações realizadas pela automação.

AWSSupport-ConfigureEC2Metadata

Descrição

Este runbook ajuda você a configurar as opções do serviço de metadados de instância (IMDS) para instâncias do Amazon Elastic Compute Cloud (Amazon). EC2 Usando este runbook é possível configurar o seguinte:

- Imponha o uso de, IMDSv2 por exemplo, metadados.
- Configurar o valor de `HttpPutResponseHopLimit`.
- Permitir ou negar o acesso a metadados da instância.

Para obter mais informações sobre os metadados da instância, consulte Como configurar o serviço de metadados da instância no Guia do usuário da Amazon EC2 .

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Aplicar IMDSv2

  Tipo: string

Valores válidos: obrigatório | opcional

Padrão: Optional

Descrição: (Opcional) Aplicar IMDSv2. Se você escolher`required`, a EC2 instância da Amazon só será usada IMDSv2. Se você quiser`optional`, poderá escolher entre IMDSv1 e IMDSv2 para acesso aos metadados.

> **Important**
>
> Se você aplicar IMDSv2, os aplicativos que eu uso IMDSv1 podem não funcionar corretamente. Antes de aplicar IMDSv2, certifique-se de que seus aplicativos que usam o IMDS sejam atualizados para uma versão compatível. IMDSv2 Para obter informações sobre o Instance Metadata Service versão 2 (IMDSv2), consulte Como configurar o serviço de metadados de instância no Guia do usuário da Amazon EC2 .

- HttpPutResponseHopLimit

  Tipo: Integer

  Valores válidos: de 0 a 64

  Padrão: 0

  Descrição: (opcional) o limite (1 a 64) de salto de resposta HTTP PUT desejado para solicitações de metadados de instância. Esse valor controla o número de saltos que a resposta PUT pode percorrer. Para evitar que a resposta saia da instância, especifique o 1 para o valor do parâmetro.
- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon cujas configurações de metadados você deseja definir.
- MetadataAccess

  Tipo: string

  Valores válidos: Enabled | Disabled

  Padrão: habilitado

Descrição: (Opcional) Permita ou negue o acesso aos metadados da instância na EC2 instância da Amazon. Se você especificar `disabled`, todos os outros parâmetros serão ignorados e o acesso aos metadados será negado para a instância.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

1. branchOnMetadataAcesso - Automação de filiais com base no valor do `MetadataAccess` parâmetro.
2. disableMetadataAccess - Chama a ação da ModifyInstanceMetadataOptions API para desativar o acesso ao endpoint de metadados.
3. branchOnHttpPutResponseHopLimit - Automação de filiais com base no valor do `HttpPutResponseHopLimit` parâmetro.
4. maintainHopLimitAndConfigureImdsVersion - Se `HttpPutResponseHopLimit` for 0, mantém o limite de salto atual e altera outras opções de metadados.
5. waitBeforeAssertingIMDSv2Estado - Espera 30 segundos antes de afirmar IMDSv2 o status.
6. setHopLimitAndConfigureImdsVersion - Se `HttpPutResponseHopLimit` for maior que 0, configura as opções de metadados usando os parâmetros de entrada fornecidos.
7. waitBeforeAssertingHopLimit - Espera 30 segundos antes de definir as opções de metadados.
8. assertHopLimit - Afirma que a `HttpPutResponseHopLimit` propriedade está definida com o valor que você especificou.
9. branchVerificationOnIMDSv2Opção - Verificação de filiais com base no valor do `EnforceIMDSv2` parâmetro.
10. assert IMDSv2 IsOptional - Afirma o `HttpTokens` valor definido como. `optional`
11. assert IMDSv2 IsEnforced - Afirma o `HttpTokens` valor definido como. `required`

12. waitBeforeAssertingMetadataState - Espera 30 segundos antes de afirmar que o estado dos metadados está desativado.
13. assertMetadataIsDesativado - Afirma que os metadados são. `disabled`
14. describeMetadataOptions - Obtém as opções de metadados após a aplicação das alterações que você especificou.

Saídas

describeMetadataOptions.Estado

describeMetadataOptions.MetadataAccess

describeMetadataOptions.IMDSv2

describeMetadataOptions.HttpPutResponseHopLimit

`AWSSupport-ContainEC2Instance`

Descrição

O `AWSSupport-ContainEC2Instance` runbook fornece uma solução automatizada para o procedimento descrito no artigo Como faço para isolar a instância da Amazon quando me deparo com uma EC2 instância potencialmente comprometida ou suspeita? A automação se ramifica de acordo com os valores que você especificar.

Como funciona?

Esse runbook de automação `AWSSupport-ContainEC2Instance` realiza a contenção de rede de uma EC2 instância da Amazon por meio de uma série de etapas coordenadas. Quando executado no `Contain` modo, ele primeiro valida os parâmetros de entrada e verifica se a instância não foi encerrada. Em seguida, ele faz backup da configuração atual do grupo de segurança em um bucket do Amazon S3 para restauração posterior. O runbook cria dois grupos de segurança: um grupo de segurança temporário de “acesso total” e um grupo de segurança final de “contenção”. Ele gradualmente faz a transição das interfaces de rede da instância de seus grupos de segurança originais para o grupo de segurança de acesso total e, finalmente, para o grupo de segurança de contenção. Se especificado, ele cria tanto não criptografados quanto criptografados AMI backups da instância. Para instâncias em um grupo de Auto Scaling, ele processa as modificações necessárias do grupo de Auto Scaling e coloca a instância no estado de espera. Quando executado no `Release` modo, ele restaura a instância em sua configuração de rede original usando as configurações de

backup do Amazon S3. O runbook oferece suporte a um `DryRun` parâmetro para visualizar ações sem fazer alterações reais e inclui mecanismos abrangentes de tratamento e geração de relatórios de erros em todos os fluxos de trabalho de contenção e liberação.

Important

- Esse runbook executa várias operações que exigem privilégios elevados, como modificar grupos de segurança, criar AMIs, e interagindo com grupos de Auto Scaling. Essas ações podem potencialmente levar ao aumento de privilégios ou impactar outras cargas de trabalho em sua conta. Você deve analisar as permissões concedidas à função especificada pelo `AutomationAssumeRole` parâmetro e garantir que elas sejam apropriadas para o caso de uso pretendido. Você pode consultar a AWS documentação a seguir para obter mais informações sobre as permissões do IAM: `AWS Identity and Access Management (IAM) PermissionsAWS Systems Manager Automation Permissions`.
- Esse runbook executa ações mutativas que podem causar indisponibilidade ou interrupção em suas cargas de trabalho. Especificamente, ele modifica os grupos de segurança associados à Amazon EC2 Instance de destino, o que pode afetar a conectividade da rede. Além disso, se a instância fizer parte de um grupo de Auto Scaling, o runbook poderá modificar a configuração do grupo, afetando potencialmente seu comportamento de escalabilidade.
- Durante o processo de contenção, esse runbook cria recursos adicionais, como grupos de segurança e AMIs. Embora esses recursos estejam marcados para identificação, você deve estar ciente de sua criação e garantir a limpeza ou o gerenciamento adequados após a conclusão do processo de contenção.
- Se o `Action` parâmetro estiver definido como`Release`, esse runbook tentará restaurar a configuração da EC2 Instância Amazon ao seu estado original. No entanto, existe o risco de que o processo de restauração falhe, deixando a instância em um estado inconsistente. O runbook fornece instruções para restauração manual em caso de falhas desse tipo, mas você deve estar preparado para lidar com possíveis problemas durante o processo de restauração.

É recomendável revisar o runbook minuciosamente, entender seus possíveis impactos e testá-lo em um ambiente que não seja de produção antes de executá-lo em seu ambiente de produção.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- escalonamento automático: CreateOrUpdateTags
- escalonamento automático: DeleteTags
- escalonamento automático: DescribeAutoScalingGroups
- escalonamento automático: DescribeAutoScalingInstances
- escalonamento automático: DescribeTags
- escalonamento automático: EnterStandby
- escalonamento automático: ExitStandby
- escalonamento 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
- kms:CreateGrant
- kms:DescribeKey
- kms:GenerateDataKeyWithoutPlaintext
- kms:ReEncryptFrom
- kms:ReEncryptTo
- s3: CreateBucket
- s3: DeleteObjectTagging
- s3: GetAccountPublicAccessBlock
- s3: GetBucketAcl
- s3: GetBucketLocation
- s3: GetBucketOwnershipControls
- s3: GetBucketPolicy
- s3: GetBucketPolicyStatus
- s3: GetBucketPublicAccessBlock
- s3: GetObject
- s3: ListBucket
- s3: PutAccountPublicAccessBlock
- s3: PutBucketPolicy
- s3: PutBucketVersioning
- s3: PutObject
- s3: PutObjectTagging

Exemplo de política:

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

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-ContainEC2Instanceem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):
     - Descrição: (Opcional) O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
     - Tipo: `AWS::IAM::Role::Arn`
   - Ação (obrigatória):

  - Descrição: (Obrigatório) Selecione `Contain` para isolar a EC2 instância da Amazon ou `Restore` tentar restaurar a configuração original da EC2 instância da Amazon a partir de um backup anterior.
  - Tipo: String
  - Allowed-pattern: `Contain|Restore`
- DryRun (Opcional):
  - Descrição: (Opcional) Quando definida como`true`, a automação não executará nenhum dos comandos; em vez disso, relatará o que teria tentado fazer, detalhando cada etapa. Valor padrão: `true`.
  - Tipo: booliano
  - Valores permitidos: `true|false`
- Criar AMIBackup (opcional):
  - Descrição: (Opcional) Quando definido como`true`, um AMI da EC2 Instância da Amazon será criada antes de realizar as ações de contenção.
  - Tipo: booliano
  - Valores permitidos: `true|false`
- KmsKey (Opcional):
  - Descrição: (Opcional) O ID da AWS KMS chave que será usada para criar um código criptografado AMI da EC2 instância de destino da Amazon. O padrão está definido como`alias/aws/ebs`.
  - Tipo: String
  - Allowed-pattern: `^(((arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}:[0-9]{12}:key/)?([a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}|mrk-[a-f0-9]{32}))|(arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}:[0-9]{12}:)?alias/.{1,})$`
- Backups 3 BucketName (condicionais):
  - Descrição: bucket (condicional) do Amazon Amazon S3 para carregar a configuração `Action` quando `Contain` estiver ou para restaurar a configuração `Action` quando estiver. `Release` Nota: Se o bucket fornecido não existir na conta, a automação criará um bucket do Amazon S3 em seu nome.
  - Tipo: `AWS::S3::Bucket::Name`
- TagIdentifier (Opcional):

- Descrição: (Opcional) Uma tag no formato `Key=BatchId,Value=78925` que será adicionada aos AWS recursos criados ou modificados por esse runbook durante o fluxo de trabalho de contenção. Essa tag pode ser usada para identificar e gerenciar recursos associados durante o processo de contenção. Durante o fluxo de trabalho de restauração, a tag especificada por esse parâmetro será removida dos recursos. Observação: as chaves e os valores das tags diferenciam maiúsculas de minúsculas.
- Tipo: String
- Allowed-pattern: `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{0,128}$`

- Backups 3 BucketAccess (condicionais):
  - Descrição: (Condicional) O ARN dos usuários ou funções do IAM que terão acesso ao bucket de backup do Amazon S3 após a execução das ações de contenção. Esse parâmetro é necessário quando `Action` é`Contain`. O`AutomationAssumeRole`, ou, na sua ausência, o usuário sob cujo contexto a automação está sendo executada é automaticamente adicionado à lista.
  - Tipo: String
  - Allowed-pattern: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
- IngressTrafficRules (Opcional):
  - Descrição: (Opcional) Um mapa separado por vírgulas das regras de entrada do grupo de segurança com Cidr, IpProtocol, FromPort e ToPort no formato a ser aplicado `[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort":"22", "ToPort":"22"}]` à instância da Amazon. EC2 Se nenhuma regra for fornecida, um grupo de segurança sem nenhuma regra de entrada será anexado à EC2 instância da Amazon, isolando-a efetivamente de qualquer tráfego de entrada.
  - Tipo: MapList
  - Allowed-pattern: `^\\{\\}$|^\\{\"Cidr\":\"[\\x00-\\x7F+]{1,128}\",\"IpProtocol\":\"[\\x00-\\x7F+]{1,128}\",\"FromPort\":\"[\\x00-\\x7F+]{1,128}\",\"ToPort\":\"[\\x00-\\x7F+]{0,255}\"\\}`
- EgressTrafficRules (Opcional):
  - Descrição: (Opcional) Um mapa separado por vírgulas das regras de saída do grupo de segurança com Cidr IpProtocol,, FromPort e ToPort no formato a ser aplicado `[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort":"22", "ToPort":"22"}]` à

instância da Amazon Amazon. EC2 Se nenhuma regra for fornecida, um grupo de segurança sem nenhuma regra de saída será anexado à EC2 instância da Amazon, impedindo efetivamente todo o tráfego de saída.

- Tipo: MapList
- Allowed-pattern: `^\\{\\}$|^\\{\"Cidr\":\"[\\x00-\\x7F+]{1,128}\",\"IpProtocol\":\"[\\x00-\\x7F+]{1,128}\",\"FromPort\":\"[\\x00-\\x7F+]{1,128}\",\"ToPort\":\"[\\x00-\\x7F+]{0,255}\"\\}`

- BackupS3 KeyName (opcional):
  - Descrição: (Opcional) Se `Action` estiver definido como`Restore`, isso especifica a chave do Amazon S3 que a automação usará para tentar restaurar a configuração da instância EC2 Amazon de destino. A chave Amazon S3 normalmente segue este formato:. `{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json` A chave pode ser obtida da saída de uma execução anterior de automação de contenção.
  - Tipo: String
  - Allowed-pattern: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$`

4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - ValidateRequiredInputs

     Valida se todas as entradas necessárias foram fornecidas.
   - AssertInstanceIsNotTerminated

     Verifica se a EC2 Instância Amazon de destino não está encerrada (excluída).
   - GetAutoScalingInstanceInfo

     Obtém o ciclo de vida da EC2 instância Amazon e o nome do grupo se a EC2 instância de destino da Amazon fizer parte de um grupo de Auto Scaling.
   - CheckBackupS3BucketName

     Verifica se o bucket do Amazon S3 de destino potencialmente `read` concede acesso `write` público a seus objetos. Um novo bucket do Amazon S3 é criado se o `BackupS3BucketName` bucket não existir.
   - BranchOnActionAndMode

Ramifica a automação com base nos parâmetros de entrada `Action` `DryRun` e.

- BranchOnAutoScalingGroupMembership

  Ramifica a automação com base no fato de a EC2 Instância Amazon de destino fazer parte do grupo Auto Scaling e em seu estado de ciclo de vida.

- DescribeAutoScalingGroups

  Obtém e armazena a configuração de grupo associada do Amazon EC2 Auto Scaling.

- ModifyAutoScalingGroup

  Modifica a configuração do grupo associado do Amazon EC2 Auto Scaling para as ações de contenção, definindo a instância da EC2 Amazon para o estado e ajustando `Standby` a capacidade do grupo Auto Scaling. `MinSize`

- BackupInstanceSecurityGroups

  Obtém e armazena a configuração dos grupos de segurança da Amazon EC2 Instance de destino.

- CreateAllAccessSecurityGroup

  Cria um grupo de segurança temporário que permite todo o tráfego de entrada que substitui os grupos de segurança da Amazon EC2 Instance de destino.

- CreateContainmentSecurityGroup

  Cria um grupo restritivo de segurança de contenção com as regras de entrada e saída especificadas e substitui o grupo temporário de acesso total por ele.

- BranchOnCreateAMIBackup

  Ramifica a automação com base no parâmetro `CreateAMIBackup` de entrada.

- AssertSourceInstanceRootVolumeIsEbs

  Verifica se o volume raiz da EC2 Instância Amazon de destino é o Amazon EBS.

- CreateImage

  Cria um AMI da EC2 Instância Amazon de destino.

- RestoreInstanceConfiguration

  Restaura a configuração de destino da Amazon EC2 Instance a partir do backup

- ReportContain

  Produz detalhes de funcionamento a seco para as ações de contenção.

- ReportRestore

  Produz detalhes de funcionamento a seco para as ações de restauração.

- ReportRestoreFailure

  Fornece instruções para restaurar a configuração original da Amazon EC2 Instance de destino durante um cenário de falha no fluxo de trabalho de restauração.

- ReportContainmentFailure

  Fornece instruções para restaurar a configuração original da Amazon EC2 Instance de destino durante um cenário de falha no fluxo de trabalho de contenção.

- FinalOutput

  Exibe os detalhes das ações de contenção.

7. Após a conclusão da execução, revise a seção Saídas para obter os resultados detalhados da execução:

   - FinalOutput.Saída

     Exibe os detalhes das ações de contenção realizadas por esse runbook quando `DryRun` está definido como False.

   - RestoreInstanceConfiguration.Saída

     Exibe as ações de restauração executadas por esse runbook quando `DryRun` está definido como False.

   - ReportContain.Saída

     Exibe os detalhes das ações de contenção realizadas por esse runbook quando `DryRun` está definido como True.

   - ReportRestore.Saída

     Exibe os detalhes das ações de restauração executadas por esse runbook quando `DryRun` está definido como True.

   - ReportContainmentFailure.Saída

Fornece instruções para restaurar a configuração original da Amazon EC2 Instance de destino durante um cenário de falha no fluxo de trabalho de contenção.

- ReportRestoreFailure.Saída

  Fornece instruções para restaurar a configuração original da Amazon EC2 Instance de destino durante um cenário de falha no fluxo de trabalho de restauração.

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação simples
- Configurando a automação
- Fluxos de trabalho de automação de suporte

AWSSupport-CopyEC2Instance

Descrição

O `AWSSupport-CopyEC2Instance` runbook fornece uma solução automatizada para o procedimento descrito no artigo do Knowledge Center Como faço para mover minha EC2 instância para outra sub-rede, zona de disponibilidade ou VPC? A automação se ramifica dependendo dos valores que você especifica para os parâmetros `Region` e `SubnetId`.

Se você especificar um valor para o `SubnetId` parâmetro, mas não um valor para o `Region` parâmetro, a automação cria um Amazon Machine Image (AMI) da instância de destino e executa uma nova instância a partir do AMI na sub-rede que você especificou.

Se você especificar um valor para o `SubnetId` parâmetro e o `Region` parâmetro, a automação cria um AMI da instância de destino, copia o AMI para o Região da AWS que você especificou e executa uma nova instância a partir do AMI na sub-rede que você especificou.

Se você especificar um valor para o `Region` parâmetro, mas não um valor para o `SubnetId` parâmetro, a automação cria um AMI da instância de destino, copia o AMI para a região que você especificou e executa uma nova instância a partir do AMI na sub-rede padrão da sua nuvem privada virtual (VPC) na região de destino.

Se nenhum valor for especificado para os `SubnetId` parâmetros `Region` ou, a automação cria um AMI da instância de destino e executa uma nova instância a partir do AMI na sub-rede padrão da sua VPC.

Para copiar um AMI para uma região diferente, você deve fornecer um valor para o `AutomationAssumeRole` parâmetro. Se a automação expirar durante a `waitForAvailableDestinationAmi` etapa, o AMI talvez ainda esteja copiando. Se for esse o caso, você pode aguardar a conclusão da cópia e iniciar a instância manualmente.

Antes de executar esta automação, observe o seguinte:

- AMIAs s são baseadas em snapshots do Amazon Elastic Block Store (Amazon EBS). Para sistemas de arquivos grandes sem um instantâneo anterior, AMI a criação pode levar várias horas. Para diminuir o AMI no momento da criação, crie um snapshot do Amazon EBS antes de criar o AMI.
- Criando um AMI não cria um snapshot, por exemplo, armazena volumes na instância. Para obter informações sobre como fazer backup de volumes de armazenamento de instâncias no Amazon EBS, consulte Como faço backup de um volume de armazenamento de instâncias na minha instância da Amazon para o Amazon EC2 EBS?
- A nova EC2 instância da Amazon tem um endereço IPv6 IP público IPv4 ou privado diferente. Você deve atualizar todas as referências aos endereços IP antigos (por exemplo, nas entradas de DNS) com os novos endereços IP atribuídos à nova instância. Se estiver usando um endereço IP elástico na instância de origem, certifique-se de anexá-lo à nova instância.
- Problemas de conflito do identificador de segurança de domínio (SID) podem ocorrer quando a cópia é iniciada e tenta entrar em contato com o domínio. Antes de capturar a AMI, use o Sysprep ou remova a instância associada ao domínio do domínio para evitar problemas de conflito. Para obter mais informações, consulte Como posso usar o Sysprep para criar e instalar o Windows reutilizável personalizado? AMIs

Executar esta automação (console)

> **Important**
>
> Não recomendamos usar este runbook para copiar instâncias do controlador de domínio do Microsoft Active Directory.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (obrigatório) o ID da instância que você deseja reinicializar.
- KeyPair

  Tipo: string

  Descrição: (opcional) o par de chaves que você deseja associar à instância recém-copiada. Se você estiver copiando a instância para uma região diferente, verifique se o par de chaves existe na região especificada.
- Região

  Tipo: string

  Descrição: (opcional) a região para a qual você deseja copiar a instância. Se você especificar um valor para esse parâmetro, mas não especificar valores para os parâmetros `SubnetId` e `SecurityGroupIds`, a automação tentará iniciar a instância na VPC padrão com o grupo de segurança padrão. Se EC2 -Classic estiver habilitado na região de destino, o lançamento falhará.

- SubnetId

  Tipo: string

  Descrição: (opcional) o ID da sub-rede na qual você deseja copiar a instância. Se EC2 -Classic estiver ativado na região de destino, você deverá fornecer um valor para esse parâmetro.

- InstanceType

  Tipo: string

  Descrição: (opcional) o tipo da instância que a instância copiada deve ser lançada. Se você não especificar um valor para esse parâmetro, será usado o tipo de instância de origem. Se o tipo de instância de origem não for suportado na região para a qual a instância está sendo copiada, a automação falhará.

- SecurityGroupIds

  Tipo: string

  Descrição: (Opcional) Uma lista separada por vírgulas do grupo de segurança IDs que você deseja associar à instância copiada. Se você não especificar um valor para esse parâmetro e a instância não estiver sendo copiada para uma região diferente, os grupos de segurança associados à instância de origem serão usados. Se você estiver copiando a instância para uma região diferente, o grupo de segurança padrão da VPC padrão na região de destino será usado.

- KeepImageSourceRegion

  Tipo: booliano

  Valores válidos: True | False

  Padrão: verdadeiro

  Descrição: (Opcional) Se você especificar `true` esse parâmetro, a automação não excluirá o AMI da instância de origem. Se você especificar `false` esse parâmetro, a automação cancela o registro do AMI e exclui os instantâneos associados.

- KeepImageDestinationRegion

  Tipo: booliano

  Valores válidos: True | False

Padrão: verdadeiro

Descrição: (Opcional) Se você especificar `true` esse parâmetro, a automação não excluirá o AMI que é copiado para a região que você especificou. Se você especificar `false` esse parâmetro, a automação cancela o registro do AMI e exclui os instantâneos associados.

- NoRebootInstanceBeforeTakingImage

  Tipo: booliano

  Valores válidos: True | False

  Padrão: False

  Descrição: (Opcional) Se você especificar `true` esse parâmetro, a instância de origem não será reiniciada antes da criação do AMI. Quando essa opção é usada, a integridade do sistema de arquivos na imagem criada não pode ser garantida.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

Se estiver copiando a instância em outra região, você também precisará das seguintes permissões:

- `ec2:CopyImage`

Etapas do documento

- describeOriginalInstanceDetalhes - Reúne detalhes da instância a serem copiados.

- assertRootVolumeIsEbs - Verifica se o tipo de dispositivo de volume raiz é `eebs`, se não, encerra a automação.
- evalInputParameters - Avalia os valores fornecidos para os parâmetros de entrada.
- createLocalAmi - Cria um AMI da instância de origem.
- tagLocalAmi - Etiqueta o AMI criado na etapa anterior.
- branchAssertRegionIsSame - Ramificações com base no fato de a instância estar sendo copiada na mesma região ou em uma região diferente.
- branchAssertSameRegionWithKeyPair - Ramifica com base no fato de um valor ter sido fornecido para o `KeyPair` parâmetro de uma instância que está sendo copiada na mesma região.
- sameRegionLaunchInstanceWithKeyPair - Lança uma EC2 instância da Amazon a partir do AMI da instância de origem na mesma sub-rede ou na sub-rede especificada usando o par de chaves que você especificou.
- sameRegionLaunchInstanceWithoutKeyPair - Lança uma EC2 instância da Amazon a partir do AMI da instância de origem na mesma sub-rede ou na sub-rede especificada sem um par de chaves.
- copyAmiToRegião - Copia o AMI para a região de destino.
- waitForAvailableDestinationAmi - Aguarda a cópia AMI estado para se torna`available`.
- destinationRegionLaunchInstância - Lança uma EC2 instância da Amazon usando a cópia AMI.
- branchAssertDestinationAmiToDelete - Ramificações com base no valor que você forneceu para o `KeepImageDestinationRegion` parâmetro.
- deregisterDestinationAmiAndDeleteSnapshots - Cancela o registro da cópia AMI e exclui os instantâneos associados.
- branchAssertSourceAmiTodelete - Ramificações com base no valor que você forneceu para o `KeepImageSourceRegion` parâmetro.
- deregisterSourceAmiAndDeleteSnapshots - Cancela o registro do AMI criado a partir da instância de origem e exclui os instantâneos associados.
- sleep: coloca a automação em repouso por 2 segundos. Estea é uma etapa terminal.

Saídas

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchInstância. DestinationInstanceId

AWSSupport-EnableWindowsEC2SerialConsole

Descrição

O runbook `AWSSupport-EnableWindowsEC2SerialConsole` ajuda você a habilitar o Amazon EC2 Serial Console, o Special Admin Console (SAC) e o menu de inicialização na sua instância EC2 do Amazon Windows. Com o recurso Amazon Elastic Compute Cloud (Amazon EC2) Serial Console, você tem acesso à porta serial da sua EC2 instância Amazon para solucionar problemas de inicialização, configuração de rede e outros problemas. O runbook automatiza as etapas necessárias para habilitar o recurso em instâncias em estado de execução e gerenciadas por AWS Systems Manager, bem como naquelas em estado parado ou não gerenciadas por. AWS Systems Manager

Como funciona?

O runbook de `AWSSupport-EnableWindowsEC2SerialConsole` automação ajuda a habilitar o SAC e o menu de inicialização nas EC2 instâncias da Amazon que executam o Microsoft Windows Server. Para instâncias em estado de execução e gerenciadas por AWS Systems Manager, o runbook executa um PowerShell script AWS Systems Manager Executar comando para ativar o SAC e o menu de inicialização. Para instâncias em estado parado ou não gerenciadas por AWS Systems Manager, o runbook usa o AWSSupport-StartEC2 RescueWorkflow para criar uma EC2 instância temporária da Amazon para realizar as alterações necessárias off-line.

Para obter mais informações, consulte Amazon EC2 Serial Console para instâncias do Windows.

Important

- Se você habilitar o SAC em uma instância, os EC2 serviços da Amazon que dependem da recuperação de senha não funcionarão no console da Amazon EC2 . Para mais informações, consulte Use SAC to troubleshoot your Windows instance (Usar o SAC para solucionar problemas de instâncias do Windows).
- Para configurar o acesso ao console serial, você deve conceder acesso ao console serial no nível da conta e, em seguida, configurar políticas AWS Identity and Access Management (IAM) para conceder acesso aos seus usuários. Você também deve configurar um usuário com senha em cada instância para que seus usuários possam usar o console de série para solução de problemas. Para obter mais informações, consulte Configurar o acesso ao Amazon EC2 Serial Console.
- Para ver se o console serial está ativado em sua conta, consulte Exibir o status de acesso da conta ao console serial.

- O acesso ao console serial só é suportado em instâncias virtualizadas criadas no Sistema Nitro.

Para obter mais informações, consulte os pré-requisitos do Amazon EC2 Serial Console.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingInstances",
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:Describe*",
                "ec2:createTags",
                "ec2:createImage",
                "ssm:DescribeAutomationExecutions",
                "ssm:DescribeInstanceInformation",
                "ssm:GetAutomationExecution",
                "ssm:ListCommandInvocations",
                "ssm:ListCommands"
            ],
            "Resource": "*"
        },
```

```
                {
                    "Effect": "Allow",
                    "Action": [
                        "ec2:AttachVolume",
                        "ec2:DetachVolume",
                        "ec2:ModifyInstanceAttribute",
                        "ec2:RebootInstances",
                        "ec2:StartInstances",
                        "ec2:StopInstances",
                        "iam:GetInstanceProfile",
                        "ssm:GetParameters",
                        "ssm:SendCommand",
                        "ssm:StartAutomationExecution"
                    ],
                    "Resource": [
                        "arn:${Partition}:ec2:${Region}:${AccountId}:instance/
${InstanceId}",
                        "arn:${Partition}:ec2:${Region}:${AccountId}:volume/
${VolumeId}",
                        "arn:${Partition}:iam::${AccountId}:instance-profile/
${InstanceProfileName}",
                        "arn:${Partition}:ssm:${Region}::parameter/aws/service/*",
                        "arn:${Partition}:ssm:${Region}::automation-definition/
AWSSupport-StartEC2RescueWorkflow:*",
                        "arn:${Partition}:ssm:${Region}::document/AWS-
ConfigureAWSPackage",
                        "arn:${Partition}:ssm:${Region}::document/AWS-
RunPowerShellScript"
                    ]
                },
                {
                    "Effect": "Allow",
                    "Action": [
                        "cloudformation:CreateStack"
                    ],
                    "Resource": "*",
                    "Condition": {
                        "StringLike": {
                            "aws:RequestTag/Name": "AWSSupport-EC2Rescue: *"
                        },
                        "ForAllValues:StringEquals": {
                            "aws:TagKeys": [
                                "AWSSupport-EC2Rescue-AutomationExecution",
                                "Name"
```

```
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStackResource",
                "cloudformation:DescribeStacks",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:RebootInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ssm:SendCommand"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/Name": "AWSSupport-EC2Rescue: *"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateLaunchTemplate",
                "ec2:DeleteLaunchTemplate",
                "ec2:RunInstances"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "cloudformation.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                    "iam:PassRole"
                ],
                "Resource": "*",
                "Condition": {
                    "StringLikeIfExists": {
                        "iam:PassedToService": [
                            "ssm.amazonaws.com",
                            "ec2.amazonaws.com"
                        ]
                    }
                }
            }
        ]
    }
```

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até o `AWSSupport-EnableWindowsEC2SerialConsole` no AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - InstanceId: (Obrigatório)

     O ID da EC2 instância da Amazon na qual você deseja habilitar o console EC2 serial da Amazon (SAC) e o menu de inicialização.
   - AutomationAssumeRole: (Opcional)

     O Amazon Resource Name (ARN) da função do IAM que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - HelperInstanceType: (Condicional)

     O tipo de EC2 instância da Amazon que o runbook provisiona para configurar o console EC2 serial da Amazon para uma instância off-line.
   - HelperInstanceProfileName: (Condicional)

O nome de um perfil de instância do IAM existente para a instância auxiliar. Se você estiver habilitando o SAC e o menu de inicialização em uma instância que está parada ou não é gerenciada por AWS Systems Manager, isso é necessário. Se um perfil de instância do IAM não for especificado, a automação cria um em seu nome.

- SubnetId: (Condicional)

  O ID da sub-rede de uma instância auxiliar. Por padrão, ele usa a mesma sub-rede em que a instância fornecida reside.

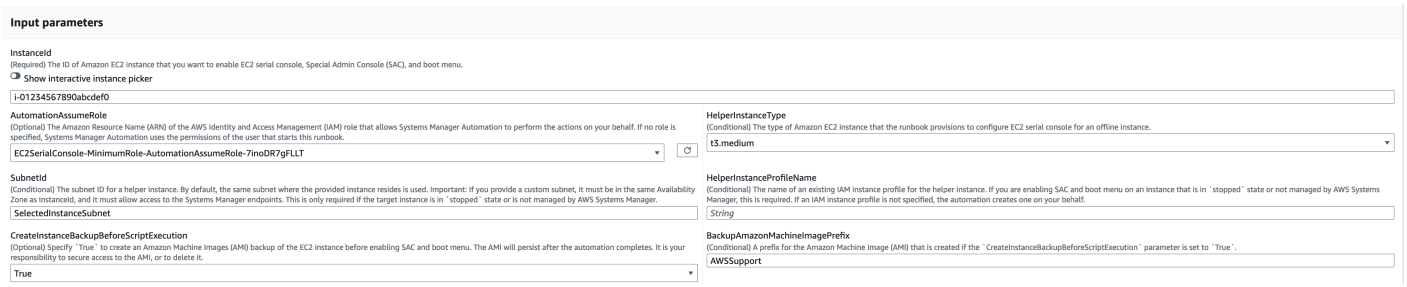
  > **Important**
  >
  > Se você fornecer uma sub-rede personalizada, ela deverá estar na mesma InstanceId zona de disponibilidade e permitir o acesso aos endpoints do Systems Manager. Isso só é necessário se a instância de destino estiver parada ou não for gerenciada pelo AWS Systems Manager.

- CreateInstanceBackupBeforeScriptExecution: (Opcional)

  Especifique True para criar um backup da Amazon Machine Images (AMI) da EC2 instância da Amazon antes de ativar o SAC e o menu de inicialização. A AMI persistirá depois da conclusão da automação. É sua responsabilidade proteger o acesso à AMI ou excluí-la.

- BackupAmazonMachineImagePrefix: (Condicional)

  Um prefixo para a Amazon Machine Image (AMI) que é criado se o `CreateInstanceBackupBeforeScriptExecution` parâmetro estiver definido como. `True`



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - CheckIfEc2SerialConsoleAccessEnabled:

Verifica se o acesso ao Amazon EC2 Serial Console está ativado no nível da conta. Nota: O acesso ao console serial não está disponível por padrão. Para obter mais informações, consulte Configurar o acesso ao Amazon EC2 Serial Console.

- CheckIfEc2InstanceIsWindows:

  Afirma se a plataforma da instância de destino é o Windows.

- GetInstanceType:

  Recupera o tipo de instância da instância de destino.

- CheckIfInstanceTypeIsNitro:

  Verifica se o hipervisor do tipo de instância é baseado em Nitro. O acesso ao console serial só é suportado em instâncias virtualizadas criadas no sistema Nitro.

- CheckIfInstanceIsInAutoScalingGroup:

  Verifica se a EC2 instância da Amazon faz parte de um grupo do Amazon EC2 Auto Scaling chamando a `DescribeAutoScalingInstances` API. Se a instância fizer parte de um grupo do Amazon EC2 Auto Scaling, ela garantirá que a instância do Porting Assistant for .NET esteja no estado de ciclo de vida em espera.

- WaitForEc2InstanceStateStablized:

  Espera que a instância esteja em execução ou parada.

- GetEc2InstanceState:

  Obtém o estado atual da instância.

- BranchOnEc2InstanceState:

  Ramificações com base no estado da instância recuperado na etapa anterior. Se esse estado de instância estiver em execução, ele vai para a `CheckIfEc2InstanceIsManagedBySSM` etapa e, se não, vai para a `CheckIfHelperInstanceProfileIsProvided` etapa.

- CheckIfEc2 InstanceIsManagedBy SMS:

  Verifica se a instância é gerenciada pelo AWS Systems Manager. Se gerenciado, o runbook ativa o SAC e o menu de inicialização usando um PowerShell comando Executar.

- BranchOnPreEC2RescueBackup:

Ramificações com base no parâmetro `CreateInstanceBackupBeforeScriptExecution` de entrada.

- CreateAmazonMachineImageBackup:

  Cria um backup da AMI da instância.

- Habilitar SACAndBootMenu:

  Ativa o SAC e o menu de inicialização executando um script PowerShell Executar comando.

- RebootInstance:

  Reinicializa a EC2 instância da Amazon para aplicar a configuração. Essa é a etapa final se a instância estiver on-line e for gerenciada pelo AWS Systems Manager.

- CheckIfHelperInstanceProfileIsProvided:

  Verifica se o `HelperInstanceProfileName` especificado existe antes de ativar o SAC e o menu de inicialização off-line usando uma EC2 instância temporária da Amazon.

- RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu:

  Executa o `AWSSupport-StartEC2RescueWorkflow` para ativar o SAC e o menu de inicialização quando a instância está parada ou não é gerenciada pelo AWS Systems Manager.

- GetExecutionDetails:

  Recupera o ID da imagem do backup e da saída do script offline.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

   - Habilitar SACAnd BootMenu .Output:

     Saída da execução do comando na `EnableSACAndBootMenu` etapa.

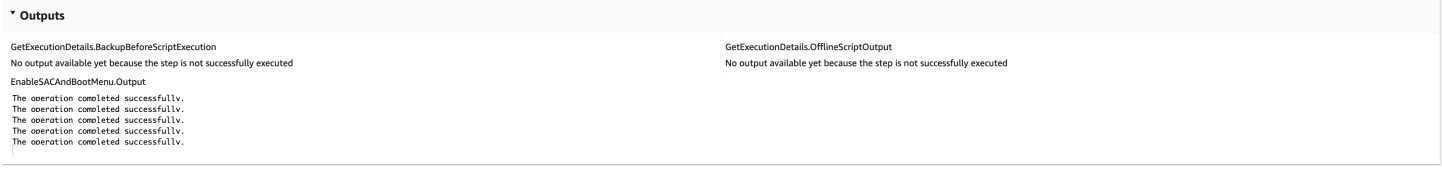
   - GetExecutionDetails.OfflineScriptOutput:

     Saída do script off-line executado na `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` etapa.

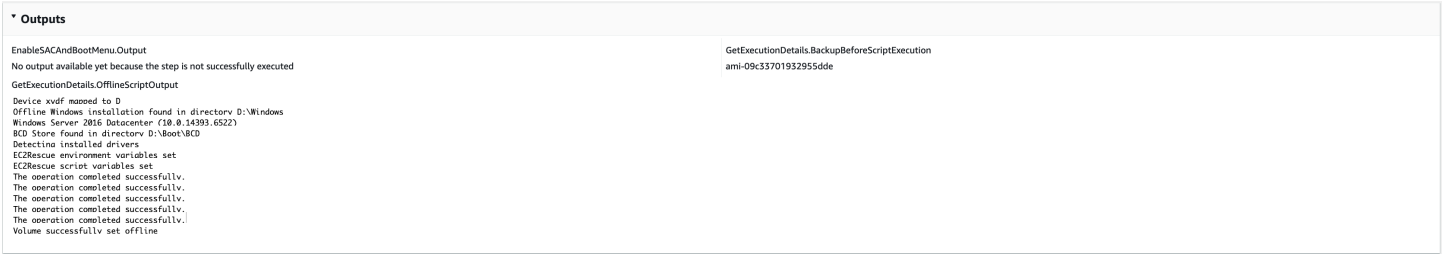
   - GetExecutionDetails.BackupBeforeScriptExecution:

     ID da imagem do backup da AMI obtido se o parâmetro `CreateInstanceBackupBeforeScriptExecution` de entrada for True.

Saída de execução em uma instância que está sendo executada e gerenciada pelo AWS Systems Manager



Saída da execução em uma instância interrompida ou não gerenciada pelo AWS Systems Manager



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSSupport-ExecuteEC2Rescue

Descrição

Este runbook usa o EC2Rescue ferramenta para solucionar e, sempre que possível, reparar problemas comuns de conectividade com a instância especificada do Amazon Elastic Compute Cloud EC2 (Amazon) para Linux ou Windows Server. Não há suporte para instâncias com volumes raiz criptografados.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- EC2RescueInstanceType

  Tipo: string

  Valores permitidos: t2.small | t2.medium | t2.large

  Padrão: t2.small

  Descrição: (Obrigatório) O tipo de EC2 instância do EC2Rescue instância. Tamanho recomendado: `t2.small`

- LogDestination

  Tipo: string

  Descrição: (opcional) nome do bucket do Amazon S3 em sua conta na qual você deseja carregar os logs de solução de problemas. Verifique se a política de buckets não concede permissões de leitura/gravação desnecessárias a partes que não precisam acessar os logs coletados.

- SubnetId

  Tipo: string

  Padrão: CreateNew VPC

Descrição: (Opcional) O ID da sub-rede do EC2Rescue instância. Por padrão, a AWS Systems Manager automação cria uma nova VPC. Como alternativa, Use `SelectedInstanceSubnet` para usar a mesma sub-rede que sua instância ou especifique um ID de sub-rede personalizado.

> **Important**
>
> A sub-rede deve estar na mesma zona de disponibilidade que o `UnreachableInstanceId`, e deve permitir acesso aos endpoints SSM.

- UnreachableInstanceId

  Tipo: string

  Descrição: (Obrigatório) ID da sua instância inacessível EC2 .

> **Important**
>
> O Systems Manager Automation interrompe essa instância e cria uma AMI antes de tentar qualquer operação. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um endereço IP elástico.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Você deve ter pelo menos `ssm:StartAutomationExecution` e `ssm:GetAutomationExecution` para poder ler a saída de automação. Para mais informações sobre as permissões necessárias, consulte [AWSSupport-StartEC2RescueWorkflow].

Etapas do documento

1. `aws:assertAwsResourceProperty`- Afirma se a instância fornecida é Windows Server:
   a. (EC2Rescue for Windows Server) Se a instância fornecida for uma Windows Server exemplo:
      i. `aws:executeAutomation`- Invoca `AWSSupport-StartEC2RescueWorkflow` com o Rescue for EC2 Windows Server script offline.
      ii. `aws:executeAwsApi`: recupera o ID AMI de backup da automação aninhada.

iii. `aws:executeAwsApi`- Recupera o resumo do EC2 Rescue da automação aninhada.

b. (EC2Rescue para Linux) Se a instância fornecida for uma instância Linux:

i. `aws:executeAutomation`- Invoca `AWSSupport-StartEC2RescueWorkflow` com os scripts offline do EC2 Rescue for Linux

ii. `aws:executeAwsApi`: recupera o ID AMI de backup da automação aninhada.

iii. `aws:executeAwsApi`- Recupera o resumo do EC2 Rescue da automação aninhada.

Saídas

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

Descrição

O `AWSSupport-ListEC2Resources` runbook retorna informações sobre EC2 instâncias da Amazon e recursos relacionados, como volumes do Amazon Elastic Block Store (Amazon EBS), endereços IP elásticos e grupos do Amazon Auto Scaling dos que você EC2 especificar. Regiões da AWS Por padrão, as informações são coletadas de todas as regiões e exibidas na saída da automação. Opcionalmente, você pode especificar um bucket do Amazon Simple Storage Service (Amazon S3) para o qual as informações serão carregadas, como um arquivo de valores separados por vírgula (.csv).

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: string

  Descrição: (opcional) o nome do bucket do S3 onde as informações coletadas são carregadas.
- DisplayResourceDeletionDocumentation

  Tipo: string

  Padrão: True

  Descrição: (opcional) se definida como `true`, a automação cria links na saída para a documentação relacionada à exclusão de seus recursos.
- RegionsToQuery

  Tipo: string

  Padrão: All

  Descrição: (Opcional) As regiões das quais você deseja coletar informações EC2 relacionadas à Amazon.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `autoscaling:DescribeAutoScalingGroups`

- ec2:DescribeAddresses
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRegions
- ec2:DescribeVolumes
- ec2:DescribeSnapshots
- elasticloadbalancing:DescribeLoadBalancers

Além disso, para carregar com sucesso as informações coletadas no bucket do S3 que você especificar, a AutomationAssumeRole requer as seguintes ações:

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

Etapas do documento

- aws:executeAwsApi: reúne as regiões ativadas para a conta.
- aws:executeScript: confirma que as regiões ativadas para a conta suportam as regiões especificadas no parâmetro RegionsToQuery.
- aws:branch: se nenhuma região estiver ativada para a conta, a automação será encerrada.
- aws:executeScript- Lista todas as EC2 instâncias da conta e das regiões que você especificar.
- aws:executeScript: lista todas as imagens de máquina da Amazon (AMI) para a conta e as regiões que você especificar.
- aws:executeScript: lista todos os volumes do EBS para a conta e as regiões que você especificar.
- aws:executeScript: lista todos os endereços IP elásticos da conta e das regiões que você especificar.
- aws:executeScript: lista todas as interfaces de rede elástica para a conta e as regiões que você especificar.
- aws:executeScript: lista todos os grupos do Auto Scaling da conta e das regiões que você especificar.

- `aws:executeScript`: lista todos os balanceadores de carga da conta e das regiões que você especificar.
- `aws:executeScript`: carrega as informações coletadas no bucket do S3 especificado se você fornecer um valor para o parâmetro `Bucket`.

AWSSupport-ManageRDPSettings

Descrição

O `AWSSupport-ManageRDPSettings` runbook permite que o usuário gerencie configurações comuns do Remote Desktop Protocol (RDP), como a porta do RDP e o Network Layer Authentication (NLA). Por padrão, o runbook lê e exibe os valores das configurações.

> **Important**
>
> As alterações nas configurações do RDP devem ser cuidadosamente analisadas antes de executar este runbook.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da instância gerenciada para gerenciar as configurações de RDP.

- NLASettingAção

  Tipo: string

  Valores válidos: Check | Enable | Disable

  Padrão: Check

  Descrição: (obrigatório) uma ação para executar na configuração NLA: Check, Enable, Disable.

- RDPPort

  Tipo: string

  Padrão: 3389

  Descrição: (Opcional) Especifique a nova porta do RDP. Usado apenas quando a ação é definida como Modify. O número da porta deve estar entre 1025 e 65535. Observação: Após a porta ser alterada, o serviço do RDP será reiniciado.

- RDPPortAção

  Tipo: string

  Valores válidos: Check | Modify

  Padrão: Check

  Descrição: (obrigatório) uma ação a ser aplicada à porta do RDP.

- RemoteConnections

  Tipo: string

  Valores válidos: Check | Enable | Disable

  Padrão: Check

Descrição: (Obrigatório) Uma ação a ser executada na TSConnections configuração FDeny.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

A EC2 instância que recebe o comando deve ter uma função do IAM com a política gerenciada SSMManaged InstanceCore da Amazon Amazon anexada. O usuário deve ter pelo menos ssm: SendCommand para enviar o comando para a instância, mais ssm: GetCommandInvocation para poder ler a saída do comando.

Etapas do documento

`aws:runCommand`- Execute o PowerShell script para alterar ou verificar as configurações de RDP na instância de destino.

Saídas

gerenciar RDPSettings .Output

`AWSSupport-ManageWindowsService`

Descrição

O runbook `AWSSupport-ManageWindowsService` permite que você pare, inicie, reinicie, pause ou desative qualquer serviço do Windows na instância de destino.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: string

  Descrição: (obrigatório) o ID da instância gerenciada para gerenciar os serviços de

- ServiceAction

  Tipo: string

  Valores permitidos: Check,Restart,Force-Restart,Start,Stop,Force-Stop,Pause

  Padrão: Check

  Descrição: (obrigatório) uma ação a ser aplicada ao serviço do Windows. Observe que `Force-Restart` e `Force-Stop` podem ser usados para reiniciar e interromper um serviço que tem serviços dependentes.

- StartupType

  Tipo: string

  Valores válidos: Verificar | Automático | Demanda | Desativado | DelayedAutoStart

  Padrão: Check

  Descrição: (Obrigatório) Um tipo de startup a ser aplicado ao serviço Windows.

- WindowsServiceName

  Tipo: string

  Descrição: (Obrigatório) Um nome de serviço válido do Windows.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

É recomendável que a EC2 instância que recebe o comando tenha uma função do IAM com a política gerenciada SSMManaged InstanceCore da Amazon Amazon anexada. O usuário deve ter pelo menos ssm: StartAutomationExecution e ssm: SendCommand para executar a automação e enviar o comando para a instância, além de ssm: GetAutomationExecution para poder ler a saída da automação.

Etapas do documento

`aws:runCommand`- Execute o PowerShell script para aplicar a configuração desejada ao serviço Windows na instância de destino.

Saídas

manageWindowsService.Saída

AWSSupport-MigrateEC2ClassicToVPC

Descrição

O `AWSSupport-MigrateEC2ClassicToVPC` runbook migra uma instância do Amazon Elastic Compute Cloud (Amazon EC2) do EC2 -Classic para uma nuvem privada virtual (VPC). Este runbook oferece suporte à migração de EC2 instâncias da Amazon do tipo de virtualização de máquina virtual de hardware (HVM) com volumes raiz do Amazon Elastic Block Store (Amazon EBS).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

Tipo: string

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- ApproverIAM

  Tipo: StringList

  Descrição: (Opcional) Os nomes de recursos da Amazon (ARNs) dos usuários do IAM que podem aprovar ou negar a ação. Esse parâmetro só é aplicável se você especificar o valor `CutOver` para o parâmetro `MigrationType`.

- DestinationSecurityGroupId

  Tipo: StringList

  Descrição: (Opcional) O ID do grupo de segurança que você deseja associar à EC2 instância da Amazon que é executada em sua VPC. Se você não especificar um valor para esse parâmetro, a automação cria um grupo de segurança em sua VPC e copia as regras do grupo de segurança em EC2 -Classic. Se as regras não forem copiadas para o novo grupo de segurança, o grupo de segurança padrão da sua VPC será associado à instância da Amazon EC2 .

- DestinationSubnetId

  Tipo: string

  Descrição: (Opcional) O ID da sub-rede para a qual você deseja migrar sua EC2 instância da Amazon. Se você não especificar um valor para esse parâmetro, a automação escolherá aleatoriamente uma sub-rede da VPC.

- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon que você deseja migrar.

- MigrationType

  Tipo: string

  Valores válidos: CutOver | Teste

Descrição: (obrigatório) o tipo de migração que você deseja executar.

A `CutOver` opção exige aprovação para interromper sua EC2 instância da Amazon que está sendo executada em EC2 -Classic. Depois que essa ação é aprovada, a EC2 instância da Amazon é interrompida e a automação cria um Amazon Machine Image (AMI). Quando o AMI o status é`available`, uma nova EC2 instância da Amazon é iniciada a partir desta AMI no `DestinationSubnetId` que você especifica em sua VPC. Se sua EC2 instância da Amazon que está sendo executada em EC2 -Classic tiver um endereço IP elástico anexado, a instância será movida para a EC2 instância Amazon recém-criada em sua VPC. Se a EC2 instância da Amazon iniciada em sua VPC falhar na criação por qualquer motivo, ela será encerrada e a aprovação será solicitada para iniciar sua EC2 instância da Amazon em -Classic. EC2

A `Test` opção cria um AMI da sua EC2 instância Amazon que está sendo executada em EC2 -Classic sem reinicialização. Como a EC2 instância da Amazon não é reinicializada, não podemos garantir a integridade do sistema de arquivos da imagem criada. Quando o AMI o status é`available`, uma nova EC2 instância da Amazon é iniciada a partir desta AMI no `DestinationSubnetId` que você especifica em sua VPC. Se sua EC2 instância da Amazon que está sendo executada em EC2 -Classic tiver um endereço IP elástico anexado, a automação verificará se o que `DestinationSubnetId` você especificou é público. Se a EC2 instância da Amazon iniciada em sua VPC falhar na criação por qualquer motivo, ela será encerrada e a automação será encerrada.

- SNSNotificationARNforAprovação

  Tipo: string

  Descrição: (opcional) o ARN do tópico do Amazon Simple Notification Service (Amazon SNS) para o qual você deseja enviar solicitações de aprovação. Esse parâmetro só é aplicável se você especificar o valor `CutOver` para o parâmetro `MigrationType`.

- TargetInstanceType

  Tipo: string

  Padrão: t2.2xlarge

  Descrição: (Opcional) O tipo de EC2 instância da Amazon que você deseja iniciar em sua VPC. Somente tipos de instância baseados em Xen, como T2, M4 ou C4, são suportados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeAwsApi- Reúne detalhes sobre a EC2 instância da Amazon que você especifica no InstanceId parâmetro.
- aws:assertAwsResourceProperty: confirma que o tipo de instância que você especifica no parâmetro TargetInstanceType é baseado em Xen.
- aws:assertAwsResourceProperty- Confirma que a EC2 instância da Amazon que você especifica no InstanceId parâmetro é do tipo de virtualização HVM.
- aws:assertAwsResourceProperty- Confirma que a EC2 instância da Amazon que você especifica no InstanceId parâmetro tem um volume raiz do Amazon EBS.
- aws:executeScript: cria um grupo de segurança conforme necessário, dependendo do valor que você especificar para o parâmetro DestinationSecurityGroupId.
- aws:branch: ramifica com base no valor que você especifica no parâmetro DestinationSubnetId.
- aws:executeAwsApi: identifica a VPC padrão na Região da AWS em que você executa essa automação.
- aws:executeAwsApi: escolhe aleatoriamente o ID de uma sub-rede localizada na VPC padrão.
- aws:createImage- Cria um AMI sem reiniciar a instância da Amazon EC2.
- aws:branch: ramifica com base no valor que você especifica para o parâmetro MigrationType.
- aws:branch: ramifica com base no valor que você especifica para o parâmetro DestinationSubnetId.
- aws:runInstances- Lança uma nova instância a partir do AMI criado sem reiniciar a EC2 instância da Amazon em EC2 -Classic.
- aws:changeInstanceState- Encerra a EC2 instância Amazon recém-lançada se a etapa anterior falhar por qualquer motivo.
- aws:runInstances- Lança uma nova instância a partir do AMI criado sem reiniciar a EC2 instância da Amazon em EC2 -Classic no, se fornecido. DestinationSubnetId
- aws:changeInstanceState- Encerra a EC2 instância Amazon recém-lançada se a etapa anterior falhar por qualquer motivo.

- `aws:assertAwsResourceProperty`- Confirma o comportamento de parada da EC2 instância Amazon em execução em EC2 -Classic.
- `aws:approve`- Aguarda a aprovação para interromper a EC2 instância da Amazon.
- `aws:changeInstanceState`- Interrompe a execução da EC2 instância Amazon em EC2 -Classic.
- `aws:changeInstanceState`- Force a interrupção da execução da EC2 instância Amazon em EC2 -Classic, se necessário.
- `aws:createImage`- Cria um AMI da EC2 instância da Amazon depois que ela foi interrompida.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `DestinationSubnetId`.
- `aws:runInstances`- Lança uma nova instância a partir do AMI criado da EC2 instância Amazon interrompida em EC2 -Classic.
- `aws:approve`- Aguarda a aprovação para encerrar a instância recém-lançada e inicia a EC2 instância Amazon em EC2 -Classic se a etapa anterior falhar por algum motivo.
- `aws:changeInstanceState`- Encerra a EC2 instância Amazon recém-lançada.
- `aws:runInstances`- Lança uma nova instância a partir do AMI criado da EC2 instância Amazon parada em EC2 -Classic a partir do `DestinationSubnetId` parâmetro.
- `aws:approve`- Aguarda a aprovação para encerrar a instância recém-lançada e inicia a EC2 instância Amazon em EC2 -Classic se a etapa anterior falhar por algum motivo.
- `aws:changeInstanceState`- Encerra a EC2 instância Amazon recém-lançada.
- `aws:changeInstanceState`- Inicia a EC2 instância da Amazon que foi interrompida em EC2 -Classic.
- `aws:branch`- Ramificações com base no fato de a EC2 instância da Amazon ter um endereço IP público.
- `aws:executeAwsApi`: verifica se o endereço IP público é um endereço IP elástico.
- `aws:branch`: ramifica com base no valor que você especifica no parâmetro `MigrationType`.
- `aws:executeAwsApi`: move o endereço IP elástico para sua VPC.
- `aws:executeAwsApi`: coleta o ID de alocação do endereço IP elástico que foi movido para a VPC.
- `aws:branch`- Ramificações com base em qual sub-rede a EC2 instância da Amazon em execução em sua VPC foi lançada.
- `aws:executeAwsApi`: anexa o endereço IP elástico à instância recém-iniciada em sua VPC.

- `aws:executeScript`- Confirma que a sub-rede que sua EC2 instância Amazon recém-lançada em execução em sua VPC é pública.

Saídas

g `etInstanceProperties.virtualizationType` - O tipo de virtualização da EC2 instância da Amazon em execução em EC2 -Classic.

`getInstanceProperties.rootDeviceType`- O tipo de dispositivo raiz da EC2 instância Amazon em execução em EC2 -Classic.

`createAMIWithoutReboot.ImageId`- O ID do AMI criado sem reiniciar a EC2 instância da Amazon em execução em EC2 -Classic.

`getDefaultVPC.VpcId`- O ID da VPC padrão em que a nova EC2 instância da Amazon é iniciada se um valor para o `DestinationSubnetId` parâmetro não for fornecido.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc`- O ID da sub-rede na VPC padrão em que a nova instância da EC2 Amazon é iniciada se um valor para `DestinationSubnetId` o parâmetro não for fornecido.

`launchTestInstanceDefaultVPC.InstanceIds`- O ID da EC2 instância Amazon recém-lançada em sua VPC padrão durante o tipo de `Test` migração.

`launchTestInstanceProvidedSubnet.InstanceIds`- O ID da EC2 instância Amazon recém-lançada na `DestinationSubnetId` que você especificou durante o tipo de `Test` migração.

`createAMIAfterStoppingInstance.ImageId`- O ID do AMI criado após interromper a execução da EC2 instância da Amazon em EC2 -Classic.

`launchCutOverInstanceProvidedSubnet.InstanceIds`- O ID da EC2 instância Amazon recém-lançada na `DestinationSubnetId` que você especificou durante o tipo de `CutOver` migração.

`launchCutOverInstanceDefaultVPC.InstanceIds`- O ID da EC2 instância Amazon recém-lançada em sua VPC padrão durante o tipo de `CutOver` migração.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic`: se a sub-rede escolhida pela automação em sua VPC padrão é pública.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic`: se a sub-rede que você especificou no `DestinationSubnetId` é pública.

AWSSupport-MigrateXenToNitroLinux

Descrição

O `AWSSupport-MigrateXenToNitroLinux` runbook clona, prepara e migra uma instância Linux Xen da Amazon Elastic Compute Cloud (EC2Amazon) para uma Nitro tipo de instância. Este runbook fornece duas opções para tipos de operação:

- `Clone&Migrate`— O fluxo de trabalho dessa opção consiste em verificações preliminares, testes e Clone&Migratefases. O workflow é executado usando o runbook `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro`.
- `FullMigration`: essa opção executa o runflow `Clone&Migrate` e, em seguida, executa a etapa adicional de Substituir volumes raiz do Amazon EBS.

> **Important**
>
> O uso desse runbook gera custos para sua conta pelo tempo de execução das EC2 instâncias da Amazon, pela criação de volumes do Amazon Elastic Block Store (Amazon EBS) e AMIs. Para obter mais detalhes, consulte Amazon EC2 Pricing e Amazon EBS Pricing.

Verificações preliminares

A automação realiza as seguintes verificações preliminares antes de continuar com a migração. Se alguma das verificações falha, a automação é encerrada. Essa fase é apenas parte do workflow `Clone&Migrate`.

- Verifica se a instância de destino já é uma Nitro tipo de instância.
- Verifica se a opção de compra de instâncias spot foi usada para a instância de destino.
- Verifica se os volumes de armazenamento de instâncias estão anexados à instância de destino.
- Verifica se a instância do sistema operacional de destino é Linux.
- Verifica se a instância de destino faz parte de um grupo do Amazon EC2 Auto Scaling. Se fizer parte de um grupo do Auto Scaling, a automação verifica se a instância está no estado `standby`.

- Verifica se a instância é gerenciada por AWS Systems Manager.

Teste

A automação cria um Amazon Machine Image (AMI) da instância de destino e inicia uma instância de teste a partir da instância recém-criada AMI. Essa fase faz parte apenas do `Clone&Migrate` fluxo de trabalho.

Se a instância de teste passar por todas as verificações de status, a automação será interrompida e a aprovação das entidades principais designadas será solicitada por meio de notificação do Amazon Simple Notification Service (Amazon SNS). Se a aprovação for fornecida, a automação encerra a instância de teste, interrompe a instância de destino e continua com a migração, enquanto a recém-criada AMI é cancelado o registro no final do fluxo de trabalho. `Clone&Migrate`

> **Note**
>
> Antes de fornecer a aprovação, recomendamos verificar se todos os aplicativos em execução na instância de destino foram fechados corretamente.

Clonar e migrar

A automação cria outra AMI da instância de destino e inicia uma nova instância para mudar para uma Nitro tipo de instância. A automação conclui as seguintes verificações preliminares antes de continuar com a migração. Se alguma das verificações falha, a automação é encerrada. Essa fase também é apenas parte do workflow `Clone&Migrate`.

- Ativa o atributo de redes avançadas (ENA).
- Instala a versão mais recente dos drivers ENA, se ainda não estiverem instalados, ou atualiza a versão dos drivers ENA para a versão mais recente. Para garantir o máximo desempenho da rede, a atualização para a versão mais recente do driver ENA é necessária se o Nitro o tipo de instância é a 6ª geração.
- Verifica se o NVMe módulo está instalado. Se o módulo estiver instalado, a automação verificará se o módulo está carregado em `initramfs`.
- Analisa `/etc/fstab` e substitui entradas por nomes de dispositivos de bloco (`/dev/sd*` ou `/dev/xvd*`) por seus respectivos. UUIDs Antes de modificar a configuração, a automação cria um backup do arquivo no caminho `/etc/fstab*`.

- Desativa a nomenclatura previsível da interface adicionando a opção `net.ifnames=0` à linha `GRUB_CMDLINE_LINUX` no arquivo `/etc/default/grub`, se ela existir, ou ao kernel em `/boot/grub/menu.lst`.
- Remove o arquivo `/etc/udev/rules.d/70-persistent-net.rules`, se ele existir. Antes de remover o arquivo, a automação cria um backup do arquivo no caminho `/etc/udev/rules.d/`.

Depois de verificar todos os requisitos, o tipo de instância é alterado para Nitro tipo de instância que você especifica. A automação espera que a instância recém-criada passe por todas as verificações de status depois de começar como Nitro tipo de instância. A automação então aguarda a aprovação dos diretores designados para criar um AMI do lançado com sucesso Nitro instância. Se a aprovação for negada, a automação será encerrada, deixando a instância recém-criada em execução e a instância de destino permanecerá parada.

Substituir um volume do Amazon EBS

Se você escolher `FullMigration` como`OperationType`, a automação migrará a EC2 instância de destino da Amazon para a Nitro tipo de instância que você especifica. A automação solicita a aprovação dos diretores designados para substituir o volume raiz do Amazon EBS da EC2 instância Amazon de destino pelo volume raiz da instância EC2 Amazon clonada. Depois que a migração for bem-sucedida, a EC2 instância clonada da Amazon será encerrada. Se a automação falhar, o volume raiz original do Amazon EBS será anexado à EC2 instância de destino da Amazon. Se o volume raiz do Amazon EBS anexado à EC2 instância de destino da Amazon tiver tags com o `aws:` prefixo aplicado, a `FullMigration` operação não será suportada.

Antes de começar

A instância de destino deve ter acesso de saída à internet. Isso é para acessar repositórios de drivers e dependências como kernel-devel, gcc, patch, rpm-build, wget, dracut, make, linux-headers e unzip. O gerenciador de pacotes é usado se necessário.

É necessário um tópico do Amazon SNS para enviar notificações de aprovações e atualizações. Para obter mais informações sobre como criar um tópico Amazon SNS, consulte Criar um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

Este runbook é compatível com os seguintes sistemas operacionais:

- RHEL 7,x - 8,5
- Amazon Linux (2018.03), Amazon Linux 2
- Debian Server

- Ubuntu Server 18.04 LTS, 20.04 LTS e 20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5, SUSE15SP2)

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Acknowledgement

  Tipo: string

  Descrição: (obrigatório) lê os detalhes completos das ações executadas por esse runbook de automação e insere **`Yes, I understand and acknowledge`** para continuar usando o runbook.
- ApproverIAM

  Tipo: string

  Descrição: (Obrigatório) As funções, usuários ou nomes ARNs de usuário do IAM que podem fornecer aprovações para a automação. Você pode especificar um máximo de 10 aprovadores.
- DeleteResourcesOnFailure

Tipo: booliano

Descrição: (Opcional) Determina se a instância recém-criada e AMI para a migração são excluídos se a automação falhar.

Valores válidos: True | False

Padrão: verdadeiro

- MinimumRequiredApprovals

  Tipo: string

  Descrição: (opcional) o número mínimo de aprovações necessárias para continuar executando a automação quando as aprovações são solicitadas.

  Valores válidos: de 1 a 10

  Padrão: 1

- NitroInstanceType

  Tipo: string

  Descrição: (Obrigatório) O Nitro tipo de instância para o qual você deseja alterar a instância. Os tipos de instância compatíveis incluem M5, M6, C5, C6, R5, R6 e T3.

  Padrão: m5.xlarge

- OperationType

  Tipo: string

  Descrição: (obrigatório) o operação que você deseja executar. A opção `FullMigration` executa as mesmas tarefas que `Clone&Migrate` e, além disso, substitui o volume raiz da sua instância de destino. O volume raiz da instância de destino é substituído pelo volume raiz da instância recém-criada após o processo de migração. A operação `FullMigration` não suporta volumes raiz definidos pelo Logical Volume Manager (LVM).

  Valores válidos: Clone&Migrate | FullMigration

- SNSTopicArn

  Tipo: string

Descrição: (obrigatório) o ARN do tópico do Amazon SNS no qual publicar a notificação. O tópico do Amazon SNS é usado para enviar as notificações de aprovação necessárias durante a automação.

- TargetInstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID das EC2 instâncias da Amazon a serem migradas.

Clone&Migrate fluxo de trabalho

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- startOfPreliminaryChecksBranch: ramifica o workflow de verificações preliminares.
- getTargetInstanceProperties: reúne detalhes da instância de destino.
- checkIfNitroInstanceTypeIsSupportedInAZ- Determina se o tipo de EC2 instância de destino da Amazon é suportado na mesma zona de disponibilidade da instância de destino.
- getXenInstanceTypeDetails: reúne detalhes sobre o tipo de instância de origem.
- checkIfInstanceHypervisorIsNitroAlready- Verifica se a instância de destino já está sendo executada como Nitro tipo de instância.
- checkIfTargetInstanceLifecycleIsSpot: verifica se a opção de compra de instância de destino é Spot.
- checkIfOperatingSystemIsLinux: verifica se o sistema operacional da instância de destino é Linux.
- verifySSMConnectivityForTargetInstance: verifica se a instância de destino é gerenciada pelo Systems Manager.
- checkIfEphemeralVolumeAreSupported: verifica se o tipo de instância atual da instância de destino é compatível com volumes de armazenamento de instância.
- verifyIfTargetInstanceHasEphemeralVolumesAttached: verifica se a instância de destino tem volumes de armazenamento de instância anexados.
- checkIfRootVolumeIsEBS: verifica se o tipo de volume raiz da instância de destino é EBS.

- `checkIfTargetInstanceIsInASG`: verifica se a instância de destino faz parte de um grupo do Auto Scaling.
- `endOfPreliminaryChecksBranch`: fim da ramificação de verificações preliminares.
- `startOfTestBranch`: ramifica para o workflow de testes.
- `createTestImage`- Cria um teste AMI da instância de destino.
- `launchTestInstanceInSameSubnet`- Lança uma instância de teste a partir do teste AMI usando a mesma configuração da instância de destino.
- `cleanupTestInstance`: encerra a instância de teste.
- `endOfTestBranch`: fim da ramificação de testes.
- `checkIfTestingBranchSucceeded`: verifica o status da ramificação de testes.
- `approvalToStopTargetInstance`: aguarda a aprovação das entidades principais designadas para interromper a instância de destino.
- `stopTargetEC2Instance`: interrompe a instância de destino.
- `forceStopTargetEC2Instance`: força a interrupção da instância de destino somente se a etapa anterior não conseguir interromper a instância.
- `startOfCloneAndMigrateBranch`- Filiais do Clone&Migrate fluxo de trabalho.
- `createBackupImage`- Cria um AMI da instância de destino para servir como backup.
- `launchInstanceInSameSubnet`- Lança uma nova instância a partir do backup AMI usando a mesma configuração da instância de origem.
- `waitForClonedInstanceToPassStatusChecks`: espera que a instância recém-criada passe por todas as verificações de status.
- `verifySSMConnectivityForClonedInstance`: verifica se a instância recém-criada é gerenciada pelo Systems Manager.
- `checkAndInstallENADrivers`: verifica se os drivers ENA estão instalados na instância recém-criada e instala os drivers, se necessário.
- `checkAndAddNVMEDrivers`- Verifica se NVMe os drivers estão instalados na instância recém-criada e instala os drivers, se necessário.
- `checkAndModifyFSTABEntries`- Verifica se os nomes dos dispositivos são usados `/etc/fstab` e os substitui por, UUIDs se necessário.
- `stopClonedInstance`: interrompe a instância recém-criada.
- `forceStopClonedInstance`: força a interrupção da instância recém-criada somente se a etapa anterior não conseguir interromper a instância.

- `checkENAAttributeForClonedInstance`: verifica se o atributo de rede avançada está ativado para a instância recém-criada.
- `setNitroInstanceTypeForClonedInstance`- Altera o tipo de instância da instância recém-criada para Nitro tipo de instância que você especifica.
- `startClonedInstance`: inicia a instância recém-criada cujo tipo de instância você alterou.
- `approvalForCreatingImageAfterDriversInstallation`- Se a instância for iniciada com sucesso como um Nitro tipo de instância, a automação aguarda a aprovação dos diretores necessários. Se a aprovação for fornecida, um AMI é criado para ser usado como dourado AMI.
- `createImageAfterDriversInstallation`- Cria um AMI para ser usado como dourado AMI.
- `endOfCloneAndMigrateBranch`- Fim de Clone&Migrate filial.
- `cleanupTestImage`- Cancela o registro do AMI criado para testes.
- `failureHandling`: verifica se você optou por encerrar recursos em caso de falha.
- `onFailureTerminateClonedInstance`: encerra a instância recém-criada se a automação falhar.
- `onFailurecleanupTestImage`- Cancela o registro do AMI criado para testes.
- `onFailureApprovalToStartTargetInstance`: se a automação falhar, aguarda a aprovação das entidades principais designadas para iniciar a instância de destino.
- `onFailureStartTargetInstance`: se a automação falhar, inicia a instância de destino.

FullMigration fluxo de trabalho

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

O workflow FullMigration executa as mesmas etapas do workflow Clone&Migrate e, além disso, executa as seguintes etapas:

- checkConcurrency- Verifica se há apenas uma automação desse runbook direcionada à EC2 instância da Amazon que você especificar. Se o runbook encontrar outra automação em andamento visando a mesma instância, a automação terminará.

- `getTargetInstanceProperties`: reúne detalhes da instância de destino.
- `checkRootVolumeTags`- Determina se o volume raiz da EC2 instância de destino da Amazon contém alguma tag AWS reservada.
- `cloneTargetInstanceAndMigrateToNitro`: inicia uma automação secundária usando o runbook `AWS-CloneXenInstanceToNitro`.
- `branchOnTheOperationType`: ramifica com base no valor que você especifica para o parâmetro `OperationType`.
- `getClonedInstanceId`: recupera o ID da instância recém-iniciada da automação secundária.
- `checkIfRootVolumeIsBasedOnLVM`: determina se a partição raiz é gerenciada pelo LVM.
- `branchOnTheRootVolumeLVMStatus`: se as aprovações mínimas exigidas forem recebidas das entidades principais, a automação prosseguirá com a substituição do volume raiz.
- `manualInstructionsInCaseOfLVM`: se o volume raiz for gerenciado pelo LVM, a automação enviará uma saída contendo instruções sobre como substituir manualmente os volumes raiz.
- `startOfReplaceRootEBSVolumeBranch`: inicia o workflow da ramificação Substituir volume raiz do EBS.
- `checkIfTargetInstanceIsManagedByCFN`- Determina se a instância de destino é gerenciada por uma AWS CloudFormation pilha.
- `branchOnCFNStackStatus`- Ramificações com base no status da CloudFormation pilha.
- `approvalForRootVolumesReplacement(WithCFN)`- Se a instância de destino foi iniciada por CloudFormation, a automação aguarda aprovação depois que a instância recém-lançada for iniciada com sucesso como Nitro tipo de instância. Quando as aprovações são fornecidas, os volumes do Amazon EBS da instância de destino são substituídos pelos volumes raiz da instância recém-iniciada.
- `approvalForRootVolumesReplacement`- Aguarda aprovação após a instância recém-lançada ser iniciada com sucesso como Nitro tipo de instância. Quando as aprovações são fornecidas, os volumes do Amazon EBS da instância de destino são substituídos pelos volumes raiz da instância recém-iniciada.
- `assertIfTargetEC2InstanceIsStillStopped` verifica se a instância de destino está em um estado `stopped` antes de substituir o volume raiz.
- `stopTargetInstanceForRootVolumeReplacement` se a instância de destino estiver em execução, a automação interromperá a instância antes de substituir o volume raiz.
- `forceStopTargetInstanceForRootVolumeReplacement` força a interrupção da instância de destino se a etapa anterior falhar.

- `stopClonedInstanceForRootVolumeReplacement` interrompe a instância recém-criada antes de substituir os volumes do Amazon EBS.
- `forceStopClonedInstanceForRootVolumeReplacement` força a interrupção da instância recém-criada se a etapa anterior falhar.
- `getBlockDeviceMappings` recupera os mapeamentos de dispositivos de blocos para as instâncias de destino e recém-criadas.
- `replaceRootEbsVolumes` substitui o volume raiz da instância de destino pelo volume raiz da instância recém-criada.
- `EndOfReplaceRootEBSVolumeBranch` fim do workflow da ramificação Substituir volume raiz do EBS.
- `checkENAAttributeForTargetInstance`- Verifica se o atributo de rede aprimorada (ENA) está ativado para a EC2 instância de destino da Amazon.
- `enableENAAttributeForTargetInstance`- Ativa o atributo ENA para a EC2 instância de destino da Amazon, se necessário.
- `setNitroInstanceTypeForTargetInstance`- Altera a instância de destino para Nitro tipo de instância que você especifica.
- `replicateRootVolumeTags`- Replica as tags no volume raiz do Amazon EBS da instância de destino da Amazon EC2 .
- `startTargetInstance`- Inicia a EC2 instância de destino da Amazon depois de alterar o tipo de instância.
- `onFailureStopTargetEC2Instance`- Interrompe a EC2 instância de destino da Amazon se ela não iniciar como uma Nitro tipo de instância.
- `onFailureForceStopTargetEC2Instance`- Forçar a interrupção da EC2 instância Amazon de destino se a etapa anterior falhar.
- `OnFailureRevertOriginalInstanceType`- Reverte a EC2 instância de destino da Amazon para o tipo de instância original se a instância de destino não iniciar como uma Nitro tipo de instância.
- `onFailureRollbackRootVolumeReplacement` reverte todas as alterações feitas pela etapa `replaceRootEbsVolumes`, se necessário.
- `onFailureApprovalToStartTargetInstance`- Aguarda a aprovação do diretor designado para iniciar a EC2 instância de destino da Amazon depois de reverter as alterações anteriores.
- `onFailureStartTargetInstance`- Inicia a EC2 instância de destino da Amazon.

- `terminateClonedEC2Instance`- Encerra a EC2 instância clonada da Amazon após substituir o volume raiz do Amazon EBS.

AWSSupport-ResetAccess

Descrição

Esse runbook usará a ferramenta EC2 Rescue na EC2 instância especificada para reativar a decodificação de senha usando o EC2 console (Windows) ou para gerar e adicionar um novo par de chaves SSH (Linux). Se você perder seu par de chaves, essa automação criará uma AMI habilitada por senha que você pode usar para iniciar uma EC2 nova instância com um par de chaves que você possui (Windows).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EC2RescueInstanceType

  Tipo: string

  Valores permitidos: t2.small | t2.medium | t2.large

Padrão: t2.small

Descrição: (Obrigatório) O tipo de EC2 instância da instância do EC2 Rescue. Tamanho recomendado: t2.small.

- InstanceId

  Tipo: string

  Descrição: ID (obrigatório) da EC2 instância para a qual você deseja redefinir o acesso.

  > **Important**
  >
  > O Systems Manager Automation interrompe essa instância e cria uma AMI antes de tentar qualquer operação. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um IP elástico.

- SubnetId

  Tipo: string

  Padrão: CreateNew VPC

  Descrição: (Opcional) O ID da sub-rede da instância do EC2 Rescue. Por padrão, a Systems Manager Automation cria uma nova VPC. Como alternativa, use SelectedInstanceSubnet para usar a mesma sub-rede da sua instância ou especificar um ID de sub-rede personalizado.

  > **Important**
  >
  > A sub-rede deve estar na mesma InstanceId zona de disponibilidade e deve permitir o acesso aos endpoints do SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

Você deve ter pelo menos ssm: StartAutomationExecution, ssm: GetParameter (para recuperar o nome do parâmetro da chave SSH) e ssm: GetAutomationExecution para poder ler a saída de

automação. Para mais informações sobre as permissões necessárias, consulte AWSSupport-StartEC2RescueWorkflow.

Etapas do documento

1. aws:assertAwsResourceProperty: declara se a instância fornecida é Windows.
   a. (EC2Rescue for Windows) Se a instância fornecida for Windows:
      i. aws:executeAutomation- Invoque AWSSupport-StartEC2RescueWorkflow com o script de redefinição de senha offline do EC2 Rescue for Windows
      ii. aws:executeAwsApi: recupera o ID AMI de backup da automação aninhada.
      iii. aws:executeAwsApi: recupera o ID AMI com senha habilitada da automação aninhada
      iv. aws:executeAwsApi- Recupere o resumo do EC2 Rescue da automação aninhada
   b. (EC2Rescue for Linux) Se a instância fornecida for Linux:
      i. aws:executeAutomation- Invoque AWSSupport-StartEC2RescueWorkflow com o script de injeção de chave SSH offline do EC2 Rescue for Linux
      ii. aws:executeAwsApi: recupera o ID AMI de backup da automação aninhada.
      iii. aws:executeAwsApi: recupera o nome do parâmetro SSM para a chave SSH injetada
      iv. aws:executeAwsApi- Recupere o resumo do EC2 Rescue da automação aninhada

Saídas

get EC2 RescueForWindowsResult .Output

getWindowsBackupAmi. ImageId

getWindowsPasswordEnabledAmi.ImageId

get EC2 RescueForLinuxResult .Output

getLinuxBackupAmi. ImageId

GetLinux Parameter.Name SSHKey

AWSSupport-ResetLinuxUserPassword

Descrição

O runbook AWSSupport-ResetLinuxUserPassword ajuda você a redefinir a senha de um usuário do sistema operacional (SO) local. Esse runbook é especialmente útil para usuários que

precisam acessar suas instâncias do Amazon Elastic Compute Cloud EC2 (Amazon) usando o console serial. O runbook cria uma EC2 instância temporária da Amazon em sua função Conta da AWS e uma função AWS Identity and Access Management (IAM) com permissões para recuperar um valor AWS Secrets Manager secreto contendo a senha.

O runbook interrompe sua EC2 instância de destino da Amazon, separa o volume raiz do Amazon Elastic Block Store (Amazon EBS) e o anexa à instância temporária da Amazon. EC2 Usando o comando Executar, um script é executado na instância temporária para definir a senha do usuário do sistema operacional que você especificar. Em seguida, o volume raiz do Amazon EBS é reconectado à sua instância de destino. O runbook também oferece uma opção para criar um snapshot do volume raiz no início da automação.

Antes de começar

Crie um segredo do Secrets Manager com o valor da senha que você deseja atribuir ao usuário do sistema operacional. O valor deve estar em texto simples. Para obter mais informações, consulte Criar um AWS Secrets Manager segredo no AWS Secrets Manager Guia do usuário.

Considerações

- Recomendamos fazer backup da sua instância antes de usar este runbook. Considere definir o valor do parâmetro `CreateSnapshot` como **`Yes`**.
- A alteração da senha do usuário local exige que o runbook interrompa sua instância. Quando uma instância é interrompida, os dados armazenados na memória ou nos volumes de armazenamento da instância são perdidos. Além disso, todos os IPv4 endereços públicos atribuídos automaticamente são liberados. Para obter mais informações sobre o que acontece quando você interrompe uma instância, consulte Pare e inicie sua instância no Guia EC2 do usuário da Amazon.
- Se os volumes do Amazon EBS anexados à sua EC2 instância Amazon de destino forem criptografados com uma chave gerenciada pelo cliente AWS Key Management Service (AWS KMS), certifique-se de que a AWS KMS chave não seja `deleted` `disabled` ou sua instância não iniciará.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da instância Amazon EC2 Linux que contém a senha de usuário do sistema operacional que você deseja redefinir.
- LinuxUserName

  Tipo: string

  Padrão: ec2-user

  Descrição: (opcional) a conta de usuário do sistema operacional cuja senha você deseja redefinir.
- SecretArn

  Tipo: string

  Descrição: (obrigatório) o ARN do segredo do Secrets Manager contendo a nova senha.
- SecurityGroupId

  Tipo: string

Descrição: (Opcional) O ID do grupo de segurança a ser anexado à EC2 instância temporária da Amazon. Se você não fornecer um valor para esse parâmetro, o grupo de segurança padrão da Amazon Virtual Private Cloud (Amazon VPC) é usado.

- SubnetId

  Tipo: string

  Descrição: (Opcional) O ID da sub-rede na qual você deseja iniciar a instância EC2 temporária da Amazon. Por padrão, a automação escolhe a mesma sub-rede da sua instância de destino. Se você optar por fornecer uma sub-rede diferente, ela deve estar na mesma zona de disponibilidade da instância de destino e ter acesso aos endpoints do Systems Manager.

- CreateSnapshot

  Tipo: string

  Valores válidos: sim | não

  Padrão: sim

  Descrição: (Opcional) Determina se um snapshot do volume raiz da sua EC2 instância Amazon de destino é criado antes da execução da automação.

- StopConsent

  Tipo: string

  Valores válidos: sim | não

  Padrão: não

  Descrição: Entre **`Yes`** para confirmar que sua EC2 instância de destino da Amazon será interrompida durante essa automação. Quando a EC2 instância da Amazon é interrompida, todos os dados armazenados na memória ou nos volumes de armazenamento da instância são perdidos e o IPv4 endereço público automático é liberado. Para obter mais informações, consulte Pare e inicie sua instância no Guia EC2 do usuário da Amazon.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- 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`

Etapas do documento

1. `aws:branch`— Filiais com base no fato de você ter fornecido consentimento para interromper a EC2 instância de destino da Amazon.
2. `aws:assertAwsResourceProperty`— Garante que o status da EC2 instância Amazon esteja em um `stopped` estado `running` ou. Caso contrário, a automação termina.
3. `aws:executeAwsApi`— Obtém as propriedades da EC2 instância Amazon.
4. `aws:executeAwsApi`— Obtém as propriedades do volume raiz.
5. `aws:branch`— Ramifica a automação dependendo se um ID de sub-rede para a EC2 instância temporária da Amazon foi fornecido.
6. `aws:assertAwsResourceProperty`— Garante que a sub-rede especificada no `SubnetId` parâmetro esteja na mesma zona de disponibilidade da EC2 instância de destino da Amazon.
7. `aws:assertAwsResourceProperty`— Garante que o volume raiz da EC2 instância Amazon de destino seja um volume do Amazon EBS.
8. `aws:assertAwsResourceProperty`— Garante que a arquitetura da EC2 instância Amazon seja `arm64` ou`x86_64`.
9. `aws:assertAwsResourceProperty`— Garante que o comportamento de desligamento da EC2 instância Amazon seja `stop` ou não`terminate`.
10. `aws:branch`— Garante que a EC2 instância da Amazon não seja uma instância spot. Caso contrário, a automação termina.
11. `aws:executeScript`— Garante que a EC2 instância da Amazon não faça parte de um grupo de auto scaling. Se a instância fizer parte de um grupo de auto scaling, a automação confirma que a EC2 instância da Amazon está em um estado de ciclo de `Standby` vida.
12. `aws:createStack`— Cria uma EC2 instância temporária da Amazon que é usada para redefinir a senha do usuário do sistema operacional que você especificar.
13. `aws:waitForAwsResourceProperty`— Espera até que a EC2 instância temporária recém-lançada da Amazon esteja em execução.
14. `aws:executeAwsApi`— Obtém o ID da EC2 instância temporária da Amazon.

15. `aws:waitForAwsResourceProperty`— Espera que a EC2 instância temporária da Amazon seja reportada conforme gerenciada pelo Systems Manager.
16. `aws:changeInstanceState`— Interrompe a EC2 instância de destino da Amazon.
17. `aws:changeInstanceState`— Força a EC2 instância de destino da Amazon a parar caso ela fique presa em um estado de parada.
18. `aws:branch`— Ramifica a automação dependendo se um snapshot do volume raiz da EC2 instância de destino da Amazon foi solicitado.
19. `aws:executeAwsApi`— Cria um snapshot do volume raiz da EC2 instância Amazon de destino do Amazon EBS.
20. `aws:waitForAwsResourceProperty`— Espera que o instantâneo esteja em um `completed` estado.
21. `aws:executeAwsApi`— Separa o volume raiz do Amazon EBS da instância de destino da Amazon EC2 .
22. `aws:waitForAwsResourceProperty`— Espera que o volume raiz do Amazon EBS seja separado da instância de destino da Amazon. EC2
23. `aws:executeAwsApi`— Anexa o volume raiz do Amazon EBS à instância temporária da Amazon EC2 .
24. `aws:waitForAwsResourceProperty`— Espera que o volume raiz do Amazon EBS seja anexado à instância temporária da Amazon EC2 .
25. `aws:runCommand`— Redefine a senha do usuário de destino executando um script de shell usando o Run Command na EC2 instância temporária da Amazon.
26. `aws:executeAwsApi`— Separa o volume raiz do Amazon EBS da instância temporária da Amazon EC2 .
27. `aws:waitForAwsResourceProperty`— Espera que o volume raiz do Amazon EBS seja separado da instância temporária da Amazon. EC2
28. `aws:executeAwsApi`— Separa o volume raiz do Amazon EBS da EC2 instância temporária da Amazon após um erro.
29. `aws:waitForAwsResourceProperty`— Espera que o volume raiz do Amazon EBS seja separado da EC2 instância temporária da Amazon após um erro.
30. `aws:branch`— Ramifica a automação dependendo se um instantâneo do volume raiz foi solicitado para determinar o caminho de recuperação em caso de erro.
31. `aws:executeAwsApi`— Reconecta o volume raiz do Amazon EBS à instância de destino da Amazon. EC2

32. `aws:waitForAwsResourceProperty`— Espera que o volume raiz do Amazon EBS seja anexado à instância da Amazon EC2 .
33. `aws:executeAwsApi`— Cria um novo volume do Amazon EBS a partir do snapshot do volume raiz da EC2 instância Amazon de destino.
34. `aws:waitForAwsResourceProperty`— Espera até que o novo volume do Amazon EBS esteja em um `available` estado.
35. `aws:executeAwsApi`— Anexa o novo volume do Amazon EBS à instância de destino como volume raiz.
36. `aws:waitForAwsResourceProperty`— Espera que o volume do Amazon EBS esteja em um `attached` estado.
37. `aws:executeAwsApi`— Descreve os eventos da AWS CloudFormation pilha se os runbooks falharem em criar ou atualizar a AWS CloudFormation pilha.
38. `aws:branch`— Ramifica a automação de acordo com o estado anterior da EC2 instância Amazon. Se o estado foi `running`, a instância será iniciada. Se estivesse em um estado `stopped`, a automação continua.
39. `aws:changeInstanceState`— Inicia a EC2 instância da Amazon, se necessário.
40. `aws:waitForAwsResourceProperty`— Espera até que a AWS CloudFormation pilha esteja em um status de terminal antes de excluí-la.
41. `aws:executeAwsApi`— Exclui a AWS CloudFormation pilha, incluindo a instância temporária da Amazon EC2 .

AWSPremiumSupport-ResizeNitroInstance

Descrição

O `AWSPremiumSupport-ResizeNitroInstance` runbook fornece uma solução automatizada para redimensionar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) criadas no Nitro System.

Para reduzir o risco potencial de perda de dados e tempo de inatividade, o runbook verifica o seguinte:

- Comportamento da interrupção da instância.
- Se a instância fizer parte de um grupo do Amazon EC2 Auto Scaling e estiver em `standby` modo.

- Estado da instância e locação.
- O tipo de instância para o qual você deseja alterar é compatível com o número de interfaces de rede atualmente conectadas à sua instância.
- A arquitetura do processador e o tipo de virtualização do tipo de instância atual e de destino são os mesmos.
- Se a instância estiver em execução, ela está passando todas as verificações de status.
- O tipo de instância que você selecionou não está disponível na mesma zona de disponibilidade.

Se a Amazon EC2 não passar nas verificações de status após alterar o tipo de instância, o runbook reverte automaticamente para o tipo de instância anterior.

Por padrão, esse runbook não alterará o tipo de instância se estiver em execução e os volumes de armazenamento de instância estiverem anexados. O runbook também não alterará o tipo de instância se a instância fizer parte de uma AWS CloudFormation pilha. Se você quiser alterar qualquer um desses comportamentos, especifique `yes` para os parâmetros `AllowInstanceStoreInstances` e `AllowCloudFormationInstances`.

O runbook fornece duas maneiras diferentes de especificar o tipo de instância para a qual você deseja alterar:

- Para automações simples direcionadas a uma única instância, especifique o tipo de instância para a qual você deseja alterar usando o parâmetro `TargetInstanceTypeFromParameter`.
- Para executar automações em grande escala para alterar o tipo de instância de várias instâncias, especifique o tipo de instância usando o parâmetro `TargetInstanceTypeFromTagValue`. Para obter informações sobre como executar automações em grande escala, consulte Executar automações em grande escala.

Se você não especificar um valor para nenhum dos parâmetros, ocorrerá uma falha na automação.

> **Important**
>
> O acesso aos runbooks da `AWSPremiumSupport-*` requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Comparar Suporte planos.

Considerações

- Recomendamos fazer backup da sua instância antes de usar este runbook.
- Para obter informações sobre compatibilidade para alterar os tipos de instância, consulte Compatibilidade para alterar o tipo de instância.
- Se a automação falhar e voltar para o tipo de instância original, consulte Solucionar problemas de alteração de tipo de instância.
- A alteração do tipo de instância exige que o runbook interrompa sua instância. Quando uma instância é interrompida ou encerrada, os dados nos volumes de armazenamento da instância são perdidos. Além disso, todos os IPv4 endereços públicos atribuídos automaticamente são liberados. Para obter informações sobre o que acontece quando você interrompe uma instância do Mac, consulte Interromper e encerrar sua instância.
- Ao usar o `SkipInstancesWithTagKey` parâmetro, você pode ignorar instâncias que têm uma chave de EC2 tag específica da Amazon aplicada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Reconhecer

Tipo: string

Descrição: (obrigatório) digite **`yes`** para confirmar que sua instância será interrompida se estiver em execução no momento.

- AllowInstanceStoreInstances

  Tipo: string

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se você especificar `yes`, você permite que o runbook seja executado em instâncias que têm volumes de armazenamento de instâncias anexados.

- AllowCloudFormationInstances

  Tipo: string

  Valores válidos: não | sim

  Padrão: não

  Descrição: (Opcional) Se você especificar`yes`, o runbook é executado em instâncias que fazem parte de uma AWS CloudFormation pilha.

- DryRun

  Tipo: string

  Valores válidos: não | sim

  Padrão: não

  Descrição: (opcional) se você especificar `yes`, o runbook valida os requisitos de redimensionamento sem fazer alterações no tipo de instância.

- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon cujo tipo você deseja alterar.

- SkipInstancesWithTagKey

Tipo: string

Descrição: (opcional) A automação ignora uma instância de destino se a chave de tag especificada for aplicada à instância.

- SleepTime

  Tipo: string

  Padrão: 3

  Descrição: (opcional) o número de segundos que esse runbook deve repousar após a conclusão.

- TagInstance

  Tipo: string

  Descrição: (Opcional) Marque as instâncias com a chave e o valor de sua escolha usando o seguinte formato:*`Key=ChangingType,Value=True`*. Essa opção permite rastrear instâncias que foram alvo desse runbook. As chaves e valores das tags diferenciam maiúsculas de minúsculas.

- TargetInstanceTypeFromParameter

  Tipo: string

  Descrição: (opcional) o tipo de instância para o qual você deseja alterar sua instância. Deixe esse parâmetro vazio se quiser usar o valor da chave de tag fornecida no parâmetro `TargetInstanceTypeFromTagValue`.

- TargetInstanceTypeFromTagValue

  Tipo: string

  Descrição: (opcional) a chave de tag aplicada às suas instâncias de destino cujo valor contém o tipo de instância para a qual você deseja alterar. Se você não especificar um valor para esse parâmetro, ele substitui qualquer valor que você especificar para esse parâmetro `TargetInstanceTypeFromParameter`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

1. aws:assertAwsResourceProperty: garante que a EC2 instância da Amazon não seja marcada com a chave de tag de recurso especificada no SkipInstancesWithTagKey parâmetro. Se a chave de tag for encontrada aplicada à instância, a etapa falhará e a automação será encerrada.
2. aws:assertAwsResourceProperty: confirma que o status da EC2 instância de destino da Amazon érunning,, pendingstopped, oustopping. Caso contrário, a automação termina.
3. aws:executeAwsApi: reúne propriedades da EC2 instância da Amazon.
4. aws:executeAwsApi: reúne detalhes sobre o tipo atual de EC2 instância da Amazon.
5. aws:branch: verifica se o tipo de instância atual e o tipo de instância especificado no parâmetro TargetInstanceTypeFromParameter são iguais. Se forem iguais, a automação termina.
6. aws:assertAwsResourceProperty: garante que a instância esteja em execução no sistema Nitro.
7. aws:branch: garante que o tipo de volume raiz da EC2 instância Amazon seja um volume do Amazon Elastic Block Store (Amazon EBS).
8. aws:assertAwsResourceProperty: confirma se o comportamento de desligamento da instância é stop, e não terminate.

9. `aws:branch`: garante que a EC2 instância da Amazon não seja uma instância spot.
10. `aws:branch`: garante que a locação da EC2 instância Amazon seja padrão e não um host dedicado ou uma instância dedicada.
11. `aws:executeScript`: confirma que há apenas uma automação desse runbook direcionada ao ID da instância atual. Se outra automação já estiver em andamento visando a mesma instância, a automação retornará um erro e terminará.
12. `aws:branch`: ramifica a automação com base no estado da EC2 instância da Amazon.
    a. Em caso `stopped` `stopping` afirmativo, a automação será executada `aws:waitForAwsResourceProperty` até que a EC2 instância da Amazon seja totalmente interrompida.
    b. Em caso `running` afirmativo`pending`, a automação será executada `aws:waitForAwsResourceProperty` até que a EC2 instância da Amazon passe nas verificações de status.
13. `aws:assertAwsResourceProperty`: confirma que a EC2 instância da Amazon não faz parte de um grupo de Auto Scaling chamando a operação `DescribeAutoScalingInstances` da API. Se a instância fizer parte de um grupo do Auto Scaling, garante que a EC2 instância da Amazon esteja em `standby` modo.
14. `aws:branch`: ramifica a automação dependendo se você deseja que a automação verifique se a EC2 instância da Amazon faz parte de uma AWS CloudFormation pilha:
    a. `aws:executeScript`Garante que a EC2 instância da Amazon não faça parte de uma AWS CloudFormation pilha chamando a operação da `DescribeStackResources` API.
15. `aws:executeAwsApi`: retorna uma lista de tipos de instância com o mesmo tipo de arquitetura de processador, tipo de virtualização, e que suporta o número de interfaces de rede atualmente conectadas à instância de destino.
16. `aws:executeAwsApi`: obtém o valor do tipo de instância de destino da chave de tag especificada no parâmetro `TargetInstanceTypeFromTagValue`.
17. `aws:executeScript`: confirma que os tipos de instâncias atual e de destino são compatíveis. Garante que o tipo de instância de destino esteja disponível na mesma sub-rede. Verifica se a entidade principal que iniciou o runbook tem permissões para alterar o tipo de instância e parar e iniciar a instância se ela estiver em execução.
18. `aws:branch`: ramifica a automação com base no valor do parâmetro `DryRun` estar definido como `yes`. Se `yes`, a automação termina.
19. `aws:branch`: verifica se o tipo de instância original e de destino são iguais. Se forem iguais, a automação termina.

20. `aws:executeAwsApi`: obtém o estado atual da instância.
21. `aws:changeInstanceState`: interrompe a EC2 instância da Amazon.
22. `aws:changeInstanceState`: força a instância a parar se ela estiver presa no estado `stopping`.
23. `aws:executeAwsApi`: altera o tipo de instância para o tipo de instância de destino.
24. `aws:sleep`: espera três segundos após alterar o tipo de instância para uma eventual consistência.
25. `aws:branch`: ramifica a automação com base no estado anterior da instância. Se foi `running`, a instância é iniciada.
    a. `aws:changeInstanceState`: inicia a EC2 instância da Amazon se ela estava em execução antes de alterar o tipo de instância.
    b. `aws:waitForAwsResourceProperty`: espera que a EC2 instância da Amazon passe pelas verificações de status. Se a instância não passar nas verificações de status, altere-a de volta para seu tipo original.
        i. `aws:changeInstanceState`: interrompe a EC2 instância da Amazon antes de alterá-la para o tipo de instância original.
        ii. `aws:changeInstanceState`: força a EC2 instância da Amazon a parar antes de alterá-la para o tipo de instância original, caso ela fique presa em um estado de parada.
        iii. `aws:executeAwsApi`: altera a EC2 instância da Amazon para seu tipo original.
        iv. `aws:sleep`: espera três segundos após alterar o tipo de instância para uma eventual consistência.
        v. `aws:changeInstanceState`: inicia a EC2 instância da Amazon se ela estava em execução antes de alterar o tipo de instância.
        vi. `aws:waitForAwsResourceProperty`: espera que a EC2 instância da Amazon passe pelas verificações de status.
26. `aws:sleep`: espera antes de terminar o runbook.

AWSSupport-RestoreEC2InstanceFromSnapshot

Descrição

O `AWSSupport-RestoreEC2InstanceFromSnapshot` runbook ajuda você a identificar e restaurar uma instância do Amazon Elastic Compute Cloud (Amazon EC2) a partir de um snapshot funcional do Amazon Elastic Block Store (Amazon EBS) do volume raiz.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EndDate

  Tipo: string

  Descrição: (opcional) A última data em que você deseja que a automação procure um snapshot.
- InplaceSwap

  Tipo: booliano

  Valores válidos: True | False

  Descrição: (opcional) se o valor desse parâmetro for definido como `true`, o volume recém-criado do snapshot substituirá o volume raiz existente anexado à sua instância.
- InstanceId

  Tipo: string

  Descrição: (obrigatório) o ID da instância de banco de dados do que você deseja reinicializar.

- LookForInstanceStatusCheck

  Tipo: booliano

  Valores válidos: True | False

  Padrão: verdadeiro

  Descrição: (opcional) se o valor desse parâmetro for definido como `true`, a automação verificará se as verificações de status da instância falham nas instâncias de teste iniciadas a partir dos snapshots.

- SkipSnapshotsBy

  Tipo: string

  Descrição: (opcional) o intervalo em que os snapshots são ignorados ao pesquisar snapshots para restaurar sua instância. Por exemplo, se houver 100 snapshots disponíveis e você especificar um valor de 2 para esse parâmetro, cada terceiro snapshot será revisado.

  Padrão: 0

- SnapshotId

  Tipo: string

  Descrição: (opcional) o ID de um snapshot do qual você deseja restaurar a instância.

- StartDate

  Tipo: string

  Descrição: (opcional) a primeira data em que você deseja que a automação procure um snapshot.

- TotalSnapshotsToLook

  Tipo: string

  Descrição: (opcional) o número de snapshots que a automação analisa.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- 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

Etapas do documento

1. aws:executeAwsApi: reúne detalhes sobre a instância de destino.
2. aws:assertAwsResourceProperty: verifica se a instância de destino existe.
3. aws:assertAwsResourceProperty: verifica se o volume raiz é um volume do Amazon EBS.
4. aws:assertAwsResourceProperty: verifica se ainda não está em execução outra automação que tenha como destino essa instância.
5. aws:executeAwsApi: marca a instância de destino.
6. aws:executeAwsApi- Cria um AMI da instância.

7. `aws:executeAwsApi`- Reúne detalhes sobre o AMI criado na etapa anterior.
8. `aws:waitForAwsResourceProperty`- Espera pelo AMI estado a ser `available` antes de prosseguir.
9. `aws:executeScript`- Lança uma nova instância a partir da recém-criada AMI.
10. `aws:assertAwsResourceProperty`: verifica se o estado da instância é `available`.
11. `aws:executeAwsApi`: reúne detalhes sobre a instância recém-iniciada.
12. `aws:branch`: ramifica com base no fato de ter fornecido um valor para o parâmetro `SnapshotId`.
13. `aws:executeScript`: retorna uma lista de snapshots dentro do período especificado.
14. `aws:executeAwsApi`: interrompe a instância.
15. `aws:waitForAwsResourceProperty`: espera que o estado do volume seja `available`.
16. `aws:waitForAwsResourceProperty`: espera que o estado da instância seja `stopped`.
17. `aws:executeAwsApi`: separa o volume de raiz.
18. `aws:waitForAwsResourceProperty`: espera que o volume raiz seja desanexado.
19. `aws:executeAwsApi`: anexa o novo volume raiz.
20. `aws:waitForAwsResourceProperty`: espera que o novo volume seja anexado.
21. `aws:executeAwsApi`: inicia a instância.
22. `aws:waitForAwsResourceProperty`: espera que o estado da instância seja `available`.
23. `aws:waitForAwsResourceProperty`: espera que as verificações de status do sistema e da instância sejam aprovadas na instância.
24. `aws:executeScript`: executa um script para encontrar um snapshot que possa ser usado para criar um volume com êxito.
25. `aws:executeScript`: executa um script para recuperar a instância usando o volume recém-criado a partir do snapshot identificado pela automação ou usando o volume criado a partir do snapshot que você especificou no parâmetro `SnapshotId`.
26. `aws:executeScript`: exclui recursos criados pela automação.

Saídas

launchCloneInstance.InstanceIds

ListSnapshotByDate. Instantâneos finais

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.Instantâneo de trabalho

InstanceRecovery.resultado

AWSSupport-SendLogBundleToS3Bucket

Descrição

O `AWSSupport-SendLogBundleToS3Bucket` runbook carrega um pacote de registros gerado pela ferramenta EC2 Rescue da instância de destino para o bucket S3 especificado. O runbook instala a versão específica da plataforma do EC2 Rescue com base na plataforma da instância de destino. EC2O Rescue é então usado para coletar todos os registros disponíveis do sistema operacional (SO).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

Tipo: string

Descrição: (Obrigatório) O ID da instância gerenciada Windows ou Linux das quais você deseja coletar os logs.

- S3 BucketName

  Tipo: string

  Descrição: (Obrigatório) Bucket do S3 para os quais carregar os logs.

- S3Path

  Tipo: string

  Padrão: `AWSSupport-SendLogBundleToS3Bucket/`

  Descrição: (Opcional) Caminho do S3 para os logs coletados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

É recomendável que a EC2 instância que recebe o comando tenha uma função do IAM com a política gerenciada SSMManaged InstanceCore da Amazon Amazon anexada. O usuário deve ter pelo menos ssm: StartAutomationExecution e ssm: SendCommand para executar a automação e enviar o comando para a instância, além de ssm: GetAutomationExecution para poder ler a saída da automação.

Etapas do documento

1. `aws:runCommand`- Instale o EC2 Rescue via`AWS-ConfigureAWSPackage`.
2. `aws:runCommand`- Execute o PowerShell script para coletar registros de solução de problemas do Windows com o EC2 Rescue.
3. `aws:runCommand`- Execute o script bash para coletar registros de solução de problemas do Linux com o EC2 Rescue.

Saídas

collectAndUploadWindowsLogBundle.Saída

collectAndUploadLinuxLogBundle.Saída

AWSSupport-StartEC2RescueWorkflow

Descrição

O AWSSupport-StartEC2RescueWorkflow runbook executa o script codificado em base64 fornecido (Bash ou Powershell) em uma instância auxiliar criada para salvar sua instância. O volume raiz da sua instância é anexado e montado na instância auxiliar, também conhecida como instância de EC2 resgate. Se sua instância for Windows, forneça um script do Powershell. Caso contrário, use Bash. O runbook define algumas variáveis de ambiente que você pode usar em seu script. As variáveis de ambiente contêm informações sobre a entrada que você forneceu, bem como informações sobre o volume raiz offline. O volume offline já está instalado e pronto para uso. Por exemplo, você pode salvar um arquivo de configuração de estado desejado para um volume raiz do Windows offline, ou chroot para um volume raiz do Linux offline, e executar uma correção offline.

Execute esta automação (console)

> **Important**
>
> EC2 As instâncias da Amazon criadas a partir do Marketplace Amazon Machine Images (AMIs) não são suportadas por essa automação.

Informações adicionais

Para codificar um script em base64, você pode usar Powershell ou Bash. Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

Bash:

```
base64 PATH_TO_FILE
```

Esta é uma lista de variáveis de ambiente que você pode usar em seus scripts offline, dependendo do sistema operacional de destino

Windows:

Variável	Descrição	Valor de exemplo
$env: RESCUE_AC COUNT_ID EC2	{{ global:ACCOUNT_ID }}	123456789012
$ env: RESCUE_DATE EC2	{{ global:DATE }}	2018-09-07
$env: RESCUE_DATE_TIME EC2	{{ global:DATE_TIME }}	2018-09-07_18.09.59
$env: EC2 RESCUE_ RW_DIR EC2	EC2Caminho de instalação do Rescue for Windows	C:\Program Files\ Amazon\ EC2 Rescue
$env: EC2 RESCUE_ RW_DIR EC2	EC2Caminho de instalação do Rescue for Windows	C:\Program Files\ Amazon\ EC2 Rescue
$env: RESCUE_EX ECUTION_ID EC2	{{ automation:EXECUTI ON_ID }}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
$ env: RESCUE_OF FLINE_CURRENT_CONT ROL_SET EC2	Caminho definido de controle atual do Windows offline	`HKLM:\AWSTempSystem \ControlSet001`
$env: RESCUE_OF FLINE_DRIVE EC2	Letra de unidade offline do Windows	D:\
$ env: RESCUE_OF FLINE_EBS_DEVICE EC2	Dispositivo EBS do volume raiz offline	xvdf
$env: RESCUE_OF FLINE_KERNEL_VER EC2	Versão de kernel do Windows offline	6.1.7601.24214
$env: RESCUE_OF FLINE_OS_ARCHITECTURE EC2	Arquitetura do Windows offline	AMD64
$ env: RESCUE_OF FLINE_OS_CAPTION EC2	Legenda off-line do Windows	Datacenter do Windows Server 2008 R2

Variável	Descrição	Valor de exemplo
$env: RESCUE_OF FLINE_OS_TYPE EC2	Tipo de sistema operacional Windows offline	Servidor
$env: RESCUE_OF FLINE_PROGRAM_FILE S_DIR EC2	Caminho de diretório de arquivos de programa do Windows offline	D:\Program Files
$env: RESCUE_OF FLINE_PROGRAM_FILE S_X86_DIR EC2	Caminho de diretório x86 de arquivos de programa do Windows offline	D:\Program Files (x86)
$env: RESCUE_OF FLINE_REGISTRY_DIR EC2	Caminho de diretório de registro do Windows offline	D:\Windows\System32\config
$ env: RESCUE_OF FLINE_SYSTEM_ROOT EC2	Caminho de diretório de raiz do sistema do Windows offline	D:\Windows
$env: RESCUE_REGION EC2	{{ global:REGION }}	us-west-1
$ env: RESCUE_S3_BUCKET EC2	{{S3BucketName }}	balde de demonstração amzn-s3-
$env: RESCUE_S3_PREFIX EC2	{{ S3Prefix }}	myprefix/
$ env: RESCUE_SO URCE_INSTANCE EC2	{{ InstanceId }}	i-abcdefgh123456789
$ script: EC2 RESCUE_OF FLINE_WINDOWS_INSTALL	Metadados de instalação do Windows offline	Objeto Powershell do cliente

Linux

Variável	Descrição	Valor de exemplo
EC2ID DA CONTA DE RESGATE	{{ global:ACCOUNT_ID }}	123456789012
EC2DATA DE RESGATE	{{ global:DATE }}	2018-09-07
EC2DATA E HORA DO RESGATE	{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_ EC2 RL_DIR	EC2Caminho de instalação do Rescue for Linux	/usr/local/ec2rl-1.1.3
EC2ID DE EXECUÇÃO DE RESGATE	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2DISPOSITIVO DE RESGATE OFFLINE	Nome do dispositivo offline	/dev/xvdf1
EC2RESCUE_OFFLINE_EBS_DEVICE	Dispositivo EBS do volume raiz offline	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	Ponto de montagem de volume raiz offline	/mnt/mount
EC2RESCUE_PYTHON	Versão do Python	python2.7
EC2REGIÃO_DE RESGATE	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{S3BucketName }}	balde de demonstração amzn-s3-
EC2PREFIXO RESCUE_S3_	{{ S3Prefix }}	myprefix/
EC2INSTÂNCIA_DE_FONTE DE RESCUE	{{ InstanceId }}	i-abcdefgh123456789

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AMIPrefix

  Tipo: String

  Padrão: `AWSSupport-EC2Rescue`

  Descrição: (Opcional) Um prefixo para o nome de backup da AMI.

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- CreatePostEC2RescueBackup

  Tipo: String

  Valores válidos: True | False

  Padrão: False

  Descrição: (Opcional) Defina-o `true` para criar uma AMI de InstanceId depois de executar o script, antes de iniciá-lo. A AMI persistirá depois da conclusão da automação. É sua responsabilidade garantir acesso à AMI ou excluí-la.

- CreatePreEC2RescueBackup

  Tipo: String

  Valores válidos: True | False

Padrão: False

Descrição: (Opcional) Defina-o `true` para criar uma AMI de InstanceId antes de executar o script. A AMI persistirá depois da conclusão da automação. É sua responsabilidade garantir acesso à AMI ou excluí-la.

- EC2RescueInstanceType

  Tipo: String

  Valores válidos: t2.small | t2.medium | t2.large | t3.small | t3.medium | t3.large | i3.large

  Padrão: t3.medium

  Descrição: (Opcional) O tipo de EC2 instância da instância do EC2 Rescue.

- InstanceId

  Tipo: String

  Descrição: ID (obrigatório) da sua EC2 instância. IMPORTANTE: AWS Systems Manager A automação interrompe essa instância. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um IP elástico.

- OfflineScript

  Tipo: String

  Descrição: (obrigatório) Script codificado em Base64 a ser executado contra a instância auxiliar. Use o Bash se sua instância de origem for Linux e PowerShell se for Windows.

- S3 BucketName

  Tipo: String

  Descrição: (Opcional) Nome do bucket do S3 em sua conta na qual você deseja carregar os logs de solução de problemas. Verifique se a política de buckets não concede permissões de leitura/gravação desnecessárias a partes que não precisam acessar os logs coletados.

- S3Prefix

  Tipo: String

Padrão: `AWSSupport-EC2Rescue`

Descrição: (Opcional) Um prefixo para os logs da S3.

- SubnetId

  Tipo: String

  Padrão: SelectedInstanceSubnet

  Descrição: (Opcional) O ID da sub-rede da instância do EC2 Rescue. Por padrão, é usada a mesma sub-rede na qual a instância fornecida reside. IMPORTANTE: Se você fornecer uma sub-rede personalizada, ela deverá estar na mesma InstanceId zona de disponibilidade e permitir o acesso aos endpoints do SSM.

- UniqueId

  Tipo: String

  Padrão: {{ automation:EXECUTION_ID }}

  Descrição: (opcional) um identificador exclusivo para o fluxo de trabalho.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

É recomendável que o usuário que executa a automação tenha a política gerenciada do Amazon SSMAutomation Role IAM anexada. Além dessa política, o usuário deve ter:

```
{
                "Version": "2012-10-17",
                "Statement": [
                   {
                      "Action": [
                         "lambda:InvokeFunction",
                         "lambda:DeleteFunction",
                         "lambda:GetFunction"
                      ],
                      "Resource": "arn:aws:lambda:*:An-AWS-Account-
ID:function:AWSSupport-EC2Rescue-*",
                      "Effect": "Allow"
                   },
```

```
                    {
                       "Action": [
                          "s3:GetObject",
                          "s3:GetObjectVersion"
                       ],
                       "Resource": [
                          "arn:aws:s3:::awssupport-ssm.*/*.template",
                          "arn:aws:s3:::awssupport-ssm.*/*.zip"
                       ],
                       "Effect": "Allow"
                    },
                    {
                       "Action": [
                          "iam:CreateRole",
                          "iam:CreateInstanceProfile",
                          "iam:GetRole",
                          "iam:GetInstanceProfile",
                          "iam:PutRolePolicy",
                          "iam:DetachRolePolicy",
                          "iam:AttachRolePolicy",
                          "iam:PassRole",
                          "iam:AddRoleToInstanceProfile",
                          "iam:RemoveRoleFromInstanceProfile",
                          "iam:DeleteRole",
                          "iam:DeleteRolePolicy",
                          "iam:DeleteInstanceProfile"
                       ],
                       "Resource": [
                          "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport-EC2Rescue-*",
                          "arn:aws:iam::An-AWS-Account-ID:instance-profile/AWSSupport-
EC2Rescue-*"
                       ],
                       "Effect": "Allow"
                    },
                    {
                       "Action": [
                          "lambda:CreateFunction",
                          "ec2:CreateVpc",
                          "ec2:ModifyVpcAttribute",
                          "ec2:DeleteVpc",
                          "ec2:CreateInternetGateway",
                          "ec2:AttachInternetGateway",
                          "ec2:DetachInternetGateway",
                          "ec2:DeleteInternetGateway",
```

```
                    "ec2:CreateSubnet",
                    "ec2:DeleteSubnet",
                    "ec2:CreateRoute",
                    "ec2:DeleteRoute",
                    "ec2:CreateRouteTable",
                    "ec2:AssociateRouteTable",
                    "ec2:DisassociateRouteTable",
                    "ec2:DeleteRouteTable",
                    "ec2:CreateVpcEndpoint",
                    "ec2:DeleteVpcEndpoints",
                    "ec2:ModifyVpcEndpoint",
                    "ec2:Describe*"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }
        ]
    }
```

Etapas do documento

1. `aws:executeAwsApi`: descreve a instância fornecida
2. `aws:executeAwsApi`: descreve o volume raiz da instância fornecida
3. `aws:assertAwsResourceProperty`: verifica se o tipo de dispositivo de volume raiz é EBS
4. `aws:assertAwsResourceProperty`: verifica se o volume raiz não está criptografado
5. `aws:assertAwsResourceProperty`: verifica o ID de sub-rede fornecido
   a. (Use a sub-rede da instância atual) - Se * SubnetId = SelectedInstanceSubnet *, execute `aws:createStack` para implantar a pilha do EC2 Rescue CloudFormation
   b. (Criar nova VPC) - Se * SubnetId = CreateNew VPC*, execute `aws:createStack` para implantar a pilha de resgate EC2 CloudFormation
   c. (Usar sub-rede personalizada) - em todos os demais casos:

      `aws:assertAwsResourceProperty`: verifique se a sub-rede fornecida está na mesma zona de disponibilidade da instância fornecida

      `aws:createStack`- Implante a CloudFormation pilha de EC2 resgate
6. `aws:invokeLambdaFunction`: execute validação adicional de entrada
7. `aws:executeAwsApi`- Atualize a CloudFormation pilha do EC2 Rescue para criar a instância auxiliar do EC2 Rescue

8. `aws:waitForAwsResourceProperty`- Aguarde a conclusão da atualização da CloudFormation pilha de EC2 resgate
9. `aws:executeAwsApi`- Descreva a saída da CloudFormation pilha do EC2 Rescue para obter o ID da instância auxiliar do EC2 Rescue
10. `aws:waitForAwsResourceProperty`- Aguarde até que a instância auxiliar do EC2 Rescue se torne uma instância gerenciada
11. `aws:changeInstanceState`: interrompe a instância fornecida
12. `aws:changeInstanceState`: interrompe a instância fornecida
13. `aws:changeInstanceState`: força a parada da instância fornecida
14. `aws:assertAwsResourceProperty`- Verifique o valor CreatePre EC2 RescueBackup de entrada
    a. (Criar backup de EC2 pré-resgate) - Se * CreatePre EC2 RescueBackup = verdadeiro*
    b. `aws:executeAwsApi`: crie uma AMI de backup da instância fornecida
    c. `aws:createTags`: marca o backup da AMI
15. `aws:runCommand`- Instale o EC2 Rescue na instância auxiliar do EC2 Rescue
16. `aws:executeAwsApi`: desanexa o volume raiz da instância fornecida
17. `aws:assertAwsResourceProperty`: verifica a plataforma da instância fornecida
    a. (Instância é Windows):

       `aws:executeAwsApi`- Conecte o volume raiz à instância auxiliar do EC2 Rescue como *xvdf*

       `aws:sleep`: repousa por 10 segundos

       `aws:runCommand`: executa o script offline fornecido no Powershell
    b. (Instância é Linux):

       `aws:executeAwsApi`- Conecte o volume raiz à instância auxiliar do EC2 Rescue como */dev/sdf*

       `aws:sleep`: repousa por 10 segundos

       `aws:runCommand`: executa o script offline fornecido no Bash
18. `aws:changeInstanceState`- Pare a instância do EC2 Rescue Helper
19. `aws:changeInstanceState`- Forçar a parada da instância do EC2 Rescue Helper
20. `aws:executeAwsApi`- Separe o volume raiz da instância auxiliar do EC2 Rescue

21. `aws:executeAwsApi`: anexa o volume raiz novamente à instância fornecida
22. `aws:assertAwsResourceProperty`- Verifique o valor CreatePost EC2 RescueBackup de entrada
    a. (Criar backup EC2 pós-resgate) - Se * CreatePost EC2 RescueBackup = verdadeiro*
    b. `aws:executeAwsApi`: crie uma AMI de backup da instância fornecida
    c. `aws:createTags`: marca o backup da AMI
23. `aws:executeAwsApi`: restaura a exclusão inicial no estado de encerramento para o volume raiz da instância fornecida
24. `aws:changeInstanceState`: restaura o estado inicial da instância fornecida (em execução/parado)
25. `aws:deleteStack`- Exclua a CloudFormation pilha de EC2 resgate

Saídas

runScriptForSaída Linux

runScriptForSaída do Windows

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSPremiumSupport-TroubleshootEC2DiskUsage

Descrição

O `AWSPremiumSupport-TroubleshootEC2DiskUsage` runbook ajuda você a investigar e potencialmente remediar problemas com o uso de discos raiz e não raiz da instância Amazon Elastic Compute Cloud (Amazon EC2). Se possível, o runbook tenta corrigir os problemas estendendo o volume e seu sistema de arquivos. Para realizar essas tarefas, esse runbook orquestra a execução de vários runbooks com base no sistema operacional da instância afetada.

O primeiro runbook, `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` ou `AWSPremiumSupport-DiagnoseDiskUsageOnLinux`, determina se os problemas de disco podem ser atenuados com a expansão do volume.

O segundo runbook, `AWSPremiumSupport-ExtendVolumesOnWindows` ou `AWSPremiumSupport-ExtendVolumesOnLinux`, usa a saída do primeiro runbook para executar

o código Python que modifica o volume. Depois que o volume for modificado, o runbook estende a partição e o sistema de arquivos dos volumes afetados.

> **Important**
>
> O acesso aos runbooks `AWSPremiumSupport-*` requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Comparar os planos do AWS Support.

Este documento foi criado em colaboração com AWS Managed Services (AMS). O AMS ajuda você a gerenciar sua AWS infraestrutura com mais eficiência e segurança. O AMS também oferece flexibilidade operacional, segurança e conformidade aprimoradas, otimização de capacidade e identificação de economia de custos. Para obter mais informações, consulte AWS Managed Services.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, Windows

Parâmetros

- InstanceId

  Tipo: string

  Valores permitidos: ^i-[a-z0-9]{8,17}$

  Descrição: (Obrigatório) ID da sua EC2 instância da Amazon.
- VolumeExpansionEnabled

  Tipo: booliano

Descrição: (opcional) sinalize para controlar se o documento estenderá os volumes e partições afetados.

Padrão: verdadeiro

- VolumeExpansionUsageTrigger

  Tipo: string

  Descrição: (opcional) uso mínimo do espaço de partição necessário para acionar a extensão (em porcentagem).

  Valores permitidos: ^[0-9]{1,2}$

  Padrão: 85

- VolumeExpansionCapSize

  Tipo: string

  Descrição: (opcional) o tamanho máximo para o qual o volume do Amazon Elastic Block Store (Amazon EBS) será aumentado (em GiB).

  Valores permitidos: ^[0-9]{1,4}$

  Padrão: 2048

- VolumeExpansionGibIncrease

  Tipo: string

  Descrição: (opcional) aumento do volume em GiB. O maior aumento líquido entre VolumeExpansionGibIncrease e VolumeExpansionPercentageIncrease será usado.

  Valores permitidos: ^[0-9]{1,4}$

  Padrão: 20

- VolumeExpansionPercentageIncrease

  Tipo: string

  Descrição: (opcional) aumento do volume em porcentagem. O maior aumento líquido entre VolumeExpansionGibIncrease e VolumeExpansionPercentageIncrease será usado.

Valores permitidos: ^[0-9]{1,2}$

Padrão: 20

- AutomationAssumeRole

  Tipo: string

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

1. `aws:assertAwsResourceProperty`: verifica se a instância é gerenciada pelo Systems Manager
2. `aws:executeAwsApi`: descreve a instância para obter a plataforma.
3. `aws:branch`: ramifica a automação com base na plataforma da instância.
   a. Se a instância for Windows:
      i. `aws:executeAutomation`: executa o runbook `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` para diagnosticar problemas de uso de disco na instância.
      ii. `aws:executeAwsApi`: obtém a saída da automação anterior.
      iii. `aws:branch`: ramifica com base na saída do diagnóstico e se houver volumes que possam ser expandidos para mitigar o alerta.
         A. Não há volumes que precisem ser expandidos: terminar a automação.
         B. Há volumes que precisam ser expandidos:
            I. `aws:executeAwsApi`- Crie um Amazon Machine Image (AMI) da instância.
            II. `aws:waitForAwsResourceProperty`- Espera pelo AMI estado a ser`available`.
            III. `aws:executeAutomation`: executa o runbook `AWSPremiumSupport-ExtendVolumesOnWindows` para realizar a modificação do volume, bem como as etapas necessárias no sistema operacional (SO) para disponibilizar o novo espaço.
   b. (A plataforma não é Windows) Se a instância de entrada não for Windows:
      i. `aws:executeAutomation`: executa o runbook `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` para diagnosticar problemas de uso de disco na instância.
      ii. `aws:executeAwsApi`: obtém a saída da automação anterior.
      iii. `aws:branch`: ramifica com base na saída do diagnóstico e se houver volumes que possam ser expandidos para mitigar o alerta.
         A. Não há volumes que precisem ser expandidos: terminar a automação.
         B. Há volumes que precisam ser expandidos:
            I. `aws:executeAwsApi`- Crie um AMI da instância.
            II. `aws:waitForAwsResourceProperty`- Espera por AMI estado a ser`available`.
            III. `aws:executeAutomation`: executa o runbook `AWSPremiumSupport-ExtendVolumesOnLinux` para realizar a modificação do volume, bem como as etapas necessárias no OS para disponibilizar o novo espaço.

Saídas

diagnoseDiskUsageAlertOnWindows.Saída

extendVolumesOnSaída do Windows

diagnoseDiskUsageAlertOnLinux.Saída

extendVolumesOnSaída Linux

BackupAMILinux. ImageId

BackupAMIWindows. ImageId

AWSSupport-TroubleshootEC2InstanceConnect

Descrição

`AWSSupport-TroubleshootEC2InstanceConnect`a automação ajuda a analisar e detectar erros que impedem a conexão com uma instância do Amazon Elastic Compute Cloud (Amazon EC2) usando o Amazon EC2 Instance Connect. Ele identifica problemas causados por uma Amazon Machine Image (AMI) não suportada, falta de instalação ou configuração de pacotes no nível do sistema operacional, permissões ausentes AWS Identity and Access Management (IAM) ou problemas de configuração de rede.

Como funciona?

O runbook usa o ID da EC2 instância Amazon, nome de usuário, modo de conexão, IP CIDR de origem, porta SSH e nome de recurso da Amazon (ARN) para a função do IAM ou usuário com problemas com o Amazon Instance Connect. EC2 Em seguida, ele verifica os pré-requisitos para se conectar a uma instância da Amazon EC2 usando o Amazon Instance EC2 Connect:

- A instância está em execução e em um estado íntegro.
- A instância está localizada em uma AWS região suportada pelo Amazon EC2 Instance Connect.
- A AMI da instância é suportada pelo Amazon EC2 Instance Connect.
- A instância pode acessar o Instance Metadata Service (IMDSv2).
- O pacote Amazon EC2 Instance Connect está devidamente instalado e configurado no nível do sistema operacional.
- A configuração da rede (grupos de segurança, ACL de rede e regras da tabela de rotas) permite a conexão com a instância por meio do Amazon EC2 Instance Connect.

- A função ou o usuário do IAM que é usado para aproveitar o Amazon EC2 Instance Connect tem acesso às chaves push para a EC2 instância da Amazon.

> **Important**
>
> - Para verificar a AMI da instância, a IMDSv2 acessibilidade e a instalação do pacote Amazon Instance EC2 Connect, a instância deve ser gerenciada por SSM. Caso contrário, ele pula essas etapas. Para obter mais informações, consulte Por que minha EC2 instância da Amazon não está sendo exibida como um nó gerenciado.
> - A verificação de rede detectará somente se o grupo de segurança e as regras de ACL de rede bloquearem o tráfego quando o SourceIp CIDR for fornecido como um parâmetro de entrada. Caso contrário, ele exibirá apenas regras relacionadas ao SSH.
> - As conexões usando o Amazon EC2 Instance Connect Endpoint não são validadas neste runbook.
> - Para conexões privadas, a automação não verifica se o cliente SSH está instalado na máquina de origem e se ele pode acessar o endereço IP privado da instância.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`
- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até o `AWSSupport-TroubleshootEC2InstanceConnect`no AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - InstanceId (Obrigatório):

     O ID da EC2 instância de destino da Amazon à qual você não conseguiu se conectar usando o Amazon EC2 Instance Connect.
   - AutomationAssumeRole (Opcional):

     O ARN da função do IAM que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - Nome de usuário (obrigatório):

     O nome de usuário usado para se conectar à EC2 instância da Amazon usando o Amazon EC2 Instance Connect. Ele é usado para avaliar se o acesso do IAM foi concedido para esse usuário específico.
   - EC2InstanceConnectRoleOrUser(Obrigatório):

     O ARN da função ou do usuário do IAM que está utilizando o Amazon EC2 Instance Connect para enviar chaves para a instância.
   - SSHPort (Opcional):

A porta SSH configurada na EC2 instância da Amazon. O valor padrão é 22. O número da porta deve estar entre1-65535.

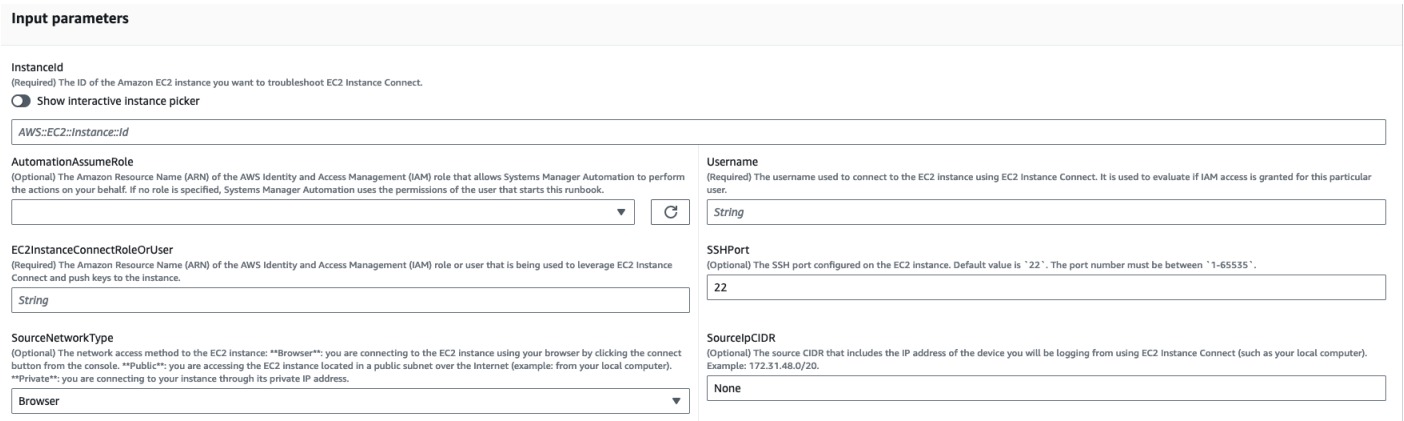
- SourceNetworkType (Opcional):

  O método de acesso à rede para a EC2 instância da Amazon:

  - Navegador: você se conecta a partir do AWS Management Console.
  - Público: você se conecta à instância localizada em uma sub-rede pública pela Internet (por exemplo, seu computador local).
  - Privado: você se conecta por meio do endereço IP privado da instância.

- SourceIpCIDR (opcional):

  O CIDR de origem que inclui o endereço IP do dispositivo (como seu computador local) do qual você se conectará usando o Amazon EC2 Instance Connect. Exemplo: 172.31.48.6/32. Se nenhum valor for fornecido com o modo de acesso público ou privado, o runbook não avaliará se o grupo de segurança da EC2 instância da Amazon e as regras de ACL de rede permitem tráfego SSH. Em vez disso, ele exibirá regras relacionadas ao SSH.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - AssertInitialState:

     Garante que o status da EC2 instância da Amazon esteja em execução. Caso contrário, a automação termina.

   - GetInstanceProperties:

Obtém as propriedades atuais da EC2 instância Amazon (PlatformDetails PublicIpAddress, VpcId,, SubnetId e MetadataHttpEndpoint).

- GatherInstanceInformationFromSMS:

  Obtém o status de ping da instância do Systems Manager e os detalhes do sistema operacional se a instância for gerenciada por SSM.

- CheckIfAWSRegionSuportado:

  Verifica se a EC2 instância da Amazon está localizada em uma AWS região compatível com o Amazon EC2 Instance Connect.

- BranchOnIfAWSRegionSuportado:

  Continua a execução se a AWS região for suportada pelo Amazon EC2 Instance Connect. Caso contrário, ele cria a saída e sai da automação.

- CheckIfInstanceAMIIsSuportado:

  Verifica se a AMI associada à instância é compatível com o Amazon EC2 Instance Connect.

- BranchOnIfInstanceAMIIsSuportado:

  Se a AMI da instância for compatível, ela executa as verificações no nível do sistema operacional, como a acessibilidade dos metadados e a instalação e configuração do pacote Amazon EC2 Instance Connect. Caso contrário, ele verifica se os metadados HTTP estão habilitados usando a AWS API e, em seguida, avança para a etapa de verificação de rede.

- Confira IMDSReachabilityFromOs:

  Executa um script Bash na instância de destino do Amazon EC2 Linux para verificar se ela é capaz de acessar o. IMDSv2

- Verifique EICPackage a instalação:

  Executa um script Bash na instância de destino do Amazon EC2 Linux para verificar se o pacote Amazon EC2 Instance Connect está instalado e configurado corretamente.

- Confira SSHConfigFromOs:

  Executa um script Bash na instância de destino do Amazon EC2 Linux para verificar se a porta SSH configurada corresponde ao parâmetro de entrada `. SSHPort `

- CheckMetadataHTTPEndpointIsEnabled:

Verifica se o endpoint HTTP do serviço de metadados da instância está ativado.

- Verifique o EICNetwork acesso:

  Verifica se a configuração da rede (grupos de segurança, ACL de rede e regras da tabela de rotas) permite a conexão com a instância por meio do Amazon EC2 Instance Connect.

- Confira IAMRoleOrUserPermissions:

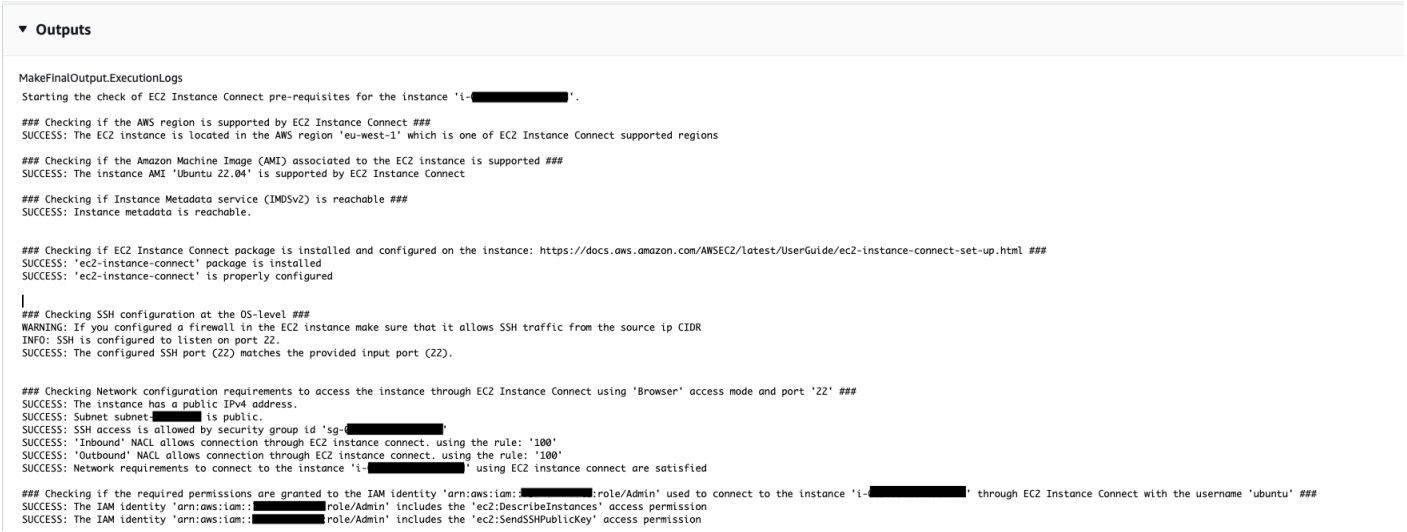
  Verifica se a função do IAM ou o usuário usado para utilizar o Amazon EC2 Instance Connect tem acesso às chaves push para a EC2 instância da Amazon usando o nome de usuário fornecido.

- MakeFinalOutput:

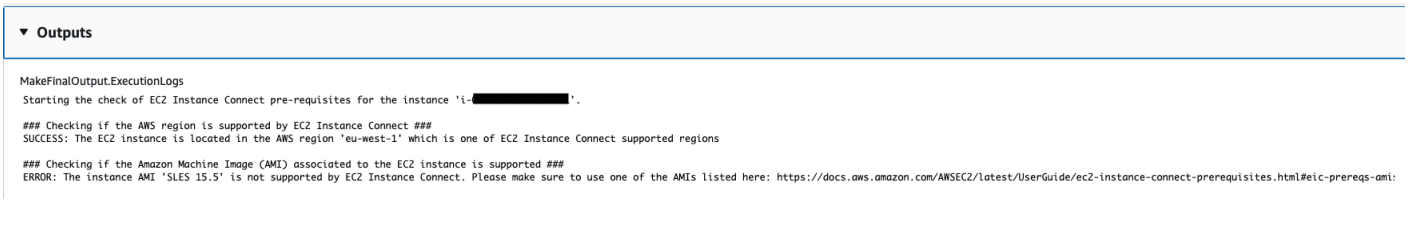
  Consolida a saída de todas as etapas anteriores.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

   Execução em que a instância de destino tem todos os pré-requisitos necessários:



   Execução em que a AMI da instância de destino não é suportada:



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- Como soluciono problemas de conexão com minha EC2 instância da Amazon usando o Amazon EC2 Instance Connect?

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

Descrição

`AWSSupport-TroubleshootLinuxMGNDRSAgentLogs`o runbook de automação é usado para detectar erros comuns ao instalar os agentes de replicação AWS Application Migration Service (AWS MGN) e AWS Elastic Disaster Recovery (AWS DRS) em servidores Linux para migrar servidores de origem para a nuvem. AWS

Como funciona?

O runbook `AWSSupport-TroubleshootLinuxMGNDRSAgentLogs` segue o caminho do Amazon Simple Storage Service (Amazon S3), no qual o log de instalação do AWS MGN ou do AWS DRS é carregado como parâmetro. `aws_replication_agent_installer.log` Em seguida, ele executa as seguintes tarefas:

- Validação: verifica se o arquivo de log fornecido é válido e se contém pelo menos uma instalação do agente.
- Análise: analisa minuciosamente a instalação mais recente do agente no arquivo de log em busca de erros conhecidos de AWS MGN ou AWS DRS.
- Detecção e resolução de erros: com base na análise, ele detecta e lista quaisquer erros ou problemas durante o processo de instalação do agente. Para cada erro detectado, o runbook fornece etapas detalhadas para ajudar a resolver ou mitigar o problema.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `s3:GetObject`
- `s3:ListBucket`

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até `AWSSupport-TroubleshootLinuxMGNDRSAgentLogs`em Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

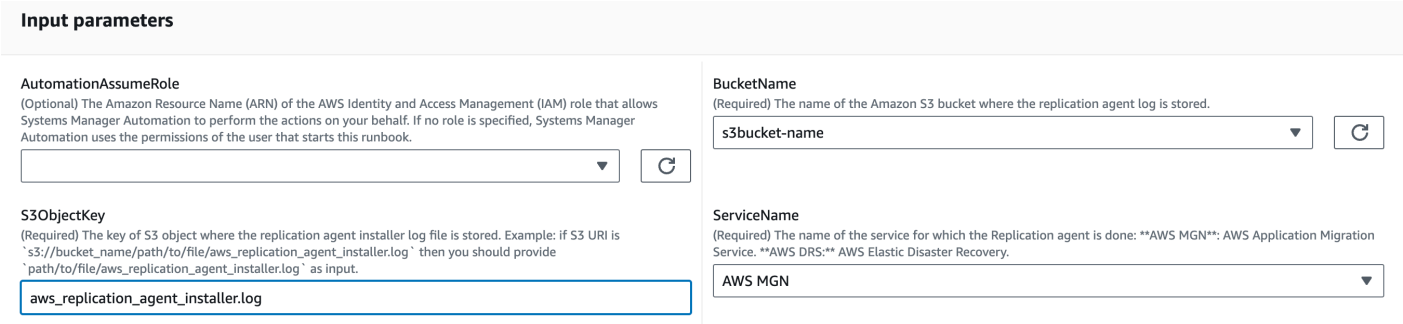
     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - BucketName (Obrigatório):

     O nome do bucket do Amazon S3 em que o log do agente de replicação é armazenado.
   - S3 ObjectKey (obrigatório):

A chave do objeto Amazon S3 em que o arquivo de log do instalador do agente de replicação está armazenado. Exemplo: Se o URI do Amazon S3 fors3://bucket_name/path/to/file/aws_replication_agent_installer.log, você deverá inserir. path/to/file/aws_replication_agent_installer.log

- ServiceName (Obrigatório):

  O nome do serviço para o qual o agente de replicação está instalado. Valores permitidos: AWS MGN ou AWS DRS



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - **`ValidateInput`**

     Garante que o arquivo de log do agente de replicação seja válido e acessível usando o nome e o caminho do bucket Amazon S3 fornecidos para o objeto e, em seguida, retorna o número de bytes da instalação mais recente do agente.

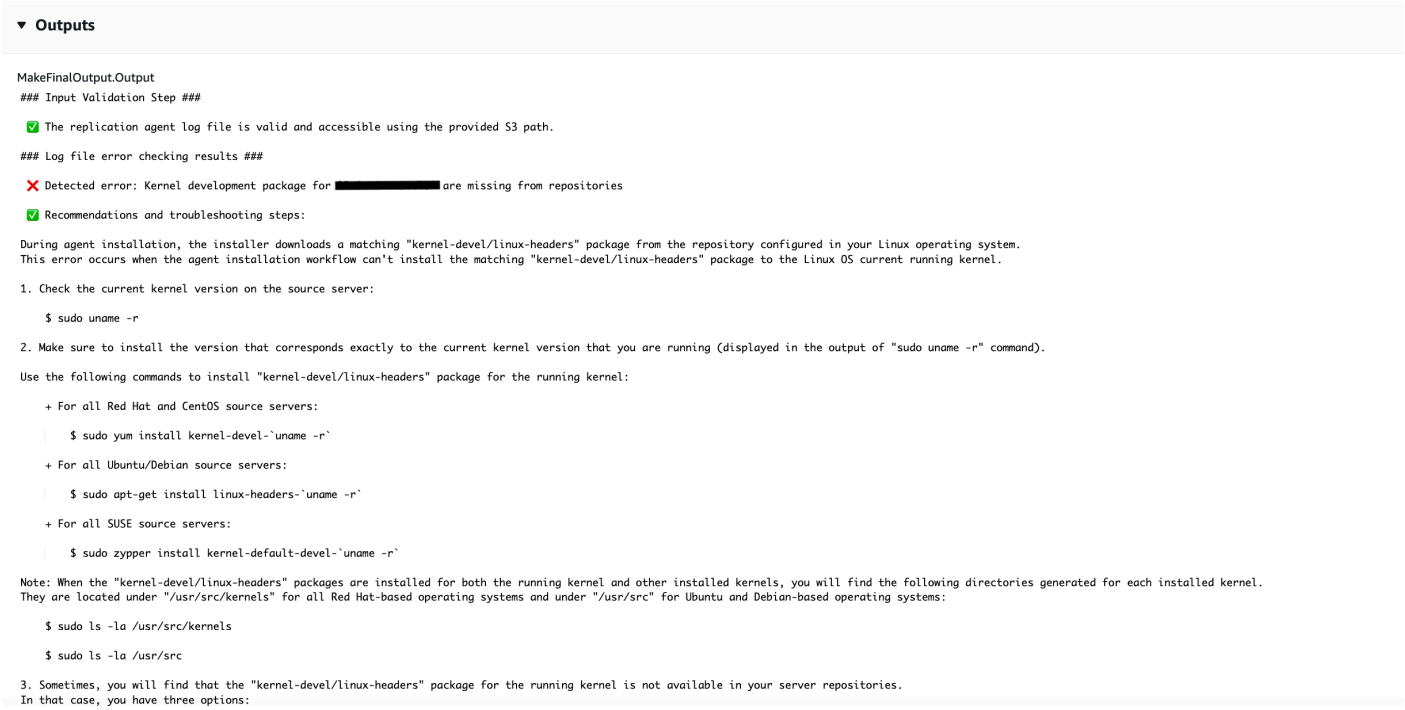
   - **`CheckReplicationAgentLogErrors`**

     Lê o arquivo de log do agente de replicação a partir do byte de instalação mais recente e pesquisa erros conhecidos de AWS MGN ou AWS DRS.

   - **`MakeFinalOutput`**

     Cria a saída das verificações anteriores, incluindo informações sobre os erros encontrados e recomendações de solução de problemas.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSSupport-TroubleshootRDP

Descrição

O runbook `AWSSupport-TroubleshootRDP` permite ao usuário verificar ou modificar configurações comuns na instância de destino que possam afetar as conexões Remote Desktop Protocol (RDP), como os perfis RDP port, Network Layer Authentication (NLA) e Windows Firewall. Opcionalmente, as alterações podem ser aplicadas offline ao interromper e iniciar a instância, se o usuário explicitamente permitir a correção offline. Por padrão, o runbook lê e exibe os valores das configurações.

> **Important**
>
> As alterações nas configurações RDP, serviço RDP e perfis de Firewall do Windows devem ser cuidadosamente analisadas antes de executar este runbook.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- Ação

  Tipo: string

  Valores válidos: CheckAll | FixAll | Personalizado

  Padrão: Custom

  Descrição: (Opcional) [Personalizado] Use os valores de Firewall RDPServiceStartupType, RDPService Ação, RDPPort Ação, NLASetting Ação e RemoteConnections para gerenciar as configurações. [CheckAll] Leia os valores das configurações sem alterá-las. [FixAll] Restaure as configurações padrão do RDP e desative o Firewall do Windows.

- AllowOffline

  Tipo: string

  Valores válidos: True | False

  Padrão: False

Descrição: (opcional) apenas correção - Defina como verdadeiro se você permitir a correção do RDP offline, caso a solução de problemas online falhe ou caso a instância fornecida não seja uma instância gerenciada. Observação: para a correção offline, a Automação do SSM interrompe a instância e cria uma AMI antes de tentar qualquer operação.

- AutomationAssumeRole

  Tipo: string

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Firewall

  Tipo: string

  Valores válidos: Check | Disable

  Padrão: Check

  Descrição: (Opcional) Marque ou desabilite o firewall do Windows (todos os perfis).

- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da instância que vai solucionar os problemas das configurações de RDP.

- NLASettingAção

  Tipo: string

  Valores válidos: Check | Disable

  Padrão: Check

  Descrição: (Opcional) Marque ou desabilite o Network Layer Authentication (NLA).

- RDPPortAção

  Tipo: string

Valores válidos: Check | Modify

Padrão: Check

Descrição: (Opcional) Marque a porta atual usada para conexões RDP, ou modifique a porta RDP de volta para 3389 e reinicie o serviço.

- RDPServiceAção

  Tipo: string

  Valores válidos: Check | Start | Restart | Force-Restart

  Padrão: Check

  Descrição: (Opcional) Verifique, inicie, reinicie ou force a reinicialização do serviço RDP (). TermService

- RDPServiceStartupType

  Tipo: string

  Valores válidos: Check | Auto

  Padrão: Check

  Descrição: (Opcional) Marque ou defina o serviço RDP para iniciar automaticamente quando o Windows é inicializado.

- RemoteConnections

  Tipo: string

  Valores válidos: Check | Enable

  Padrão: Check

  Descrição: (Opcional) Uma ação a ser executada na TSConnections configuração FDeny: Verificar, Ativar.

- S3 BucketName

  Tipo: string

Descrição: (Opcional) Apenas offline - Nome do bucket do S3 em sua conta na qual você deseja carregar os logs de solução de problemas. Verifique se a política de buckets não concede permissões de leitura/gravação desnecessárias a partes que não precisam acessar os logs coletados.

- SubnetId

  Tipo: string

  Padrão: SelectedInstanceSubnet

  Descrição: (Opcional) Somente off-line - O ID de sub-rede da instância do EC2 Rescue usado para realizar a solução de problemas off-line. Se nenhum ID de sub-rede for especificado, a AWS Systems Manager Automation criará uma nova VPC. IMPORTANTE: A sub-rede deve estar na mesma InstanceId zona de disponibilidade e permitir o acesso aos endpoints do SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

É recomendável que a EC2 instância que recebe o comando tenha uma função do IAM com a política gerenciada SSMManaged InstanceCore da Amazon Amazon anexada. Para a correção on-line, o usuário deve ter pelo menos ssm:DescribeInstanceInformation, ssm: StartAutomationExecution e ssm: SendCommand para executar a automação e enviar o comando para a instância, além de ssm: GetAutomationExecution para poder ler a saída da automação. Para a correção off-line, o usuário deve ter pelo menos ssm: DescribeInstanceInformation, ssm:, ec2: StartAutomationExecution DescribeInstances, mais ssm: GetAutomationExecution para poder ler a saída de automação. `AWSSupport-TroubleshootRDP`chamadas `AWSSupport-ExecuteEC2Rescue` para realizar a correção off-line - revise as permissões `AWSSupport-ExecuteEC2Rescue` para garantir que você possa executar a automação com êxito.

Etapas do documento

1. `aws:assertAwsResourceProperty`- Verifique se a instância é uma Windows Server instância
2. `aws:assertAwsResourceProperty`: verifica se a instância é uma instância gerenciada
3. (Solução de problemas online) Se a instância é uma instância gerenciada, então:
   a. `aws:assertAwsResourceProperty`: verifica o valor da ação fornecido
   b. (Verificação on-line) Se a Ação = CheckAll, então:

`aws:runPowerShellScript`- Executa o PowerShell script para obter o status dos perfis do Firewall do Windows.

`aws:executeAutomation`: chama `AWSSupport-ManageWindowsService` para obter o status do serviço RDP.

`aws:executeAutomation`: chama `AWSSupport-ManageRDPSettings` para obter as configurações do RDP.

c. (Correção online) Se a Ação = FixAll, então:

`aws:runPowerShellScript`- Executa o PowerShell script para desativar todos os perfis do Firewall do Windows.

`aws:executeAutomation`: chama `AWSSupport-ManageWindowsService` para iniciar o serviço RDP.

`aws:executeAutomation`: chama `AWSSupport-ManageRDPSettings` para ativar conexões remotas e desativar o NLA.

d. (Gerenciamento online) Se Action = Custom, então:

`aws:runPowerShellScript`- Executa o PowerShell script para gerenciar os perfis do Firewall do Windows.

`aws:executeAutomation`: chama `AWSSupport-ManageWindowsService` para gerenciar o serviço RDP.

`aws:executeAutomation`: chama `AWSSupport-ManageRDPSettings` para gerenciar as configurações do RDP.

4. (Correção offline) Se a instância não for uma instância gerenciada, então:

a. `aws:assertAwsResourceProperty`- Afirmar AllowOffline = verdadeiro

b. `aws:assertAwsResourceProperty`- Afirmar ação = FixAll

c. `aws:assertAwsResourceProperty`- Afirmar o valor de SubnetId

(Use a sub-rede da instância fornecida) Se for SubnetId SELECTED_INSTANCE_SUBNET

`aws:executeAwsApi`: recupera a sub-rede da instância atual.

`aws:executeAutomation`: executa `AWSSupport-ExecuteEC2Rescue` com a sub-rede da instância fornecida.

d. (Use a sub-rede personalizada fornecida) Se não SubnetId for SELECTED_INSTANCE_SUBNET

`aws:executeAutomation`- Execute `AWSSupport-ExecuteEC2Rescue` com o SubnetId valor fornecido.

Saídas

manageFirewallProfiles.Saída

gerenciar RDPService configurações. Saída

gerenciar RDPSettings .Output

checkFirewallProfiles.Saída

verifique RDPService Configurações. Saída

verifique RDPSettings .Saída

disableFirewallProfiles.Saída

RDPServiceRestaurar configurações padrão. Saída

RDPSettingsRestaurar predefinição.Saída

solução de problemas. Saída RDPOffline

solução de problemas. Saída RDPOffline WithSubnetId

AWSSupport-TroubleshootSSH

Descrição

O `AWSSupport-TroubleshootSSH` runbook instala a ferramenta Amazon EC2 Rescue para Linux e, em seguida, usa a ferramenta EC2 Rescue para verificar ou tentar corrigir problemas comuns que impedem uma conexão remota com a máquina Linux via SSH. Opcionalmente, as alterações podem ser aplicadas offline ao interromper e iniciar a instância, se o usuário explicitamente permitir a correção offline. Por padrão, o runbook opera em modo somente leitura.

Execute esta automação (console)

Para obter informações sobre como trabalhar com o runbook `AWSSupport-TroubleshootSSH`, consulte este `AWSSupport-TroubleshootSSH`tópico de solução de problemas do AWS Premium Support.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- Ação

  Tipo: string

  Valores válidos: CheckAll | FixAll

  Padrão: CheckAll

  Descrição: (Obrigatório) Especifique se deseja verificar se há problemas sem corrigi-los ou verificar e corrigir automaticamente todos os problemas detectados.
- AllowOffline

  Tipo: string

  Valores válidos: True | False

  Padrão: False

  Descrição: (Opcional) Apenas correção - Defina como verdadeiro se você permitir a correção do SSH offline, caso a solução de problemas online falhe ou caso a instância fornecida não seja uma instância gerenciada. Observação: para a correção offline, a Automação do SSM interrompe a instância e cria uma AMI antes de tentar qualquer operação.

- AutomationAssumeRole

  Tipo: string

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (Obrigatório) ID da sua EC2 instância para Linux.
- S3 BucketName

  Tipo: string

  Descrição: (Opcional) Apenas offline - Nome do bucket do S3 em sua conta na qual você deseja carregar os logs de solução de problemas. Verifique se a política de buckets não concede permissões de leitura/gravação desnecessárias a partes que não precisam acessar os logs coletados.
- SubnetId

  Tipo: string

  Padrão: SelectedInstanceSubnet

  Descrição: (Opcional) Somente off-line - O ID de sub-rede da instância do EC2 Rescue usado para realizar a solução de problemas off-line. Se nenhum ID de sub-rede for especificado, a AWS Systems Manager Automation criará uma nova VPC.

  > **Important**
  >
  > A sub-rede deve estar na mesma InstanceId zona de disponibilidade e deve permitir o acesso aos endpoints do SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

É recomendável que a EC2 instância que recebe o comando tenha uma função do IAM com a política gerenciada SSMManaged InstanceCore da Amazon Amazon anexada. Para a correção on-line, o usuário deve ter pelo menos ssm:DescribeInstanceInformation, ssm: StartAutomationExecution e ssm: SendCommand para executar a automação e enviar o comando para a instância, além de ssm: GetAutomationExecution para poder ler a saída da automação. Para a correção off-line, o usuário deve ter pelo menos ssm: DescribeInstanceInformation, ssm:, ec2: StartAutomationExecution DescribeInstances, mais ssm: GetAutomationExecution para poder ler a saída de automação. `AWSSupport-TroubleshootSSH`chamadas `AWSSupport-ExecuteEC2Rescue` para realizar a correção off-line - revise as permissões `AWSSupport-ExecuteEC2Rescue` para garantir que você possa executar a automação com êxito.

Etapas do documento

1. `aws:assertAwsResourceProperty`: verifica se a instância é uma instância gerenciada
   a. (Correção online) Se a instância não for uma instância gerenciada, então:
      i. `aws:configurePackage`- Instale o EC2 Rescue for Linux via`AWS-ConfigureAWSPackage`.
      ii. `aws:runCommand`- Execute o script bash para executar o EC2 Rescue for Linux.
   b. (Correção offline) Se a instância não for uma instância gerenciada, então:
      i. `aws:assertAwsResourceProperty`- Afirmar AllowOffline = verdadeiro
      ii. `aws:assertAwsResourceProperty`- Afirmar ação = FixAll
      iii. `aws:assertAwsResourceProperty`- Afirmar o valor de SubnetId
      iv. (Use a sub-rede da instância fornecida) Se devemos SubnetId executar `AWSSupport-ExecuteEC2Rescue` com `aws:executeAutomation` a sub-rede da instância fornecida. SelectedInstanceSubnet
      v. (Use a sub-rede personalizada fornecida) Se não SubnetId for SelectedInstanceSubnet usada `aws:executeAutomation` para executar `AWSSupport-ExecuteEC2Rescue` com o SubnetId valor fornecido.

Saídas

troubleshootSSH.Output

solução de problemas. Saída SSHOffline

solução de problemas. Saída SSHOffline WithSubnetId

AWSSupport-TroubleshootSUSERegistration

Descrição

O AWSSupport-TroubleshootSUSERegistration runbook ajuda você a identificar por que registrar uma Amazon Elastic Compute Cloud (Amazon) EC2 SUSE Linux Enterprise Server falha na instância com o SUSE Update Infrastructure. A saída de automação fornece etapas para resolver ou ajuda você a solucionar o problema, a questão. Se a instância passar por todas as verificações durante a automação, ela será registrada na infraestrutura de atualização SUSE.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon que você deseja solucionar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:ListCommands`

Etapas do documento

- `aws:assertAwsResourceProperty`- Verifica se a EC2 instância da Amazon é gerenciada por AWS Systems Manager.
- `aws:runCommand`- Verifica se a plataforma de EC2 instância da Amazon é SLES.
- `aws:runCommand`: verifica se a versão `cloud-regionsrv-client` do pacote é superior ou igual à versão 9.0.10 necessária.
- `aws:runCommand`: verifica se o link simbólico do produto base está quebrado e corrige o link se ele estiver quebrado.
- `aws:runCommand`: verifica se o arquivo hosts (`/etc/hosts`) contém registros de `smt-ec2-suscloud.net`. A automação remove todas as entradas duplicadas.
- `aws:runCommand`: verifica se o comando `curl` está instalado.
- `aws:runCommand`- Verifica se a EC2 instância da Amazon pode acessar o endereço 169.254.169.254 do Instance Metadata Service (IMDS).
- `aws:runCommand`- Verifica se a EC2 instância da Amazon tem um código de cobrança ou código de AWS Marketplace produto.
- `aws:runCommand`- Verifica se a EC2 instância da Amazon pode alcançar pelo menos 1 servidor regional via HTTPS.
- `aws:runCommand`- Verifica se a EC2 instância da Amazon pode acessar os servidores da Ferramenta de Gerenciamento de Assinaturas (SMT) via HTTP.
- `aws:runCommand`- Verifica se a EC2 instância da Amazon pode acessar os servidores da Ferramenta de Gerenciamento de Assinaturas (SMT) por HTTPS.
- `aws:runCommand`- Verifica se a EC2 instância da Amazon pode acessar o `smt-ec2.susecloud.net` endereço via HTTPS.

- `aws:runCommand`- Registra a EC2 instância da Amazon com o SUSE Update Infrastructure.
- `aws:executeScript`: reúne e gera a saída de todas as etapas anteriores.

AWSSupport-TroubleshootWindowsPerformance

Descrição

O runbook `AWSSupport-TroubleshootWindowsPerformance` ajuda a solucionar problemas contínuos de desempenho na instância Windows do Amazon Elastic Compute Cloud (Amazon EC2). O runbook captura registros da instância de destino e analisa as métricas de desempenho de CPU, memória, disco e rede. Opcionalmente, a automação pode capturar um despejo do processo para ajudá-lo a determinar a causa potencial da degradação do desempenho. A automação também captura os registros de eventos e do sistema usando a `EC2Rescue`ferramenta mais recente, se você permitir que esse runbook a instale.

Como funciona?

O runbook executa as seguintes etapas:

- Verifica os pré-requisitos na EC2 instância da Amazon.
- Gera registros de desempenho no disco raiz da instância EC2 do Amazon Windows
- Armazena os registros capturados na pasta `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Se um bucket do Amazon Simple Storage Service (Amazon S3) for fornecido e a função de assumir a automação tiver as permissões necessárias, os logs capturados serão enviados para o bucket do Amazon S3.
- Instala a `EC2Rescue` ferramenta mais recente na instância do Amazon EC2 Windows para capturar eventos e registros do sistema se você optar por instalá-la, mas ela não analisa o despejo do processo e os registros capturados por. `EC2Rescue`

> **Important**
>
> - Para executar esse runbook, a instância do Amazon EC2 Windows deve ser gerenciada pelo AWS Systems Manager. Para obter mais informações, consulte Por que minha EC2 instância da Amazon não está sendo exibida como um nó gerenciado.

- Para executar esse runbook, a instância do Amazon EC2 Windows deve estar em execução nas versões Windows 8.1/Windows Server 2012 R2 (6.3) ou mais recentes com PowerShell 4.0 ou superior. Para obter mais informações, consulte a versão do sistema operacional Windows.
- Para a geração de registros de desempenho, é necessário pelo menos 10 GB de espaço livre no dispositivo raiz. Se o disco raiz for maior que 100 GB, o espaço livre deverá ser maior que 10% do tamanho do disco. Se você despejar um processo durante a execução, o espaço livre deverá ser maior que 10 GB mais o tamanho total da memória consumida pelo processo quando o processo consumir mais de 10 GB de memória.
- Os registros gerados no dispositivo raiz não são excluídos automaticamente.
- O runbook não desinstala a `EC2Rescue` ferramenta. Para obter mais informações, consulte Usar `EC2Rescue` para Windows Server.
- É uma prática recomendada executar essa automação durante um impacto no desempenho. Você também pode executá-lo periodicamente usando uma associação AWS Systems Manager do State Manager ou agendando janelas de AWS Systems Manager manutenção.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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) A função do IAM anexada ao perfil da instância ou ao usuário do IAM configurado na instância exige as seguintes ações para carregar os registros no bucket do Amazon S3 especificado para o parâmetro: *LogUploadBucketName*

- s3:PutObject
- s3:GetObject
- s3:ListBucket

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-TroubleshootWindowsPerformanceem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se

nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.

- InstanceId (Obrigatório):

  O ID da instância de destino EC2 do Amazon Windows em que você deseja executar a automação. A instância deve ser gerenciada pelo Systems Manager para executar a automação.

- CaptureProcessDump (Opcional):

  O tipo de despejo do processo a ser capturado. A automação pode capturar um despejo de processo para o processo que está potencialmente causando o impacto no desempenho no início da automação. O volume raiz da instância requer pelo menos 10 GB de espaço livre (maior que 10% do tamanho do disco quando o tamanho do volume raiz é maior que 100 GB e 10 GB mais o tamanho total da memória consumida pelo processo quando o processo consome mais de 10 GB de memória).

- LogCaptureDuration (Opcional):

  O número de minutos, entre `1` e`15`, em que essa automação capturará os registros enquanto o problema estiver presente. O padrão é `5`.

- LogUploadBucketName (Opcional):

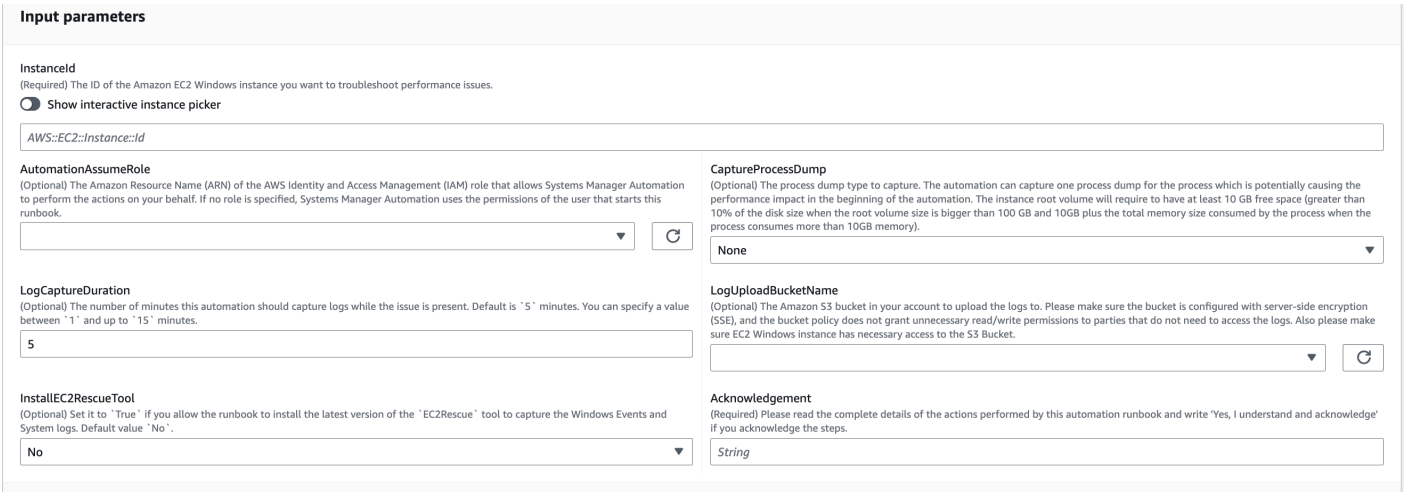
  O bucket do Amazon S3 na sua conta em que você deseja fazer o upload dos registros. O bucket deve ser configurado com criptografia do lado do servidor (SSE), e a política do bucket não deve conceder permissões desnecessárias de leitura/gravação a partes que não precisam acessar os registros capturados. A instância EC2 do Amazon Windows deve ter acesso ao bucket do Amazon S3.

- Instalação EC2 RescueTool (opcional):

  Defina `Yes` para permitir que o runbook instale a versão mais recente da `EC2Rescue` ferramenta para capturar os registros de eventos e do sistema do Windows. O padrão é `No`.

- Reconhecimento (obrigatório):

  Leia os detalhes completos das ações realizadas por esse runbook de automação e, se concordar, digite`Yes, I understand and acknowledge`.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - **`CheckConcurrency:`**

     Garante que haja apenas uma execução desse runbook direcionada à instância. Se o runbook encontrar outra execução direcionada à mesma instância, ele retornará um erro e terminará.

   - **`AssertInstanceIsWindows:`**

     Afirma que a EC2 instância da Amazon está sendo executada no sistema operacional Windows. Caso contrário, a automação termina.

   - **`AssertInstanceIsManagedInstance:`**

     Afirma que a EC2 instância da Amazon é gerenciada por AWS Systems Manager. Caso contrário, a automação termina.

   - **`VerifyPrerequisites:`**

     Verifica a PowerShell versão no sistema operacional da instância e garante que a instância possa ser conectada por meio do Systems Manager para executar PowerShell comandos. Essa automação oferece suporte à PowerShell versão 4.0 e superior em execução nas versões Windows 8.1/Server 2012 R2 (6.3) ou mais recentes. Se a versão for mais antiga, a automação falhará. Quando você opta por fazer o upload de registros para o bucket do Amazon S3, essa automação verifica se o PowerShell módulo AWS Tools for está disponível. Caso contrário, a automação termina.

   - **`BranchOnProcessDump:`**

Ramifica com base em se você o configurou para capturar o despejo de processos que afetaram o desempenho.

- **CaptureProcessDump:**

  Verifica se a instância tem espaço suficiente para executar essa automação (quando você escolhe CPU/Memória mais alta).

- **CapturePerformanceLogs:**

  Verifica o espaço em disco novamente e executa o PowerShell script na instância para criar contadores perfmon e iniciar o registro do Monitor de Desempenho e do Gravador de Desempenho do Windows. O script é interrompido depois que o definido `LogCaptureDuration` é atendido.

- **SummarizePerformanceLogs:**

  Resume o relatório XML gerado na etapa anterior,`CapturePerformanceLogs`, para encontrar o processo responsável que consome mais WorkingSet 64 (memória) e% de tempo de processador (CPU) mostrados como saída na automação. Ele gera informações semelhantes para uso de LogicalDisk, Interface de Rede, Memória TCPv4 IPv4,, UDPv4 e as salva `analysis_output.log` na pasta de saída.

- **BranchOnInstallEC2Rescue:**

  Ramifica se você configurá-lo para instalar a `EC2Rescue` ferramenta mais recente na EC2 instância da Amazon.

- **InstallEC2RescueTool:**

  Instala a `EC2Rescue` ferramenta no sistema operacional da instância para capturar `EC2Rescue` registros usando`AWS-ConfigureAWSPackage`.

- **RunEC2RescueTool:**

  Executa a `EC2Rescue` ferramenta no sistema operacional da instância para capturar todos os registros necessários. `EC2Rescue`captura somente os registros necessários para economizar espaço.

- **BranchOnIfS3BucketProvided:**

  Ramifica com base na entrada do usuário de `LogUploadBucketName` para ver se há um nome de bucket disponível para fazer upload de registros.

- **`GetS3BucketPublicStatus:`**

  Determina se um bucket do Amazon S3 é fornecido e, em caso afirmativo, confirma que o bucket do Amazon S3 não é público e está configurado com SSE.

- **`UploadLogResult:`**

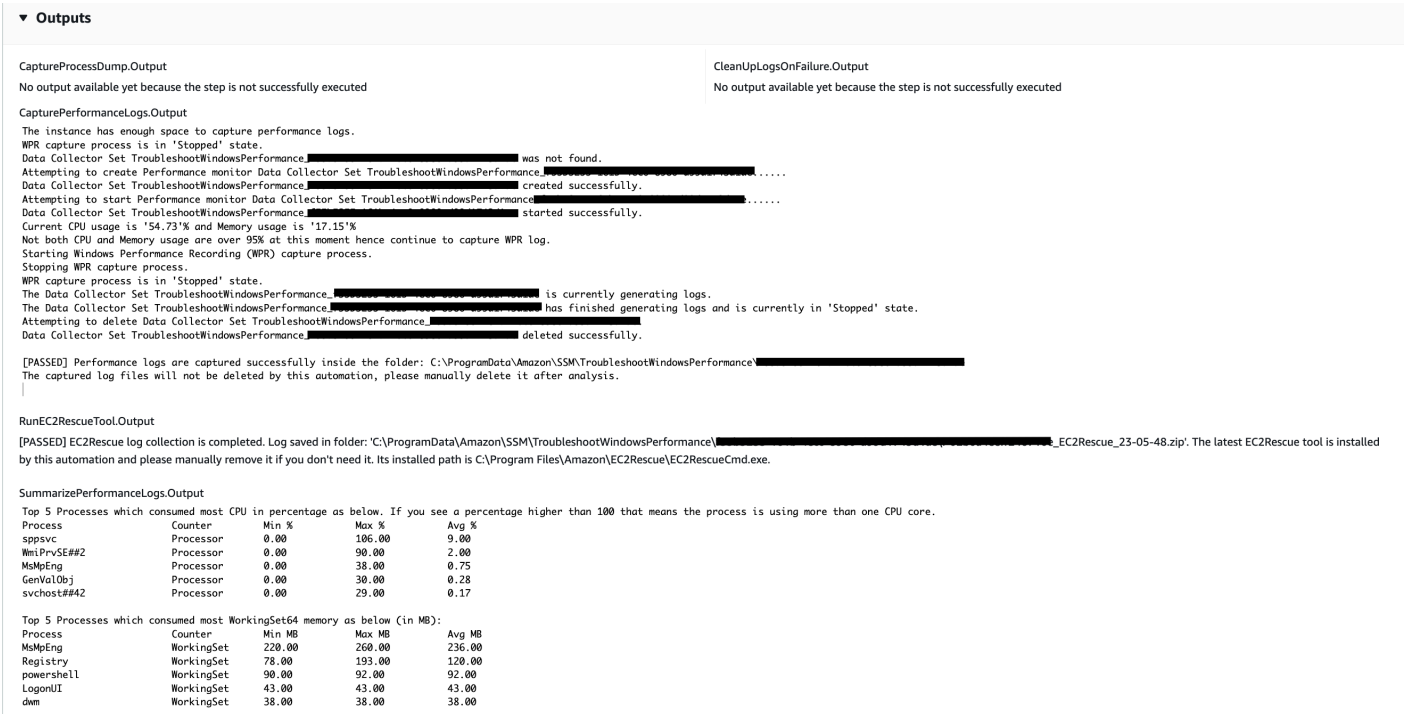
  Carrega os registros no bucket Amazon S3 fornecido. Se a PowerShell versão for 5.0 ou superior, ela compactará os registros em um arquivo ZIP e os carregará. Ele exclui o arquivo ZIP após a conclusão do upload. Se a PowerShell versão estiver abaixo de 5.0, ele carregará os arquivos diretamente para uma pasta.

- **`CleanUpLogsOnFailure:`**

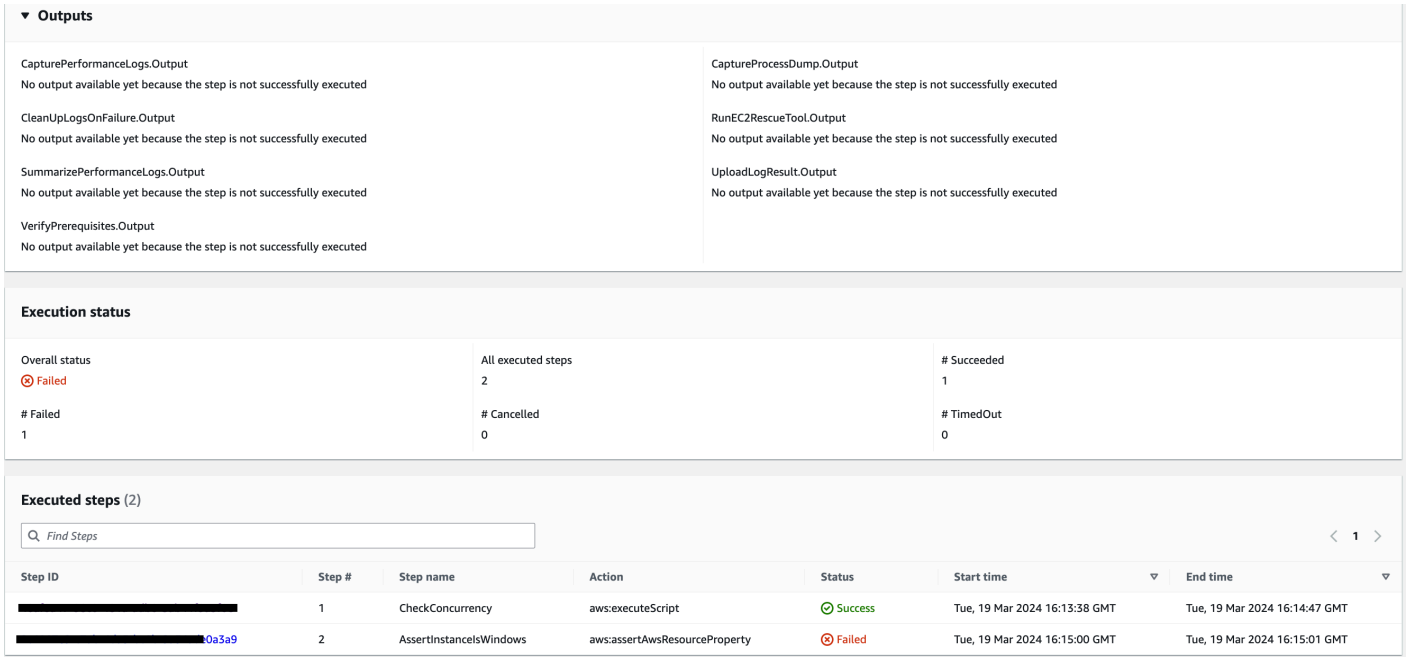
  Limpa todos os registros gerados pela `CapturePerformanceLogs` etapa quando ela falha. A `CleanUpLogsOnFailure` etapa pode falhar ou atingir o tempo limite se o SSM Agent não estiver funcionando corretamente ou se o sistema Windows não estiver respondendo.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

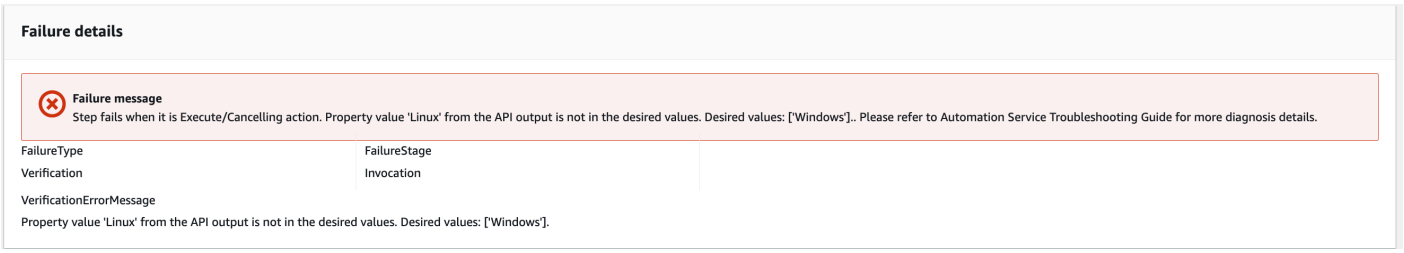
   Execução em que a instância de destino tem todos os pré-requisitos necessários.



   Execução em que a instância de destino está na plataforma Linux e a execução falhou. Você selecionaria o ID da etapa para ver os detalhes da falha.



Os detalhes da falha da etapa`AssertInstanceIsWindows`.



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

`AWSSupport-TroubleshootWindowsUpdate`

Descrição

O `AWSSupport-TroubleshootWindowsUpdate` runbook é usado para identificar problemas que podem falhar nas atualizações do Windows para instâncias Windows do Amazon Elastic Compute Cloud EC2 (Amazon).

Como funciona?

O runbook executa as seguintes etapas:

- Verifica se a EC2 instância de destino da Amazon é gerenciada pelo AWS Systems Manager.
- Verifica se as versões AWS Systems Manager Agent (SSM Agent) e Windows Server são compatíveis com as operações de patch do Systems Manager.
- Verifica o espaço em disco disponível recomendado para atualizações do Windows e se a reinicialização está pendente. Uma reinicialização pendente normalmente indica que as atualizações estão pendentes, e uma reinicialização é necessária antes de realizar atualizações adicionais.
- Define as configurações de proxy no nível do sistema operacional, o que pode ajudar a solucionar problemas de conectividade.
- Executa um teste de conectividade de endpoint do Amazon Simple Storage Service (Amazon S3) e chama a operação de API para recuperar `GetDeployablePatchSnapshotForInstance`o snapshot atual da linha de base do patch que o nó gerenciado usa.
- Se a conexão falhar, oferece a opção de executar o `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook para analisar a conectividade da instância com os endpoints do Amazon S3.
- Valida a configuração das atualizações do Windows e testa o Windows Server Update Services (WSUS) (se aplicável).

Important

- Não há suporte para controladores de domínio do Active Directory.
- Não há suporte para a versão 2008 R2 do Windows Server ou versões anteriores.
- O SSM Agent 1.2.371 ou versões anteriores não são compatíveis.
- O `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook é usado `VPC Reachability Analyzer`para analisar a conectividade de rede entre uma fonte e um ponto final de serviço. Você é cobrado por análise executada entre a origem e o destino. Para obter mais detalhes, consulte Preço da Amazon VPC.

- O `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook não está disponível em todas as regiões em que o Systems Manager é suportado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

> **Note**
>
> Para executar o runbook secundárioAWSSupport-AnalyzeAWSEndpointReachabilityFromEC2, adicione as permissões listadas neste documento.

Instruções

Siga estas etapas para configurar a automação:

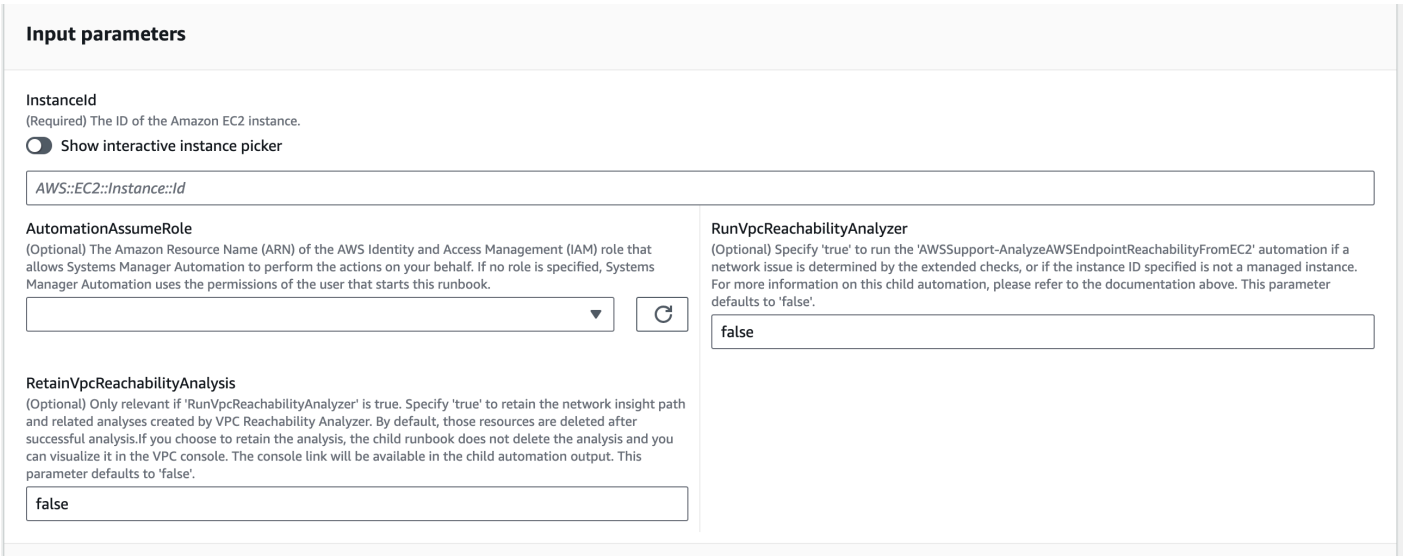
1. Navegue até AWSSupport-TroubleshootWindowsUpdateem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - InstanceId (Obrigatório):

     Insira o ID da EC2 instância da Amazon em que a atualização do Windows falhou.
   - RunVpcReachabilityAnalyzer(Opcional):

     Especifique `true` a execução da `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` automação se um problema de rede for determinado pelas verificações estendidas ou se o ID da instância especificado não for uma instância gerenciada. Para obter mais informações sobre essa automação infantil, consulte a documentação. O valor padrão é `false`.
   - RetainVpcReachabilityAnalysis(Opcional):

     Só é relevante se `RunVpcReachabilityAnalyzer` for`true`. Especifique `true` para manter o caminho do insight da rede e as análises relacionadas criadas por`Reachability Analyzer`. Por padrão, esses recursos são excluídos após uma análise bem-sucedida. Se você optar por manter a análise, o runbook secundário não excluirá a análise e você poderá visualizá-la no console da Amazon VPC. O link do console estará disponível na saída de automação infantil. O valor padrão`false`.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - **`getWindowsServerAndSSMAgentVersion:`**

     Verifica se a instância de destino é gerenciada pelo SSM Agent AWS Systems Manager e obtém detalhes sobre a versão do SSM Agent e a versão do Windows.
   - **`assertifInstanceIsSsmManaged:`**

     Garante que a EC2 instância da Amazon seja gerenciada pelo AWS Systems Manager (SSM), caso contrário, a automação termina.
   - **`CheckProxy:`**

     Verifica todos os tipos de proxy para a instância do Windows.
   - **`CheckPrerequisites:`**

     Obtém a versão do SSM Agent e a versão do Windows e determina se é um controlador de domínio (DC) do Active Directory. Se a instância for um DC ou se o SSM Agent ou a versão do Windows não for suportada, o runbook será interrompido.
   - **`CheckDiskSpace:`**

     Obtém e valida o espaço em disco disponível na instância do Windows se for suficiente para realizar a atualização do Windows.
   - **`CheckPendingReboot:`**

Verifica se há alguma reinicialização pendente na instância do Windows.

- **CheckS3Connectivity:**

  Verifica se a instância pode alcançar os endpoints do Amazon S3 para. `Patchbaseline`

- **branchOnRunVpcReachabilityAnalyzer:**

  Se `RunVpcReachabilityAnalyzer` for verdade, ele ramifica a automação para executar uma análise mais profunda da depuração da conectividade do Amazon S3.

- **GenerateEndpoints:**

  Gera um endpoint para ter uma verificação de conectividade estendida para o endpoint Amazon S3.

- **analyzeAwsEndpointReachabilityFromEC2:**

  Chama o runbook de automação,`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`. para verificar a acessibilidade da instância selecionada aos endpoints necessários.

- **CheckWindowsUpdateServices:**

  Verifica o status do serviço Windows Update e o tipo de início.

- **CheckWindowsUpdateSettings:**

  Verifica as políticas do Windows Update configuradas na instância do Windows.

- **CheckWSUSSettings:**

  Verifica se a atualização do Windows está configurada com o WSUS ou o Microsoft Update Catalog e verifica a conectividade.

- **CheckWUGlobalSettings:**

  Verifica as configurações globais do Windows Update definidas na instância do Windows.

- **GenerateLogs:**

  Faz o download dos registros do Windows Update e do CBS na área de trabalho da instância e verifica se há falhas nos registros de eventos do Windows.

- **FinalReport:**

  Gera um relatório completo de todas as etapas.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

```
FinalReport.Results
"
==================================================Prerequisites Check==================================================
Result: ✅ [PASSED]
INFO: The target instance is not an Active Directory Domain Controller.
INFO: The platform 10.0.20348 is supported.
INFO: The SSM Agent version 3.2.1705.0 is supported.

==================================================Disk Space Check==================================================
Result: ✅ [PASSED]
INFO: Disk space on drive C: is recommended to run Windows updates.

==================================================Pending Reboot Check==================================================
Result: ✅ [PASSED]
INFO: There is no pending reboot.

==================================================Amazon S3 Connectivity Check==================================================
Result: ✅ [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

==================================AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2==================================
Result: ✅ [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

==================================================Windows Update Services Status==================================================
Result: ✅ [PASSED]
Getting Services Status and types for Windows Update...
The service 'Application Identity' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Application Identity'
Service 'Application Identity' started successfully
The service 'Background Intelligent Transfer Service' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Background Intelligent Transfer Service'
Service 'Background Intelligent Transfer Service' started successfully
INFO: The service 'Cryptographic Services' status is currently 'Running'
The service 'Windows Installer' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Windows Installer'
Service 'Windows Installer' started successfully
INFO: The service 'Windows Modules Installer' status is currently 'Running'
INFO: The service 'Windows Update' status is currently 'Running'

==================================================Windows Proxy Settings==================================================
Result: ✅ [PASSED]
No WinInet Proxy is set on the system
No Winhttp Proxy is set on the system
There is no proxy setting for SSM Agent
System Wide Environment HTTP Proxy is not set.
System Wide Environment HTTPS Proxy is not set.
System Wide Environment NO PROXY is not set.
There is no HTTP Proxy configured at local system account user environment.


==================================================Windows Update Settings==================================================
Result: ✅ [PASSED]
INFO: Windows Update (Policies): Never check for updates
INFO: To modify this setting is in Computer Configuration\\Adminisrative Template\\Windows Component\\Windows
Update\\Configure Automatic Updates. For more details please check this document: https://learn.microsoft.com/de-
de/security-updates/windowsupdateservices/18127451

==================================================Windows Update Global Settings==================================================
Result: ✅ [PASSED]
Windows Update Client has no restrictions

==================================================Copy of Windows Update and CBS logs==================================================
Result: ✅ [PASSED]
No errors found in Microsoft-Windows-WindowsUpdateClient events.
INFO: Logs copied to the C:\\Windows\\TEMP\\c176a507-d074-4402-8a5b-631dd643f33a folder
"
```

Referências

Automação do Systems Manager

- Executar esta automação (console)

- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

Documentação relacionada ao AWS serviço

- Consulte o artigo TroubleShoot Windows Update para obter mais informações.

AWSSupport-UpgradeWindowsAWSDrivers

Descrição

O `AWSSupport-UpgradeWindowsAWSDrivers` runbook atualiza ou repara os AWS drivers de armazenamento e de rede na instância especificada EC2 . O runbook tenta instalar as versões mais recentes dos AWS drivers on-line chamando o SSM Agent. Se o SSM Agent não puder ser contatado, o runbook poderá realizar uma instalação offline dos AWS drivers, se solicitado explicitamente.

Este runbook é compatível com os seguintes sistemas operacionais:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

> **Note**
>
> Observação: tanto a atualização online e offline criará uma AMI antes de tentar quaisquer operações, que persistem após a conclusão da automação. É sua responsabilidade garantir acesso à AMI ou excluí-la. O método on-line reinicia a instância como parte do processo de atualização, enquanto o método off-line exige que a EC2 instância fornecida seja interrompida e depois iniciada.

> **Important**
>
> Se suas instâncias se conectarem AWS Systems Manager usando VPC endpoints, esse runbook falhará, a menos que seja usado na região us-east-1. Este runbook também falhará em um controlador de domínio. Para atualizar os drivers AWS fotovoltaicos em um controlador de domínio, consulte Atualizar um controlador de domínio (atualização AWS fotovoltaica).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AllowOffline

  Tipo: String

  Valores válidos: True | False

  Padrão: False

  Descrição: (Opcional) Defina como verdadeiro se você permitir uma atualização de drivers offline, caso a instalação online não possa ser realizada. Observação: o método off-line exige que a EC2 instância fornecida seja interrompida e depois iniciada. Dados armazenados em volumes de armazenamento de instâncias serão perdidos. O endereço IP público será alterado se você não estiver usando um IP elástico.
- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ForceUpgrade

  Tipo: String

  Valores válidos: True | False

  Padrão: False

  Descrição: (opcional) apenas offline: defina como verdadeiro se você permitir que a atualização de drivers offline prossiga, mesmo que sua instância já tenha os drivers mais recentes instalados.

- InstanceId

  Tipo: String

  Descrição: (Obrigatório) ID da sua EC2 instância paraWindows Server.

- SubnetId

  Tipo: String

  Padrão: SelectedInstanceSubnet

  Descrição: (Opcional) Somente off-line - O ID de sub-rede da instância do EC2 Rescue usado para realizar a atualização dos drivers off-line. Se nenhum ID de sub-rede for especificado, o Systems Manager Automation criará uma nova VPC.

  > **Important**
  >
  > A sub-rede deve estar na mesma InstanceId zona de disponibilidade e permitir o acesso aos endpoints do SSM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

A EC2 instância que recebe o comando deve ter, no mínimo, uma função do IAM que inclua permissões para ssm: StartAutomationExecution e ssm: SendCommand para executar a automação e enviar o comando para a instância, além de ssm: GetAutomationExecution para poder ler a saída da automação. Você pode anexar a política `AmazonSSMManagedInstanceCore` gerenciada pela Amazon à sua função do IAM para fornecer essas permissões. No entanto, recomendamos usar a função do IAM `AmazonSSMAutomationRole` de automação para essa finalidade. Para obter mais informações, consulte Usar o IAM para configurar perfis para o Automation.

Se você estiver executando uma atualização offline, consulte as permissões necessárias por `AWSSupport-StartEC2RescueWorkflow`.

Etapas do documento

1. `aws:assertAwsResourceProperty`: verifica se a instância de entrada é Windows.
2. `aws:assertAwsResourceProperty`: verifica se a instância de entrada é uma instância gerenciada. Se esse for o caso, a atualização online é iniciada; caso contrário, a atualização offline é avaliada.
   a. (Atualização online) Se a instância de entrada for uma instância gerenciada:
      i. `aws:createImage`: cria um backup da AMI.
      ii. `aws:createTags`: marca o backup da AMI.
      iii. `aws:runCommand`- Instala o driver de rede ENA.
      iv. `aws:runCommand`- Instala o NVMe driver.
      v. `aws:runCommand`- Instala o driver AWS fotovoltaico.
   b. (Atualização offline) Se a instância de entrada não for uma instância gerenciada:
      i. `aws:assertAwsResourceProperty`: verifica se o sinalizador AllowOffline está definido como `true`. Se esse for o caso, a atualização offline é iniciada; caso contrário, a automação termina.
      ii. `aws:changeInstanceState`: interrompe a parada da instância
      iii. `aws:changeInstanceState`: força a parada da instância de origem.
      iv. `aws:createImage`: cria uma AMI de backup da instância de origem.
      v. `aws:createTags`: marca uma AMI de backup da instância de origem.
      vi. `aws:executeAwsApi`: ativa o ENA para a instância
      vii. `aws:assertAwsResourceProperty`- Afirme a ForceUpgrade bandeira.

viii(Forçar atualização offline) Se ForceUpgrade = true, execute `aws:executeAutomation` para invocar `AWSSupport-StartEC2RescueWorkflow` com o script de atualização forçada do driver. Isso instala os drivers independentemente da versão atual instalada

ix. (Atualização offline) Se ForceUpgrade = false, execute `aws:executeAutomation` para invocar `AWSSupport-StartEC2RescueWorkflow` com o script de atualização de drivers.

Saídas

preUpgradeBackup.ImageId

preOfflineUpgradeBackup. ImageId

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

upgradeDriversOffline.Saída

forceUpgradeDriversOffline. Saída

Amazon ECS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic Container Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-CollectECSInstanceLogs
- AWS-InstallAmazonECSAgent
- AWS-ECSRunTask
- AWSSupport-TroubleshootECSContainerInstance
- AWSSupport-TroubleshootECSTaskFailedToStart
- AWS-UpdateAmazonECSAgent

AWSSupport-CollectECSInstanceLogs

Descrição

O AWSSupport-CollectECSInstanceLogs runbook coleta arquivos de log relacionados ao sistema operacional e ao Amazon Elastic Container Service (Amazon ECS) de uma instância do Amazon Elastic Compute Cloud (Amazon) para ajudá-lo a solucionar problemas comuns do EC2 Amazon ECS. Enquanto a automação coleta os arquivos de log associados, são feitas alterações no sistema de arquivos. Essas mudanças incluem a criação de diretórios temporários e um diretório de log, a cópia de arquivos de log para esses diretórios e a compactação dos arquivos de log em um arquivo.

Se você especificar um valor para o LogDestination parâmetro, a instância de destino deverá ter a Interface de Linha de AWS Comando (AWS CLI) para instâncias do Linux ou AWS as Ferramentas para Windows PowerShell para instâncias do Windows instaladas. A automação avalia o status da política do bucket do Amazon Simple Storage Service (Amazon S3) especificado por você. Para ajudar na segurança dos registros coletados da sua EC2 instância Amazon, se o status da política isPublic estiver definido como ou se a true lista de controle de acesso (ACL) conceder READ|WRITE permissões ao grupo predefinido do All Users Amazon S3, os registros não serão carregados. Além disso, se o bucket fornecido não estiver disponível em sua conta, os logs não serão carregados. Para obter mais informações sobre os grupos predefinidos do Amazon S3, consulte os grupos predefinidos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, Windows

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ECSInstanceIdentificação

  Tipo: String

  Descrição: (obrigatório) O ID da instância da qual deseja coletar os logs. A instância especificada deve ser gerenciada pelo Systems Manager.

- LogDestination

  Tipo: String

  Descrição: (Opcional) O bucket do Amazon S3 em seu local Conta da AWS para fazer o upload dos registros arquivados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`

Recomendamos que a EC2 instância da Amazon especificada no `ECSInstanceId` parâmetro tenha uma função do IAM com a política gerenciada da `AmazonSSMManagedInstanceCore` Amazon anexada. Para fazer o upload do arquivo de log para o bucket do Amazon S3 que foi especificado no parâmetro `LogDestination`, as seguintes permissões devem ser adicionadas:

- `s3:PutObject`
- `s3:ListBucket`
- `s3:GetBucketPolicyStatus`

- `s3:GetBucketAcl`

Etapas do documento

- `assertInstanceIsManaged` :Verifica se a instância especificada no parâmetro `ECSInstanceId` é gerenciada pelo Systems Manager.
- `getInstancePlatform` :Obtém informações sobre a plataforma do sistema operacional (OS) da instância especificada no parâmetro `ECSInstanceId`.
- `verifyInstancePlatform` :Ramifica a automação com base na plataforma do sistema operacional.
- `runLogCollectionScriptOnLinux` :Reúne arquivos de log relacionados ao sistema operacional e ao Amazon ECS em instâncias do Linux e cria um arquivo de arquivamento no diretório `/var/log/collectECSlogs`.
- `runLogCollectionScriptOnWindows` :Reúne arquivos de log relacionados ao sistema operacional e ao Amazon ECS em instâncias do Windows e cria um arquivo de arquivamento no diretório `C:\ProgramData\collectECSlogs`.
- `verifyIfS3BucketProvided` :Verifica se um valor foi especificado para o parâmetro `LogDestination`.
- `runUploadScript` :Ramifica a etapa de automação com base na plataforma do sistema operacional.
- `runUploadScriptOnLinux` :Carrega o arquivo de log no bucket do Amazon S3 especificado no parâmetro `LogDestination` e exclui o arquivo de log arquivado do sistema operacional.
- `runUploadScriptOnWindows` :Carrega o arquivo de log no bucket do Amazon S3 especificado no parâmetro `LogDestination` e exclui o arquivo de log arquivado do sistema operacional.

AWS-InstallAmazonECSAgent

Descrição

O `AWS-InstallAmazonECSAgent` runbook instala o agente do Amazon Elastic Container Service (Amazon ECS) na instância do Amazon Elastic Compute Cloud (EC2Amazon) que você especificar. Este runbook é compatível somente com instâncias do Amazon Linux e do Amazon Linux 2.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceIds

  Tipo: StringList

  Descrição: (Obrigatório) A IDs das EC2 instâncias da Amazon nas quais você deseja instalar o agente do Amazon ECS.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`

Etapas do documento

`aws:executeScript`- Instala o agente do Amazon ECS nas EC2 instâncias da Amazon que você especificar no `InstanceIds` parâmetro.

Saídas

InstallAmazonECSAgent. SuccessfulInstances - O ID da instância em que a instalação do agente do Amazon ECS foi bem-sucedida.

InstallAmazonECSAgent. FailedInstances - O ID da instância em que a instalação do agente Amazon ECS falhou.

InstallAmazonECSAgent. InProgressInstances - O ID da instância em que a instalação do agente Amazon ECS está em andamento.

AWS-ECSRunTask

Descrição

O `AWS-ECSRunTask` runbook executa a tarefa do Amazon Elastic Container Service (Amazon ECS) especificada por você.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- capacityProviderStrategy

  Tipo: String

  Descrição: (Opcional) A estratégia do provedor de capacidade a ser usada para a tarefa.

- cluster

  Tipo: String

  Descrição: (Opcional) O nome abreviado ou ARN do cluster no qual executar sua tarefa. Se você não especificar um cluster, o cluster padrão será usado.

- contagem

  Tipo: String

  Descrição: (Opcional) O número de instanciações da tarefa especificada a serem colocadas em seu cluster. Você pode especificar até 10 tarefas para cada solicitação.

- habilitar ECSManaged tags

  Tipo: booliano

  Descrição: (Opcional) Especifica se as tags gerenciadas do Amazon ECS devem ser usadas para a tarefa. Para obter mais informações, consulte Marcar seus recursos do Amazon ECS, no Guia do Desenvolvedor do Amazon Elastic Container Service.

- enableExecuteCommand

  Tipo: booliano

  Descrição: (Opcional) Determina se a funcionalidade de execução do comando deve ser ativada para os contêineres nessa tarefa. Se verdadeiro, isso ativa a funcionalidade de execução do comando em todos os contêineres da tarefa.

- grupo

  Tipo: String

  Descrição: (Opcional) O nome do grupo de tarefas a ser associado à tarefa. O valor padrão é o nome da família da definição da tarefa. Por exemplo, `family:my-family-name`

- Tipo de lançamento

  Tipo: String

  Valores válidos: EC2 | FARGATE | EXTERNAL

  Descrição: (Opcional) A infraestrutura na qual executar sua tarefa autônoma.

- networkConfiguration

  Tipo: String

  Descrição: (Opcional) A configuração de rede para a tarefa. Esse parâmetro é necessário para definições de tarefas que usam o modo de `awsvpc` rede para receber sua própria interface de rede elástica e não é compatível com outros modos de rede.

- substituições

  Tipo: String

  Descrição: (Opcional) Uma lista de substituições de contêiner no formato JSON que especificam o nome de um contêiner na definição de tarefa especificada e as substituições que ele deve receber. Você pode substituir o comando padrão de um contêiner especificado na definição da tarefa ou na imagem do Docker com uma substituição de comando. Você também pode substituir as variáveis de ambiente existentes que são especificadas na definição da tarefa ou na imagem do Docker em um contêiner. Além disso, você pode adicionar novas variáveis de ambiente com uma substituição de ambiente.

- Restrições de posicionamento

  Tipo: String

  Descrição: (Opcional) Uma matriz de objetos de restrição de posicionamento para usar na tarefa. Você pode especificar até 10 restrições para cada tarefa, incluindo restrições na definição da tarefa e aquelas especificadas em tempo de execução.

- Estratégia de colocação

  Tipo: String

  Descrição: (Opcional) Os objetos da estratégia de posicionamento a serem usados na tarefa. Você pode especificar no máximo 5 regras de estratégia para cada tarefa.

- platformVersion

Tipo: String

Descrição: (Opcional) A versão da plataforma que a tarefa usa. Uma versão da plataforma é especificada somente para tarefas hospedadas no Fargate. Se não for especificada uma versão da plataforma, a versão da plataforma `LATEST` será usada.

- propagateTags

  Tipo: String

  Descrição: (Opcional) Determina se as tags se propagam da definição da tarefa para a tarefa. Se nenhum valor for especificado, as tags não serão propagadas. As tags só podem ser propagadas para a tarefa durante sua criação.

- referenceId

  Tipo: String

  Descrição: (Opcional) O ID de referência a ser usado para a tarefa. O ID de referência pode ter um tamanho máximo de 1024 caracteres.

- Iniciado por

  Tipo: String

  Descrição: (Opcional) Uma tag opcional especificada quando uma tarefa é iniciada. Isso ajuda você a identificar quais tarefas pertencem a um trabalho específico filtrando os resultados de uma operação de `ListTasks` API. São permitidos até 36 letras (maiúsculas e minúsculas), números, hífens (-) e sublinhados (_).

- tags

  Tipo: String

  Descrição: (Opcional) Metadados que você deseja aplicar à tarefa para ajudá-lo a categorizar e organizar tarefas. Cada tag consiste em uma chave e um valor definidos pelo usuário.

- Definição de tarefa

  Tipo: String

Descrição: (Opcional) O `family` e `revision` (`family:revision`) ou o ARN completo da definição da tarefa a ser executada. Se uma revisão não for especificada, a `ACTIVE` revisão mais recente será usada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ecs:RunTask`

Etapas do documento

`aws:executeScript`- Executa a tarefa do Amazon ECS com base nos valores que você especifica para os parâmetros de entrada do runbook.

AWSSupport-TroubleshootECSContainerInstance

Descrição

O `AWSSupport-TroubleshootECSContainerInstance` runbook ajuda você a solucionar problemas de uma instância do Amazon Elastic Compute Cloud (Amazon EC2) que não consegue se registrar em um cluster do Amazon ECS. Essa automação analisa se os dados do usuário da instância contêm as informações corretas do cluster, se o perfil de instância contém as permissões necessárias e problemas de configuração de rede.

> **Important**
>
> Para executar essa automação com sucesso, o estado da sua EC2 instância Amazon deve ser`running`, e o estado do cluster do Amazon ECS deve ser`ACTIVE`.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

  Descrição: (obrigatório) O nome do cluster do Amazon ECS no qual a instância não conseguiu se registrar.
- InstanceId

  Tipo: String

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon que você deseja solucionar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

aws:ExecuteScript: analisa se a EC2 instância da Amazon atende aos pré-requisitos necessários para se registrar em um cluster do Amazon ECS.

AWSSupport-TroubleshootECSTaskFailedToStart

Descrição

O runbook AWSSupport-TroubleshootECSTaskFailedToStart ajuda a solucionar o motivo pelo qual uma tarefa do Amazon Elastic Container Service (Amazon ECS) em um cluster do Amazon ECS não foi iniciada. Você deve executar esse runbook da Região da AWS mesma forma que sua tarefa que falhou ao iniciar. O runbook analisa os seguintes problemas comuns que podem impedir o início de uma tarefa:

- Conectividade de rede com o registro de contêiner configurado
- Permissões do IAM ausentes exigidas pela função de execução da tarefa
- Conectividade do serviço de endpoint da VPC
- Configuração de regras do grupo de segurança
- AWS Secrets Manager referências de segredos
- Configuração de registro em log

> **Note**
>
> Se a análise determinar que a conectividade de rede precisa ser testada, uma função do Lambda e o perfil do IAM necessário serão criados em sua conta. Esses atributos são usados para simular a conectividade de rede da tarefa que falhou. A automação exclui esses atributos quando eles não são mais necessários. No entanto, se a automação não conseguir excluir os atributos, isso deverá ser feito manualmente.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

  Descrição: (obrigatório) O nome do cluster do Amazon ECS em que a tarefa não foi iniciada.
- CloudwatchRetentionPeriod

  Tipo: inteiro

  Descrição: (Opcional) O período de retenção, em dias, para que os registros da função Lambda sejam armazenados no Amazon CloudWatch Logs. Isso será necessário somente se a análise determinar que a conectividade de rede precisa ser testada.

  Valores válidos: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

  Padrão: 30
- TaskId

Tipo: String

Descrição: (obrigatório) O ID da tarefa que falhou. Use a tarefa que falhou mais recentemente.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `cloudtrail:LookupEvents`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ecr:DescribeImages`
- `ecr:GetRepositoryPolicy`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeServices`
- `ecs:DescribeTaskDefinition`
- `ecs:DescribeTasks`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`

- iam:GetRole
- iam:ListRoles
- iam:PassRole
- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy
- kms:DescribeKey
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:GetFunctionConfiguration
- lambda:InvokeFunction
- lambda:TagResource
- logs:DescribeLogGroups
- logs:PutRetentionPolicy
- secretsmanager:DescribeSecret
- ssm:DescribeParameters
- sts:GetCallerIdentity

Etapas do documento

- aws:executeScript :Verifica se o usuário ou a função que iniciou a automação tem as permissões necessárias do IAM. Se não tiver permissões suficientes para usar esse runbook, as permissões necessárias ausentes serão incluídas na saída da automação.
- aws:branch :Ramificações com base no fato de você ter permissões para todas as ações necessárias para o runbook.
- aws:executeScript :Cria uma função do Lambda em sua VPC se a análise determinar que a conectividade de rede precisa ser testada.
- aws:branch :Ramificações com base nos resultados da etapa anterior.
- aws:executeScript :Analisa as possíveis causas da falha em iniciar a tarefa.
- aws:executeScript :Exclui atributos criados por essa automação.
- aws:executeScript :Formata a saída da automação para retornar os resultados da análise ao console. Você pode consultar a análise depois dessa etapa antes que a automação seja concluída.

- `aws:branch` :Ramifica com base no fato de a função do Lambda e os recursos associados terem sido criados e precisarem ser excluídos.
- `aws:sleep` :Permanece em repouso por 30 minutos para que a interface de rede elástica da função do Lambda possa ser excluída.
- `aws:executeScript` :Exclui a interface de rede da função do Lambda.
- `aws:executeScript` :Formata a saída da etapa de exclusão da interface de rede da função do Lambda.

AWS-UpdateAmazonECSAgent

Descrição

O `AWS-UpdateAmazonECSAgent` runbook atualiza o agente do Amazon Elastic Container Service (Amazon ECS) na instância do Amazon Elastic Compute Cloud (Amazon) que você especificar. EC2 Este runbook é compatível somente com instâncias do Amazon Linux e do Amazon Linux 2.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ClusterARN

  Tipo: StringList

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do cluster do Amazon ECS no qual as instâncias de contêineres estão registradas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeImage`
- `ec2:DescribeInstance`
- `ec2:DescribeInstanceAttribute`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

Etapas do documento

`aws:executeScript` :Atualiza o atendente do Amazon ECS no cluster do Amazon ECS especificado nos parâmetros de `ClusterARN`.

Saídas

UpdateAmazonECSAgent. UpdatedContainers - O ID da instância em que a atualização do agente do Amazon ECS foi bem-sucedida.

UpdateAmazonECSAgent. FailedContainers - O ID da instância em que a atualização do agente do Amazon ECS falhou.

UpdateAmazonECSAgent. InProgressContainers - O ID da instância em que a atualização do agente do Amazon ECS está em andamento.

Amazon EFS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic File System. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-CheckAndMountEFS

`AWSSupport-CheckAndMountEFS`

Descrição

O `AWSSupport-CheckAndMountEFS` runbook verifica os pré-requisitos para montar seu sistema de arquivos Amazon Elastic File System (Amazon EFS) e monta o sistema de arquivos na instância do Amazon Elastic Compute Cloud (Amazon) que você especificar. EC2 Esse runbook oferece suporte à montagem do sistema de arquivos Amazon EFS com o nome DNS ou com o endereço IP do destino de montagem.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Ação

  Tipo: String

  Valores válidos: Verifique | CheckAndMount

  Descrição: (obrigatório) determina se o runbook verifica os pré-requisitos ou verifica os pré-requisitos e monta o sistema de arquivos.

- EfsId

  Tipo: String

  Descrição: (obrigatório) O ID do sistema de arquivos que deseja montar.

- InstanceId

  Tipo: String

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon na qual você deseja montar o sistema de arquivos.

- MountOptions

  Tipo: String

  Descrição: (opcional) As opções suportadas pelo auxiliar de montagem do Amazon EFS que deseja usar ao montar o sistema de arquivos. Se a opção `tls` for especificada, verifique se o stunnel foi atualizado na instância de destino.

- MountPoint

  Tipo: String

  Descrição: (opcional) O diretório em que deseja montar o sistema de arquivos. Se você especificar o valor `Check` para o parâmetro `Action`, esse parâmetro não deverá ser especificado.

- MountTargetIP

Tipo: String

Descrição: (opcional) O endereço IP do alvo de montagem. A montagem por endereço IP funciona em ambientes em que o DNS está desativado, como nuvens privadas virtuais (VPCs) com nomes de host DNS desativados. Além disso, você pode usar essa opção se seu ambiente usar um provedor de DNS diferente do Amazon Route 53 (Route 53).

- Região

  Tipo: String

  Descrição: (Obrigatório) Região da AWS Onde a EC2 instância e o sistema de arquivos da Amazon estão localizados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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:*`

Etapas do documento

- `aws:executeScript`- Reúne detalhes sobre a EC2 instância da Amazon que você especifica no `InstanceId` parâmetro.
- `aws:executeScript` :Reúne detalhes sobre o sistema de arquivos especificado no parâmetro `EfsId`.
- `aws:executeScript`- Verifica se o grupo de segurança associado ao sistema de arquivos permite o tráfego na porta 2049 a partir da EC2 instância da Amazon que você especifica no `InstanceId` parâmetro.
- `aws:assertAwsResourceProperty`- Verifica se a EC2 instância da Amazon que você especifica no `InstanceId` parâmetro é gerenciada pelo Systems Manager e se o status é`Online`.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Action`.
- `aws:runCommand` :Verifica os pré-requisitos para montar o sistema de arquivos especificado no parâmetro `EfsId`.
- `aws:runCommand`- Verifica os pré-requisitos para montar o sistema de arquivos especificado no `EfsId` parâmetro e monta o sistema de arquivos na EC2 instância da Amazon que você especifica no parâmetro. `InstanceId`

Amazon EKS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Elastic Kubernetes Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-CollectEKSInstanceLogs
- AWS-CreateEKSClusterWithFargateProfile
- AWS-CreateEKSClusterWithNodegroup
- AWS-DeleteEKSCluster

- AWS-MigrateToNewEKSSelfManagedNodeGroup
- AWSPremiumSupport-TroubleshootEKSCluster
- AWSSupport-TroubleshootEKSWorkerNode
- AWS-UpdateEKSCluster
- AWS-UpdateEKSManagedNodeGroup
- AWS-UpdateEKSSelfManagedLinuxNodeGroups
- AWSSupport-SetupK8sApiProxyForEKS
- AWSSupport-TroubleshootEbsCsiDriversForEks

AWSSupport-CollectEKSInstanceLogs

Descrição

O `AWSSupport-CollectEKSInstanceLogs` runbook reúne arquivos de log relacionados ao sistema operacional e ao Amazon Elastic Kubernetes Service (Amazon EKS) de uma instância do Amazon Elastic Compute Cloud EC2 (Amazon) para ajudá-lo a solucionar problemas comuns. Enquanto a automação reúne os arquivos de log associados, são feitas alterações na estrutura do sistema de arquivos, incluindo a criação de diretórios temporários, a cópia dos arquivos de log nos diretórios temporários e a compactação dos arquivos de log em um arquivamento. Essa atividade pode resultar `CPUUtilization` no aumento da EC2 instância. Para obter mais informações sobre`CPUUtilization`, consulte Métricas de instância no Guia CloudWatch do usuário da Amazon.

Se especificar um valor para o parâmetro `LogDestination`, a automação avaliará o status da política do bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Para ajudar na segurança dos registros coletados da sua EC2 instância, se o status da política `isPublic` estiver definido como ou se a `true` lista de controle de acesso (ACL) conceder `READ|WRITE` permissões ao grupo predefinido do `All Users` Amazon S3, os registros não serão carregados. Para obter mais informações sobre grupos predefinidos do Amazon S3, consulte Grupos predefinidos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

> **Note**
>
> Essa automação requer pelo menos 10% do espaço em disco disponível no volume raiz do Amazon Elastic Block Store (Amazon EBS) anexado à sua instância. EC2 Se não houver espaço em disco disponível suficiente no volume raiz, a automação será interrompida.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EKSInstanceIdentificação

  Tipo: String

  Descrição: ID (obrigatório) da EC2 instância do Amazon EKS da qual você deseja coletar os registros.
- LogDestination

  Tipo: String

  Descrição: (opcional) O bucket do S3 em sua conta para fazer o upload dos logs arquivados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `ssm:SendCommand`

Recomendamos que a EC2 instância que recebe o comando tenha uma função do IAM com a política gerenciada SSMManaged InstanceCore da Amazon Amazon anexada. Para carregar o arquivo de log no bucket do S3 especificado no parâmetro `LogDestination`, a permissão `s3:PutObject` deve ser adicionada.

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma se o sistema operacional do valor especificado no parâmetro `EKSInstanceId` é Linux.
- `aws:runCommand` :Reúne arquivos de log relacionados ao sistema operacional e ao Amazon EKS, compactando-os em um arquivo no diretório `/var/log`.
- `aws:branch` :Confirma se um valor foi especificado para o parâmetro de `LogDestination`.
- `aws:runCommand` :Carrega o arquivo de log no bucket do S3 especificado no parâmetro `LogDestination`.

AWS-CreateEKSClusterWithFargateProfile

Descrição

O `AWS-CreateEKSClusterWithFargateProfile` runbook cria um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) usando um. AWS Fargate

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ClusterName

  Tipo: String

  Descrição: (Obrigatório) Um nome exclusivo para o cluster.

- ClusterRoleArn

  Tipo: String

  Descrição: (Obrigatório) O ARN da função do IAM que fornece permissões para o plano de controle do Kubernetes fazer chamadas para operações de AWS API em seu nome.

- FargateProfileName

  Tipo: String

  Descrição: (Obrigatório) O nome do perfil do Fargate.

- FargateProfileRoleArn

  Tipo: String

  Descrição: (Obrigatório) O ARN da função IAM de execução do Amazon EKS Pod.

- FargateProfileSelectors

  Tipo: String

  Descrição: (Obrigatório) Os seletores para combinar os pods com o perfil do Fargate.

- SubnetIds

  Tipo: StringList

  Descrição: (Obrigatório) A IDs das sub-redes que você deseja usar para seu cluster Amazon EKS. O Amazon EKS cria interfaces de rede elásticas nessas sub-redes para comunicação entre seus nós e o plano de controle do Kubernetes. Você deve especificar pelo menos duas sub-redes IDs.

- EKSEndpointPrivateAccess

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Defina esse valor para permitir acesso privado `True` ao endpoint do servidor da API Kubernetes do seu cluster. Se você habilitar o acesso privado, as solicitações de API do Kubernetes originadas da VPC do cluster usarão o endpoint da VPC privada. Se você desabilitar o acesso privado e tiver nós ou AWS Fargate pods no cluster, certifique-se de `publicAccessCidrs` incluir os blocos CIDR necessários para comunicação com os nós ou pods Fargate.

- EKSEndpointPublicAccess

  Tipo: booliano

  Padrão: False

  Descrição: (Opcional) Defina esse valor para desativar `False` o acesso público ao endpoint do servidor da API Kubernetes do seu cluster. Se você desativar o acesso público, o servidor da API Kubernetes do seu cluster só poderá receber solicitações de dentro da VPC em que foi lançado.

- PublicAccessCIDRs

  Tipo: StringList

  Descrição: (Opcional) Os blocos CIDR que têm acesso permitido ao endpoint público do servidor da API Kubernetes do seu cluster. A comunicação com o endpoint em endereços fora dos blocos CIDR especificados é negada. Se você desativou o acesso privado ao endpoint e tem nós ou pods Fargate no cluster, certifique-se de especificar os blocos CIDR necessários.

- SecurityGroupIds

  Tipo: StringList

  Descrição: (Opcional) Especifique um ou mais grupos de segurança para associar às interfaces de rede elástica criadas em sua conta pelo Amazon EKS.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- 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

Etapas do documento

- Create EKSCluster (aws:executeAwsApi) - Cria um cluster Amazon EKS.
- Verify EKSCluster IsActive (aws: waitForAwsResourceProperty) - Verifica se o estado do cluster éACTIVE.
- CreateFargateProfile (aws:executeAwsApi) - Cria um Fargate para o cluster.
- VerifyFargateProfileIsActive (aws: waitForAwsResourceProperty) - Verifica se o estado do perfil Fargate é. ACTIVE

Saídas

CreateEKSCluster.CreateClusterResponse

Descrição: Resposta recebida da chamada CreateCluster da API.

CreateFargateProfile.CreateFargateProfileResponse

Descrição: Resposta recebida da chamada CreateFargateProfile da API.

AWS-CreateEKSClusterWithNodegroup

Descrição

O AWS-CreateEKSClusterWithNodegroup runbook cria um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) usando um grupo de nós para capacidade.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

  Descrição: (Obrigatório) Um nome exclusivo para o cluster.
- ClusterRoleArn

  Tipo: String

  Descrição: (Obrigatório) O ARN da função do IAM que fornece permissões para o plano de controle do Kubernetes fazer chamadas para operações de AWS API em seu nome.

- NodegroupName

  Tipo: String

  Descrição: (Obrigatório) Um nome exclusivo para o grupo de nós.

- NodegroupRoleArn

  Tipo: String

  Descrição: (Obrigatório) O ARN da função do IAM a ser associada ao seu grupo de nós. O daemon kubelet do node worker node do Amazon EKS faz chamadas em seu nome. AWS APIs Os nós recebem permissões para essas chamadas de API por meio de um perfil de instância do IAM e políticas associadas. Antes de iniciar os nós e registrá-los em um cluster, você deve criar um perfil do IAM para uso desses nós quando eles forem iniciados.

- SubnetIds

  Tipo: StringList

  Descrição: (Obrigatório) A IDs das sub-redes que você deseja usar para seu cluster Amazon EKS. O Amazon EKS cria interfaces de rede elásticas nessas sub-redes para comunicação entre seus nós e o plano de controle do Kubernetes. Você deve especificar pelo menos duas sub-redes IDs.

- EKSEndpointPrivateAccess

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Defina esse valor para permitir acesso privado `True` ao endpoint do servidor da API Kubernetes do seu cluster. Se você habilitar o acesso privado, as solicitações de API do Kubernetes originadas da VPC do cluster usarão o endpoint da VPC privada. Se você desabilitar o acesso privado e tiver nós ou AWS Fargate pods no cluster, certifique-se de `publicAccessCidrs` incluir os blocos CIDR necessários para comunicação com os nós ou pods Fargate.

- EKSEndpointPublicAccess

  Tipo: booliano

  Padrão: False

Descrição: (Opcional) Defina esse valor para desativar `False` o acesso público ao endpoint do servidor da API Kubernetes do seu cluster. Se você desativar o acesso público, o servidor da API Kubernetes do seu cluster só poderá receber solicitações de dentro da VPC em que foi lançado.

- PublicAccessCIDRs

  Tipo: StringList

  Descrição: (Opcional) Os blocos CIDR que têm acesso permitido ao endpoint público do servidor da API Kubernetes do seu cluster. A comunicação com o endpoint em endereços fora dos blocos CIDR especificados é negada. Se você desativou o acesso privado ao endpoint e tem nós ou pods Fargate no cluster, certifique-se de especificar os blocos CIDR necessários.

- SecurityGroupIds

  Tipo: StringList

  Descrição: (Opcional) Especifique um ou mais grupos de segurança para associar às interfaces de rede elástica criadas em sua conta pelo Amazon EKS.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

Etapas do documento

- Create EKSCluster (aws:executeAwsApi) - Cria um cluster Amazon EKS.
- Verify EKSCluster IsActive (aws: waitForAwsResourceProperty) - Verifica se o estado do cluster é`ACTIVE`.
- CreateNodegroup (aws:executeAwsApi) - Cria um grupo de nós para o cluster.
- VerifyNodegroupIsActive (aws: waitForAwsResourceProperty) - Verifica se o estado do grupo de nós é`ACTIVE`.

Saídas

- `CreateEKSCluster.CreateClusterResponse`: resposta recebida da chamada `CreateCluster` da API.
- `CreateNodegroup.CreateNodegroupResponse`: resposta recebida da chamada `CreateNodegroup` da API.

AWS-DeleteEKSCluster

Descrição

Esse runbook exclui os atributos associados a um cluster do Amazon EKS, incluindo grupos de nós e perfis do Fargate. Opcionalmente, você pode optar por excluir todos os nós autogerenciados, as AWS CloudFormation pilhas usadas para criar os nós e a pilha de VPC CloudFormation do seu cluster. Para obter mais informações sobre como excluir um cluster do ECS, consulte Excluir um cluster no Guia do usuário do Amazon EKS.

> **Note**
>
> Se tiver serviços ativos no cluster associados a um balanceador de carga, você deve excluir esses serviços antes de excluir o cluster. Caso contrário, o sistema não poderá excluir os balanceadores de carga. Utilizar o procedimento a seguir para localizar e excluir serviços antes de executar o runbook `AWS-DeleteEKSCluster`.

Para localizar e excluir serviços no cluster

1. Instalar o utilitário de linha de comando Kubernetes, `kubectl`. Para obter mais informações, consulte Instalar o kubectl no Manual do usuário do Amazon EKS.
2. Executar o comando a seguir para listar todos os serviços em execução no cluster.

```
kubectl get svc --all-namespaces
```

3. Executar o comando a seguir para excluir todos os serviços que tenham um valor de IP EXTERNO associado. Esses serviços são liderados por um balanceador de carga e devem ser excluídos no Kubernetes para permitir que o balanceador de carga e os atributos associados sejam liberados corretamente.

```
kubectl delete svc
service-name
```

Agora você pode executar o runbook `AWS-DeleteEKSCluster`.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EKSClusterNome

  Tipo: String

Descrição: (obrigatório) O nome do cluster do Amazon EKS a ser excluído.

- VPCCloudFormationStack

  Tipo: String

  Descrição: nome da AWS CloudFormation pilha (opcional) para VPC para o cluster EKS que está sendo excluído. Isso exclui a AWS CloudFormation pilha da VPC e todos os recursos criados pela pilha.

- VPCCloudFormationStackRole

  Tipo: String

  Descrição: (Opcional) O ARN de uma função do IAM que AWS CloudFormation pressupõe a exclusão da pilha de VPC. CloudFormation AWS CloudFormation usa as credenciais da função para fazer chamadas em seu nome.

- SelfManagedNodeStacks

  Tipo: String

  Descrição: (Opcional) Lista separada por vírgulas de nomes de AWS CloudFormation pilha para nós autogerenciados. Isso excluirá as AWS CloudFormation pilhas para nós autogerenciados.

- SelfManagedNodeStacksRole

  Tipo: String

  Descrição: (Opcional) O ARN de uma função do IAM que AWS CloudFormation pressupõe a exclusão dos Node Stacks autogerenciados. AWS CloudFormation usa as credenciais da função para fazer chamadas em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `sts:AssumeRole`
- `eks:ListNodegroups`
- `eks:DeleteNodegroup`
- `eks:ListFargateProfiles`

- `eks:DeleteFargateProfile`
- `eks:DeleteCluster`
- `cfn:DescribeStacks`
- `cfn:DeleteStack`

Etapas do documento

- `aws:executeScript`- DeleteNodeGroups: Encontre e exclua todos os grupos de nós no cluster EKS.
- `aws:executeScript`- DeleteFargateProfiles: Encontre e exclua todos os perfis do Fargate no cluster EKS.
- `aws:executeScript`- DeleteSelfManagedNodes: Exclua todos os nós autogerenciados e as CloudFormation pilhas usadas para criar os nós.
- `aws:executeScript`- ExcluirEKSCluster: exclua o cluster EKS.
- `aws:executeScript`- Excluir VPCCloudFormationStack: exclua a pilha de VPC CloudFormation .

`AWS-MigrateToNewEKSSelfManagedNodeGroup`

Descrição

O `AWS-MigrateToNewEKSSelfManagedNodeGroup` runbook ajuda você a criar um novo grupo de nós Linux do Amazon Elastic Kubernetes Service (Amazon EKS) para o qual migrar seu aplicativo existente. Para obter mais informações, consulte Migração para um novo grupo de nós no Guia do usuário do Amazon EKS.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- OldStackName

  Tipo: String

  Descrição: (Obrigatório) O nome ou ID da pilha existente AWS CloudFormation .

- NewStackName

  Tipo: String

  Descrição: (Opcional) O nome da nova AWS CloudFormation pilha criada para seu novo grupo de nós. Se você não especificar um valor para esse parâmetro, o nome da pilha será criado usando o formato:`NewNodeGroup-`*`ClusterName`*`-`*`AutomationExecutionID`*.

- ClusterControlPlaneSecurityGroup

  Tipo: String

  Descrição: (Opcional) O ID do grupo de segurança que você deseja que os nós usem para se comunicar com o plano de controle do Amazon EKS. Se você não especificar um valor para esse parâmetro, o grupo de segurança especificado em sua AWS CloudFormation pilha existente será usado.

- NodeInstanceType

  Tipo: String

  Descrição: (Opcional) O tipo de instância que você deseja usar para o novo grupo de nós. Se você não especificar um valor para esse parâmetro, o tipo de instância especificado na sua AWS CloudFormation pilha existente será usado.

- NodeGroupName

Tipo: String

Descrição: (Opcional) O nome do seu novo grupo de nós. Se você não especificar um valor para esse parâmetro, o nome do grupo de nós especificado na AWS CloudFormation pilha existente será usado.

- NodeAutoScalingGroupDesiredCapacity

  Tipo: String

  Descrição: (Opcional) O número desejado de nós para escalar quando sua nova pilha for criada. Esse número deve ser maior ou igual ao `NodeAutoScalingGroupMinSize` valor e menor ou igual ao`NodeAutoScalingGroupMaxSize`. Se você não especificar um valor para esse parâmetro, a capacidade desejada do grupo de nós especificada em sua AWS CloudFormation pilha existente será usada.

- NodeAutoScalingGroupMaxSize

  Tipo: String

  Descrição: (Opcional) O número máximo de nós para os quais seu grupo de nós pode ser expandido. Se você não especificar um valor para esse parâmetro, o tamanho máximo do grupo de nós especificado em sua AWS CloudFormation pilha existente será usado.

- NodeAutoScalingGroupMinSize

  Tipo: String

  Descrição: (Opcional) O número mínimo de nós para os quais seu grupo de nós pode escalar. Se você não especificar um valor para esse parâmetro, o tamanho mínimo do grupo de nós especificado em sua AWS CloudFormation pilha existente será usado.

- NodeImageId

  Tipo: String

  Descrição: (opcional) O ID do Amazon Machine Image (AMI) a ser usado pelo grupo de nós.

- NodeImageIdSSMParam

  Tipo: String

Descrição: (opcional) O parâmetro público do Systems Manager para o AMI a ser usado pelo grupo de nós.

- NodeVolumeSize

  Tipo: String

  Descrição: (Opcional) O tamanho do volume raiz dos seus nós em GiB. Se você não especificar um valor para esse parâmetro, o tamanho do volume do nó especificado na AWS CloudFormation pilha existente será usado.

- NodeVolumeType

  Tipo: String

  Descrição: (Opcional) O tipo de volume do Amazon EBS que você deseja usar para o volume raiz dos seus nós. Se você não especificar um valor para esse parâmetro, o tipo de volume especificado na AWS CloudFormation pilha existente será usado.

- KeyName

  Tipo: String

  Descrição: (Opcional) O par de chaves que você deseja atribuir aos seus nós. Se você não especificar um valor para esse parâmetro, o par de chaves especificado na AWS CloudFormation pilha existente será usado.

- Sub-redes

  Tipo: StringList

  Descrição: (Opcional) Uma lista separada por vírgulas da sub-rede IDs que você deseja usar para seu novo grupo de nós. Se você não especificar um valor para esse parâmetro, as sub-redes especificadas na sua AWS CloudFormation pilha existente serão usadas.

- Desativar IMDSv1

  Tipo: booliano

  Descrição: (Opcional) Especifique `true` para desativar o serviço de metadados de instância versão 1 (IMDSv1). Por padrão, os nós suportam IMDSv1 IMDSv2 e.

- BootstrapArguments

Tipo: String

Descrição: (Opcional) Argumentos adicionais que você deseja passar para o script de bootstrap do nó.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetParameters`
- `autoscaling:CreateAutoScalingGroup`
- `autoscaling:CreateOrUpdateTags`
- `autoscaling:DeleteTags`
- `autoscaling:DescribeAutoScalingGroups`
- `autoscaling:DescribeScalingActivities`
- `autoscaling:DescribeScheduledActions`
- `autoscaling:SetDesiredCapacity`
- `autoscaling:TerminateInstanceInAutoScalingGroup`
- `autoscaling:UpdateAutoScalingGroup`
- `cloudformation:CreateStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateStack`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateLaunchTemplateVersion`
- `ec2:CreateLaunchTemplate`
- `ec2:CreateSecurityGroup`
- `ec2:CreateTags`

- ec2:DeleteLaunchTemplate
- ec2:DeleteSecurityGroup
- ec2:DescribeAvailabilityZones
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstanceStatus
- ec2:DescribeInstances
- ec2:DescribeKeyPairs
- ec2:DescribeLaunchTemplateVersions
- ec2:DescribeLaunchTemplates
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress
- ec2:RunInstances
- ec2:TerminateInstances
- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam:GetInstanceProfile
- iam:GetRole
- iam:PassRole

Etapas do documento

- DetermineParameterValuesForNewNodeGroup (aws:ExecuteScript) - Reúne os valores dos parâmetros a serem usados no novo grupo de nós.
- CreateStack (aws:createStack) - Cria a AWS CloudFormation pilha para o novo grupo de nós.
- GetNewStackNodeInstanceRole (aws:executeAwsApi) - Obtém a função da instância do nó.

- GetNewStackSecurityGroup (aws:executeAwsApi) - A etapa obtém o grupo de segurança do nó.
- AddIngressRulesToNewNodeSecurityGroup (aws:executeAwsApi) - Adiciona regras de entrada ao grupo de segurança recém-criado para que ele possa aceitar tráfego daquele atribuído ao seu grupo de nós anterior.
- AddIngressRulesToOldNodeSecurityGroup (aws:executeAwsApi) - Adiciona regras de entrada ao grupo de segurança anterior para que ele possa aceitar tráfego daquele atribuído ao seu grupo de nós recém-criado.
- VerifyStackComplete (aws: assertAwsResource Property) - Verifica se o status da nova pilha é. `CREATE_COMPLETE`

Saídas

DetermineParameterValuesForNewNodeGroup. NewStackParameters - Os parâmetros usados para criar a nova pilha.

GetNewStackNodeInstanceRole. NewNodeInstanceRole - A função da instância do nó para o novo grupo de nós.

GetNewStackSecurityGroup. NewNodeSecurityGroup - O ID do grupo de segurança para o novo grupo de nós.

DetermineParameterValuesForNewNodeGroup. NewStackName - O nome da AWS CloudFormation pilha para o novo grupo de nós.

CreateStack. StackId - O ID da AWS CloudFormation pilha para o novo grupo de nós.

`AWSPremiumSupport-TroubleshootEKSCluster`

Descrição

O runbook `AWSPremiumSupport-TroubleshootEKSCluster` diagnostica problemas comuns com um cluster do Amazon Elastic Kubernetes Service (Amazon EKS), a infraestrutura subjacente, e fornece etapas de remediação recomendadas.

> **Important**
>
> O acesso aos runbooks da `AWSPremiumSupport-*` requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Compare AWS Support Plans.

Se especificar um valor para o parâmetro `S3BucketName`, a automação avaliará o status da política do bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Para ajudar na segurança dos registros coletados da sua EC2 instância, se o status da política `isPublic` estiver definido como ou se a `true` lista de controle de acesso (ACL) conceder `READ|WRITE` permissões ao grupo predefinido do `All Users` Amazon S3, os registros não serão carregados. Para obter mais informações sobre grupos predefinidos do Amazon S3, consulte Grupos predefinidos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

  Descrição: (obrigatório) O nome do cluster do Amazon EKS que deseja solucionar.
- S3 BucketName

  Tipo: String

Descrição: (Obrigatório) O nome do bucket privado do Amazon S3 em que o relatório gerado pelo runbook deve ser carregado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Além disso, a política AWS Identity and Access Management (IAM) anexada ao usuário ou à função que inicia a automação deve permitir a `ssm:GetParameter` operação com os seguintes AWS Systems Manager parâmetros públicos para obter a última recomendação do Amazon EKS Amazon Machine Image (AMI) para os nós de trabalho.

- `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 carregar o relatório gerado pelo runbook em um bucket do Amazon S3, as seguintes permissões são necessárias para o bucket do Amazon S3 especificado.

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

Etapas do documento

- aws:executeAwsApi :Reúne detalhes do cluster Amazon EKS especificado.
- aws:executeScript- Reúne detalhes das instâncias do Amazon Elastic Compute Cloud EC2 (Amazon), grupos AMI de Auto Scaling e tipos de instâncias gráficas da EC2 Amazon GPU.
- aws:executeScript- Reúne detalhes da nuvem privada virtual (VPC), sub-redes, gateways de tradução de endereços de rede (NAT), rotas de sub-rede, grupos de segurança e listas de controle de acesso à rede (ACLs) do cluster Amazon EKS.
- aws:executeScript :Reúne detalhes dos perfis de instância do IAM anexados e das políticas de perfis.
- aws:executeScript :Reúne detalhes do bucket do Amazon S3 especificado no parâmetro S3BucketName.
- aws:executeScript :Classifica as sub-redes da Amazon VPC como públicas ou privadas.
- aws:executeScript :Verifica as sub-redes da Amazon VPC em busca de tags que são necessárias como parte de um cluster do Amazon EKS.
- aws:executeScript :Verifica as sub-redes da Amazon VPC em busca das tags que são necessárias para as sub-redes do Elastic Load Balancing.

- `aws:executeScript`- Verifica se as EC2 instâncias da Amazon do nó de trabalho usam a versão mais recente otimizada AMI do Amazon EKS
- `aws:executeScript` :Verifica se os grupos de segurança da Amazon VPC estão conectados aos nós de processamento quanto às tags necessárias.
- `aws:executeScript` :Verifica as regras do cluster do Amazon EKS e do grupo de segurança da Amazon VPC do nó de processamento quanto às regras de entrada recomendadas para o cluster do Amazon EKS.
- `aws:executeScript` :Verifica as regras do cluster do Amazon EKS e do grupo de segurança da Amazon VPC do nó de processamento para ver as regras de saída recomendadas do cluster do Amazon EKS.
- `aws:executeScript` :Verifica a configuração de rede da ACL para as sub-redes da Amazon VPC.
- `aws:executeScript`- Verifica se as EC2 instâncias do nó de trabalho da Amazon têm as políticas gerenciadas necessárias.
- `aws:executeScript` :Verifica se os grupos do Auto Scaling têm as tags necessárias para o escalonamento automático do cluster.
- `aws:executeScript`- Verifica se as EC2 instâncias do nó de trabalho da Amazon estão conectadas à Internet.
- `aws:executeScript` :Gera um relatório com base nas saídas das etapas anteriores. Se um valor for especificado para o parâmetro `S3BucketName`, o relatório gerado será carregado no bucket do Amazon S3.

AWSSupport-TroubleshootEKSWorkerNode

Descrição

O `AWSSupport-TroubleshootEKSWorkerNode` runbook analisa um nó de trabalho do Amazon Elastic Compute Cloud (Amazon EC2) e um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) para ajudá-lo a identificar e solucionar causas comuns que impedem que os nós de trabalho se juntem a um cluster. O runbook fornece orientações para ajudar a resolver quaisquer problemas identificados.

> **Important**
>
> Para executar essa automação com sucesso, o estado do seu nó de EC2 trabalho da Amazon deve ser`running`, e o estado do cluster do Amazon EKS deve ser`ACTIVE`.

[Executar esta automação (console)]

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

  Descrição: (obrigatório) O nome do cluster do Amazon EKS.
- WorkerID

  Tipo: String

  Descrição: (Obrigatório) O ID do nó de EC2 trabalho da Amazon que não conseguiu se juntar ao cluster.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma que o cluster Amazon EKS especificado no parâmetro `ClusterName` existe e está no estado `ACTIVE`.

- `aws:assertAwsResourceProperty`- Confirma que o nó de EC2 trabalho da Amazon que você especifica no `WorkerID` parâmetro existe e está em um `running` estado.
- `aws:executeScript` :Executa um script Python que ajuda a identificar possíveis causas da falha do nó de processamento em ingressar no cluster.

`AWS-UpdateEKSCluster`

Descrição

O `AWS-UpdateEKSCluster` runbook ajuda você a atualizar seu cluster do Amazon Elastic Kubernetes Service (Amazon EKS) para a versão do Kubernetes que você deseja usar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

Descrição: (Obrigatório) O nome do seu cluster Amazon EKS.

- Versão

  Tipo: String

  Descrição: (Obrigatório) A versão do Kubernetes para a qual você deseja atualizar seu cluster.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `eks:DescribeUpdate`
- `eks:UpdateClusterVersion`

Etapas do documento

- `aws:executeAwsApi`- Atualiza a versão do Kubernetes que é usada pelo seu cluster Amazon EKS.
- `aws:waitForAwsResourceProperty`- Espera que o status da atualização seja`Successful`.

AWS-UpdateEKSManagedNodeGroup

Descrição

O runbook `AWS-UpdateEKSManagedNodeGroup` ajuda a atualizar um grupo de nós gerenciados do Amazon Elastic Kubernetes Service (Amazon EKS). Você pode escolher uma atualização de `Version` ou de `Configuration`.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

  Descrição: (obrigatório) O nome do cluster cujo grupo de nós deseja atualizar.
- NodeGroupName

  Tipo: String

  Descrição: (obrigatório) O nome do grupo de nós a ser atualizado.
- UpdateType

  Tipo: String

  Valores válidos: Update Node Group Version | Update Node Group Configurations

  Padrão: Atualizar versão do grupo de nós

  Descrição: (obrigatório) O tipo de atualização que deseja realizar no grupo de nós.

Os parâmetros a seguir se aplicam somente ao tipo de atualização de `Version`:

- AMIReleaseVersão

  Tipo: String

  Descrição: (opcional) A versão da AMI otimizada do Amazon EKS que deseja usar. A versão mais recente é usada por padrão.

- ForceUpgrade

  Tipo: booliano

  Descrição: (opcional) Se verdadeiro, a atualização não falhará em resposta a uma violação do orçamento de interrupção do pod.

- KubernetesVersion

  Tipo: String

  Descrição: (opcional) A versão do Kubernetes para a qual atualizar o grupo de nós.

- LaunchTemplateId

  Tipo: String

  Descrição: (opcional) O ID do modelo de execução.

- LaunchTemplateName

  Tipo: String

  Descrição: (opcional) O nome do modelo de execução.

- LaunchTemplateVersion

  Tipo: String

  Descrição: (Opcional) A versão do modelo de lançamento do Amazon Elastic Compute Cloud (Amazon EC2). Esse parâmetro só é válido se um grupo de nós foi criado a partir de um modelo de execução.

Os parâmetros a seguir se aplicam somente ao tipo de atualização de `Configuration`:

- AddOrUpdateNodeGroupLabels

  Tipo: StringMap

  Descrição: (opcional) Rótulos do Kubernetes que deseja adicionar ou atualizar.

- AddOrUpdateKubernetesTaintsEffect

  Tipo: StringList

Descrição: (opcional) As taints do Kubernetes que deseja adicionar ou atualizar.

- MaxUnavailableNodeGroups

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número máximo de nós indisponíveis ao mesmo tempo durante uma atualização de versão.

- MaxUnavailablePercentageNodeGroup

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) A porcentagem de nós não disponíveis durante uma atualização de versão.

- NodeGroupDesiredSize

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número atual de nós que o grupo de nós gerenciados deve manter.

- NodeGroupMaxSize

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número máximo de nós para o qual o grupo de nós gerenciados pode ser aumentado na escala horizontalmente.

- NodeGroupMinSize

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número mínimo de nós para o qual o grupo de nós gerenciados pode ser reduzido na escala horizontalmente.

- RemoveKubernetesTaintsEffect

Tipo: StringList

Descrição: (opcional) As taints do Kubernetes que deseja remover.

- RemoveNodeGroupLabels

  Tipo: StringList

  Descrição: (opcional) Uma lista separada por vírgulas dos rótulos que deseja remover.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

Etapas do documento

- `aws:executeScript`: atualiza um grupo de nós do cluster Amazon EKS de acordo com os valores especificados para os parâmetros de entrada do runbook.
- `aws:waitForAwsResourceProperty`: espera que o status de atualização do cluster seja `Successful`.

AWS-UpdateEKSSelfManagedLinuxNodeGroups

Descrição

O runbook `AWS-UpdateEKSSelfManagedLinuxNodeGroups` atualiza grupos de nós autogerenciados em seu cluster do Amazon Elastic Kubernetes Service (Amazon EKS) usando uma pilha do AWS CloudFormation .

Se o cluster usa ajuste de escala automático, recomendamos reduzir a implantação para duas réplicas antes de usar esse runbook.

Como escalar uma implantação para duas réplicas

1. Instale o utilitário de linha de comando Kubernetes, `kubectl`. Para obter mais informações, consulte Instalar o kubectl no Manual do usuário do Amazon EKS.

2. Execute o seguinte comando:

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. Execute o runbook `AWS-UpdateEKSSelfManagedLinuxNodeGroups`.
4. Escale a implantação para o número desejado de réplicas executando o comando a seguir.

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

  Descrição: (obrigatório) O nome do cluster do Amazon EKS.
- NodeGroupName

  Tipo: String

Descrição: (obrigatório) O nome do grupo de nós gerenciados.

- ClusterControlPlaneSecurityGroup

  Tipo: String

  Descrição: (obrigatório) O ID do grupo de segurança do ambiente de gerenciamento.

- Desativar IMDSv1

  Tipo: booliano

  Descrição: (Opcional) Determina se você deseja permitir a versão 1 do Instance Metadata Service (IMDSv1) e. IMDSv2

- KeyName

  Tipo: String

  Descrição: (opcional) O nome da chave para as instâncias.

- NodeAutoScalingGroupDesiredCapacity

  Tipo: String

  Descrição: (opcional) O número de nós que o grupo de nós deve manter.

- NodeAutoScalingGroupMaxSize

  Tipo: String

  Descrição: (opcional) O número máximo de nós para o qual o grupo de nós pode ser expandido.

- NodeAutoScalingGroupMinSize

  Tipo: String

  Descrição: (opcional) O número mínimo de nós para o qual o grupo de nós pode ser reduzido.

- NodeInstanceType

  Tipo: String

  Padrão: T3.large

  Descrição: (opcional) O tipo de instância a ser usado para o grupo de nós.

- NodeImageId

  Tipo: String

  Descrição: (opcional) O ID do Amazon Machine Image (AMI) a ser usado pelo grupo de nós.
- NodeImageIdSSMParam

  Tipo: String

  Padrão:/aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

  Descrição: (opcional) O parâmetro público do Systems Manager para o AMI a ser usado pelo grupo de nós.
- StackName

  Tipo: String

  Descrição: (Obrigatório) O nome da AWS CloudFormation pilha usada para atualizar o grupo de nós.
- Sub-redes

  Tipo: String

  Descrição: (Obrigatório) Uma lista separada por vírgulas das IDs sub-redes que você deseja que seu cluster use.
- VpcId

  Tipo: String

  Padrão: Default

  Descrição: (obrigatório) A nuvem privada virtual (VPC) em que seu cluster está implantado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DeleteNodegroup`

- `eks:DeleteCluster`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

Etapas do documento

- `aws:executeScript` :Atualiza um grupo de nós do cluster Amazon EKS de acordo com os valores especificados para os parâmetros de entrada do runbook.
- `aws:waitForAwsResourceProperty`- Espera que o status de atualização da AWS CloudFormation pilha seja retornado.

AWSSupport-SetupK8sApiProxyForEKS

Descrição

O runbook de automação do AWSSupport-SetupK8 sApiProxy ForEks fornece uma maneira de criar uma AWS Lambda função que atua como proxy para fazer chamadas de API do plano de controle para o endpoint do cluster Amazon Elastic Kubernetes Service. Ele serve como um alicerce para runbooks que exigem a realização de chamadas de API no plano de controle para automatizar tarefas e solucionar problemas com um cluster Amazon EKS.

> **Important**
>
> Todos os recursos criados por essa automação são marcados para que possam ser facilmente encontrados. As tags usadas são:
>
> - `AWSSupport-SetupK8sApiProxyForEKS`: true

> **Note**
>
> - A automação é um runbook auxiliar e não pode ser executada como um runbook independente. Ela é invocada como uma automação secundária para runbooks que exigem chamadas de API de plano de controle para o cluster Amazon EKS.
> - Certifique-se de executar a `Cleanup` operação após o uso para evitar custos indesejados.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

  Descrição: (Obrigatório) O nome do cluster Amazon Elastic Kubernetes Service.
- Operação

  Tipo: String

  Descrição: (Obrigatório) Operação a ser executada: `Setup` provisiona a função Lambda na conta, `Cleanup` desprovisionará recursos criados como parte da fase de configuração.

Valores permitidos: `Setup` | `Cleanup`

Padrão: Configuração

- LambdaRoleArn

  Tipo: String

  Descrição: (Opcional) O ARN da função do IAM que permite que a AWS Lambda função acesse os serviços e recursos da AWS necessários. Se nenhuma função for especificada, esse Systems Manager Automation criará uma função do IAM para Lambda em sua conta com o nome `Automation-K8sProxy-Role-<ExecutionId>` que inclui as políticas gerenciadas: e. `AWSLambdaBasicExecutionRole` `AWSLambdaVPCAccessExecutionRole`

Como funciona?

O runbook executa as seguintes etapas:

- Valida se a automação está sendo executada como uma execução secundária. O runbook não funcionará quando invocado como um runbook autônomo, pois ele não executa nenhum trabalho significativo sozinho.
- Verifica a AWS CloudFormation pilha existente da função proxy Lambda para o cluster especificado.
  - Se a pilha existir, a infraestrutura existente será reutilizada em vez de recriá-la.
  - Um contador de referência é mantido usando tags para garantir que um runbook não exclua a infraestrutura se ela estiver sendo reutilizada por outro runbook para o mesmo cluster.
- Execute o tipo de operação (`Setup`/`Cleanup`) especificado para a invocação:
  - Configuração: cria ou descreve os recursos existentes.

    Limpeza: remove os recursos provisionados, se a infraestrutura não estiver sendo usada por nenhum outro runbook.

Permissões obrigatórias do IAM

O `AutomationAssumeRole` parâmetro exige que as seguintes permissões concedidas `LambdaRoleArn` não sejam passadas:

- `cloudformation:CreateStack`

- cloudformation:DescribeStacks
- cloudformation:DeleteStack
- cloudformation:UpdateStack
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DeleteNetworkInterface
- eks:DescribeCluster
- lambda:CreateFunction
- lambda:DeleteFunction
- lambda:ListTags
- lambda:GetFunction
- lambda:ListTags
- lambda:TagResource
- lambda:UntagResource
- lambda:UpdateFunctionCode
- logs:CreateLogGroup
- logs:PutRetentionPolicy
- logs:TagResource
- logs:UntagResource
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:ListTagsForResource
- iam:CreateRole
- iam:AttachRolePolicy
- iam:DetachRolePolicy
- iam:PassRole

- iam:GetRole
- iam:DeleteRole
- iam:TagRole
- iam:UntagRole
- tag:GetResources
- tag:TagResources

Quando LambdaRoleArn fornecida, a automação não precisa criar a função e as seguintes permissões podem ser excluídas:

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

Abaixo está um exemplo de política que demonstra as permissões necessárias para AutomationAssumeRole quando não LambdaRoleArn é aprovada:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": [
    "tag:GetResources",
    "tag:TagResources",
    "ec2:CreateNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DeleteNetworkInterface",
    "eks:DescribeCluster",
    "iam:GetRole",
    "cloudformation:DescribeStacks",
```

```
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "lambda:GetFunction",
    "lambda:ListTags",
    "logs:ListTagsForResource"
   ],
   "Resource": "*",
   "Effect": "Allow",
   "Sid": "AllowActionsWithoutConditions"
  },
  {
   "Condition": {
    "StringEquals": {
     "aws:RequestTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
    }
   },
   "Action": "iam:CreateRole",
   "Resource": [
    "arn:<partition>:iam:::<account-id>::role/Automation-K8sProxy*"
   ],
   "Effect": "Allow",
   "Sid": "AllowCreateRoleWithRequiredTag"
  },
  {
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
    }
   },
   "Action": [
    "iam:DeleteRole",
    "iam:TagRole",
    "iam:UntagRole"
   ],
   "Resource": [
    "arn:<partition>:iam:::<account-id>::role/Automation-K8sProxy*"
   ],
   "Effect": "Allow",
   "Sid": "IAMActions"
  },
  {
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
```

```
    },
    "StringLike": {
     "iam:PolicyARN": [
      "arn:<partition>:iam::<partition>:policy/service-role/
AWSLambdaBasicExecutionRole",
      "arn:<partition>:iam::<partition>:policy/service-role/
AWSLambdaVPCAccessExecutionRole"
     ]
    }
   },
   "Action": [
    "iam:AttachRolePolicy",
    "iam:DetachRolePolicy"
   ],
   "Resource": [
    "arn:<partition>:iam:::<account-id>::role/Automation-K8sProxy*"
   ],
   "Effect": "Allow",
   "Sid": "AttachRolePolicy"
  },
  {
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
    }
   },
   "Action": [
    "lambda:CreateFunction",
    "lambda:DeleteFunction",
    "lambda:TagResource",
    "lambda:UntagResource",
    "lambda:UpdateFunctionCode"
   ],
   "Resource": "arn:<partition>:lambda::<region-id>:::<account-
id>::function:Automation-K8sProxy*",
   "Effect": "Allow",
   "Sid": "LambdaActions"
  },
  {
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
    }
   },
```

```
    "Action": [
     "cloudformation:CreateStack",
     "cloudformation:DeleteStack",
     "cloudformation:UpdateStack"
    ],
    "Resource": "arn:<partition>:cloudformation::<region-id>:::<account-id>::stack/
AWSSupport-SetupK8sApiProxyForEKS*",
    "Effect": "Allow",
    "Sid": "CloudFormationActions"
   },
   {
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
     }
    },
    "Action": [
     "logs:CreateLogGroup",
     "logs:CreateLogStream",
     "logs:PutLogEvents",
     "logs:PutRetentionPolicy",
     "logs:TagResource",
     "logs:UntagResource"
    ],
    "Resource": [
     "arn:<partition>:logs::<region-id>:::<account-id>::log-group:/aws/lambda/
Automation-K8sProxy*",
     "arn:<partition>:logs::<region-id>:::<account-id>::log-group:/aws/lambda/
Automation-K8sProxy*:*"
    ],
    "Effect": "Allow",
    "Sid": "LogsActions"
   },
   {
    "Condition": {
     "StringLikeIfExists": {
      "iam:PassedToService": "lambda.amazonaws.com"
     }
    },
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:<partition>:iam:::<account-id>::role/Automation-K8sProxy-Role*"
```

```
    ],
    "Effect": "Allow",
    "Sid": "PassRoleToLambda"
   }
  ]
}
```

Caso `LambdaRoleArn` seja aprovado, certifique-se de que ele tenha uma AWSLambdaBasicExecutionRole política anexada para clusters públicos e, além disso, AWSLambdaVPCAccessExecutionRole para clusters privados.

Recursos criados

Os seguintes recursos são criados durante a `Setup` operação:

1. AWS Lambda função
2. Função do IAM: função de execução do Lambda, se não for fornecida.
3. CloudWatch Grupo de registros (Lambda Logs)

A função Lambda e a função de execução são mantidas até que a *`Cleanup`* operação seja executada. O grupo de registros do Lambda será retido por 30 dias ou até que seja excluído manualmente.

Instruções

O runbook é um utilitário auxiliar projetado para ser executado a partir de outros runbooks como uma automação infantil. Ele facilita a criação de uma infraestrutura que permite que o runbook principal faça chamadas à API do plano de controle do Amazon EKS K8s. Para usar o runbook, você pode seguir as etapas abaixo no contexto da automação principal.

1. Fase de configuração: invoque a automação usando a operação de `aws:executeAutomation` ação do runbook que gostaria de fazer chamadas de API do plano de controle do Amazon EKS K8s com a operação definida como. `Setup`

   Exemplo de parâmetros de entrada:

   ```
   {
     "AutomationAssumeRole": "<role-arn>",
     "ClusterName": "<eks-cluster-name>",
     "Operation": "Setup"
   ```

```
}
```

A saída da `aws:executeAutomation` etapa conterá o ARN da função proxy Lambda.

2. Usando o Lambda Proxy: invoque a função Lambda dentro da `aws:executeScript` ação usando `boto3`'s `Lambda.Client.invoke(...)` com uma lista de caminhos de chamada de API e token portador. A função Lambda executará `GET` chamadas HTTP para o caminho especificado passando o token portador como parte do cabeçalho de autorização.

   Exemplo do evento de invocação do Lambda:

   ```
   {
       "ApiCalls": ["/api/v1/pods/", ...],
       "BearerToken": "..."
   }
   ```

   > **Note**
   >
   > O token portador deve ser gerado como parte do script de automação principal. Você precisa garantir que o principal que executa o runbook principal tenha permissão somente de leitura para o cluster Amazon EKS especificado.

3. Fase de limpeza: invoque a automação usando a operação de `aws:executeAutomation` ação do runbook que gostaria de fazer chamadas de API do plano de controle do Amazon EKS K8s com a operação definida como. `Cleanup`

   Exemplo de parâmetros de entrada:

   ```
   {
     "AutomationAssumeRole": "<role-arn>",
     "ClusterName": "<eks-cluster-name>",
     "Operation": "Cleanup"
   }
   ```

Etapas de automação

1. ValidateExecution
   - Verifica se a automação não está sendo executada como uma execução autônoma.
2. CheckForExistingStack

- Verifica se uma AWS CloudFormation pilha já foi provisionada para o nome do cluster especificado.
- Retorna o status de existência da pilha e se é seguro excluí-la.

3. BranchOnIsStackExists
   - Etapa de decisão que se ramifica com base na existência da pilha.
   - Rotas para atualizar o nome da pilha existente ou continuar com a ramificação da operação.
4. UpdateStackName
   - Atualiza a `StackName` variável com o nome da pilha existente.
   - Executado somente se a pilha já existir.
5. BranchOnOperation
   - Encaminha a automação com base no `Operation` parâmetro (`Setup`/`Cleanup`).
   - Para`Setup`: Rotas para criar uma nova pilha ou descrever os recursos existentes.
   - Para`Cleanup`: Prossegue com a exclusão da pilha, se for seguro excluir.
6. GetClusterNetworkConfig
   - Descreve o cluster Amazon EKS para obter a configuração da VPC.
   - Recupera dados do endpoint, da VPC ID, da sub-rede IDs, do grupo de segurança e da CA.
7. ProvisionResources
   - Cria uma AWS CloudFormation pilha com os recursos necessários.
   - Provisiona a função Lambda com a configuração de rede necessária.
   - Marca todos os recursos para rastreamento e gerenciamento.
8. DescribeStackResources
   - Recupera informações sobre a pilha criada/existente.
   - Obtém o ARN da função Lambda provisionada.
9. BranchOnIsLambdaDeploymentRequired
   - Determina se a implantação do código Lambda é necessária.
   - Só prossegue com a implantação de pilhas recém-criadas.
10. DeployLambdaFunctionCode
    - Implanta o código da função Lambda usando o pacote de implantação.
    - Atualiza a função com a implementação do proxy.
11. AssertLambdaAvailable

- Verifica se a atualização do código da função Lambda foi bem-sucedida.
- Espera que a função esteja no `Successful` estado.

12PerformStackCleanup

- Exclui a AWS CloudFormation pilha e os recursos associados.
- Executado durante `Cleanup` a operação ou em caso de falha na `Setup` operação.

Saídas

LambdaFunctionArn: ARN da função proxy Lambda

Referências

Automação do Systems Manager

- Executar uma automação
- Configurar a automação
- Fluxos de trabalho de automação de suporte

AWSSupport-TroubleshootEbsCsiDriversForEks

Descrição

O `AWSSupport-TroubleshootEbsCsiDriversForEks` runbook ajuda a solucionar problemas com montagens de volume do Amazon Elastic Block Store no Amazon Elastic Kubernetes Service (Amazon EKS) e problemas de driver do Amazon EBS Container Storage Interface (CSI)

> **Important**
>
> Atualmente, o driver CSI do Amazon EBS em execução não AWS Fargate é suportado.

Como funciona?

O runbook `AWSSupport-TroubleshootEbsCsiDriversForEks` executa as seguintes etapas de alto nível:

- Verifica se o cluster de destino do Amazon EKS existe e está no estado ativo.

- Implanta os recursos de autenticação necessários para fazer chamadas de API do Kubernetes com base no fato de o complemento ser gerenciado ou autogerenciado pelo Amazon EKS.
- Executa verificações e diagnósticos de saúde do controlador CSI do Amazon EBS.
- Executa verificações de permissões do IAM nas funções dos nós e nas funções da conta de serviço.
- Diagnostica problemas persistentes de criação de volume para o pod de aplicativo especificado.
- Verifica o node-to-pod agendamento e examina os eventos do pod.
- Coleta registros relevantes do Kubernetes e do aplicativo, enviando-os para o bucket especificado do Amazon S3.
- Executa verificações de integridade dos nós e verifica a conectividade com os EC2 endpoints da Amazon.
- Analisa os anexos persistentes do dispositivo de bloqueio de volume e o status de montagem.
- Limpa a infraestrutura de autenticação criada durante a solução de problemas.
- Gera um relatório abrangente de solução de problemas combinando todos os resultados do diagnóstico.

Note

- O modo de autenticação do cluster Amazon EKS deve ser definido como `API` ou`API_AND_CONFIG_MAP`. Recomendamos usar a entrada Amazon EKS Access. O runbook exige permissões de controle de acesso baseado em funções (RBAC) do Kubernetes para realizar as chamadas de API necessárias.
- Se você não especificar uma função do IAM para a função Lambda (`LambdaRoleArn`parâmetro), a automação cria uma função nomeada `Automation-K8sProxy-Role-<ExecutionId>` na sua conta. Essa função inclui as políticas gerenciadas `AWSLambdaBasicExecutionRole` `AWSLambdaVPCAccessExecutionRole` e.
- Algumas etapas de diagnóstico exigem que os nós de trabalho do Amazon EKS sejam instâncias gerenciadas pelo Systems Manager. Se os nós não forem instâncias gerenciadas pelo Systems Manager, as etapas que exigem acesso ao Systems Manager serão ignoradas, mas outras verificações continuarão.

- A automação inclui uma etapa de limpeza que remove os recursos da infraestrutura de autenticação. Essa etapa de limpeza é executada mesmo quando as etapas anteriores falham, o que ajuda a evitar recursos órfãos em sua conta. AWS

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Instruções

Siga estas etapas para configurar a automação:

1. Crie uma função de automação de SSM TroubleshootEbsCsiDriversForEks-SSM-Role em sua conta. Verifique se a relação de confiança contém a seguinte política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. Anexe a política abaixo à função do IAM para conceder as permissões necessárias para realizar as ações especificadas nos recursos especificados.
   - Se você espera fazer o upload de registros de execução e recursos para o bucket do Amazon S3 na AWS mesma região, arn:{partition}:s3:::BUCKET_NAME/* substitua os seus em. OptionalRestrictPutObjects

- O bucket do Amazon S3 deve apontar para o bucket correto do Amazon S3 se você `S3BucketName` selecionar na execução do SSM.
- Essa permissão é opcional se você não especificar `S3BucketName`
- O bucket do Amazon S3 deve ser privado e estar na mesma AWS região em que você executa a automação do SSM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OptionalRestrictPutObjects",
            "Effect": "Allow",
            "Action": ["s3:PutObject"],
            "Resource": ["arn:{partition}:s3:::BUCKET_NAME/*"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeInstanceStatus",
                "ec2:GetEbsEncryptionByDefault",
                "eks:DescribeAddon",
                "eks:DescribeAddonVersions",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile",
                "iam:GetOpenIDConnectProvider",
                "iam:GetRole",
                "iam:ListOpenIDConnectProviders",
                "iam:SimulatePrincipalPolicy",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "ssm:DescribeInstanceInformation",
                "ssm:GetAutomationExecution",
                "ssm:GetDocument",
                "ssm:ListCommandInvocations",
                "ssm:ListCommands",
                "ssm:SendCommand",
                "ssm:StartAutomationExecution"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "SetupK8sApiProxyForEKSActions",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:UpdateStack",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "eks:DescribeCluster",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:GetRole",
                "iam:TagRole",
                "iam:UntagRole",
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:InvokeFunction",
                "lambda:ListTags",
                "lambda:TagResource",
                "lambda:UntagResource",
                "lambda:UpdateFunctionCode",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:ListTagsForResource",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy",
                "logs:TagResource",
                "logs:UntagResource",
                "ssm:DescribeAutomationExecutions",
                "tag:GetResources",
                "tag:TagResources"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "PassRoleToAutomation",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:*:iam::*:role/TroubleshootEbsCsiDriversForEks-SSM-Role",
                "arn:*:iam::*:role/Automation-K8sProxy-Role-*"
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "iam:PassedToService": [
                        "lambda.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AttachRolePolicy",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "iam:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
                }
            }
        }
    ]
}
```

3. Conceda as permissões necessárias para o cluster RBAC (Role-Based Access Control) do Amazon EKS. A abordagem recomendada é criar uma entrada de acesso no seu cluster Amazon EKS.

   No console do Amazon EKS, navegue até seu cluster. Para entradas de acesso do Amazon EKS, verifique se sua configuração de acesso está definida como `API_AND_CONFIG_MAP` ou`API`.

Para ver as etapas para configurar o modo de autenticação para entradas de acesso, consulte Configurando entradas de acesso.

Selecione Criar entrada de acesso.

- Para o ARN principal do IAM, selecione a função do IAM que você criou para a automação do SSM na etapa anterior.
- Em Tipo, selecione `Standard`.

4. Adicione uma política de acesso:
   - Em Escopo do Access, selecione`Cluster`.
   - Em Nome da política, selecione`AmazonEKSAdminViewPolicy`.

   Escolha Add policy.

   Se você não estiver usando entradas de acesso para gerenciar as permissões da API Kubernetes, `aws-auth` ConfigMap atualize e crie uma associação de função entre seu usuário ou função do IAM. Certifique-se de que sua entidade do IAM tenha as seguintes permissões de API Kubernetes somente para leitura:
   - 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. Execute a automação AWSSupport-TroubleshootEbsCsiDriversForEks (console)
6. Selecione Execute automation (Executar automação).
7. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

  - Descrição: (Opcional) O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o SSM Automation execute as ações em seu nome. A função precisa ser adicionada à sua entrada de acesso ao cluster Amazon EKS ou à permissão RBAC para permitir chamadas de API do Kubernetes.
  - Tipo: `AWS::IAM::Role::Arn`
  - Example: `TroubleshootEbsCsiDriversForEks-SSM-Role`
- EksClusterName:
  - Descrição: O nome do cluster de destino do Amazon Elastic Kubernetes Service (Amazon EKS).
  - Tipo: `String`
- ApplicationPodName:
  - Descrição: O nome do pod do aplicativo Kubernetes com problemas com o driver CSI do Amazon EBS.
  - Tipo: `String`
- ApplicationNamespace:
  - Descrição: O namespace Kubernetes para o pod do aplicativo com problemas com o driver CSI do Amazon EBS.
  - Tipo: `String`
- EbsCsiControllerDeploymentName (Opcional):
  - Descrição: (Opcional) O nome da implantação do pod controlador CSI do Amazon EBS.
  - Tipo: `String`
  - Padrão: `ebs-csi-controller`
- EbsCsiControllerNamespace (Opcional):
  - Descrição: (Opcional) O namespace Kubernetes para o pod controlador CSI do Amazon EBS.
  - Tipo: `String`
  - Padrão: `kube-system`
- S3 BucketName (opcional):
  - Descrição: (Opcional) O nome do bucket de destino do Amazon S3 para o qual os registros de solução de problemas serão carregados.
  - Tipo: `AWS::S3::Bucket::Name`
- LambdaRoleArn (Opcional):

- Descrição: (Opcional) O ARN da função do IAM que permite que a AWS Lambda função acesse os AWS serviços e recursos necessários.
- Tipo: `AWS::IAM::Role::Arn`

Selecione Executar.

8. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução.

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Fluxos de trabalho de automação de suporte

Para obter mais informações sobre o Amazon EBS CSI Driver, consulte Amazon EBS CSI Driver.

Elastic Beanstalk

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Elastic Beanstalk Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-CollectElasticBeanstalkLogs
- AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming
- AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications
- AWSSupport-TroubleshootElasticBeanstalk

`AWSSupport-CollectElasticBeanstalkLogs`

Descrição

O `AWSSupport-CollectElasticBeanstalkLogs` runbook reúne arquivos de log AWS Elastic Beanstalk relacionados de uma Windows Server instância do Amazon Elastic Compute Cloud

(Amazon EC2) lançada pelo Elastic Beanstalk para ajudá-lo a solucionar problemas comuns. Enquanto a automação reúne os arquivos de log associados, são feitas alterações na estrutura do sistema de arquivos, incluindo a criação de diretórios temporários, a cópia dos arquivos de log nos diretórios temporários e a compactação dos arquivos de log em um arquivamento. Essa atividade pode resultar em um aumento `CPUUtilization` na EC2 instância da Amazon. Para obter mais informações sobre`CPUUtilization`, consulte Métricas de instância no Guia CloudWatch do usuário da Amazon.

Se especificar um valor para o parâmetro `S3BucketName`, a automação avaliará o status da política do bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Para ajudar na segurança dos registros coletados da sua EC2 instância Amazon, se o status da política `isPublic` estiver definido como ou se a `true` lista de controle de acesso (ACL) conceder `READ|WRITE` permissões ao grupo predefinido do `All Users` Amazon S3, os registros não serão carregados. Para obter mais informações sobre grupos predefinidos do Amazon S3, consulte Grupos predefinidos do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Se não for especificado um valor para o parâmetro `S3BucketName`, a automação carregará o pacote de log para o bucket padrão do Amazon S3 do Elastic Beanstalk na Região da AWS em que a automação é executada. O diretório é nomeado de acordo com a estrutura `elasticbeanstalk-` *`region`* `-` *`accountID`* a seguir. Os *`accountID`* valores *`region`* e serão diferentes com base na região em Conta da AWS que você executa a automação. O pacote de logs será salvo no diretório `resources/environments/logs/bundle/` *`environmentID`* `/` *`instanceID`* . Os *`instanceID`* valores *`environmentID`* e serão diferentes com base no seu ambiente do Elastic Beanstalk e na instância EC2 da Amazon da qual você está coletando registros.

Por padrão, o perfil de instância AWS Identity and Access Management (IAM) anexado às EC2 instâncias Amazon do ambiente do Elastic Beanstalk tem as permissões necessárias para carregar o pacote no bucket Amazon S3 padrão do Elastic Beanstalk para seu ambiente. Se você especificar um valor para o `S3BucketName` parâmetro, o perfil da instância anexado à EC2 instância da Amazon deverá permitir as `s3:PutObject` açõess`3:GetBucketAcl`,, `s3:GetBucketPolicys3:GetBucketPolicyStatus`, e para o bucket e o caminho especificados do Amazon S3.

> **Note**
>
> Essa automação requer pelo menos 500 MB de espaço em disco disponível no volume raiz do Amazon Elastic Block Store (Amazon EBS) anexado à sua instância da Amazon. EC2

Se não houver espaço em disco disponível suficiente no volume raiz, a automação será interrompida.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- EnvironmentId

  Tipo: String

  Descrição: (obrigatório) O ID do seu ambiente do Elastic Beanstalk do qual deseja coletar o pacote de logs.

- InstanceId

  Tipo: String

  (Obrigatório) O ID da EC2 instância da Amazon em seu ambiente do Elastic Beanstalk do qual você deseja coletar o pacote de registros.

- S3 BucketName

  Tipo: String

  (opcional) O bucket do Amazon S3 para o qual deseja fazer o upload dos logs arquivados.

- S3 BucketPath

  Tipo: String

  (opcional) O caminho do bucket do Amazon S3 para o qual deseja fazer o upload do pacote de log. Esse parâmetro será ignorado se um valor para o parâmetro `S3BucketName` não for especificado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`

Etapas do documento

- `aws:assertAwsResourceProperty`- Confirma que a EC2 instância da Amazon que você especifica no `InstanceId` parâmetro é gerenciada pela AWS Systems Manager.
- `aws:assertAwsResourceProperty`- Confirma que a EC2 instância da Amazon que você especifica no `InstanceId` parâmetro é uma Windows Server instância.
- `aws:runCommand` :Verifica se a instância faz parte de um ambiente do Elastic Beanstalk, se há espaço em disco suficiente para agrupar os logs e se o bucket do Amazon S3 para o qual os logs seriam enviados é público.
- `aws:runCommand` :Coleta os arquivos de log e carrega o arquivo no bucket do Amazon S3 especificado no parâmetro `S3BucketName` ou no bucket padrão do seu ambiente do Elastic Beanstalk se um valor não for especificado.

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

Descrição

O AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming runbook permite o registro no ambiente AWS Elastic Beanstalk (Elastic Beanstalk) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- EnvironmentId

  Tipo: String

  Descrição: (obrigatório) O ID do ambiente do Elastic Beanstalk no qual deseja habilitar o log.

Permissões obrigatórias do IAM

O parâmetro AutomationAssumeRole requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Etapas do documento

- `aws:executeAwsApi` :Permite o log no ambiente do Elastic Beanstalk especificado no parâmetro `EnvironmentId`.
- `aws:waitForAwsResourceProperty` :Espera que o status do ambiente mude para `Ready`.
- `aws:executeScript` :Verifica se o log foi habilitado no ambiente do Elastic Beanstalk.

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

Descrição

O `AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications` runbook habilita notificações para o ambiente AWS Elastic Beanstalk (Elastic Beanstalk) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- EnvironmentId

  Tipo: String

  Descrição: (obrigatório) O ID do ambiente do Elastic Beanstalk para o qual deseja habilitar notificações.
- TopicArn

  Tipo: String

  Descrição: (obrigatório) O ARN do tópico do Amazon Simple Notification Service (Amazon SNS) para o qual deseja enviar notificações.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

Etapas do documento

- `aws:executeAwsApi` :Habilita notificações para o ambiente do Elastic Beanstalk especificado no parâmetro `EnvironmentId`.
- `aws:waitForAwsResourceProperty` :Espera que o status do ambiente mude para `Ready`.
- `aws:executeScript` :Verifica se as notificações foram habilitadas para o ambiente do Elastic Beanstalk.

AWSSupport-TroubleshootElasticBeanstalk

Descrição

O `AWSSupport-TroubleshootElasticBeanstalk` runbook ajuda você a solucionar os possíveis motivos pelos quais seu AWS Elastic Beanstalk ambiente está em um estado `Degraded` ou`Severe`. Essa automação verifica os seguintes AWS recursos associados ao seu ambiente do Elastic Beanstalk:

- Detalhes de configuração para um balanceador de carga, AWS CloudFormation pilha, grupo Amazon Auto EC2 Scaling, instâncias do Amazon Elastic Compute Cloud (EC2Amazon) e nuvem privada virtual (VPC).
- Problemas de configuração de rede com as regras do grupo de segurança, tabelas de rotas e listas de controle de acesso à rede (ACLs) associadas às suas sub-redes.
- Verifica a conectividade com os endpoints do Elastic Beanstalk e o acesso público à Internet.
- Verifica o status do balanceador de carga.
- Verifica o status das EC2 instâncias da Amazon.
- Recupera um pacote de registros do seu ambiente do Elastic Beanstalk e, opcionalmente, carrega os arquivos para o. Suporte

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ApplicationName

  Tipo: String

  Descrição: (obrigatório) O nome da aplicação do Elastic Beanstalk.

- EnvironmentName

  Tipo: String

  Descrição: (obrigatório) O nome do seu ambiente do Elastic Beanstalk.

- AWSS3UploaderLink

  Tipo: String

  Descrição: (Opcional) Uma URL fornecida por você Suporte para fazer o upload do pacote de registros do seu ambiente do Elastic Beanstalk para o. Essa opção está disponível somente para clientes que compraram um Suporte plano e abriram um caso de Support.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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*

Etapas do documento

- aws:executeScript- Verifica se o diretor AWS Identity and Access Management (IAM) que iniciou a automação tem as permissões necessárias para realizar todas as ações definidas no runbook.
- aws:branch :Ramifica o fluxo de trabalho com base nos resultados da etapa anterior.
- aws:executeScript- Coleta informações sobre o ambiente do Elastic Beanstalk, incluindo o balanceador de carga, a pilha, o grupo Auto Scaling AWS CloudFormation , as instâncias da Amazon e a configuração da VPC. EC2
- aws:executeScript- Verifica problemas de conectividade de rede com as tabelas de rotas e ACLs associados às sub-redes em sua VPC.
- aws:executeScript- Verifica problemas de conectividade de rede com as regras do grupo de segurança associadas às suas EC2 instâncias da Amazon.
- aws:executeScript- Verifica as verificações de status das EC2 instâncias da Amazon.
- aws:executeScript :Gera um link para um pacote de logs do seu ambiente do Elastic Beanstalk.
- aws:executeScript- Carrega o pacote de registros para. Suporte
- aws:executeScript :Gera um relatório de itens de ação para ajudar a solucionar problemas que estejam afetando o status do ambiente do Elastic Beanstalk.

Elastic Load Balancing

AWS Systems Manager A automação fornece runbooks predefinidos para o Elastic Load Balancing. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-DropInvalidHeadersForALB
- AWS-EnableCLBAccessLogs
- AWS-EnableCLBConnectionDraining
- AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing
- AWSConfigRemediation-EnableELBDeletionProtection
- AWSConfigRemediation-EnableLoggingForALBAndCLB
- AWSSupport-TroubleshootCLBConnectivity
- AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing
- AWS-UpdateALBDesyncMitigationMode
- AWS-UpdateCLBDesyncMitigationMode

`AWSConfigRemediation-DropInvalidHeadersForALB`

Descrição

O runbook `AWSConfigRemediation-DropInvalidHeadersForALB` habilita que o application load balancer especificado remova cabeçalhos HTTP com cabeçalhos inválidos.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LoadBalancerArn

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do balanceador de carga para o qual deseja eliminar cabeçalhos inválidos.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeAwsApi` :Habilita a definição de descartar cabeçalhos inválidos para o balanceador de carga especificado no parâmetro `LoadBalancerArn`.
- `aws:executeScript` :Verifica se a definição de descartar cabeçalhos inválidos foi habilitada para o balanceador de carga especificado no parâmetro `LoadBalancerArn`.

AWS-EnableCLBAccessLogs

Descrição

O `AWS-EnableCLBAccessLogs` runbook permite registros de acesso para um Classic Load Balancer.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EmitInterval

  Tipo: inteiro

  Valores válidos: 5 | 60

  Padrão: 60

  Descrição: (Opcional) O intervalo para publicar os registros de acesso em minutos.
- LoadBalancerNames

  Tipo: String

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos Classic Load Balancers para os quais você deseja habilitar os registros de acesso.
- S3 BucketName

  Tipo: String

Descrição: (Obrigatório) O nome do bucket do Amazon Simple Storage Service (Amazon S3) onde os registros de acesso são armazenados.

- S3 BucketPrefix

  Tipo: String

  Descrição: (Opcional) A hierarquia lógica que você criou para seu bucket do Amazon S3, por exemplo. `my-bucket-prefix/prod` Se o prefixo não for fornecido, o log será colocado no nível raiz do bucket.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeAwsApi`- Habilita registros de acesso para os Classic Load Balancers que você especifica no `LoadBalancerNames` parâmetro.

Saídas

Ativar CLBAccess registros. SuccessesLoadBalancers - Lista de nomes de balanceadores de carga nos quais os registros de acesso foram habilitados com sucesso.

Ativar CLBAccess registros. FailedLoadBalancers - MapList dos nomes dos balanceadores de carga em que a ativação dos registros de acesso falhou e o motivo da falha.

AWS-EnableCLBConnectionDraining

Descrição

O `AWS-EnableCLBConnectionDraining` runbook permite a drenagem da conexão em um Classic Load Balancer (CLB) até o valor de tempo limite especificado. A drenagem da conexão permite que o CLB conclua solicitações em andamento feitas para instâncias que estão cancelando o registro ou não estão íntegras, com o tempo limite especificado sendo o tempo limite em que ele mantém as conexões ativas antes de relatar a instância como cancelada. Para obter mais

informações sobre a drenagem de conexão CLBs, consulte Configurar a drenagem de conexão para seu Classic Load Balancer no Guia do usuário para Classic Load Balancers.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LoadBalancerName

  Tipo: String

  Descrição: (Obrigatório) O nome do balanceador de carga no qual você deseja ativar a drenagem da conexão.
- ConnectionTimeout

  Tipo: inteiro

  Valores válidos: 1-3600

  Padrão: 300

  Descrição: (Obrigatório) O valor do tempo limite de conexão para o balanceador de carga. O valor do tempo limite pode ser definido entre 1 e 3600 segundos.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- ModifyLoadBalancerConnectionDraining (aws:executeAwsApi): ativa a drenagem da conexão e define o valor de tempo limite especificado para o balanceador de carga que você especificar.
- VerifyLoadBalancerConnectionDrainingEnabled(aws: assertAwsResource Propriedade): Verifica se a drenagem da conexão está habilitada para o balanceador de carga.
- VerifyLoadBalancerConnectionDrainingTimeout(aws: assertAwsResource Propriedade): verifica se o valor do tempo limite da conexão para o balanceador de carga corresponde ao valor especificado.

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

Descrição

O runbook `AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` habilita o balanceamento de carga entre zonas para o Classic Load Balancer (CLB) especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- LoadBalancerName

  Tipo: String

  Descrição: (obrigatório) O nome do CLB no qual deseja habilitar o balanceamento de carga entre zonas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeAwsApi` :Habilita o uso do balanceamento de carga entre zonas para o CLB especificado no parâmetro `LoadBalancerName`.
- `aws:assertAwsResourceProperty` :Verifica se o balanceamento de carga entre zonas foi habilitado no CLB.

AWSConfigRemediation-EnableELBDeletionProtection

Descrição

O runbook `AWSConfigRemediation-EnableELBDeletionProtection` habilita a proteção contra exclusão para o balanceador de carga elástico (ELB) especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LoadBalancerArn

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do ELB no qual deseja habilitar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeScript` :Habilita a proteção contra exclusão no ELB especificado no parâmetro `LoadBalancerArn`.

AWSConfigRemediation-EnableLoggingForALBAndCLB

Descrição

O `AWSConfigRemediation-EnableLoggingForALBAndCLB` runbook permite o registro do AWS Application Load Balancer ou de um Classic Load Balancer (CLB) especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LoadBalancerId

  Tipo: String

Descrição: (obrigatório) O nome do Classic Load Balancer ou o ARN do Application Load Balancer.

- S3 BucketName

  Tipo: String

  Descrição: (obrigatório) O nome do bucket do Amazon S3.

- S3 BucketPrefix

  Tipo: String

  Descrição: (opcional) A hierarquia lógica criada para o bucket do Amazon Simple Storage Service (Amazon S3), por exemplo, `my-bucket-prefix/prod`. Se o prefixo não for fornecido, o log será colocado no nível raiz do bucket.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeScript` :Habilita e verifica o log do Classic Load Balancer ou do Application Load Balancer.

AWSSupport-TroubleshootCLBConnectivity

Descrição

O `AWSSupport-TroubleshootCLBConnectivity` runbook ajuda você a solucionar problemas de conectividade entre instâncias do Classic Load Balancer (CLB) e do Amazon Elastic Compute Cloud (Amazon). EC2 Além disso, os problemas de conectividade entre um cliente e o CLB são analisados. Este runbook também analisa as verificações de integridade do CLB, verifica se as melhores práticas estão sendo seguidas e cria um painel de solução de problemas. Opcionalmente, você pode fazer

upload da saída de automação para um bucket do Amazon Simple Storage Service (Amazon S3). No entanto, esse runbook não é compatível com o upload de saída para buckets do S3 que são acessíveis ao público. Recomendamos criar um bucket do S3 temporário para essa automação.

> **Important**
>
> O uso desse runbook pode gerar cobranças pelo painel criado. Para obter mais informações, consulte Amazon CloudWatch Pricing

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InvestigationType

  Tipo: String

  Valores válidos: Best Practices | Connectivity Issues | Troubleshooting Dashboard

  Descrição: (obrigatório) As operações que deseja que o runbook execute.

- LoadBalancerName

  Tipo: String

  Descrição: (obrigatório) O nome do CLB.

- S3Location

  Tipo: String

  Descrição: (opcional) O nome do bucket do S3 para o qual enviar os resultados da automação. Não há suporte para buckets acessíveis publicamente. Se seu bucket do S3 usa criptografia do lado do servidor, o usuário ou a função que executa essa automação deve ter permissões de `kms:GenerateDataKey` para a chave AWS KMS .

- S3 LocationPrefix

  Tipo: String

  Descrição: (opcional) O prefixo de chave (subpasta) do Amazon S3 para o qual deseja fazer o upload da saída de automação. O formato de saída é armazenado no seguinte formato: amzn-s3-demo-bucket/*S3LocationPrefix*/{{}} _ {{automation:*InvestigationType*}} .txt. *EXECUTION_ID*

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeScript :Verifica se o CLB especificado no parâmetro LoadBalancerName existe.
- aws:branch :Ramificações com base no valor especificado para o parâmetro InvestigationType.
- aws:executeScript :Executa verificações de conectividade com o CLB.
- aws:executeScript :Verifica se a configuração do CLB segue as melhores práticas do Elastic Load Balancing.
- aws:executeScript- Cria um CloudWatch painel da Amazon para seu CLB.
- aws:executeScript :Cria um arquivo de texto com os resultados da automação e o carrega no bucket do Amazon S3 especificado no parâmetro S3Location.

Saídas

RunBestPractices.Resumo

RunConnectivityChecks.Resumo

CreateTroubleshootingDashboard.Saída

UploadOutputToS3. Saída

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

Descrição

O runbook `AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` habilita o balanceamento de carga entre zonas para o network load balancer (NLB) especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- LoadBalancerArn

Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do NLB no qual deseja habilitar o balanceamento de carga entre zonas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- `aws:executeAwsApi` :Habilita o balanceamento de carga entre zonas para o NLB especificado no parâmetro `LoadBalancerArn`.
- `aws:executeScript`: Verifica se o balanceamento de carga entre zonas foi habilitado no NLB.

AWS-UpdateALBDesyncMitigationMode

Descrição

O `AWS-UpdateALBDesyncMitigationMode` runbook atualizará o modo de mitigação de dessincronização em um Application Load Balancer (ALB) para o modo de mitigação especificado. O modo de mitigação de dessincronização determina como o balanceador de carga lida com solicitações que podem representar um risco de segurança para seu aplicativo.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LoadBalancerArn

  Tipo: String

  Descrição: (Obrigatório) O nome de recurso da Amazon (ARN) do ALB do qual você deseja modificar o modo de mitigação de dessincronização.
- DesyncMitigationMode

  Tipo: String

  Valores válidos: monitor | defensivo | mais rigoroso

  Descrição: (Obrigatório) O modo de mitigação que você deseja que o ALB use. Para obter informações sobre os modos de mitigação de dessincronização, consulte Modo de mitigação de dessincronização no Guia do usuário para balanceadores de carga de aplicativos.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- VerifyLoadBalancerType (aws: assertAwsResource Property) - Verifica se o valor especificado para o parâmetro `LoadBalancerArn` de entrada é para um balanceador de carga do aplicativo antes de prosseguir para a próxima etapa.
- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - Atualiza o ALB para usar o especificado`DesyncMitigationMode`.
- VerifyLoadBalancerDesyncMitigationMode (aws:ExecuteScript) - Verifica se o modo de mitigação de dessincronização foi atualizado para o ALB de destino.

Saídas

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Carga útil da mensagem do script verificando a modificação em seu ALB.

AWS-UpdateCLBDesyncMitigationMode

Descrição

O `AWS-UpdateCLBDesyncMitigationMode` runbook atualizará o modo de mitigação de dessincronização em um Classic Load Balancer (CLB) para o modo de mitigação especificado. O modo de mitigação de dessincronização determina como o balanceador de carga lida com solicitações que podem representar um risco de segurança para seu aplicativo.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- LoadBalancerName

  Tipo: String

  Descrição: (Obrigatório) O nome do CLB do qual você deseja modificar o modo de mitigação de dessincronização.

- DesyncMitigationMode

  Tipo: String

  Valores válidos: monitor | defensivo | mais rigoroso

  Descrição: (Obrigatório) O modo de mitigação que você deseja que o CLB use. Para obter informações sobre os modos de mitigação de dessincronização, consulte Modo de mitigação de dessincronização no Guia do usuário para balanceadores de carga de aplicativos.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

Etapas do documento

- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - Atualiza o CLB para usar o especificado`DesyncMitigationMode`.
- VerifyLoadBalancerDesyncMitigationMode (aws:ExecuteScript) - Verifica se o modo de mitigação de dessincronização foi atualizado para o CLB de destino.

Saídas

VerifyLoadBalancerDesyncMitigationMode. ModificationResult - Carga útil da mensagem do script verificando a modificação em seu CLB.

Amazon EMR

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon EMR. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-AnalyzeEMRLogs
- AWSSupport-DiagnoseEMRLogsWithAthena

`AWSSupport-AnalyzeEMRLogs`

Descrição

Esse runbook ajuda a identificar erros ao executar um trabalho em um cluster do Amazon EMR. O runbook analisa uma lista de logs definidos no sistema de arquivos e procura uma lista de palavras-chave predefinidas. Essas entradas de registro são usadas para criar CloudWatch eventos da Amazon Events para que você possa realizar as ações necessárias com base nos eventos. Opcionalmente, o runbook publica entradas de registro no grupo de CloudWatch registros Amazon Logs de sua escolha. Atualmente, esse runbook procura os seguintes erros e padrões nos arquivos de log:

- container_out_of_memory :O contêiner YARN ficou sem memória, o trabalho em execução pode falhar.
- yarn_nodemanager_health: O nó de TAREFA ou CORE está com pouco espaço em disco e não poderá executar tarefas.
- node_state_change: o nó de TAREFA ou CORE não pode ser acessado pelo nó PRINCIPAL.
- step_failure: Uma etapa do EMR falhou.
- no_core_nodes_running: Nenhum nó CENTRAL está em execução no momento, o cluster não está íntegro.
- hdfs_missing_blocks: Há blocos HDFS ausentes que podem levar à perda de dados.

- hdfs_high_util: A utilização do HDFS é alta, o que pode afetar as tarefas e a integridade do cluster.
- instance_controller_restart: O processo do Instance-Controller foi reiniciado. Esse processo é essencial para a integridade do cluster.
- instance_controller_restart_legacy: O processo do Instance-Controller foi reiniciado. Esse processo é essencial para a integridade do cluster.
- high_load: A alta média de carga detectada pode afetar os relatórios de integridade do nó ou resultar em tempos limite ou lentidão.
- yarn_node_blacklisted: O nó de TAREFA ou CORE foi colocado na lista negra do YARN para executar tarefas.
- yarn_node_lost: O nó de TAREFA ou CORE foi marcado como PERDIDO pelo YARN, possíveis problemas de conectividade.

As instâncias associadas ao `ClusterID` que você especifica devem ser gerenciadas pelo AWS Systems Manager. Você pode executar essa automação uma vez, programar a automação para ser executada em um intervalo de tempo específico ou remover uma programação criada anteriormente por uma automação. Este runbook é compatível com as versões 5.20 a 6.30 do Amazon EMR.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- ClusterID

  Tipo: String

  Descrição: (obrigatório) O ID do cluster cujos logs de nós que deseja analisar.

- Operação

  Tipo: String

  Valores válidos: Run Once | Schedule | Remove Schedule

  Descrição: (obrigatório) A operação a ser executada no cluster.

- IntervalTime

  Tipo: String

  Valores válidos: 5 minutes | 10 minutes | 15 minutes

  Descrição: (opcional) A duração do tempo entre a execução da automação. Esse parâmetro só é aplicável se for especificado `Schedule` para o parâmetro `Operation`.

- LogToCloudWatchLogs

  Tipo: String

  Valores válidos: sim | não

  Descrição: (Opcional) Se você especificar `yes` o valor desse parâmetro, a automação criará um grupo de CloudWatch registros de registros com o nome especificado no `CloudWatchLogGroup` parâmetro para armazenar todas as entradas de registro correspondentes.

- CloudWatchLogGroup

  Tipo: String

  Descrição: (Opcional) O nome do grupo de CloudWatch registros de registros em que você deseja armazenar todas as entradas de registro correspondentes. Esse parâmetro só é aplicável se for especificado `yes` para o parâmetro `LogToCloudWatchLogs`.

- CreateLogInsightsDashboard

Tipo: String

Valores válidos: sim | não

Descrição: (Opcional) Se você especificar`yes`, o CloudWatch painel será criado se ainda não existir. Esse parâmetro só é aplicável se for especificado `yes` para o parâmetro `LogToCloudWatchLogs`.

- CreateMetricFilters

  Tipo: String

  Valores válidos: sim | não

  Descrição: (Opcional) Especifique `yes` se você deseja criar filtros métricos para o grupo de CloudWatch registros de registros. Esse parâmetro só é aplicável se for especificado `yes` para o parâmetro `LogToCloudWatchLogs`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeAwsApi :Coleta informações sobre o cluster do Amazon EMR especificado no parâmetro ClusterID.
- aws:branch :Ramificações com base na entrada.
  - Se a operação fornecida for Run Once ou Schedule:
    - aws:assertAwsResourceProperty :Verifica se o cluster está disponível.
    - aws:executeAwsApi- Reúne todas IDs as instâncias em execução no cluster.
    - aws:assertAwsResourceProperty :Verifica se o SSM Agent está sendo executado em todas as instâncias do cluster.
    - aws:branch :Ramificações com base na especificação de executar a automação uma vez ou em um cronograma.
      - Se a operação fornecida for Run Once:
        - aws:branch :Ramificações com base no valor especificado para o parâmetro LogToCloudWatchLogs.

- Se o valor de `LogToCloudWatchLogs` for `yes`:
  - `aws:executeScript`- Verifica se `CloudWatchLogGroup` já existe um grupo de CloudWatch registros de registros com o nome especificado no parâmetro. Caso contrário, o grupo será criado com o nome especificado.
  - `aws:branch` :Ramificações com base no valor especificado para o parâmetro `CreateMetricFilters`.
    - Se o valor de `CreateMetricFilters` for `yes`:
      - `aws:executeAwsApi` :12 etapas são executadas para cada filtro métrico
      - `aws:branch` :Ramificações com base no valor especificado para o parâmetro `CreateLogInsightsDashboard`.
        - Se o valor de `CreateLogInsightsDashboard` for `yes`:
          - `aws:executeAwsApi`- Cria um CloudWatch painel com o mesmo nome especificado no `CloudWatchLogGroup` parâmetro, caso ele ainda não exista.
        - Se o valor de `CreateLogInsightsDashboard` for no:
          - `aws:runCommand` :Executa um script de shell para encontrar padrões de log em cada instância no cluster.
    - Se o valor de `CreateMetricFilters` for no:
      - `aws:branch` :Ramificações com base no valor especificado no parâmetro `CreateLogInsightsDashboard`.
        - Se o valor de `CreateLogInsightsDashboard` for `yes`:
          - `aws:executeAwsApi`- Cria um CloudWatch painel com o mesmo nome especificado no `CloudWatchLogGroup` parâmetro, caso ele ainda não exista.
        - Se o valor de `CreateLogInsightsDashboard` for no:
          - `aws:runCommand` :Executa um script de shell para encontrar padrões de log em cada instância no cluster.
- Se o valor de `LogToCloudWatchLogs` for no:
  - `aws:executeAwsApi` :Executa um script de shell para encontrar padrões de log em cada instância no cluster.
- Se a operação fornecida for `Schedule`:

    - `aws:createStack`- Cria um EventBridge evento da Amazon que tem como alvo esse runbook.
- Se a operação fornecida for `Remove Schedule`:
    - `aws:executeAwsApi` :Verifica se existe um cronograma para o cluster.
    - `aws:deleteStack` :Exclui a programação.

Saídas

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstances.Instância IDs

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists.saída

FindLogPatternOnEMRNode.CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

Descrição

O `AWSSupport-DiagnoseEMRLogsWithAthena` runbook ajuda a diagnosticar os registros do Amazon EMR usando o Amazon Athena em integração com o Data Catalog. AWS Glue O Amazon Athena é usado para consultar os arquivos de log do Amazon EMR para contêineres, registros de nós ou ambos, com parâmetros opcionais para intervalos de datas específicos ou pesquisas baseadas em palavras-chave.

O runbook pode recuperar automaticamente a localização do log do Amazon EMR para um cluster existente, ou você pode especificar a localização do log do Amazon S3. Para analisar os registros, o runbook:

- Cria um AWS Glue banco de dados e executa consultas da Amazon Athena Data Definition Language (DDL) no local de log Amazon S3 do Amazon EMR para criar tabelas para logs de cluster e uma lista de problemas conhecidos.

- Executa consultas de linguagem de manipulação de dados (DML) para pesquisar padrões de problemas conhecidos nos registros do Amazon EMR. As consultas retornam uma lista dos problemas detectados, sua contagem de ocorrências e o número de palavras-chave correspondentes por caminho de arquivo do Amazon S3.
- Os resultados são enviados para um bucket do Amazon S3 que você especifica sob o prefixo. `saw_diagnose_EMR_known_issues`
- O runbook retorna os resultados da consulta do Amazon Athena, destacando descobertas, recomendações e referências aos artigos do Amazon Knowledge Center (KC) provenientes de um subconjunto predefinido.
- Em caso de conclusão ou falha, o AWS Glue banco de dados e os arquivos de problemas conhecidos enviados para o bucket do Amazon S3 são excluídos.

Como funciona?

`AWSSupport-DiagnoseEMRLogsWithAthena`Realize análises dos registros do Amazon EMR usando o Amazon Athena para detectar erros e destacar descobertas, recomendações e artigos relevantes do Knowledge Center.

O runbook executa as seguintes etapas:

- Obtenha a localização do log do cluster do Amazon EMR usando o ID do cluster ou insira a localização do Amazon S3 para recuperar a localização e o tamanho do log.
- Forneça uma estimativa de custos do Athena com base no tamanho da localização do registro.
- Obtenha aprovação para continuar solicitando a aprovação dos diretores designados do IAM antes de executar as consultas do Athena e continuar com as próximas etapas.
- Faça upload de problemas conhecidos para o bucket especificado do Amazon S3, crie um AWS Glue banco de dados e tabelas.
- Execute consultas do Athena nos dados de registros do Amazon EMR. As consultas podem pesquisar por intervalo de datas, palavras-chave, ambos os critérios ou ser executadas sem filtros com base nas entradas fornecidas.
- Analise os resultados para destacar descobertas, recomendações e artigos relevantes de KC.
- Links de saída para resultados de consultas DML do Amazon Athena.
- Limpe o ambiente removendo o banco de dados criado, as tabelas e os problemas conhecidos carregados.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

O AutomationAssumeRole parâmetro requer as seguintes ações para usar o runbook com êxito:

- Atena: GetQueryExecution
- Atena: StartQueryExecution
- Atena: GetPreparedStatement
- Atena: CreatePreparedStatement
- cola: GetDatabase
- cola: CreateDatabase
- cola: DeleteDatabase
- cola: CreateTable
- cola: GetTable
- cola: DeleteTable
- redução do mapa elástico: DescribeCluster
- s3: ListBucket
- s3: GetBucketVersioning
- s3: ListBucketVersions
- s3: GetBucketPublicAccessBlock
- s3: GetBucketPolicyStatus
- s3: GetObject
- s3: GetBucketLocation
- preços: GetProducts
- preços: GetAttributeValues
- preços: DescribeServices

- preços: ListPriceLists

> **Important**
>
> Para restringir o acesso somente aos recursos necessários para essa automação, anexe a política a seguir à função do IAM que confia no Serviço SSM. Substitua a partição, a região e a conta pelos valores apropriados para a partição, a região e o número da conta em que o livro de execução é executado.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticmapreduce:DescribeCluster",
        "glue:GetDatabase",
        "athena:GetQueryExecution",
        "athena:StartQueryExecution",
        "athena:GetPreparedStatement",
        "athena:CreatePreparedStatement",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:ListBucketVersions",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "pricing:GetProducts",
        "pricing:GetAttributeValues",
        "pricing:DescribeServices",
        "pricing:ListPriceLists"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RestrictPutObjects",
      "Effect": "Allow",
      "Action": [
```

```
        "s3:PutObject"
      ],
      "Resource": [
        "arn:{Partition}:s3:::*/*/results/*",
        "arn:{partition}:s3:::*/*/saw_diagnose_emr_known_issues/*"
      ]
    },
    {
      "Sid": "RestrictDeleteAccess",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": [
        "arn:{Partition}:s3:::*/*/saw_diagnose_emr_known_issues/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource": [
        "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/*",
        "arn:{Partition}:glue:{Region}:{Account}:userDefinedFunction/
saw_diagnose_emr_database_*/*",
        "arn:{Partition}:glue:{Region}:{Account}:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:CreateTable",
        "glue:GetTable",
        "glue:DeleteTable"
      ],
      "Resource": [
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
saw_diagnose_emr_known_issues",
```

```
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
saw_diagnose_emr_logs_table",
        "arn:{Partition}:glue:{Region}:{Account}:table/saw_diagnose_emr_database_*/
j_*",
        "arn:{Partition}:glue:{Region}:{Account}:database/saw_diagnose_emr_database_*",
        "arn:{Partition}:glue:{Region}:{Account}:catalog"
      ]
    }
  ]
}
```

Instruções

Siga estas etapas para configurar a automação:

1. Navegue AWSSupport-DiagnoseEMRLogsWithAthena AWS Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - ClusterID (obrigatório):

     O ID do cluster do Amazon EMR.
   - S3 LogLocation (opcional):

     A localização do log do Amazon S3 do Amazon EMR. Insira a localização do URL no estilo Path do Amazon S3, por exemplo:. `s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/` Forneça esse parâmetro se o cluster do Amazon EMR tiver sido encerrado por mais de dias. `30`
   - S3 BucketName (obrigatório):

     O nome do bucket do Amazon S3 para fazer o upload de uma lista de problemas conhecidos e a saída das consultas do Amazon Athena. O bucket deve ter o Block Public Access ativado e estar na mesma AWS região e conta do cluster do Amazon EMR.
   - Aprovadores (obrigatório):

A lista de diretores AWS autenticados que podem aprovar ou rejeitar a ação. Você pode especificar os principais usando qualquer um dos seguintes formatos: nome de usuário, ARN do usuário, ARN da função do IAM ou ARN da função de suposição do IAM. O número máximo de aprovadores é 10.

- FetchNodeLogsOnly (Opcional):

  Se configurada como`true`, a automação diagnostica os registros de contêineres do aplicativo Amazon EMR. O valor padrão é `false`.

- FetchContainersLogsOnly(Opcional):

  Se configurada como`true`, a automação diagnostica os registros de contêineres do Amazon EMR. O valor padrão é `false`.

- EndSearchDate (Opcional):

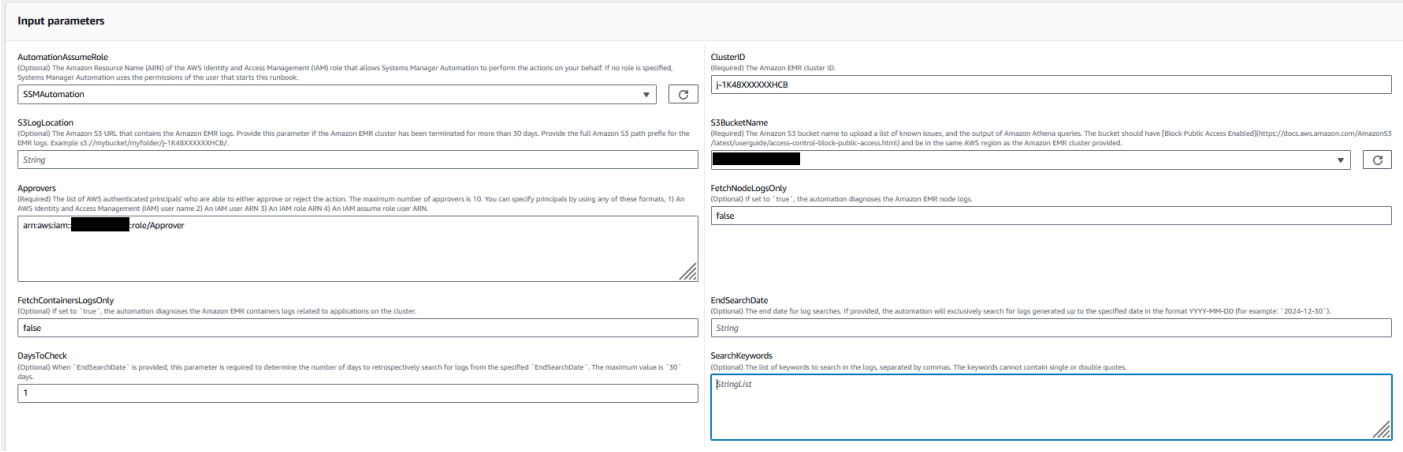
  A data de término das pesquisas de registros. Se fornecida, a automação pesquisará exclusivamente os registros gerados até a data especificada no formato YYYY-MM-DD (por exemplo:`2024-12-30`).

- DaysToCheck (Opcional):

  Quando `EndSearchDate` fornecido, esse parâmetro é necessário para determinar o número de dias para pesquisar retrospectivamente os registros do especificado. `EndSearchDate` O valor máximo é de `30` dias. O valor padrão é `1`.

- SearchKeywords (Opcional):

  A lista de palavras-chave a serem pesquisadas nos registros, separadas por vírgulas. As palavras-chave não podem conter aspas simples ou duplas.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - getLogLocation:

     Recupera a localização do log do Amazon S3 consultando o ID do cluster do Amazon EMR especificado. Se a automação não conseguir consultar a localização do log a partir do ID do cluster do Amazon EMR, o runbook usa o `S3LogLocation` parâmetro de entrada.
   - branchOnValidRegistro:

     Verifica a localização dos registros do Amazon EMR. Se a localização for válida, faça uma estimativa dos custos potenciais do Amazon Athena ao executar consultas nos registros do Amazon EMR.
   - estimateAthenaCosts:

     Determina o tamanho dos registros do Amazon EMR e fornece uma estimativa de custo para a execução de escaneamentos do Athena no conjunto de dados de log. Para regiões não comerciais (não AWS partições), essa etapa fornece apenas o tamanho do log sem estimar os custos. Os custos podem ser calculados usando a documentação de preços do Athena na região especificada.
   - Aprovar a automação:

     Aguarda a aprovação dos diretores designados do IAM para prosseguir com as próximas etapas da automação. A notificação de aprovação contém o custo estimado do escaneamento do Amazon Athena nos registros do Amazon EMR e detalhes sobre os recursos que estão sendo provisionados pela automação.
   - uploadKnownIssuesExecuteAthenaQueries:

     Carrega os problemas conhecidos predefinidos no bucket do Amazon S3 especificado no parâmetro. `S3BucketName` Cria AWS Glue banco de dados e tabelas. Executa consultas do Amazon Athena no banco de dados com base AWS Glue nos parâmetros de entrada.
   - getQueryExecutionStatus:

     Espera até que a execução da consulta do Amazon Athena esteja `SUCCEEDED` pronta. A consulta DML do Amazon Athena pesquisa erros e exceções nos logs do cluster do Amazon EMR.
   - analyzeAthenaResults:

Analisa os resultados do Amazon Athena para fornecer descobertas, recomendações e artigos do Knowledge Center (KC) provenientes de um conjunto predefinido de mapeamentos.

- getAnalyzeResultsConsulta 1: ExecutionStatus

  Espera até que a execução da consulta esteja em andamentoSUCCEEDED. A consulta DML do Amazon Athena analisa os resultados da consulta DML anterior. Essa consulta de análise retornará exceções correspondentes com resoluções e artigos KC

- getAnalyzeResultsConsulta 2: ExecutionStatus

  Espera até que a execução da consulta esteja em andamentoSUCCEEDED. A consulta DML do Amazon Athena analisa os resultados da consulta DML anterior. Essa consulta de análise retornará uma lista de exceções/erros detectados em cada caminho de log do Amazon S3.

- printAthenaQueriesMensagem:

  Imprime links para os resultados das consultas DML do Amazon Athena.

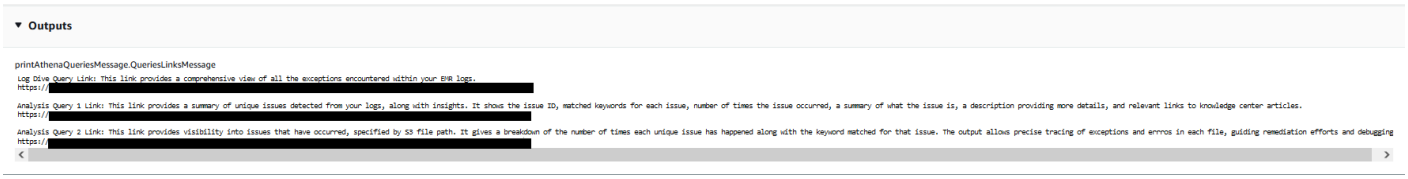
- Recursos de limpeza:

  Limpa os recursos excluindo o AWS Glue banco de dados criado e exclui arquivos de problemas conhecidos que foram criados no bucket de registros do Amazon EMR.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

   A saída fornece três links para os resultados da consulta do Athena:

   - Lista de todos os erros e exceções frequentes encontrados nos registros do cluster do Amazon EMR, junto com os locais de log correspondentes (prefixo Amazon S3).
   - Resumo das exceções exclusivas conhecidas que correspondem aos registros do Amazon EMR, junto com as resoluções recomendadas e os artigos do KC para ajudar na solução de problemas.
   - Detalhes sobre onde erros e exceções específicos aparecem nos caminhos de log do Amazon S3, para apoiar diagnósticos adicionais.



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- Consulte Solução de problemas de clusters do Amazon EMR para obter mais informações

OpenSearch Serviço Amazon

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon OpenSearch Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-DeleteOpenSearchDomain
- AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain
- AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups
- AWSSupport-TroubleshootOpenSearchRedYellowCluster
- AWSSupport-TroubleshootOpenSearchHighCPU

`AWSConfigRemediation-DeleteOpenSearchDomain`

Descrição

O `AWSConfigRemediation-DeleteOpenSearchDomain` runbook exclui um determinado domínio do Amazon OpenSearch Service usando a DeleteDomainAPI.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- DomainName

  Tipo: String

  Valores permitidos: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  Descrição: (Obrigatório) O nome do domínio do Amazon OpenSearch Service que você deseja excluir.
- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DeleteDomain`
- `es:DescribeDomain`

Etapas do documento

- `aws:executeScript`- Aceita o nome OpenSearch de domínio do Amazon Service como entrada, o exclui e verifica a exclusão.

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

Descrição

O AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain runbook é ativado EnforceHTTPS em um determinado domínio do Amazon OpenSearch Service usando a UpdateDomainConfigAPI.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- DomainName

  Tipo: String

  Valores permitidos: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  Descrição: (Obrigatório) O nome do domínio do Amazon OpenSearch Service que você deseja usar para aplicar HTTPS.
- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Etapas do documento

- `aws:executeScript`- Ativa a opção de `EnforceHTTPS` endpoint no domínio do Amazon OpenSearch Service que você especifica no `DomainName` parâmetro.

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

Descrição

O `AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups` runbook atualiza a configuração do grupo de segurança em um determinado domínio do Amazon OpenSearch Service usando a UpdateDomainConfigAPI.

> **Note**
>
> AWS Os grupos de segurança só podem ser aplicados aos domínios do Amazon OpenSearch Service configurados para acesso à Amazon Virtual Private Cloud (VPC), e não aos domínios do Amazon OpenSearch Service configurados para acesso público.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- DomainName

  Tipo: String

  Descrição: (Obrigatório) O nome do domínio do Amazon OpenSearch Service que você deseja usar para atualizar grupos de segurança.
- SecurityGroupList

  Tipo: StringList

  Descrição: (Obrigatório) O grupo de segurança IDs que você deseja atribuir ao domínio do Amazon OpenSearch Service.
- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

Etapas do documento

- `aws:executeScript`- Atualiza a configuração do grupo de segurança no domínio do Amazon OpenSearch Service que você especifica no `DomainName` parâmetro.

AWSSupport-TroubleshootOpenSearchRedYellowCluster

Descrição

`AWSSupport-TroubleshootOpenSearchRedYellowCluster`o runbook de automação é usado para identificar a causa do status de integridade do cluster vermelho ou amarelo e orientá-lo na alteração do cluster de volta para verde.

Como funciona?

O runbook `AWSSupport-TroubleshootOpenSearchRedYellowCluster` ajuda você a solucionar a causa do cluster vermelho ou amarelo e fornece as próximas etapas para resolver esse problema analisando a configuração do cluster e a utilização de recursos.

O runbook executa as seguintes etapas:

- Chama a DescribeDomainAPI no domínio de destino para obter a configuração do cluster.
- Verifica se o domínio do OpenSearch Serviço é baseado na Internet (público) ou na Amazon Virtual Private Cloud (VPC).
- Cria uma AWS Lambda função pública ou baseada no Amazon VPC, dependendo da configuração do cluster. Observação: a função Lambda contém o código de solução de problemas que executa o OpenSearch Serviço APIs no cluster para determinar por que o cluster está no estado vermelho ou amarelo.
- Exclui a função Lambda.
- Exibe as verificações realizadas e as próximas etapas recomendadas para resolver o problema do cluster vermelho ou amarelo.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

O `LambdaExecutionRole` parâmetro requer as seguintes ações para usar o runbook com êxito:

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DeleteNetworkInterface`

Visão geral da `LambdaExecutionRole` política:

Veja a seguir um exemplo de uma função de execução AWS Identity and Access Management (função IAM) da função Lambda que concede à função permissão para acessar AWS serviços e recursos exigidos por esse runbook. Para obter mais informações, consulte Função de execução do Lambda.

> **Note**
>
> O`ec2:DescribeNetworkInterfaces`,`ec2:CreateNetworkInterface`, e só `ec2:DeleteNetworkInterface` são necessários se seu cluster de OpenSearch serviços for baseado em Amazon VPC para permitir que a função Lambda crie e gerencie as interfaces de rede Amazon VPC. Para obter mais informações, consulte Conectando redes externas a recursos em uma função de execução do Amazon VPC e do Lambda.

```
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": "es:ESHttpGet",
                    "Resource": [
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-
name>/",
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cluster/health",
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cat/indices",
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cat/allocation",
                        "arn:<partition>:es:<region>:<account-id>:domain/<domain-name>/
_cluster/allocation/explain"
                    ]
                },
                {
                    "Condition": {
                        "ArnLikeIfExists": {
                            "ec2:Vpc": "arn:<partition>:ec2:<region>:<account-id>:vpc/
<vpc_id>"
```

```
                    }
                },
                "Action": [
                    "ec2:DeleteNetworkInterface",
                    "ec2:CreateNetworkInterface",
                    "ec2:DescribeNetworkInterfaces",
                    "ec2:UnassignPrivateIpAddresses",
                    "ec2:AssignPrivateIpAddresses"
                ],
                "Resource": "*",
                "Effect": "Allow"
            }

        ]
    }
```

Instruções

Siga estas etapas para configurar a automação:

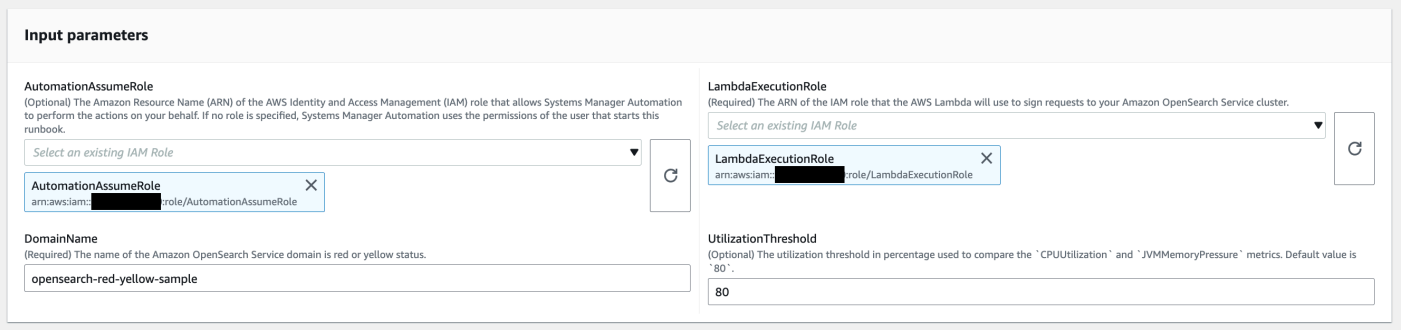
1. Navegue até o AWSSupport-TroubleshootOpenSearchRedYellowClusterno AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - LambdaExecutionRole (Obrigatório):

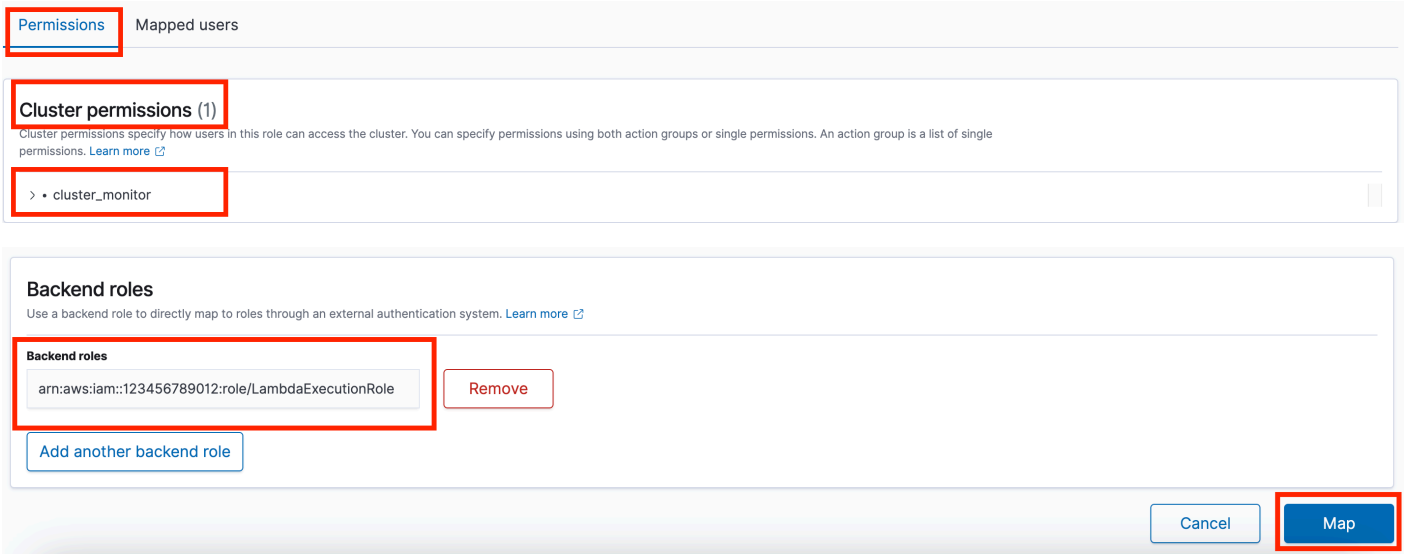
     O ARN da função do IAM que o Lambda usará para assinar solicitações no seu cluster do Amazon Service. OpenSearch
   - DomainName (Obrigatório):

     O nome do domínio do OpenSearch serviço com o status de integridade do cluster vermelho ou amarelo.
   - UtilizationThreshold (Opcional):

A porcentagem do limite de utilização usada para comparar as métricas CPUUtilization e de JVMMemory pressão. O valor padrão é 80.



4. Se você ativou o controle de acesso refinado em um cluster de OpenSearch serviços, certifique-se de que o arn da `LambdaExecutionRole` função esteja mapeado para uma função com pelo menos permissão. `cluster_monitor`



5. Selecione Executar.
6. A automação é iniciada.
7. O runbook de automação realiza as seguintes etapas:
   - GetClusterConfiguration:

     Busca a configuração do cluster OpenSearch de serviços.
   - Crie AWSLambdaFunctionStack:

     Cria uma função Lambda temporária em sua conta usando. AWS CloudFormation A função Lambda é usada para executar o OpenSearch Serviço. APIs
   - WaitForAWSLambdaFunctionStack:

Espera que a CloudFormation pilha seja concluída.

- GetClusterMetricsFromCloudWatch:

  Obtém as métricas relacionadas ao cluster Amazon CloudWatch ClusterStatus CPUUtilization,, e JVMMemory Pressure OpenSearch Service e sua data de criação.

- RunOpenSearchAPIs:

  Usa a função Lambda para chamar o OpenSearch Serviço APIs e analisar os dados das métricas do cluster para diagnosticar a causa do status do cluster vermelho ou amarelo.

- Excluir AWSLambdaFunctionStack:

  Exclui a função Lambda criada por essa automação em sua conta.

8. Depois de concluído, revise a seção Outputs para obter os resultados detalhados da execução.

   - RootCause:

     Fornece uma visão geral da causa identificada para que a integridade do cluster esteja no estado vermelho ou amarelo.

   - IssueDescription:

     Fornece detalhes sobre por que o cluster está no estado vermelho ou amarelo e as possíveis etapas para retornar o cluster ao estado verde.

Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- Consulte Solução de problemas do Amazon OpenSearch Service para obter mais informações

AWSSupport-TroubleshootOpenSearchHighCPU

Descrição

O AWSSupport-TroubleshootOpenSearchHighCPU runbook fornece uma solução automatizada para coletar dados de diagnóstico de um domínio do Amazon OpenSearch Service para solucionar problemas de alta CPU.

Como funciona?

O AWSSupport-TroubleshootOpenSearchHighCPU runbook ajuda a solucionar problemas de alta utilização da CPU no domínio do Amazon OpenSearch Service.

O runbook executa as seguintes etapas:

- Executa a DescribeDomainAPI no domínio fornecido do Amazon OpenSearch Service para obter os metadados do cluster.
- Verifica se o domínio do Amazon OpenSearch Service é público ou baseado no Amazon VPC e, com a ajuda de AWS CloudFormation, cria uma função pública ou baseada no Amazon AWS Lambda VPC.
- A função Lambda busca dados de diagnóstico dos domínios do Amazon OpenSearch Service.
- Usa uma máquina de AWS Step Functions estado para orquestrar várias execuções de funções Lambda para coletar dados mais abrangentes.
- Armazena os dados coletados em um grupo de CloudWatch registros da Amazon por 24 horas por padrão.
- Exclui os recursos criados, exceto o grupo de CloudWatch registros.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

O LambdaExecutionRole parâmetro requer as seguintes ações para usar o runbook com êxito:

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface
- logs:CreateLogStream
- logs:PutLogEvents

A função de execução do Lambda concede à função permissão para acessar AWS serviços e recursos exigidos por esse runbook. Para obter mais informações, consulte Função de execução do Lambda.

> **Note**
>
> Osec2:DescribeNetworkInterfaces,ec2:CreateNetworkInterface, e só ec2:DeleteNetworkInterface são necessários se seu cluster de OpenSearch serviços for baseado em Amazon VPC para permitir que a função Lambda crie e gerencie as interfaces de rede Amazon VPC. Para obter mais informações, consulte Conectando redes externas a recursos em uma função de execução do Amazon VPC e do Lambda.

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até o AWSSupport-TroubleshootOpenSearchHighCPUno AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

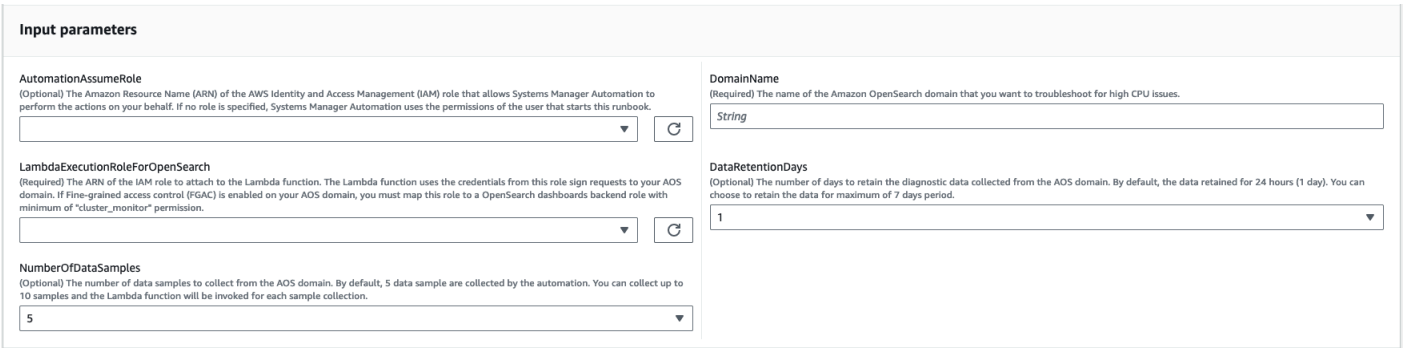
     O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - DomainName (Obrigatório):

     O nome do domínio do Amazon OpenSearch Service que você deseja solucionar para problemas de alta CPU.
   - LambdaExecutionRoleForOpenSearch(Obrigatório):

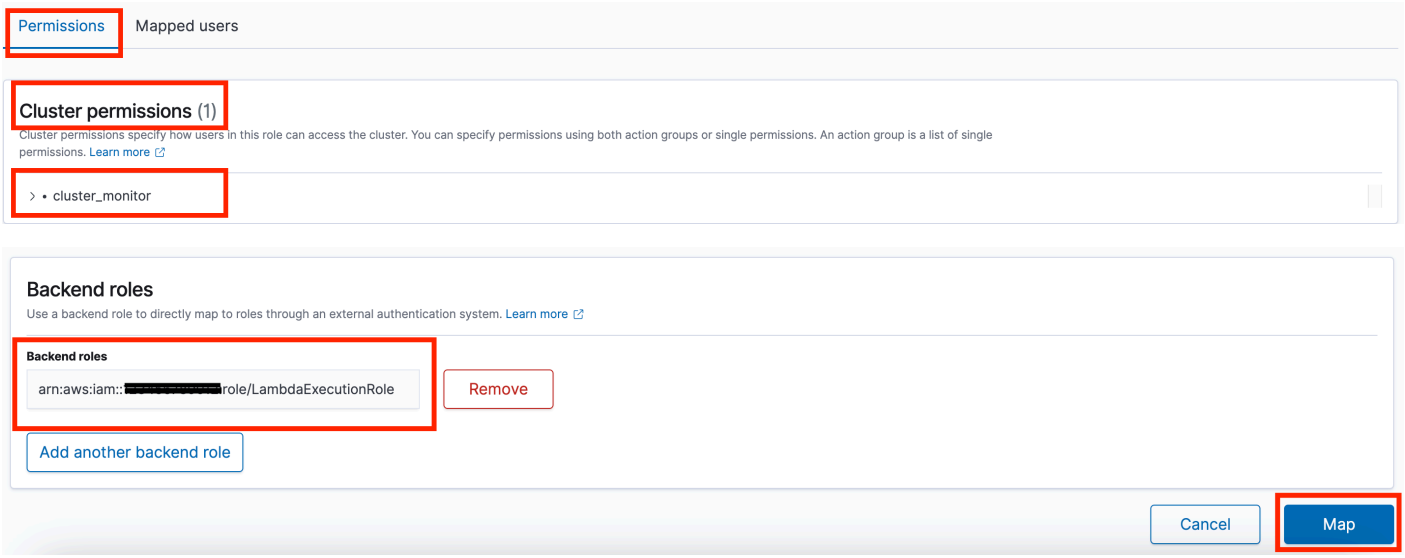
     O ARN da função do IAM a ser anexada à função Lambda. A função Lambda usa as credenciais dessa função para assinar solicitações no domínio do Amazon OpenSearch Service. Se o controle de acesso refinado estiver habilitado no domínio do Amazon OpenSearch Service, você deverá mapear essa função para uma função de back-end do OpenSearch Service Dashboards com uma permissão mínima de “cluster_monitor”.
   - DataRetentionDays (Opcional):

     O número de dias para reter os dados de diagnóstico coletados do domínio do Amazon OpenSearch Service. Por padrão, os dados são retidos por 24 horas (um dia). Você pode optar por reter os dados por no máximo 30 dias.
   - NumberOfDataSamples (Opcional):

     O número de amostras de dados a serem coletadas do domínio do Amazon OpenSearch Service. Por padrão, 5 amostras de dados são coletadas. Você pode coletar até 10 amostras e a função Lambda será invocada para cada coleta de amostras.



4. Se você ativou o controle de acesso refinado em um cluster de OpenSearch serviços, certifique-se de que o arn da `LambdaExecutionRole` função esteja mapeado para uma função com pelo menos permissão. `cluster_monitor`



5. Selecione Executar.
6. A automação é iniciada.
7. O runbook de automação realiza as seguintes etapas:
   - Verifique a simultaneidade:

     Garante que haja apenas uma execução desse runbook visando o domínio especificado do Amazon OpenSearch Service. Se o runbook encontrar outra execução com o mesmo nome de domínio, ele retornará um erro e terminará.
   - getDomainConfig:

     Obtém os detalhes da configuração do domínio OpenSearch de serviço de destino.
   - Recursos de provisão:

Provisiona os recursos para coleta de dados usando AWS CloudFormation.

- waitForStackCriação:

  Espera que a AWS CloudFormation pilha seja concluída.

- describeStackResources:

  Descreve a AWS CloudFormation pilha e obtém o ARN da máquina de estado.

- runStateMachine:

  Invoca a função Lambda do coletor de dados uma ou mais vezes executando uma máquina de estado Step Functions.

- describeErrorsFromStackEvents:

  Descreve os erros da AWS CloudFormation pilha em busca de erros.

- unstageOpenSearchAltoCPUAutomation:

  Exclui a `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation pilha.

- describeErrorsFromStackDeletion:

  Descreve os erros encontrados ao excluir a AWS CloudFormation pilha.

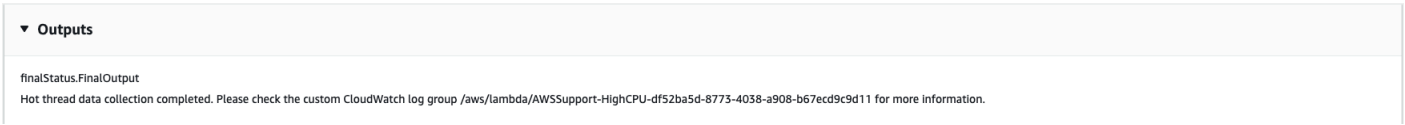
- Status final:

  Retorna a saída final do `AWSSupport-TroubleshootOpenSearchHighCPU` runbook.

8. Depois de concluído, revise a seção Outputs para obter os resultados detalhados da execução.

   - Status final. FinalOutput:

     Fornece o grupo de CloudWatch registros em que os dados de diagnóstico são armazenados.



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação

- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- Consulte Solução de problemas do Amazon OpenSearch Service para obter mais informações

EventBridge

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. EventBridge Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-AddOpsItemDedupStringToEventBridgeRule
- AWS-DisableEventBridgeRule

`AWS-AddOpsItemDedupStringToEventBridgeRule`

Descrição

O `AWS-AddOpsItemDedupStringToEventBridgeRule` runbook adiciona uma string de desduplicação para todos os AWS Systems Manager OpsItems associados a uma regra da Amazon. EventBridge Este runbook não adicionará uma string de eliminação de duplicação se a regra já tiver uma. Para saber mais sobre cadeias de caracteres de desduplicação e OpsItems, consulte Reduzindo a duplicação OpsItems no Guia do usuário.AWS Systems Manager

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DedupString

  Tipo: String

  Descrição: (obrigatório) A string de eliminação de deduplicação que deseja adicionar à regra.
- RuleName

  Tipo: String

  Descrição: (obrigatório) O nome da regra à qual deseja adicionar a string de deduplicação.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

Etapas do documento

- `aws:executeScript`- Adiciona uma sequência de deduplicação à EventBridge regra especificada no `RuleName` parâmetro.

AWS-DisableEventBridgeRule

Descrição

O *AWS-DisableEventBridgeRule* runbook desativa a EventBridge regra da Amazon que você especifica. Para saber mais sobre as regras EventBridge , consulte as regras da Amazon EventBridge no Guia do usuário da Amazon. EventBridge

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EventBusName

  Tipo: String

  Padrão: Default

  Descrição: (opcional) O barramento de eventos associado à regra a ser desabilitada.
- RuleName

  Tipo: String

  Descrição: (obrigatório) O nome da regra que deseja desabilitar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

Etapas do documento

- `aws:executeAwsApi`- Desativa a EventBridge regra especificada no `RuleName` parâmetro.

AWS Glue

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Glue Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-TroubleshootGlueConnection

`AWSSupport-TroubleshootGlueConnection`

Descrição

O AWSSupport-TroubleshootGlueConnectionsrunbook ajuda a solucionar problemas de AWS Glue conexão. O destino da conexão testada deve ser alcançado por meio de uma conexão JDBC e pode ser um cluster/instância do Amazon Relational Database Service (Amazon RDS), um cluster do Amazon Redshift ou qualquer outro destino acessível por meio do JDBC. Nos dois primeiros casos, a ferramenta Reachability Analyzer é usada para determinar se a conectividade entre a origem AWS Glue() e o destino (Amazon RDS ou Amazon Redshift) foi concedida.

Se o destino da conexão não for o Amazon RDS nem o Amazon Redshift, a conectividade ainda será testada criando AWS Lambda uma função na mesma AWS Glue sub-rede da conexão (um ponto de presença da rede) e verificando se o nome do destino pode ser resolvido e se está acessível na porta de destino.

Important

Para executar as verificações do Reachability Analyzer, as interfaces de rede elástica serão criadas em cada uma das sub-redes da fonte de dados da conexão. Verifique se você tem espaço livre suficiente IPs nessas sub-redes e se o consumo de um IP não afetará sua carga de trabalho antes de executar essa automação.

Important

Todos os recursos criados por essa automação são marcados para que possam ser facilmente encontrados. As tags usadas são:

- `AWSSupport-TroubleshootGlueConnection`: true
- `AutomationExecutionId`: *`Amazon EC2 Systems Manager Execution Id`*

Como funciona?

O runbook executa as seguintes etapas:

- Descreve a AWS Glue conexão para obter as informações de origem (sub-rede e grupos de segurança) para as verificações de conectividade.
- Busca as informações de destino (sub-rede e grupos de segurança) da fonte de dados referenciada na URL do JDBC ou dos parâmetros e, se estiverem presentes. `DatasourceSecurityGroups` `DatasourceSubnets`
- Se a fonte de dados presente na URL do JDBC for uma instância ou cluster do Amazon RDS ou um cluster do Amazon Redshift, essa automação é criada ENIs usando as informações de origem e de destino coletadas nas etapas anteriores e usa o Reachability Analyzer para realizar uma verificação de conectividade entre elas.
- Uma função Lambda (ponto de presença da rede, no contexto dessa automação) é usada para realizar verificações de conectividade L4 e resolução de nomes.
- A mesma função Lambda é usada para realizar as verificações no endpoint do Amazon S3.
- O Policy Simulator é usado para determinar se a função do IAM usada na conexão tem as permissões necessárias.
- A automação verifica se o grupo de segurança usado pela conexão tem a configuração esperada.

- Um relatório é gerado contendo as possíveis causas da falha na operação de conexão de teste e/ou também os testes bem-sucedidos que foram realizados.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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**
>
> Além das ações acima mencionadas, a Amazon `AutomationAssumeRole` deve ter a Amazon VPCReachability AnalyzerFullAccessPolicy como uma política gerenciada anexada para que os testes do Reachability Analyzer sejam realizados com sucesso.

Aqui está um exemplo de uma política que poderia ser concedida para`AutomationAssumeRole`:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "TaggedAWSResourcesPermissions",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AWSSupport-TroubleshootGlueConnection": "true"
                }
            },
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:TagRole",
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:TagResource",
                "logs:DeleteLogGroup",
                "logs:CreateLogGroup",
                "logs:PutRetentionPolicy",
                "logs:TagResource",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TaggedEC2ResourcesPermissions",
            "Effect": "Allow",
```

```
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSSupport-TroubleshootGlueConnection": "true"
                }
            },
            "Action": [
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutRolePolicy",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "iam:ResourceTag/AWSSupport-TroubleshootGlueConnection": "true"
                }
            },
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "InvokeFunction",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:*:lambda:*:*:function:point-of-presence-*"
        },
        {
            "Sid": "UnTaggedActions",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInsightsPath",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:StartNetworkInsightsAnalysis",
                "glue:GetConnection",
                "glue:GetDataCatalogEncryptionSettings",
```

```
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInsightsPaths",
                "ec2:DescribeNetworkInsightsAnalyses",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpcAttribute",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:SimulatePrincipalPolicy",
                "kms:DescribeKey",
                "lambda:GetFunction",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:*:iam::*:role/point-of-presence-*",
            "Condition": {
                "StringLikeIfExists": {
                    "iam:PassedToService": "lambda.amazonaws.com"
                }
            }
        }
    ]
}
```

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-TroubleshootGlueConnectionem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:

- AutomationAssumeRole (Opcional):

  O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.

- TestConnectionRole (Obrigatório)

  O Amazon Resource Name (ARN) da função do IAM que é usada durante o teste de conexão.

- ConnectionName (Obrigatório)

  AWS Glue falha no nome da conexão de teste que você deseja solucionar.

- PersistReachabilityAnalyzerResults(Opcional)

  O sinalizador informando se os resultados da execução do Reachability Analyzer devem ser mantidos ou não. Padrão: `false.`

- PointOfPresenceLogRetentionPeriod(Opcional)

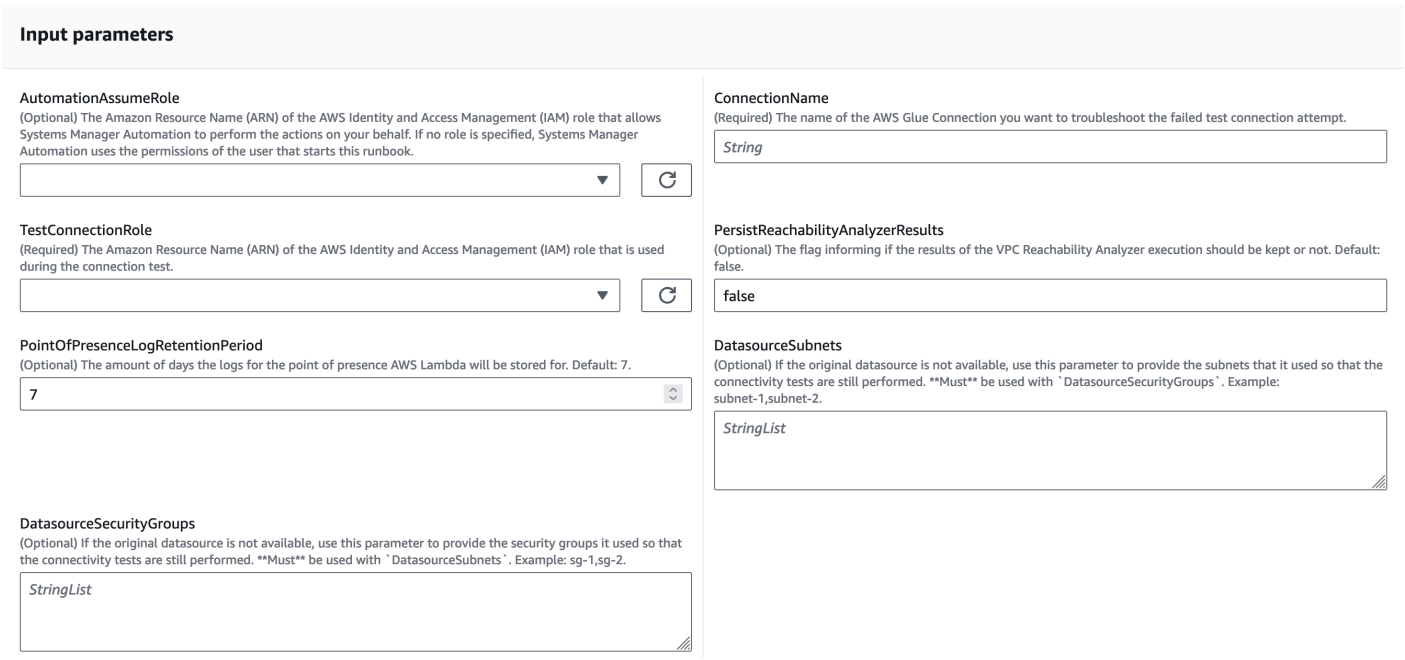
  A quantidade de dias pelos quais os registros do ponto de presença Lambda serão armazenados. Padrão: 7.

- DatasourceSubnets (Opcional)

  Se a fonte de dados original não estiver disponível, use esse parâmetro para fornecer as sub-redes usadas para que os testes de conectividade ainda sejam executados. Deve ser usado com`DatasourceSecurityGroups`. Exemplo: `subnet-1,subnet-2`.

- DatasourceSecurityGroups (Opcional)

  Se a fonte de dados original não estiver disponível, use esse parâmetro para fornecer os grupos de segurança usados para que os testes de conectividade ainda sejam executados. Deve ser usado com`DatasourceSubnets`. Exemplo: `sg-1,sg-2`.



4. Selecione Executar.
5. A automação é iniciada.
6. O runbook de automação realiza as seguintes etapas:
   - ParseInputs:

     Essa etapa valida a combinação de entradas. Se ambos `DatasourceSecurityGroups` `DatasourceSubnets` forem fornecidos, eles serão válidos e retornados como estão. Se nenhuma for fornecida, duas listas vazias serão retornadas. Se apenas um deles for fornecido, a etapa gera uma`ValueException`.
   - GetConnectionDetails:

     Essas etapas retornam os detalhes da AWS Glue conexão fornecida.
   - ParseSecurityGroupList:

     Essa etapa é usada para concatenar o `SecurityGroupIdList` in a para `String` futura utilização nessa automação.
   - GetConnectionData:

     Determina, com base na URL do JDBC, que tipo de conexão entre: `RedShiftRdsInstance`, e. `RdsCluster` `Other` Além disso, retorna o domínio e a porta usados na conexão JDBC, o Amazon VPC da conexão e seus servidores de nomes de domínio.
   - GetNetworkDetails:

Obtém as informações da sub-rede e do grupo de segurança do destino do Amazon RDS ou do Amazon Redshift.

- CrieENITemplate:

  Gera o AWS CloudFormation modelo usado para criar as interfaces de rede usadas para testar a conectividade. Isso é necessário para executar a ferramenta Reachability Analyzer.

- CrieENIStack:

  Cria a AWS CloudFormation pilha a partir do modelo criado na etapa anterior.

- GetStackDetails:

  Descreve a AWS CloudFormation pilha criada na pilha anterior e recupera as `SourceNetworkInterface` informações de um. `TargetNetworkInterfaces`

- RunSourceToTargetCheck:

  Executa verificações entre a origem e o destino ENIs criados na etapa anterior usando a ferramenta Reachability Analyzer.

- ExcluirENIStack:

  Exclui a AWS CloudFormation pilha que cria interfaces de rede

- CreateNetworkPointOfPresence:

  AWS CloudFormation cria a função Lambda usada como ponto de presença da rede.

- GetFunctionName:

  Executa uma chamada de API AWS CloudFormation describe stack para recuperar o nome da função Lambda criada na etapa anterior.

- RunEndpointChecks:

  Usa o ponto de presença da rede para determinar se o endpoint presente na conexão JDBC é solucionável e acessível na porta declarada.

- Verifica a conectividade do CheckS3:

  Verifica a conectividade de rede a partir da AWS Glue conexão com o serviço Amazon S3.

- DeletePointOfPresence:

  Exclui a AWS CloudFormation pilha que cria o ponto de presença da rede Lambda.

- IAMRolePermissões de teste:

  Verifica se a função do IAM usada para o teste tem as permissões necessárias para executá-la.

- CheckConnectionSecurityGroupReferencingRule:

  Verifica se o grupo de segurança usado na AWS Glue conexão está permitindo todo o tráfego de entrada de si mesmo. Ele retornará uma lista dos grupos de segurança sem essa regra, se houver.

- GenerateReport:

  Gera um relatório contendo uma lista de descobertas (possíveis motivos para a falha no teste de conexão) e as próximas etapas (tentativas de resolver a falha do teste de conexão).

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

   - Resultados da automação

     Nesta seção, você encontrará cenários que descrevem as possíveis causas da falha da operação de conexão de teste (descobertas) e como elas podem ser corrigidas (próximas etapas). Se a automação não conseguir encontrar a causa da falha no teste, isso também será informado nesta seção.

   - Testes bem-sucedidos

     Nesta seção, você encontrará cenários que informam o que foi testado com sucesso por essa automação. Testes bem-sucedidos são úteis caso a automação não consiga identificar a causa da falha na conexão de teste, pois reduzem o escopo da investigação ao informar o que não está contribuindo para o problema.

   - Erros de automação

     Nesta seção, você encontrará cenários que descrevem problemas que ocorreram durante a automação, que podem ter limitado o número de testes que a automação poderia realizar. A descrição do cenário informará qual etapa falhou.

```
TroubleshootGlueConnection
_____________________________________________________________________________________________________________________
Automation Results
Bellow are possible causes for the issue being troubleshoot and their fixes.

------------------------------------------------------------

# Scenario: AWS Glue connection's VPC using Amazon Provided DNS
🔍 Findings:
  - The JDBC URL's endpoint dumy-instance.c3c3tj8ogvmj.us-east-1.rds.amazonaws.com could not be resolved from the AWS Glue
connection's subnet subnet-
  - Glue connection's VPC (vpc-[redacted]) is using AWS DNS Resolver but no issue could be found.
→ Next steps:
  - Please check the following links for further DNS troubleshooting:
- https://repost.aws/knowledge-center/vpc-find-cause-of-failed-dns-queries.
- https://repost.aws/knowledge-center/vpc-peering-troubleshoot-dns-resolution
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-support


# Scenario: Checking AWS Glue connection IAM role trust relationship
🔍 Findings:
  - The IAM role arn:aws:iam::[redacted]:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-lLu7FYAp9bfi used for
the AWS Glue connection test has no trust relationship with the AWS Glue service.
→ Next steps:
  - Please add the AWS Glue service to the arn:aws:iam::[redacted]:role/SAW-Core-Test-AWSSupport-Trou-
IncorrectGlueTestRole-lLu7FYAp9bfi trust relationship. More details on the following link:
- https://docs.aws.amazon.com/directoryservice/latest/admin-guide/edit_trust.html


# Scenario: Glue test connection role IAM check
🔍 Findings:
  - The IAM role (arn:aws:iam::[redacted]:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-lLu7FYAp9bfi) used to
test the connection is not allowed to perform 'glue:TestConnection'.
→ Next steps:
  - Please add the 'glue:TestConnection' action to the role used for the AWS Glue connection test:
arn:aws:iam::[redacted]:role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-lLu7FYAp9bfi.


_____________________________________________________________________________________________________________________
✓ Successful Tests
Below are the successful tests performed by the automation, for further troublehsooting.

------------------------------------------------------------

# Scenario: Datasource security group
  ✓ The target's security group(s) allow(s) inbound connections from the Glue connection.


# Scenario: Checking connection security group self referencing rule
  ✓ The AWS Glue connection has a self referencing inbound rule allowing all traffic.
```

Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

Amazon FSx

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. FSx Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-ValidateFSxWindowsADConfig

AWSSupport-ValidateFSxWindowsADConfig

Descrição

O AWSSupport-ValidateFSxWindowsADConfig runbook é usado para validar a configuração autogerenciada do Active Directory (AD) de um servidor de arquivos Amazon FSx para Windows

Como funciona?

O runbook AWSSupport-ValidateFSxWindowsADConfig executa o script de FSx validação da Amazon na instância temporária do Windows Amazon Elastic Compute Cloud (Amazon EC2) lançada pelo runbook na sub-rede da Amazon. FSx O script executa várias verificações para validar a conectividade da rede com AD/DNS servidores autogerenciados e as permissões da conta de FSx serviço da Amazon. O runbook pode validar um Amazon FSx para Windows File Server com falha ou configurado incorretamente ou criar um novo FSx Amazon para Windows File Server com AD autogerenciado.

Por padrão, o runbook cria a instância do Amazon EC2 Windows, o grupo de segurança para acesso AWS Systems Manager (SSM), a função AWS Identity and Access Management (IAM) e a política usadas AWS CloudFormation na sub-rede da Amazon FSx . Se você quiser executar o script em uma EC2 instância existente da Amazon, forneça o ID no parâmetroInstanceId. Em caso de execução bem-sucedida, ele exclui os CloudFormation recursos. No entanto, para reter os recursos, defina o RetainCloudFormationStack parâmetro comotrue.

O CloudFormation modelo cria uma função do IAM em seu nome com as permissões necessárias para anexar à EC2 instância da Amazon para executar o script de FSx validação da Amazon. Para especificar um perfil de instância do IAM existente para a instância temporária, use o InstanceProfileName parâmetro. A função do IAM associada deve conter as seguintes permissões:

- ec2:DescribeSubnetse ec2:DescribeVpcs permissões e a Amazon Managed PolicyAmazonSSMManagedInstanceCore.
- Permissões para obter o nome de usuário e a senha da conta de FSx serviço Amazon do Systems Manager chamando a GetSecretValue API.
- Permissões para colocar o objeto no bucket do Amazon Simple Storage Service (Amazon S3) para a saída do script.

Pré-requisitos

A sub-rede em que a EC2 instância temporária da Amazon é criada (ou a instância existente fornecida no `InstanceId` parâmetro) deve permitir acesso aos endpoints AWS Systems Manager, AWS Secrets Manager, e do Amazon S3 para executar o script usando `AmazonFSxADValidation` o SSM Run Command.

AWS Secrets Manager configuração

O script de validação se conecta ao domínio do Microsoft AD recuperando o nome de usuário e a senha da conta FSx de serviço da Amazon com uma chamada em tempo de execução para o Secrets Manager. Siga as etapas em Criar um AWS Secrets Manager segredo para criar um novo segredo do Secrets Manager. Certifique-se de que o nome de usuário e a senha sejam armazenados usando um key/value par no formato`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`". Consulte Autenticação e controle de acesso AWS Secrets Manager para obter informações sobre como proteger o acesso a segredos.

Para obter mais informações sobre a ferramenta, consulte os `README.md` arquivos `TROUBLESHOOTING.md` e no FSx ADValidation arquivo da Amazon.

Execução do Runbook

Execute o runbook com os parâmetros Amazon FSx ID ou AD. A seguir está o fluxo de trabalho do runbook:

- Obtém os parâmetros do Amazon FSx ID ou usa os parâmetros de entrada do AD.
- Cria a instância de validação temporária EC2 do Amazon Windows na FSx sub-rede Amazon, grupo de segurança para acesso SSM, função do IAM e uso da política (condicional). CloudFormation Se o `InstanceId` parâmetro for especificado, ele será usado.
- Faz o download e executa o script de validação na EC2 instância da Amazon de destino na sub-rede FSx primária da Amazon.
- Fornece o código do resultado da validação do AD na saída de automação. Além disso, a saída completa do script é carregada no bucket do Amazon S3.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Exemplo de política do IAM para a função Automation Assume

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

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-ValidateFSxWindowsADConfigem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para validar o AD autogerenciado com uma FSx Amazon existente com falha ou configuração incorreta, insira os seguintes parâmetros:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma

função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.

- FSxID (condicional):

  O ID do servidor de arquivos da Amazon FSx para Windows. Isso é necessário para validar a Amazon existente que falhou ou está mal configurada. FSx

- SecretArn (Obrigatório):

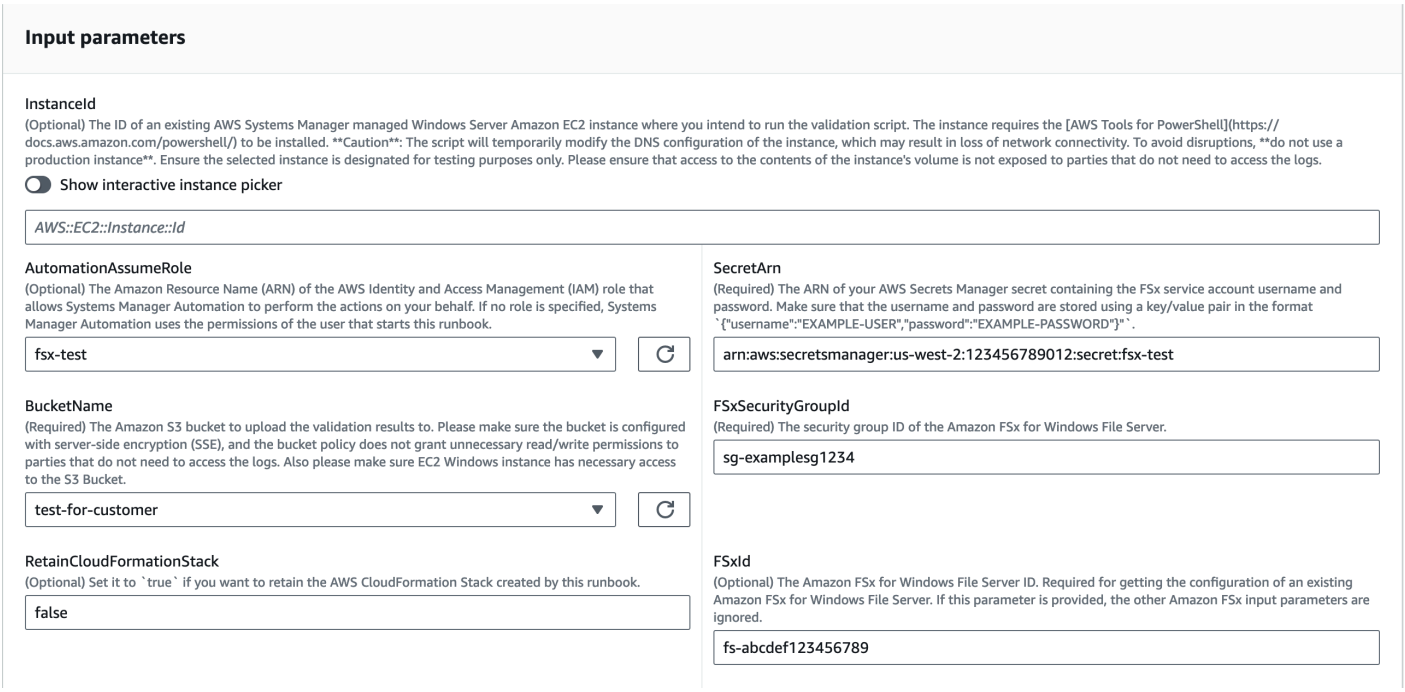
  O ARN do seu segredo do Secrets Manager contendo o nome de usuário e a senha da conta FSx de serviço da Amazon. Certifique-se de que o nome de usuário e a senha sejam armazenados usando um key/value par no formato`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`. A CloudFormation pilha cria a instância de validação com permissões `GetSecretValue` para executar esse ARN.

- FSxSecurityGroupId (Obrigatório):

  O ID do grupo de segurança do Amazon FSx para Windows File Server.

- BucketName (Obrigatório):

  O bucket do Amazon S3 para o qual carregar os resultados da validação. Certifique-se de que o bucket esteja configurado com criptografia do lado do servidor (SSE) e que a política do bucket não conceda read/write permissões desnecessárias às partes que não precisam acessar os registros. Certifique-se também de que a instância EC2 do Amazon Windows tenha o acesso necessário ao bucket do Amazon S3.



4. Para validar a configuração autogerenciada do AD para uma nova FSx criação da Amazon, insira os seguintes parâmetros:

   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.

   - SecretArn (Obrigatório):

     O ARN do seu segredo do Secrets Manager contendo o nome de usuário e a senha da conta FSx de serviço da Amazon. Certifique-se de que o nome de usuário e a senha sejam armazenados usando um key/value par no formato`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`. A CloudFormation pilha cria a instância de validação com permissões `GetSecretValue` para executar esse ARN.

   - FSxSecurityGroupId (Obrigatório):

     O ID do grupo de segurança do Amazon FSx para Windows File Server.

   - BucketName (Obrigatório):

     O bucket do Amazon S3 para o qual carregar os resultados da validação. Certifique-se de que o bucket esteja configurado com criptografia do lado do servidor (SSE) e que a política do bucket

não conceda read/write permissões desnecessárias às partes que não precisam acessar os registros. Certifique-se também de que a instância EC2 do Amazon Windows tenha o acesso necessário ao bucket do Amazon S3.

- FSxPreferredSubnetId(Condicional):

  A sub-rede preferencial do Amazon FSx para Windows File Server.

- DomainName (Condicional):

  O nome de domínio totalmente qualificado do seu domínio autogerenciado do Microsoft AD.

- DnsIpAddresses (Condicional):

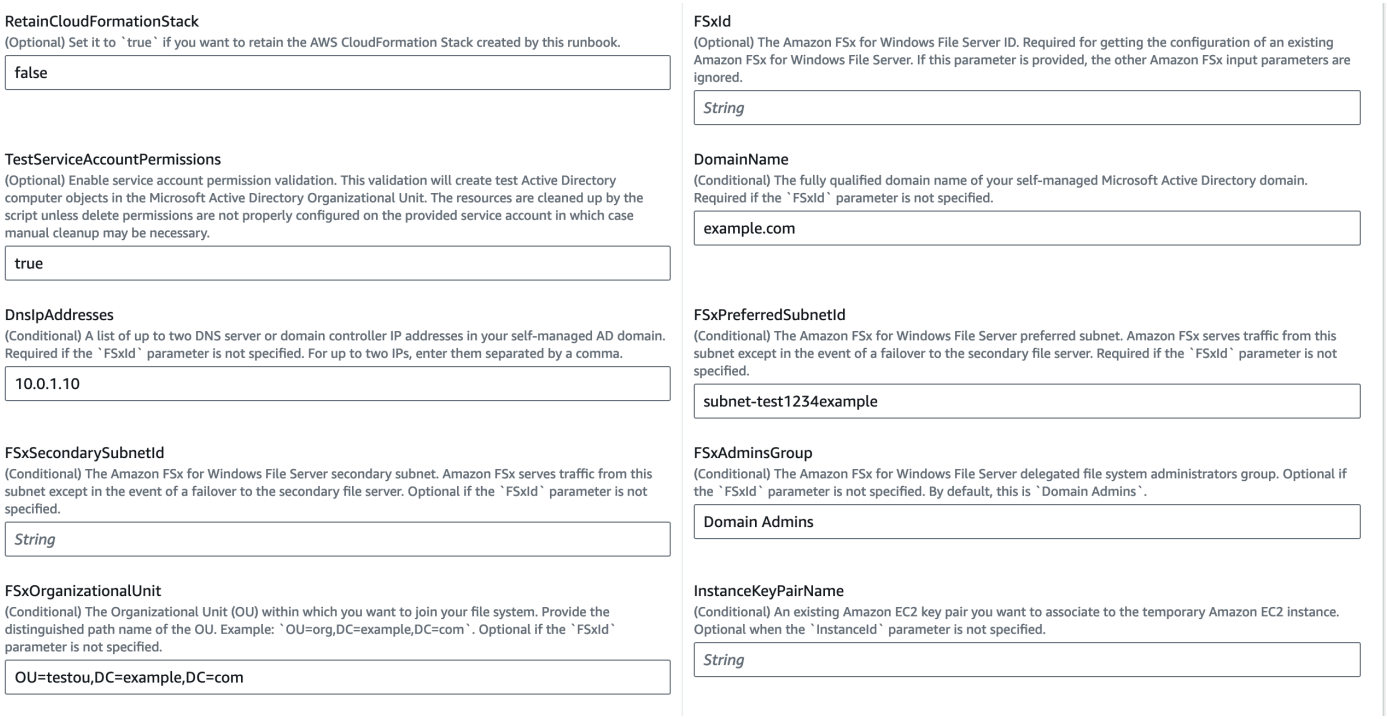
  Uma lista de até dois endereços IP de servidor DNS ou controlador de domínio em seu domínio autogerenciado do AD. Para até dois IPs, insira-os separados por uma vírgula.

- FSxAdminsGroup (Condicional):

  O grupo delegado de administradores de sistemas de arquivos do Amazon FSx para Windows File Server. Por padrão, ele é `Domain Admins`.

- FSxOrganizationalUnit(Condicional):

  A Unidade Organizacional (OU) na qual você deseja unir seu sistema de arquivos. Forneça o nome do caminho distinto da OU. Exemplo: `OU=org,DC=example,DC=com`.



5. Selecione Executar.

6. A automação é iniciada.
7. O bucket realiza as seguintes etapas:
   - CheckBucketPublicStatus(AWS: ExecuteScript):

     Verifica se o bucket do Amazon S3 de destino potencialmente concede acesso público de leitura e and/or gravação a seus objetos.
   - BranchOnInputParameters(aws: branch):

     Ramifica os parâmetros de entrada fornecidos, como Amazon FSx ID ou FSx parâmetros da Amazon.
   - AssertFileSystemTypeIsWindows(aws: assertAwsResource Propriedade):

     Se o Amazon FSx ID for fornecido, valida que o tipo de sistema de arquivos é Amazon FSx para Windows File Server.
   - GetValidationInputs(AWS: ExecuteScript):

     Retorna a configuração autogerenciada do Microsoft AD exigida pelo CloudFormation modelo para criar a EC2 instância da Amazon.
   - BranchOnInstanceId (aws: branch):

     Ramificações na entrada fornecida`InstanceId`. Se `InstanceId` for fornecido, o script de validação é executado na EC2 instância de destino da Amazon a partir da automação`step:RunValidationScript`.
   - Criar EC2 InstanceStack (AWS: CreateStack):

     Cria a EC2 instância da Amazon na sub-rede preferencial usando AWS CloudFormation onde a `AmazonFSxADValidation` ferramenta será executada
   - DescribeStackResources(leis:executeAwsApi):

     Descreve a CloudFormation pilha para obter o ID temporário da EC2 instância Amazon.
   - WaitForEC2InstanceToBeManaged(leis: waitForAwsResourceProperty):

     Espera até que a EC2 instância da Amazon seja gerenciada pelo Systems Manager para executar o script de validação usando o SSM Run Command.
   - GetAmazonFSxADValidationAnexo (awsexecuteAwsApi):

     Obtém o URL da `AmazonFSxADValidation` ferramenta a partir dos anexos do runbook.

- RunValidationScript(AWS: RunCommand):

  Executa a `AmazonFSxADValidation` ferramenta na EC2 instância temporária da Amazon e armazena o resultado no bucket do Amazon S3 especificado no `BucketName` parâmetro.

- DescribeErrorsFromStackEvents(AWS: ExecuteScript):

  Descreve os eventos da CloudFormation pilha se os runbooks não conseguirem criar a pilha.

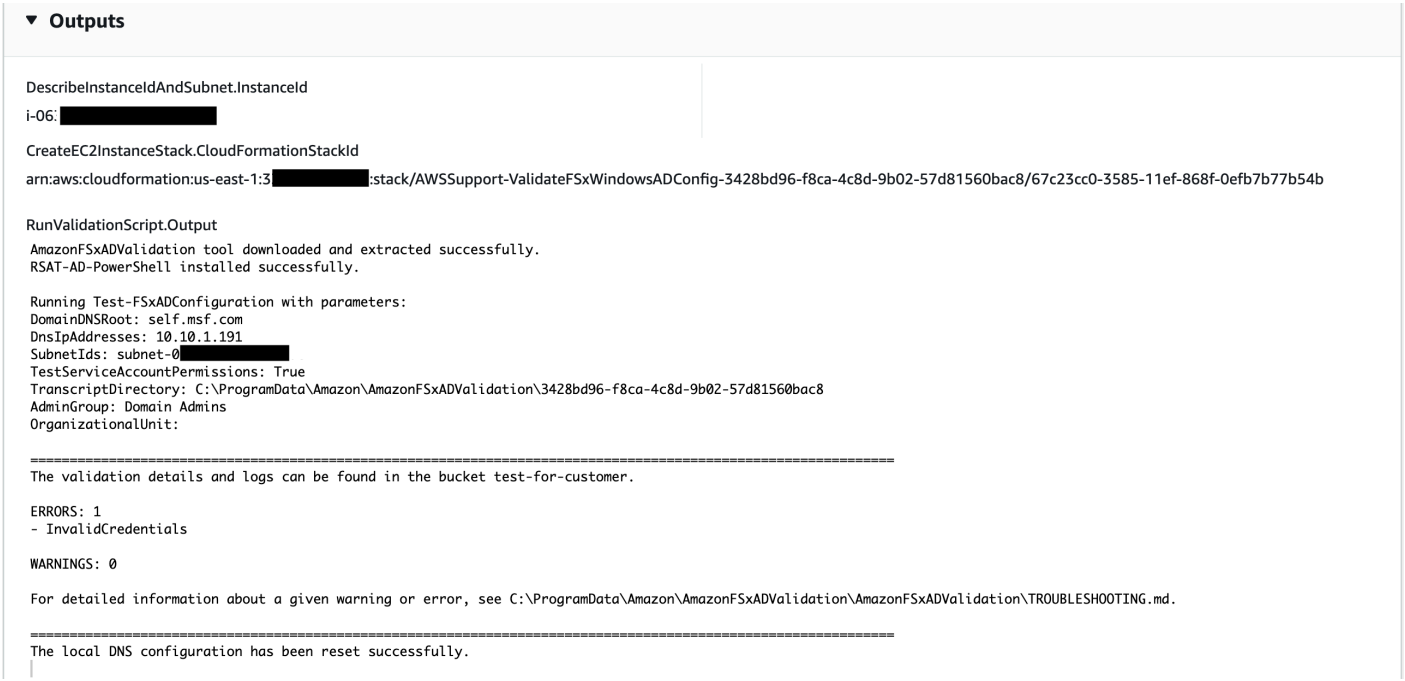
- BranchOnRetainCloudFormationStack(aws: branch):

  Ramifica os `InstanceId` parâmetros `RetainCloudFormationStack` e para determinar se a CloudFormation pilha deve ser excluída.

- DeleteCloudFormationStack(AWS: DeleteStack):

  Exclui a AWS CloudFormation pilha.

8. Depois de concluído, revise a seção Saídas para ver os resultados da execução:



   O runbook fará o upload dos resultados da execução do script de validação para o bucket do Amazon S3.

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- O que é o Amazon FSx para Windows File Server?
- Validando a configuração autogerenciada do AD para o Amazon FSx for Windows File Server

GuardDuty

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. GuardDuty Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-CreateGuardDutyDetector

`AWSConfigRemediation-CreateGuardDutyDetector`

Descrição

O `AWSConfigRemediation-CreateGuardDutyDetector` runbook cria um detector Amazon GuardDuty (GuardDuty) no Região da AWS local onde você executa a automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `guardduty:CreateDetector`
- `guardduty:GetDetector`

Etapas do documento

- `aws:executeAwsApi`- Cria um GuardDuty detector.
- `aws:assertAwsResourceProperty` :Verifica se o `Status` do detector é `ENABLED`.

IAM

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Identity and Access Management Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-TroubleshootIAMAccessDeniedEvents
- AWS-AttachIAMToInstance
- AWS-DeleteIAMInlinePolicy
- AWSConfigRemediation-DeleteIAMRole

- AWSConfigRemediation-DeleteIAMUser
- AWSConfigRemediation-DeleteUnusedIAMGroup
- AWSConfigRemediation-DeleteUnusedIAMPolicy
- AWSConfigRemediation-DetachIAMPolicy
- AWSConfigRemediation-EnableAccountAccessAnalyzer
- AWSSupport-GrantPermissionsToIAMUser
- AWSConfigRemediation-RemoveUserPolicies
- AWSConfigRemediation-ReplaceIAMInlinePolicy
- AWSConfigRemediation-RevokeUnusedIAMUserCredentials
- AWSConfigRemediation-SetIAMPasswordPolicy
- AWSSupport-ContainIAMPrincipal

AWSSupport-TroubleshootIAMAccessDeniedEvents

Descrição

O runbook de AWSSupport-TroubleshootIAMAccessDeniedEvents automação ajuda a solucionar problemas de acesso negado AWS Identity and Access Management (IAM). O runbook consulta eventos recentes CloudTrail de acesso negado relacionados à entidade IAM e à fonte de eventos de AWS serviço especificadas. Ele analisa eventos em uma janela de tempo configurável de até 24 horas, processando até 10 eventos por execução. Cada evento de acesso negado identificado é examinado para ajudar a entender o contexto da negação e das ações tentadas. A automação analisa as políticas de IAM baseadas em identidade e em recursos. Para políticas baseadas em identidade, ele examina as políticas em linha e gerenciadas anexadas à entidade do IAM. Para políticas baseadas em recursos, ele avalia políticas em vários serviços, AWS incluindo Amazon Simple Storage Service (Amazon S3), (AWS Key Management Service)AWS KMS, Amazon Simple Notification Service (AWS Lambda Amazon SNS), Amazon Elastic Container Registry (Amazon ECR), Amazon API Gateway, Amazon Elastic File System (CodeArtifactAmazon EFS), Amazon Simple Amazon Queue Service (Amazon SQS), Amazon Service, Signer e. AWS Cloud9 OpenSearch AWS AWS Serverless Application Repository AWS Secrets Manager

O runbook utiliza recursos de simulação de políticas do IAM para avaliar essas políticas em relação às ações negadas encontradas nos CloudTrail eventos. O runbook aproveita os recursos de simulação de políticas do IAM, tanto SimulatePrincipalPolicy para usuários do IAM quanto SimulateCustomPolicypara funções do IAM, para avaliar essas políticas em relação às ações

negadas encontradas nos CloudTrail eventos. A automação gera um relatório que ajuda a identificar as ações específicas que foram negadas, diferenciando entre negações implícitas e explícitas, listando as políticas responsáveis pelas negações de acesso e fornecendo explicações para cada negação. O relatório também sugere possíveis resoluções, como identificar declarações de permissão ausentes ou declarações de negação conflitantes

Como funciona?

O runbook executa as seguintes etapas:

- Descreve e valida `RequesterARN` (função ou usuário) para obter informações como tipo de entidade do IAM e ID do IAM.
- Busca CloudTrail eventos associados ao`RequesterARN`,`EventSource`, e `ResourceARN` se fornecidos.
- Analisa os CloudTrail eventos para obter a ação que foi executada quando o erro Access Denied foi retornado e, em seguida, examina todas as políticas do IAM, como políticas embutidas e gerenciadas anexadas à entidade do IAM, bem como políticas baseadas em recursos. Em seguida, ele simula essas políticas em relação às ações encontradas nos erros de acesso negado dos CloudTrail eventos em questão para determinar a causa do erro.
- Produz um relatório determinando o tipo de erro de Acesso Negado, as políticas responsáveis pelos erros e fornece sugestões para uma possível solução para o erro.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- 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

Exemplo de política:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:GetUser",
                "iam:GetRole",
                "iam:SimulatePrincipalPolicy",
                "iam:ListUserPolicies",
                "iam:ListRolePolicies",
                "iam:GetRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:GetPolicy",
                "iam:GetUserPolicy",
                "iam:GetPolicyVersion",
                "iam:ListAttachedUserPolicies",
                "ssm:StartAutomationExecution",
                "ssm:StopAutomationExecution",
                "cloudtrail:LookupEvents",
                "iam:SimulateCustomPolicy"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetBucketPolicy",
                "kms:GetKeyPolicy",
                "lambda:GetPolicy",
                "sns:GetTopicAttributes",
                "ecr:GetRepositoryPolicy",
                "apigateway:GET",
                "codeartifact:GetRepositoryPermissionsPolicy",
                "elasticfilesystem:GetFileSystemPolicy",
                "sqs:GetQueueAttributes",
                "cloud9:GetEnvironment",
                "es:DescribeDomain",
                "signer:GetSigningProfile",
                "serverlessrepo:GetApplication",
                "secretsmanager:GetResourcePolicy"
            ],
```

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

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-TroubleshootIAMAccessDeniedEventsem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):
     - Descrição: (Opcional) O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o SSM Automation execute as ações em seu nome. A função precisa ser adicionada à sua entrada de acesso ao cluster Amazon EKS ou à permissão RBAC para permitir chamadas de API do Kubernetes.
     - Tipo: `AWS::IAM::Role::Arn`
   - RequestERARN (obrigatório):
     - Descrição: (Obrigatório) O ARN do usuário ou função do IAM para o qual você deseja investigar as permissões de acesso em um recurso específico AWS .
     - Tipo: String
     - Padrão de permissão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
   - ResourceArn (opcional):
     - Descrição: (Opcional) O ARN do recurso para AWS o qual o acesso negado é avaliado. O recurso de AWS destino deve existir na mesma região em que o runbook de automação é executado.
     - Tipo: String
     - Padrão de permissão: `^$|^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 (Obrigatório):
  - Descrição: (Obrigatório) O endpoint da API da Amazon de onde o CloudTrail evento se originou. Por exemplo: `s3.amazonaws.com`.
  - Tipo: String
  - Padrão de permissão: `^([a-zA-Z0-9.-]+)\\.amazonaws\\.com$`
- EventName (Opcional):
  - Descrição: (Opcional) O nome da ação da Amazon API associada ao CloudTrail evento. Por exemplo: `s3:CreateBucket`.
  - Tipo: String
  - Padrão de permissão: `^$|^[a-z0-9]+:[A-Za-z0-9]+$`
- LookBackHours (Opcional):
  - Descrição: (Opcional) O número de horas para analisar os CloudTrail eventos ao pesquisar `Access Denied` eventos. Intervalo válido: `1` até `24` horas.
  - Tipo: inteiro
  - Padrão de permissão: `^([1-9]|1[0-9]|2[0-4])$`
  - Padrão: 12
- MaxEvents (Opcional):
  - Descrição: (Opcional) O número máximo de CloudTrail `Access Denied` eventos retornados ao pesquisar eventos. Intervalo válido: `1` até `5` eventos.
  - Tipo: inteiro
  - Padrão de permissão: `^([1-9]|1[0-9]|2[0-4])$`
  - Padrão: 3
- UseContextEntries (Opcional):
  - Descrição: (Opcional) Se você especificar`true`, a automação extrairá detalhes sobre o contexto da solicitação de API do CloudTrail evento e os incluirá na simulação da política do IAM.
  - Tipo: booliano
  - Padrão de permissão: `^([1-9]|1[0-9]|2[0-4])$`
  - Padrão: 3

4. Selecione Executar.
5. A automação é iniciada.

6. O bucket realiza as seguintes etapas:
   - ValidateRequesterArn

     Valida e desconstrói o `RequesterArn` ARN, recuperando informações sobre o usuário ou a função de destino do IAM.
   - GetCloudTrailEventsWithAccessDeniedError

     Consulta os CloudTrail `Access Denied` eventos recentes relacionados à entidade e ao AWS serviço `EventSource` do IAM especificados.
   - Avalie IAMRequester as políticas

     Avalia as permissões do IAM da entidade IAM solicitante em relação às ações dos CloudTrail eventos. Essa avaliação inclui a análise de políticas baseadas em identidade e baseadas em recursos associadas ao solicitante. A automação utiliza os recursos de simulação de políticas do IAM para avaliar essas políticas no contexto das ações negadas identificadas nos CloudTrail eventos.
7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:
   - PermissionEvaluationResults

     Produz um relatório que ajuda a identificar as ações específicas que foram negadas, diferenciando entre negações implícitas e explícitas. Ele também lista as políticas responsáveis pelas negações de acesso e fornece explicações para cada negação. O relatório também sugere possíveis resoluções, como identificar declarações de permissão ausentes ou declarações de negação conflitantes

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS-AttachIAMToInstance

Descrição

Anexe uma função AWS Identity and Access Management (IAM) a uma instância gerenciada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ForceReplace

  Tipo: booliano

  Descrição: (opcional) Sinalizador para especificar se deseja substituir o perfil do IAM existente ou não.

  Padrão: verdadeiro
- InstanceId

  Tipo: String

  Descrição: (obrigatório) O ID da instância a qual você deseja associar um perfil do IAM.
- RoleName

  Tipo: String

Descrição: (obrigatório) O nome do perfil do IAM a ser adicionado à instância gerenciada.

Etapas do documento

1. `aws:executeAwsApi`- DescribeInstanceProfile - Encontre o perfil da instância do IAM anexado à EC2 instância.
2. `aws:branch`- CheckInstanceProfileAssociations - Verifique o perfil da instância do IAM anexado à EC2 instância.
   a. Se um perfil de instância do IAM estiver anexado e `ForceReplace` estiver definido como `true`:
      i. `aws:executeAwsApi`- DisassociateIamInstanceProfile - Desassocie o perfil da instância do IAM da EC2 instância.
   b. `aws:executeAwsApi`- ListInstanceProfilesForRole - Liste os perfis de instância para a função IAM fornecida.
   c. `aws:branch`- CheckInstanceProfileCreated - Verifique se a função do IAM fornecida tem um perfil de instância associado.
      i. Se a o perfil do IAM tiver um perfil de instância associado:
         A. `aws:executeAwsApi`- Anexar IAMProfile ToInstance - anexe a função do perfil da instância do IAM à EC2 instância.
      i. Se o perfil do IAM não tiver um perfil de instância associado:
         A. `aws:executeAwsApi`- CreateInstanceProfileForRole - Crie uma função de perfil de instância para a função do IAM especificada.
         B. `aws:executeAwsApi`- AddRoleToInstanceProfile - Anexe a função do perfil da instância à função do IAM especificada.
         C. `aws:executeAwsApi`- GetInstanceProfile - Obtenha os dados do perfil da instância para a função do IAM especificada.
         D. `aws:executeAwsApi`- Anexar IAMProfile ToInstanceWithRetry - anexe a função do perfil da instância do IAM à EC2 instância.

Saídas

Anexar IAMProfileToInstanceWithRetry. AssociationId

GetInstanceProfile.InstanceProfileName

GetInstanceProfile.InstanceProfileArn

Anexar IAMProfileToInstance. AssociationId

ListInstanceProfilesForRole.InstanceProfileName

ListInstanceProfilesForRole.InstanceProfileArn

AWS-DeleteIAMInlinePolicy

Descrição

O `AWS-DeleteIAMInlinePolicy` runbook exclui todas as políticas em linha AWS Identity and Access Management (IAM) anexadas às identidades do IAM que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- IamArns

  Tipo: String

Descrição: (Obrigatório) Uma lista separada por vírgulas das ARNs identidades do IAM das quais você deseja excluir as políticas em linha. Essa lista pode incluir usuários, grupos ou funções do IAM.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

Etapas do documento

- `aws:executeScript`- Exclui as políticas embutidas do IAM anexadas às identidades específicas do IAM.

AWSConfigRemediation-DeleteIAMRole

Descrição

O runbook `AWSConfigRemediation-DeleteIAMRole` exclui o perfil do AWS Identity and Access Management (IAM) especificado. Essa automação não exclui perfis de instância associados ao perfil do IAM ou funções vinculadas ao serviço.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- IAMRoleID

  Tipo: String

  Descrição: (obrigatório) O ID do perfil do IAM a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfilesForRole`
- `iam:ListRolePolicies`
- `iam:ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

Etapas do documento

- `aws:executeScript` :Reúne o nome do perfil do IAM especificado no parâmetro `IAMRoleID`.

- `aws:executeScript` :Reúne políticas e perfis de instância associados ao perfil do IAM.
- `aws:executeScript` :Exclui as políticas anexadas.
- `aws:executeScript` :Exclui o perfil do IAM e verifica se o perfil foi excluído.

AWSConfigRemediation-DeleteIAMUser

Descrição

O runbook `AWSConfigRemediation-DeleteIAMUser` exclui o usuário do AWS Identity and Access Management (IAM) especificado. Essa automação exclui ou desanexa os seguintes atributos associados ao usuário do IAM:

- Chaves de acesso
- Políticas gerenciadas anexadas
- Credenciais do git
- Associações ao grupo IAM
- Senha de usuário do IAM
- Políticas em linha
- Dispositivos de autenticação multifator (MFA)
- Assinatura de certificados
- Chaves públicas de SSH

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- IAMUserIdentificação

  Tipo: String

  Descrição: (obrigatório) O ID do usuário do IAM a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeScript :Reúne o nome do usuário do IAM especificado no parâmetro IAMUserId.
- aws:executeScript :Reúne chaves de acesso, certificados, credenciais, dispositivos de MFA e chaves SSH associadas ao usuário do IAM.
- aws:executeScript :Reúne associações e políticas de grupos para o usuário do IAM.
- aws:executeScript :Exclui chaves de acesso, certificados, credenciais, dispositivos de MFA e chaves SSH associadas ao usuário do IAM.
- aws:executeScript :Exclui associações e políticas de grupos para o usuário do IAM.
- aws:executeScript :Exclui o usuário do IAM e verifica se a função foi excluída.

AWSConfigRemediation-DeleteUnusedIAMGroup

Descrição

O runbook AWSConfigRemediation-DeleteUnusedIAMGroup exclui um grupo do IAM que não contém nenhum usuário.

O runbook AWSConfigRemediation-DeleteUnusedIAMGroup exclui um grupo do IAM que não contém nenhum usuário.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- GroupName

  Tipo: String

  Descrição: (obrigatório) O nome do grupo do IAM a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteGroup`
- `iam:DeleteGroupPolicy`
- `iam:DetachGroupPolicy`

Etapas do documento

- `aws:executeScript` :Remove as políticas gerenciadas e em linha do IAM anexadas ao grupo de destino do IAM e, em seguida, exclui o grupo do IAM.

AWSConfigRemediation-DeleteUnusedIAMPolicy

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedIAMPolicy` exclui uma política do AWS Identity and Access Management (IAM) que não está anexada a nenhum usuário, grupo ou perfil.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- IAMResourceIdentificação

  Tipo: String

  Descrição: (obrigatório) O identificador de atributo da política do IAM a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DeletePolicy`

- `iam:DeletePolicyVersion`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`
- `iam:ListPolicyVersions`

Etapas do documento

- `aws:executeScript` :Exclui a política especificada no parâmetro `IAMResourceId` e verifica se a política foi excluída.

`AWSConfigRemediation-DetachIAMPolicy`

Descrição

O runbook `AWSConfigRemediation-DetachIAMPolicy` desvincula a política do AWS Identity and Access Management (IAM) especificada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- IAMResourceIdentificação

  Tipo: String

  Descrição: (obrigatório) O ID da política do IAM a ser desvinculada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DetachGroupPolicy`
- `iam:DetachRolePolicy`
- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`

Etapas do documento

- `aws:executeScript` :Desvincula a política do IAM de todos os atributos.

AWSConfigRemediation-EnableAccountAccessAnalyzer

Descrição

O `AWSConfigRemediation-EnableAccountAccessAnalyzer` runbook cria um analisador de acesso AWS Identity and Access Management (IAM) em seu. Conta da AWS Para obter mais informações sobre o analisador de acesso, consulte Utilizando o IAM Access Analyzer da AWS no Guia do usuário do IAM.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AnalyzerName

  Tipo: String

  Descrição: (obrigatório) Nome do analizador a ser criado.
- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

Etapas do documento

- `aws:executeAwsApi` :Cria um analisador de acesso para sua conta.
- `aws:waitForAwsResourceProperty` :Espera que o status do analisador de acesso seja `ACTIVE`.
- `aws:assertAwsResourceProperty` :Confirma que o status do analisador de acesso é `ACTIVE`.

AWSSupport-GrantPermissionsToIAMUser

Descrição

Este runbook concede as permissões especificadas a um grupo do IAM (novo ou existente) e adiciona o usuário do IAM existente a ele. As políticas das quais você pode escolher: Faturamento ou Suporte. Para ativar o acesso de faturamento para o IAM, lembre-se de ativar o acesso do usuário do IAM e do usuário federado às páginas de Gerenciamento de custo e Faturamento.

> **Important**
>
> Se você fornecer um grupo do IAM existente, todos os usuários do IAM atualmente no grupo recebem as novas permissões.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- IAMGroupNome

Tipo: String

Padrão: ExampleSupportAndBillingGroup

Descrição: (Obrigatório) Pode ser um grupo novo ou existente. Deve estar em conformidade com as Limitações de nome das entidades do IAM.

- IAMUserNome

  Tipo: String

  Padrão: ExampleUser

  Descrição: (Obrigatório) Deve ser um usuário existente.

- LambdaAssumeRole

  Tipo: String

  Descrição: (opcional) O ARN da função assumida pelo lambda.

- Permissões

  Tipo: String

  Valores válidos: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

  Padrão: SupportAndBillingFullAccess

  Descrição: (obrigatório) Escolha um dos itens a seguir: `SupportFullAccess` concede acesso total à central de suporte. `BillingFullAccess` concede acesso total ao painel de faturamento. `SupportAndBillingFullAccess` concede acesso total à central de suporte e ao painel de faturamento. Mais informações sobre políticas estão em Detalhes do documento.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

As permissões necessárias dependem de como o `AWSSupport-GrantPermissionsToIAMUser` é executado.

Executando como o usuário ou o perfil conectado no momento

É recomendável anexar a política gerenciada `AmazonSSMAutomationRole` da Amazon e as seguintes permissões adicionais para poder criar a função do Lambda e o perfil do IAM para passar para o Lambda:

```
{
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Action": [
                                "lambda:InvokeFunction",
                                "lambda:CreateFunction",
                                "lambda:DeleteFunction",
                                "lambda:GetFunction"
                            ],
                            "Resource":
 "arn:aws:lambda:*:ACCOUNTID:function:AWSSupport-*",
                            "Effect": "Allow"
                        },
                        {
                            "Effect" : "Allow",
                            "Action" : [
                                "iam:CreateGroup",
                                "iam:AddUserToGroup",
                                "iam:ListAttachedGroupPolicies",
                                "iam:GetGroup",
                                "iam:GetUser"
                            ],
                            "Resource" : [
                                "arn:aws:iam::*:user/*",
                                "arn:aws:iam::*:group/*"
                            ]
                        },
                        {
                            "Effect" : "Allow",
                            "Action" : [
                                "iam:AttachGroupPolicy"
                            ],
                            "Resource": "*",
                            "Condition": {
                                "ArnEquals": {
                                    "iam:PolicyArn": [
                                        "arn:aws:iam::aws:policy/job-function/Billing",
                                        "arn:aws:iam::aws:policy/AWSSupportAccess"
```

```
                                ]
                            }
                        }
                    },
                    {
                        "Effect" : "Allow",
                        "Action" : [
                            "iam:ListAccountAliases",
                            "iam:GetAccountSummary"
                        ],
                        "Resource" : "*"
                    }
                ]
            }
```

Usando AutomationAssumeRole e LambdaAssumeRole

O usuário deve ter as StartAutomationExecution permissões ssm: no runbook e iam: PassRole nas funções do IAM passadas como e. AutomationAssumeRoleLambdaAssumeRole Aqui estão as permissões que cada função do IAM precisa:

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

Etapas do documento

1. `aws:createStack`- Execute o AWS CloudFormation modelo para criar uma função Lambda.
2. `aws:invokeLambdaFunction` :Executar o Lambda para definir as permissões do IAM.
3. `aws:deleteStack`- Excluir CloudFormation modelo.

Saídas

configureIAM.Payload

AWSConfigRemediation-RemoveUserPolicies

Descrição

O runbook `AWSConfigRemediation-RemoveUserPolicies` exclui as políticas em linha do AWS Identity and Access Management (IAM) e desvincula todas as políticas gerenciadas anexadas ao usuário especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- IAMUserID

  Tipo: String

  Descrição: (obrigatório) O ID do usuário cujas políticas serão removidas.
- PolicyType

  Tipo: String

  Valores válidos: All | Inline | Managed

  Padrão: All

  Descrição: (obrigatório) O tipo de política do IAM a ser removida do usuário.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam:ListAttachedUserPolicies`
- `iam:ListUserPolicies`
- `iam:ListUsers`

Etapas do documento

- `aws:executeScript` :Exclui e desvincula as políticas do IAM do usuário especificado no parâmetro `IAMUserID`.

AWSConfigRemediation-ReplaceIAMInlinePolicy

Descrição

O `AWSConfigRemediation-ReplaceIAMInlinePolicy` runbook substitui uma política em linha AWS Identity and Access Management (IAM) por uma política de IAM gerenciada replicada. Para

uma política em linha anexada a um usuário, grupo ou perfil, as permissões da política embutida são clonadas em uma política do IAM gerenciada. A política gerenciada do IAM é adicionada ao recurso e a política embutida é removida. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- InlinePolicyName

  Tipo: StringList

  Descrição: (obrigatório) A política do IAM em linha a ser substituída.
- ResourceId

  Tipo: String

  Descrição: (obrigatório) O ID do usuário, grupo ou perfil do IAM cujo a política embutida será substituída.

Permissões obrigatórias do IAM

O parâmetro AutomationAssumeRole requer as seguintes ações para usar o runbook com êxito.

- 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

Etapas do documento

- aws:executeScript :Substituir a política do IAM em linha por uma política da AWS replicada no recurso especificado.

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

Descrição

O AWSConfigRemediation-RevokeUnusedIAMUserCredentials runbook revoga senhas não utilizadas AWS Identity and Access Management (IAM) e chaves de acesso ativas. Esse runbook também desativa as chaves de acesso expiradas e exclui os perfis de login expirados. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- IAMResourceIdentificação

  Tipo: String

  Descrição: (obrigatório) O ID do recurso do IAM cujas credenciais não utilizadas serão revogadas.
- MaxCredentialUsageAge

  Tipo: String

  Padrão: 90

  Descrição: (obrigatório) O número de dias em que a credencial deve ter sido usada.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`

- ssm:GetAutomationExecution
- config:ListDiscoveredResources
- iam:DeleteAccessKey
- iam:DeleteLoginProfile
- iam:GetAccessKeyLastUsed
- iam:GetLoginProfile
- iam:GetUser
- iam:ListAccessKeys
- iam:UpdateAccessKey

Etapas do documento

- aws:executeScript :Revoga as credenciais do IAM para o usuário especificado no parâmetro IAMResourceId. As chaves de acesso expiradas são desativadas e os perfis de login expirados são excluídos.

> **Note**
>
> Certifique-se de configurar o MaxCredentialUsageAge parâmetro desta ação de remediação para corresponder ao maxAccessKeyAge parâmetro da AWS Config regra que você usa para acionar esta ação: access-keys-rotated.

AWSConfigRemediation-SetIAMPasswordPolicy

Descrição

O runbook AWSConfigRemediation-SetIAMPasswordPolicy define a política de senha de usuário do AWS Identity and Access Management (IAM) para sua Conta da AWS.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- AllowUsersToChangePassword

  Tipo: booliano

  Padrão: False

  Descrição: (Opcional) Se definido como`true`, todos os usuários do IAM em Conta da AWS você podem usar o AWS Management Console para alterar suas senhas.
- HardExpiry

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definido como `true`, os usuários do IAM são impedidos de redefinir suas senhas após a expiração desta.
- MaxPasswordAge

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número de dias em que a senha de um usuário do IAM é válida.
- MinimumPasswordLength

Tipo: inteiro

Padrão: 6

Descrição: (opcional) O número mínimo de caracteres que uma senha de usuário do IAM pode ter.

- PasswordReusePrevention

  Tipo: inteiro

  Padrão: 0

  Descrição: (opcional) O número de senhas anteriores que um usuário do IAM é impedido de reutilizar.

- RequireLowercaseCharacters

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definida como `true`, a senha de um usuário do IAM deve conter um caractere minúsculo do alfabeto latino básico ISO (a a z).

- RequireNumbers

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definida como `true`, a senha de um usuário do IAM deve conter um caractere numérico (0 a 9).

- RequireSymbols

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definida como `true`, a senha de um usuário do IAM deve conter um caractere não alfanumérico (! @ # $ % ^ * ( ) _ + - = [ ] { } | ').

- RequireUppercaseCharacters

  Tipo: booliano

Padrão: False

Descrição: (opcional) Se definida como `true`, a senha de um usuário do IAM deve conter um caractere maiúsculo do alfabeto latino básico ISO (A a Z).

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

Etapas do documento

- `aws:executeScript` :Define a política de senha de usuário do IAM com base nos valores especificados para os parâmetros do runbook da sua Conta da AWS.

AWSSupport-ContainIAMPrincipal

Descrição

No caso de um incidente de segurança ou suspeita de comprometimento de um usuário AWS Identity and Access Management (IAM) User/Role ou do AWS Identity Center (IDC), o isolamento rápido da identidade afetada é crucial, preservando sua configuração para investigação. O `AWSSupport-ContainIAMPrincipal` runbook fornece uma abordagem estruturada e reversível para conter identidades IAM ou IDC comprometidas, bloqueando efetivamente seu acesso aos AWS recursos e evitando a possível disseminação do comprometimento.

Esse processo automatizado permite a investigação sem alteração permanente da configuração da identidade, permitindo a restauração do acesso normal quando considerado apropriado. O processo de contenção mantém o usuário ou a função no IAM ou o usuário no IDC, ao mesmo tempo que o isola efetivamente de todas as atividades da rede. Esse isolamento impede que o recurso de identidade contido se comunique com recursos dentro da sua Amazon Virtual Private Cloud ou acesse recursos da Internet. A contenção foi projetada para ser reversível, permitindo a restauração do acesso normal quando considerado apropriado.

Como funciona?

O `AWSSupport-ContainIAMPrincipal` runbook implementa um processo abrangente de contenção para usuários, funções e usuários do Identity Center do IAM. Quando executado no `Contain` modo, ele primeiro valida todos os parâmetros de entrada e executa verificações de segurança no bucket do Amazon S3 especificado. Em seguida, ele reúne informações detalhadas sobre o principal alvo do IAM e aplica medidas de contenção apropriadas com base no tipo principal. Para usuários do IAM, ele desativa as chaves de acesso, remove o acesso ao console e anexa uma política de negação. Para funções do IAM, ele anexa uma política de negação que revoga permissões para sessões criadas antes da contenção. Para usuários do Identity Center, ele remove conjuntos de permissões, associações de grupos e aplica uma política de negação. Durante todo o processo, o runbook faz backup da configuração original em um bucket do Amazon S3 para possível restauração. Quando executado no `Restore` modo, ele tenta reverter o principal para seu estado de pré-contenção usando a configuração de backup. O runbook inclui a `DryRun` opção de visualizar as alterações sem aplicá-las e fornece relatórios abrangentes sobre operações bem-sucedidas e cenários de falha.

Important

- Uso de privilégios elevados: este documento SSM executa várias operações que exigem privilégios elevados, como modificar as políticas de identidade do IAM e do IDC e aplicar configurações de quarentena. Essas ações podem potencialmente levar a um aumento de privilégios ou impactar outras cargas de trabalho que dependem das identidades alvo. Você deve analisar as permissões concedidas à função especificada pelo `AutomationAssumeRole` parâmetro e garantir que elas sejam apropriadas para o caso de uso pretendido. Você pode consultar a AWS documentação a seguir para obter mais informações sobre as permissões do IAM:
  - Permissões de Identity and Access Management (IAM)
  - AWS Permissões de automação do Systems Manager
- Riscos de indisponibilidade da carga de trabalho: este documento do Systems Manager executa ações de isolamento que podem causar indisponibilidade ou interrupção em suas cargas de trabalho. Quando executado durante um evento de segurança, ele restringirá o acesso ao recurso afetado revogando as permissões de AWS API das identidades IAM e IDC especificadas, impedindo que elas façam chamadas ou ações de AWS API. Isso pode afetar qualquer aplicativo ou serviço que dependa dessas identidades.

- Criação de recursos adicionais: O documento de automação pode criar condicionalmente recursos adicionais, como um bucket do Amazon Simple Storage Service (Amazon S3) e objetos do Amazon S3 armazenados nele, dependendo dos parâmetros de execução. Esses recursos incorrerão em cobranças adicionais com base no seu AWS uso.
- Riscos de restauração: se o parâmetro Action estiver definido como`Restore`, esse documento SSM tentará restaurar a configuração de identidade do IAM ou do IDC ao seu estado original. No entanto, existe o risco de que o processo de restauração falhe, deixando a identidade do IAM ou do IDC em um estado inconsistente. O documento fornece instruções para restauração manual em caso de falhas desse tipo, mas você deve estar preparado para lidar com possíveis problemas durante o processo de restauração.

É recomendável revisar o runbook minuciosamente, entender seus possíveis impactos e testá-lo em um ambiente que não seja de produção antes de executá-lo em seu ambiente de produção.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

Permissões obrigatórias do IAM

O `AutomationAssumeRole` parâmetro requer as seguintes permissões para usar o runbook com êxito:

- 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: desativar MFADevice
- objetivo: AttachRolePolicy
- objetivo: AttachUserPolicy

- objetivo: DeleteRolePolicy
- Eu sou: TAG MFADevice
- objetivo: PutRolePolicy
- objetivo: TagPolicy
- objetivo: TagRole
- objetivo: TagUser
- objetivo: UntagUser
- objetivo: UntagRole
- organizações: ListAccounts
- então: ListPermissionSetsProvisionedToAccount
- então: GetInlinePolicyForPermissionSet
- então: ListInstances
- diretório sso: SearchUsers
- então: ListPermissionSets
- então: ListAccountAssignments
- diretório sso: DescribeUser
- loja de identidades: ListUsers
- loja de identidades: ListGroups
- loja de identidades: IsMemberInGroups
- loja de identidades: ListGroupMemberships
- gerente de segredos: CreateSecret
- gerente de segredos: DeleteSecret
- então: DeleteAccountAssignment
- então: PutInlinePolicyToPermissionSet
- então: CreateAccountAssignment
- então: DeleteInlinePolicyFromPermissionSet
- então: TagResource
- então: UntagResource
- loja de identidades: DeleteGroupMembership
- loja de identidades: CreateGroupMembership

Aqui está um exemplo de uma política do IAM que concede as permissões necessárias para`AutomationAssumeRole`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucket",
                "s3:ListBucket",
                "s3:GetBucketPublicAccessBlocks",
                "s3:GetAccountPublicAccessBlocks",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketAcl",
                "s3:GetObject",
                "s3:CreateBucket",
                "s3:PutObject"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:GetUserPolicy",
                "iam:GetRole",
                "iam:ListUserPolicies",
                "iam:ListAttachedUserPolicies",
                "iam:ListAccessKeys",
                "iam:ListMfaDevices",
                "iam:ListVirtualMFADevices",
                "iam:GetLoginProfile",
                "iam:GetPolicy",
                "iam:GetRolePolicy",
                "iam:ListPolicies",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:UpdateAccessKey",
                "iam:CreateAccessKey",
```

```
                "iam:DeleteLoginProfile",
                "iam:DeleteAccessKey",
                "iam:PutUserPolicy",
                "iam:DeleteUserPolicy",
                "iam:DeactivateMFADevice",
                "iam:AttachRolePolicy",
                "iam:AttachUserPolicy",
                "iam:DeleteRolePolicy",
                "iam:TagMFADevice",
                "iam:PutRolePolicy",
                "iam:TagPolicy",
                "iam:TagRole",
                "iam:TagUser",
                "iam:UntagUser",
                "iam:UntagRole"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SSOPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:ListInstances",
                "sso-directory:SearchUsers",
                "sso:ListPermissionSets",
                "sso:ListAccountAssignments",
                "sso-directory:DescribeUser",
                "sso:DeleteAccountAssignment",
                "sso:PutInlinePolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:TagResource",
                "sso:UntagResource"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "IdentityStorePermissions",
            "Effect": "Allow",
            "Action": [
                "identitystore:ListUsers",
                "identitystore:ListGroups",
                "identitystore:IsMemberInGroups",
                "identitystore:ListGroupMemberships",
                "identitystore:DeleteGroupMembership",
                "identitystore:CreateGroupMembership"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SecretsManagerPermissions",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:DeleteSecret"
            ],
            "Resource": "*"
        }
    ]
}
```

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até o AWSSupport-ContainIAMPrincipalno console do AWS Systems Manager.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):
     - Descrição: (Opcional) O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
     - Tipo: `AWS::IAM::Role::Arn`

- PrincipalType (Obrigatório):
  - Descrição: (Obrigatório) O tipo principal AWS do IAM: usuário do IAM, função do IAM ou usuário do Identity Center.
  - Tipo: String
  - Valores permitidos: `IAM user|IAM role|Identity Center user`
- PrincipalName (Obrigatório):
  - Descrição: (Obrigatório) O nome do diretor do IAM. Para usuários do Identity Center, forneça o nome de usuário.
  - Tipo: String
  - Allowed-pattern: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/+=,@]{1,1024}$`
- Ação (obrigatória):
  - Descrição: (Obrigatório) Selecione `Contain` para isolar o IAM principal de destino ou `Restore` para tentar restaurar o IAM principal para sua configuração original a partir de um backup anterior.
  - Tipo: String
  - Valores permitidos: `Contain|Restore`
- DryRun (Opcional):
  - Descrição: (Opcional) Quando definida como`true`, a automação não fará nenhuma alteração no principal do IAM de destino; em vez disso, ela exibirá o que teria tentado alterar, detalhando cada etapa. Valor padrão: `true`.
  - Tipo: booliano
  - Valores permitidos: `true|false`
- ActivateDisabledKeys (Condicional):
  - Descrição: (Condicional) Se o parâmetro de entrada Ação estiver definido como `Restore` e o PrincipalType estiver definido como usuário do IAM, essa opção determinará se essa automação deve tentar ativar as chaves de acesso associadas se desativada. Observe que a integridade de uma chave de acesso comprometida não pode ser verificada. AWS não recomenda fortemente a reativação de uma chave comprometida. Em vez disso, é aconselhável gerar novas chaves. Valor padrão: `false`.
  - Tipo: booliano
  - Valores permitidos: `true|false`
- Backups.3.BucketName (condicionais):

- Descrição: (Condicional) O bucket do Amazon Amazon S3 para fazer backup da configuração principal do IAM quando a Ação está definida como ou `Contain` para restaurar a configuração a partir de quando a Ação está. `Restore` Observe que, se a Ação especificada for `Contain` e o runbook não conseguir acessar o bucket ou se um valor não for fornecido, um novo bucket será criado em sua conta com o nome`awssupport-containiamprincipal-<random-string>`. Se DryRun estiver definido para `true` esse parâmetro é obrigatório.
- Tipo: `AWS::S3::Bucket::Name`

- Backups 3 KeyName (condicionais):
  - Descrição: (Condicional) Se a Ação for definida como`Restore`, isso especifica a chave Amazon Amazon S3 que a automação usará para tentar restaurar a configuração principal do IAM. A chave Amazon Amazon S3 normalmente segue este formato:. `{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json` A chave pode ser obtida a partir da saída de uma execução anterior de automação de contenção.
  - Tipo: String
  - Allowed-pattern: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$`
- Backups 3 BucketAccess (condicionais):
  - Descrição: (Condicional) O ARN dos usuários ou funções do IAM que terão acesso ao bucket de backup do Amazon Amazon S3 após a execução das ações de contenção. Esse parâmetro é necessário quando a Ação é`Contain`. O AutomationAssumeRole, ou, na sua ausência, o usuário sob cujo contexto a automação está sendo executada é automaticamente adicionado à lista.
  - Tipo: StringList
  - Allowed-pattern: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
- TagIdentifier (Opcional):
  - Descrição: (Opcional) Marque o diretor do IAM com uma tag de sua escolha usando o seguinte formato:`Key=<EXAMPLE_KEY>,Value=<EXAMPLE_VALUE>`. Essa opção permite que você acompanhe os principais do IAM que foram alvo desse runbook. Observação: as chaves e os valores das tags diferenciam maiúsculas de minúsculas.
  - Tipo: String
  - Allowed-pattern: `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{0,128}$`

4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - ValidateRequiredInputs

     Valida os parâmetros de entrada de automação necessários com base no `Action` especificado.
   - CheckBackupS3BucketName

     Verifica se o bucket do Amazon Amazon S3 de destino potencialmente `read` concede acesso `write` público a seus objetos. No caso de fluxo de trabalho de contenção, um novo bucket Amazon Amazon S3 é criado se `BackupS3BucketName` o bucket não existir.
   - BranchOnAction

     Ramifica a automação com base no valor do especificado`Action`.
   - BranchOnPrincipalTypeAndDryRun

     Ramifica a automação com base no tipo de IAM principal (usuário do IAM, função do IAM ou usuário do Identity Center) e se ela está sendo executada no `DryRun` modo.
   - BranchOnPrincipalTypeForContain

     Ramifica a automação para a `Contain` ação baseada e o tipo principal do IAM (usuário do IAM, função do IAM ou usuário do Identity Center) especificado na entrada.
   - Obtenha IAMUser

     Obtém a hora de criação e o nome de usuário do IAM de destino.
   - Obtenha IAMUser detalhes

     Obtém e armazena a configuração do usuário de destino do IAM, incluindo políticas embutidas, políticas gerenciadas, chaves de acesso, dispositivos de MFA e perfil de login.
   - Atualizações 3 KeyForUser

     Atualiza a variável de automação 'S3Key' a partir da saída da etapa. `GetIAMUserDetails`
   - Obtenha IAMRole

     Obtém a hora de criação, o nome da função e o caminho da função de destino do IAM.
   - Obtenha IAMRole detalhes

Obtém e armazena a configuração da função de destino do IAM, incluindo políticas embutidas e políticas gerenciadas anexadas à função.

- Atualizações 3 KeyForRole

  Atualiza a variável de automação 'S3Key' a partir da saída da etapa. `GetIAMRoleDetails`

- GetIdentityStoreId

  Obtém o ID da instância AWS do IAM Identity Center associada à AWS conta.

- Obtenha IDCUser

  Obtém a ID do usuário alvo do Identity Center usando a ID do Identity Store.

- Reúna IDCUser os detalhes

  Obtém e armazena a configuração do usuário alvo do Identity Center, incluindo atribuições de contas, conjuntos de permissões associados e políticas em linha.

- Atualizações 3 KeyFor IDCUser

  Atualiza a variável de automação 'S3Key' a partir da saída da etapa. `GatherIDCUserDetails`

- BranchOnIdentityContain

  Ramifica a automação com base no valor `DryRun` e no tipo principal do IAM para a `Contain` ação.

- BranchOnDisableAccessKeys

  Ramifica a automação com base no fato de o usuário do IAM ter chaves de acesso que precisam ser desativadas.

- DisableAccessKeys

  Desativa as chaves de acesso do usuário do IAM ativas.

- BranchOnDisableConsoleAccess

  Ramifica com base no fato de o usuário do IAM ter acesso ao AWS Management Console ativado ou não.

- DisableConsoleAccess

  Remove o acesso baseado em senha do usuário do IAM ao Management Console. AWS

- AttachInlineDenyPolicyToUser

Anexa uma política de negação ao usuário do IAM para revogar permissões para tokens de sessão mais antigos.

- AttachInlineDenyPolicyToRole

  Anexa uma política de negação à função do IAM para revogar permissões para tokens de sessão mais antigos.

- RemovePermissionSets

  Remove os conjuntos de permissões associados ao usuário do Identity Center.

- Remover IDCUser de IDCGroups

  Remove o usuário do Identity Center dos grupos do Identity Center.

- AttachInlineDenyPolicyToPermissionSet

  Anexa uma política de negação aos conjuntos de permissões associados ao usuário do Identity Center.

- BranchOnReactivateKeys

  Ramifica a automação com base no `ActivateDisabledKeys` parâmetro durante o processo de restauração.

- DetachInlineDenyPolicy

  Remove a política de negação associada à função do IAM durante o processo de contenção.

- DetachInlineDenyPolicyFromPermissionSet

  Remove a política de negação anexada aos conjuntos de permissões durante o processo de contenção.

- ReportContain

  Produz informações detalhadas sobre as ações de contenção que seriam executadas quando `DryRun` definido como. `True`

- ReportRestore

  Produz informações detalhadas sobre as ações de restauração que seriam executadas quando `DryRun` estiver definido como. `True`

- ReportContainFailure

Fornece instruções abrangentes para restaurar manualmente a configuração original do diretor do IAM durante um cenário de falha no fluxo de trabalho de contenção.

- ReportRestoreFailure

  Fornece instruções detalhadas para concluir manualmente a restauração da configuração original do IAM principal durante um cenário de falha no fluxo de trabalho de restauração.

7. Após a conclusão da execução, revise a seção Saídas para obter os resultados detalhados da execução:

   - ContémIAMPrincipal. Saída

     Fornece informações detalhadas sobre as ações de contenção realizadas quando a Ação é definida como Conter e DryRun é definida como False. Inclui informações sobre o local do backup, políticas de negação aplicadas e configurações modificadas.

   - RestaurarIAMPrincipal. Saída

     Fornece informações detalhadas sobre as ações de restauração realizadas quando a Ação está definida como Restaurar e DryRun está definida como False. Inclui informações sobre as configurações restauradas e quaisquer problemas encontrados durante a restauração.

   - ReportContain.Saída

     Produz informações detalhadas sobre as ações de contenção que seriam executadas quando a Ação fosse definida como Conter e DryRun definida como Verdadeira. Inclui uma comparação das configurações atuais e pós-contenção.

   - ReportRestore.Saída

     Produz informações detalhadas sobre as ações de restauração que seriam executadas quando a Ação estivesse definida como Restaurar e DryRun definida como Verdadeira. Mostra a configuração atual e a configuração original que seria restaurada.

   - ReportContainFailure.Saída

     Fornece instruções abrangentes para restaurar manualmente a configuração original do diretor do IAM durante um cenário de falha no fluxo de trabalho de contenção.

   - ReportRestoreFailure.Saída

     Fornece instruções detalhadas para concluir manualmente a restauração da configuração original do IAM principal durante um cenário de falha no fluxo de trabalho de restauração.

Saídas

Depois que a execução for concluída, revise a seção Saídas para obter os resultados detalhados:

- ContémIAMPrincipal. Saída

  Fornece informações detalhadas sobre as ações de contenção realizadas quando a Ação é definida como Conter e DryRun é definida como False. Inclui informações sobre o local do backup, políticas de negação aplicadas e configurações modificadas.
- RestaurarIAMPrincipal. Saída

  Fornece informações detalhadas sobre as ações de restauração realizadas quando a Ação está definida como Restaurar e DryRun está definida como False. Inclui informações sobre as configurações restauradas e quaisquer problemas encontrados durante a restauração.
- ReportContain.Saída

  Produz informações detalhadas sobre as ações de contenção que seriam executadas quando a Ação fosse definida como Conter e DryRun definida como Verdadeira. Inclui uma comparação das configurações atuais e pós-contenção.
- ReportRestore.Saída

  Produz informações detalhadas sobre as ações de restauração que seriam executadas quando a Ação estivesse definida como Restaurar e DryRun definida como Verdadeira. Mostra a configuração atual e a configuração original que seria restaurada.
- ReportContainFailure.Saída

  Fornece instruções abrangentes para restaurar manualmente a configuração original do diretor do IAM durante um cenário de falha no fluxo de trabalho de contenção.
- ReportRestoreFailure.Saída

  Fornece instruções detalhadas para concluir manualmente a restauração da configuração original do IAM principal durante um cenário de falha no fluxo de trabalho de restauração.

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação simples

- Configurando a automação
- Fluxos de trabalho de automação de suporte

Amazon Kinesis Data Streams

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Kinesis Data Streams. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableKinesisStreamEncryption

`AWS-EnableKinesisStreamEncryption`

Descrição

O `AWS-EnableKinesisStreamEncryption` runbook permite a criptografia em um Amazon Kinesis Data Streams (Kinesis Data Streams). Os aplicativos produtores que gravam em um fluxo criptografado encontrarão erros se não tiverem acesso à chave AWS Key Management Service (AWS KMS).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- KinesisStreamName

  Tipo: string

  Descrição: (Obrigatório) O nome do stream no qual você deseja habilitar a criptografia.

- KeyId

  Tipo: string

  Padrão: alias/aws/kinesis

  Descrição: (Obrigatório) A AWS KMS chave gerenciada pelo cliente que você deseja usar para criptografia. Esse valor pode ser um identificador global exclusivo, um ARN para um alias ou uma chave ou um nome de alias prefixado por “alias/”. Você também pode usar a chave AWS gerenciada usando o valor padrão do parâmetro.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

Etapas do documento

- VerifyKinesisStreamStatus (`aws:waitforAwsResourceProperty`) - Verifica o status do Kinesis Data Streams.
- EnableKinesisStreamEncryption (`aws:executeAwsApi`) - Ativa a criptografia para o Kinesis Data Streams.

- VerifyKinesisStreamUpdateComplete (`aws:waitForAwsResourceProperty`) - Aguarda o retorno do status do Kinesis Data Streams. `ACTIVE`
- VerifyKinesisStreamEncryption (`aws:assertAwsResourceProperty`) - Verifica se a criptografia está ativada para o Kinesis Data Streams.

AWS KMS

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Key Management Service Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-CancelKeyDeletion
- AWSConfigRemediation-EnableKeyRotation

`AWSConfigRemediation-CancelKeyDeletion`

Descrição

O `AWSConfigRemediation-CancelKeyDeletion` runbook cancela a exclusão da chave gerenciada pelo cliente AWS Key Management Service (AWS KMS) especificada por você.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- KeyId

  Tipo: String

  Descrição: (obrigatório) O ID da chave gerenciada pelo cliente da qual deseja cancelar a exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CancelKeyDeletion`
- `kms:DescribeKey`

Etapas do documento

- `aws:executeAwsApi` :Cancela a exclusão da chave gerenciada pelo cliente especificada no parâmetro `KeyId`.
- `aws:assertAwsResourceProperty` :Confirma que a exclusão da chave está desabilitada em sua chave gerenciada pelo cliente.

AWSConfigRemediation-EnableKeyRotation

Descrição

O `AWSConfigRemediation-EnableKeyRotation` runbook permite a rotação automática de chaves para a chave simétrica AWS Key Management Service (AWS KMS) gerenciada pelo cliente.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- KeyId

  Tipo: String

  Descrição: (obrigatório) O ID da chave gerenciada pelo cliente na qual deseja habilitar a rotação automática de chaves.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

Etapas do documento

- `aws:executeAwsApi` :Permite a rotação automática da chave gerenciada pelo cliente especificada no parâmetro `KeyId`.

- `aws:assertAwsResourceProperty` :Confirma se a rotação automática de chaves está habilitada na chave gerenciada pelo cliente.

Lambda

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Lambda Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing
- AWSConfigRemediation-DeleteLambdaFunction
- AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK
- AWSConfigRemediation-MoveLambdaToVPC
- AWSSupport-RemediateLambdaS3Event
- AWSSupport-TroubleshootLambdaInternetAccess
- AWSSupport-TroubleshootLambdaS3Event

`AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing`

Descrição

O `AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing` runbook permite o rastreamento AWS X-Ray ao vivo na AWS Lambda função que você especifica no `FunctionName` parâmetro.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- FunctionName

  Tipo: String

  Descrição: (obrigatório) O nome ou ARN da função do Lambda para ativar o rastreamento.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `lambda:UpdateFunctionConfiguration`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Etapas do documento

- `aws:executeAwsApi` :Ativa o rastreamento de raio-X na função do Lambda especificada no parâmetro `FunctionName`.
- `aws:assertAwsResourceProperty` :Verifica se o rastreamento de X-Ray foi ativado na função do Lambda.

Saídas

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - Resposta da chamada `UpdateFunctionConfiguration` da API.

AWSConfigRemediation-DeleteLambdaFunction

Descrição

O runbook `AWSConfigRemediation-DeleteLambdaFunction` exclui a função AWS Lambda especificada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LambdaFunctionName

  Tipo: String

  Descrição: (obrigatório) O nome da função do Lambda a ser excluída.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

Etapas do documento

- `aws:executeAwsApi` :Exclui a função do Lambda especificada no parâmetro `LambdaFunctionName`.
- `aws:executeScript` :Verifica se a função do Lambda foi excluída.

`AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK`

Descrição

O `AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` runbook criptografa, em repouso, as variáveis de ambiente para a função (AWS Lambda Lambda) que você especifica usando uma chave gerenciada pelo cliente AWS Key Management Service (AWS KMS). Esse runbook só deve ser usado como uma linha de base para garantir que as variáveis de ambiente da sua função do Lambda sejam criptografadas de acordo com as melhores práticas de segurança mínimas recomendadas. Recomendamos criptografar várias funções com diferentes chaves gerenciadas pelo cliente.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- FunctionName

  Tipo: String

  Descrição: (obrigatório) O nome ou ARN da função do Lambda cujas variáveis de ambiente serão criptografadas.

- KMSKeyArn

  Tipo: String

  Descrição: (Obrigatório) O ARN da chave gerenciada pelo AWS KMS cliente que você deseja usar para criptografar as variáveis de ambiente da função Lambda.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Etapas do documento

- `aws:waitForAwsResourceProperty` :Espera que a propriedade `LastUpdateStatus` fique `Successful`.
- `aws:executeAwsApi`- Criptografa as variáveis de ambiente da função Lambda que você especifica `FunctionName` no parâmetro usando AWS KMS a chave gerenciada pelo cliente especificada no `KMSKeyArn` parâmetro.
- `aws:assertAwsResourceProperty` :Confirma que a criptografia está habilitada nas variáveis de ambiente da sua função do Lambda.

AWSConfigRemediation-MoveLambdaToVPC

Descrição

O runbook `AWSConfigRemediation-MoveLambdaToVPC` move uma função AWS Lambda do (Lambda) para uma Amazon Virtual Private Cloud (Amazon VPC).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- FunctionName

  Tipo: String

  Descrição: (obrigatório) O nome da função do Lambda a ser movida para uma Amazon VPC.
- SecurityGroupIds

  Tipo: String

  Descrição: (Obrigatório) O grupo de segurança que IDs você deseja atribuir às interfaces de rede elástica (ENIs) associadas à sua função Lambda.
- SubnetIds

Tipo: String

Descrição: (Obrigatório) A sub-rede na qual IDs você deseja criar as interfaces de rede elástica (ENIs) associadas à sua função Lambda.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

Etapas do documento

- `aws:executeAwsApi` :Atualiza a configuração da Amazon VPC para a função do Lambda especificada no parâmetro `FunctionName`.
- `aws:waitForAwsResourceProperty` :Espera que a função do Lambda `LastUpdateStatus` seja `successful`.
- `aws:executeScript` :Verifica se a configuração da função do Lambda da Amazon VPC foi atualizada com sucesso.

`AWSSupport-RemediateLambdaS3Event`

Descrição

O `AWSSupport-TroubleshootLambdaS3Event` runbook fornece uma solução automatizada para os procedimentos descritos nos artigos do AWS Knowledge Center Por que minha notificação de eventos do Amazon S3 não aciona minha função Lambda? e Por que recebo o erro “Não é possível validar as seguintes configurações de destino” ao criar uma notificação de evento do Amazon S3 para acionar minha função Lambda? Esse runbook ajuda você a identificar e corrigir o motivo pelo qual uma notificação de evento do Amazon Simple Storage Service (Amazon S3) falhou em acionar a função especificada. AWS Lambda Se a saída do runbook sugerir a validação e a configuração da

simultaneidade da função do Lambda, consulte Invocação assíncrona e escalabilidade de funções do AWS Lambda.

> **Note**
>
> O erro “Não foi possível validar as seguintes configurações de destino” também podem ocorrer devido a configurações incorretas de eventos do Amazon Simple Notification Service (Amazon SNS) e do Amazon Simple Queue Service (Amazon SQS) do Amazon S3. Esse runbook verifica somente as configurações da função do Lambda. Se, depois de usar o runbook, você ainda estiver recebendo o erro “Não foi possível validar as seguintes configurações de destino”, revise todas as configurações de eventos existentes do Amazon SNS e do Amazon SQS Amazon S3.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LambdaFunctionArn

  Tipo: String

Descrição: (obrigatório) O ARN da função do Lambda.

- S3 BucketName

  Tipo: String

  Descrição: (obrigatório) O nome do bucket do Amazon S3 cujas notificações de eventos acionam a função do Lambda.

- Ação

  Tipo: String

  Valores válidos: Troubleshoot | Remediate

  Descrição: (obrigatório) As operações que você deseja que o runbook execute. A opção `Troubleshoot` ajuda a identificar qualquer problema, mas não executa nenhuma ação de mutação para resolver o problema. A opção `Remediate` ajuda a identificar e tenta resolver problemas para você.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

Etapas do documento

- `aws:branch` :Ramifica com base na entrada especificada para o parâmetro `Action`.

Se o valor especificado for `Troubleshoot`:

- `aws:executeAutomation` :Executa o runbook `AWSSupport-TroubleshootLambdaS3Event`.
- `aws:executeAwsApi` :Verifica a saída do runbook `AWSSupport-TroubleshootLambdaS3Event` executado na etapa anterior.

Se o valor especificado for `Remediate`:

- `aws:executeScript` :Executa um script para corrigir os problemas descritos na seção Por que minha notificação de eventos do Amazon S3 não aciona minha função do Lambda? e Por que recebo o erro “Não foi possível validar as seguintes configurações de destino” ao criar uma notificação de evento do Amazon S3 para acionar minha função do Lambda? Artigos do Centro de Conhecimentos.

Saídas

checkoutput.Output

remediatelambdas3event.Output

AWSSupport-TroubleshootLambdaInternetAccess

Descrição

O `AWSSupport-TroubleshootLambdaInternetAccess` runbook ajuda você a solucionar problemas de acesso à Internet para uma AWS Lambda função que foi lançada na Amazon Virtual Private Cloud (Amazon VPC). Recursos como rotas de sub-rede, regras de grupos de segurança e regras de lista de controle de acesso (ACL) à rede são revisados para confirmar se o acesso de saída à Internet é permitido.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- FunctionName

  Tipo: String

  Descrição: (obrigatório) O nome da função do Lambda para a qual deseja solucionar problemas de acesso à Internet.
- destinationIp

  Tipo: String

  Descrição: (obrigatório) O endereço IP de destino com o qual deseja estabelecer uma conexão de saída.
- destinationPort

  Tipo: String

  Padrão: 443

  Descrição: (opcional) A porta de destino com o qual deseja estabelecer uma conexão de saída.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`

- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

Etapas do documento

- `aws:executeScript` :Verifica a configuração de vários recursos na VPC onde a função do Lambda foi lançada.
- `aws:branch` :Ramifica com base no fato de a função do Lambda especificada estar em uma VPC ou não.
- `aws:executeScript` :Analisa as rotas da tabela de rotas da sub-rede em que a função do Lambda foi iniciada e verifica se as rotas para um gateway de conversão de endereços de rede (NAT) e um gateway da internet estão presentes. Confirma que a função do Lambda não está em uma sub-rede pública.
- `aws:executeScript` :Verifica se o grupo de segurança associado à função do Lambda permite acesso externo à Internet com base nos valores especificados para os parâmetros `destinationIp` e `destinationPort`.
- `aws:executeScript` :Verifica se as regras da ACL associadas às sub-redes da função do Lambda e o gateway NAT permitem acesso externo à Internet com base nos valores especificados para os parâmetros `destinationIp` e `destinationPort`.

Saídas

checkVpc.vpc :o ID da VPC em que a função do Lambda foi lançada.

CheckVPC.subnet - A IDs das sub-redes em que sua função Lambda foi lançada.

checkVpc.securityGroups :grupos de segurança associados à função do Lambda.

checkNACL.NACL :Mensagem de análise com nomes de recursos. `LambdaIp` refere-se ao endereço IP privado da interface de rede elástica para a função do Lambda. O objeto `LambdaIpRules` é gerado somente para sub-redes que têm uma rota para um gateway NAT. O conteúdo a seguir é um exemplo de saída.

```
{
   "subnet-1234567890":{
      "NACL":"acl-1234567890",
```

```
      "destinationIp_Egress":"Allowed",
      "destinationIp_Ingress":"notAllowed",
      "Analysis":"This NACL has an allow rule for Egress traffic but there is no
 Ingress rule. Please allow the destination IP / destionation port in Ingress rule",
      "LambdaIpRules":{
         "{LambdaIp}":{
            "Egress":"notAllowed",
            "Ingress":"notAllowed",
            "Analysis":"This is a NAT subnet NACL. It does not have ingress or egress
 rule allowed in it for Lambda's corresponding private ip {LambdaIp} Please allow this
 IP in your egress and ingress NACL rules"
         }
      }
   },
   "subnet-0987654321":{
      "NACL":"acl-0987654321",
      "destinationIp_Egress":"Allowed",
      "destinationIp_Ingress":"notAllowed",
      "Analysis":"This NACL has an allow rule for Egress traffic but there is no
 Ingress rule. Please allow the destination IP / destionation port in Ingress rule"
   }
}
```

checkSecurityGroups.secgrps - Análise do grupo de segurança associado à sua função Lambda. O conteúdo a seguir é um exemplo de saída.

```
{
   "sg-123456789":{
      "Status":"Allowed",
      "Analysis":"This security group has allowed destintion IP and port in its
 outbuond rule."
   }
}
```

checkSubnet.subnets :Análise das sub-redes na VPC associadas à função do Lambda. O conteúdo a seguir é um exemplo de saída.

```
{
   "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

Descrição

O `AWSSupport-TroubleshootLambdaS3Event` runbook fornece uma solução automatizada para os procedimentos descritos nos artigos do AWS Knowledge Center Por que minha notificação de eventos do Amazon S3 não aciona minha função Lambda? e Por que recebo o erro “Não é possível validar as seguintes configurações de destino” ao criar uma notificação de evento do Amazon S3 para acionar minha função Lambda? Esse runbook ajuda você a identificar por que uma notificação de evento do Amazon Simple Storage Service (Amazon S3) falhou em acionar a função especificada. AWS Lambda Se a saída do runbook sugerir a validação e a configuração da simultaneidade da função do Lambda, consulte Invocação assíncrona e escalabilidade de funções do AWS Lambda.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- LambdaFunctionArn

  Tipo: String

  Descrição: (obrigatório) O ARN da função do Lambda que a notificação de eventos do Amazon S3 aciona.

- S3 BucketName

  Tipo: String

  Descrição: (obrigatório) O nome do bucket do Amazon S3 cujas notificações de eventos acionam a função do Lambda.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

Etapas do documento

- `aws:executeScript` :Executa o script para validar as definições de configuração da notificação de eventos do Amazon S3. Valida a política do IAM baseada em recursos para sua função Lambda e gera um comando AWS Command Line Interface (AWS CLI) para adicionar as permissões necessárias se as permissões necessárias estiverem ausentes da política. Valida outras políticas de recursos de funções Lambda que fazem parte das notificações de eventos para o mesmo bucket do S3 e gera AWS CLI um comando como saída se as permissões necessárias estiverem ausentes.

Saídas

lambdaS3Event.output

Amazon Managed Workflows for Apache Airflow

AWS Systems Manager A automação fornece runbooks predefinidos para fluxos de trabalho gerenciados da Amazon para Apache Airflow. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-TroubleshootMWAAEnvironmentCreation

`AWSSupport-TroubleshootMWAAEnvironmentCreation`

Descrição

O `AWSSupport-TroubleshootMWAAEnvironmentCreation` runbook fornece informações para depurar problemas de criação de ambientes do Amazon Managed Workflows for Apache Airflow (Amazon MWAA) e realizar verificações, juntamente com os motivos documentados, da melhor forma possível, para ajudar a identificar a falha.

Como funciona?

O runbook executa as seguintes etapas:

- Recupera os detalhes do ambiente Amazon MWAA.
- Verifica as permissões da função de execução.
- Verifica se o ambiente tem permissões para usar a AWS KMS chave fornecida para registro e se o grupo de CloudWatch registros necessário existe.
- Analisa os registros no grupo de registros fornecido para localizar quaisquer erros.
- Verifica a configuração da rede para verificar se o ambiente Amazon MWAA tem acesso aos endpoints necessários.
- Gera um relatório com as descobertas.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

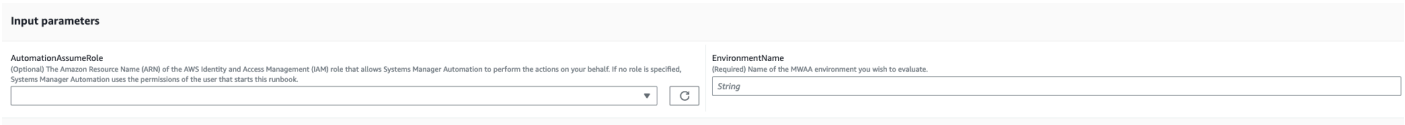
Instruções

Siga estas etapas para configurar a automação:

1. Navegue até `AWSSupport-TroubleshootMWAAEnvironmentCreation`em Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - EnvironmentName (Obrigatório):

     Nome do ambiente Amazon MWAA que você deseja avaliar.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - **`GetMWAAEnvironmentDetails:`**

     Recupera os detalhes do ambiente Amazon MWAA. Se essa etapa falhar, o processo de automação será interrompido e exibido como`Failed`.
   - **`CheckIAMPermissionsOnExecutionRole:`**

     Verifica se a função de execução tem as permissões necessárias para os recursos do Amazon MWAA, Amazon S3, CloudWatch Logs e CloudWatch Amazon SQS. Se detectar uma chave gerenciada pelo cliente AWS Key Management Service (AWS KMS), a automação valida as permissões necessárias da chave. Essa etapa emprega a `iam:SimulateCustomPolicy`

API para verificar se a função de execução da automação atende a todas as permissões necessárias.

- **CheckKMSPolicyOnKMSKey:**

  Verifica se a política de AWS KMS chaves permite que o ambiente Amazon MWAA use a chave para criptografar CloudWatch registros. Se a AWS KMS chave for AWS gerenciada, a automação ignora essa verificação.

- **CheckIfRequiredLogGroupsExists:**

  Verifica se os grupos de CloudWatch log necessários para o ambiente Amazon MWAA existem. Caso contrário, a automação verifica CloudTrail `CreateLogGroup` os `DeleteLogGroup` eventos. Essa etapa também verifica a existência de `CreateLogGroup` eventos.

- **BranchOnLogGroupsFindings:**

  Ramificações com base na existência de grupos de CloudWatch registros relacionados ao ambiente Amazon MWAA. Se existir pelo menos um grupo de registros, a automação o analisará para localizar erros. Se nenhum grupo de registros estiver presente, a automação pulará a próxima etapa.

- **CheckForErrorsInLogGroups:**

  Analisa os grupos de CloudWatch registros para localizar erros.

- **GetRequiredEndPointsDetails:**

  Recupera os endpoints de serviço utilizados pelo ambiente Amazon MWAA.

- **CheckNetworkConfiguration:**

  Verifica se a configuração de rede do ambiente Amazon MWAA atende aos requisitos, incluindo verificações de grupos de segurança, rede ACLs, sub-redes e configurações de tabela de rotas.

- **CheckEndpointsConnectivity:**

  Invoca a automação `AWSSupport-ConnectivityTroubleshooter` secundária para validar a conectividade do Amazon MWAA com os endpoints necessários.

- **CheckS3BlockPublicAccess:**

  Verifica se o bucket Amazon S3 do ambiente Amazon MWAA `Block Public Access` foi ativado e também analisa as configurações gerais do Amazon S3 Block Public Access da conta.

- **GenerateReport:**

Coleta informações da automação e imprime o resultado ou a saída de cada etapa.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:
   - Verificando as permissões da função de execução do ambiente Amazon MWAA:

     Verifica se a função de execução tem as permissões necessárias para os recursos do Amazon MWAA, Amazon S3, CloudWatch Logs e CloudWatch Amazon SQS. Se uma AWS KMS chave gerenciada pelo cliente for detectada, a automação valida as permissões necessárias da chave.
   - Verificando a política AWS KMS chave do ambiente Amazon MWAA:

     Verifica se a função de execução possui as permissões necessárias para os recursos do Amazon MWAA, Amazon S3 CloudWatch , Logs e CloudWatch Amazon SQS. Além disso, se uma AWS KMS chave gerenciada pelo cliente for detectada, a automação verificará as permissões necessárias da chave.
   - Verificando os grupos de CloudWatch registros do ambiente Amazon MWAA:

     Verifica se os grupos de CloudWatch log necessários para o ambiente Amazon MWAA existem. Caso contrário, a automação verifica CloudTrail a localização `CreateLogGroup` e `DeleteLogGroup` os eventos.
   - Verificando as tabelas de rotas do ambiente Amazon MWAA:

     Verifica se as tabelas de rotas da Amazon VPC no ambiente Amazon MWAA estão configuradas corretamente.
   - Verificando os grupos de segurança do ambiente Amazon MWAA:

     Verifica se os grupos de segurança Amazon VPC do ambiente Amazon MWAA estão configurados corretamente.
   - Verificando a rede do ambiente Amazon MWAA: ACLs

     Verifica se os grupos de segurança da Amazon VPC no ambiente Amazon MWAA estão configurados corretamente.
   - Verificando as sub-redes do ambiente Amazon MAA:

     Verifica se as sub-redes do ambiente Amazon MWAA são privadas.
   - A verificação do ambiente Amazon MWAA exigia conectividade de endpoints:

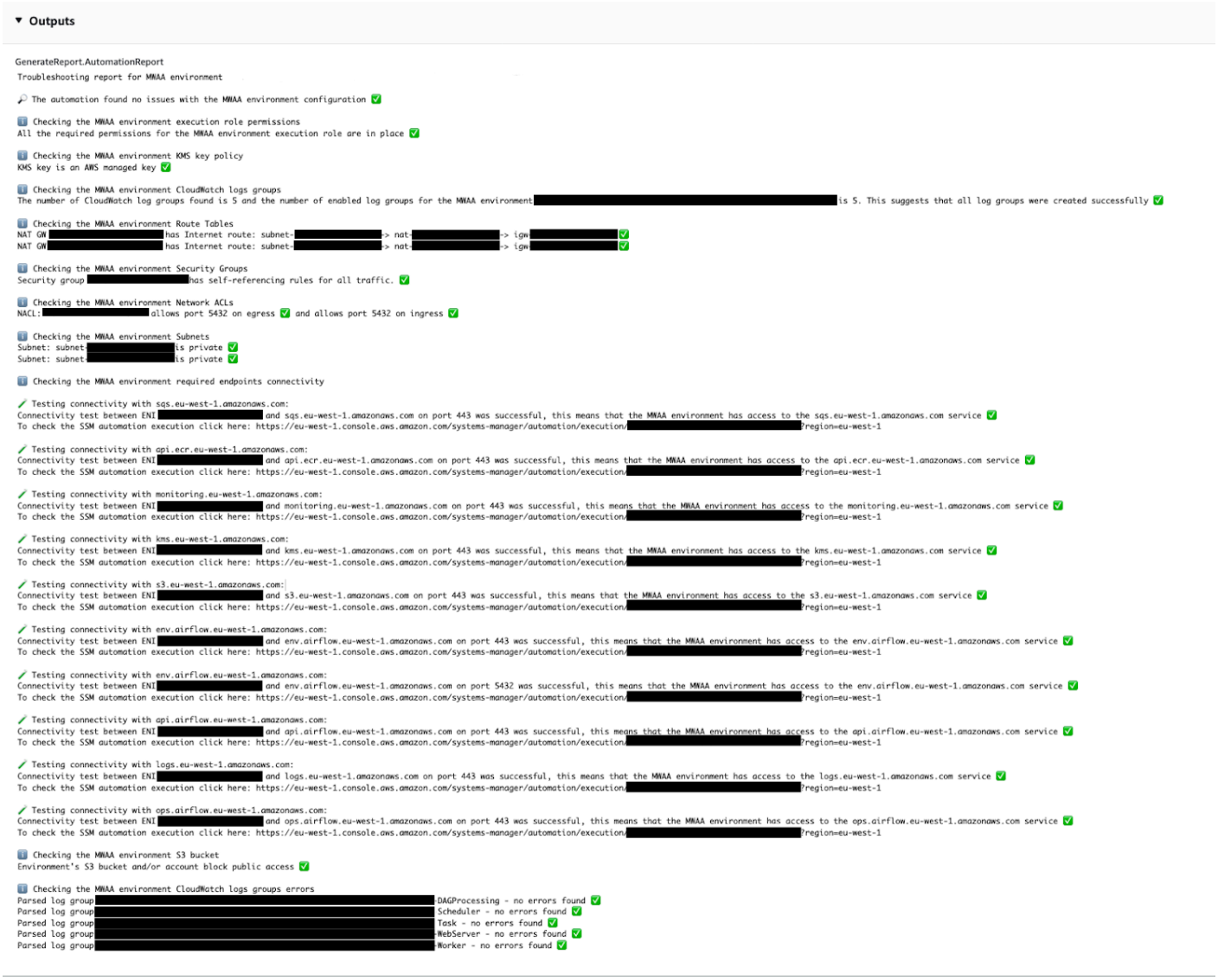
     Verifica se o ambiente Amazon MWAA pode acessar os endpoints necessários. Para isso, a automação invoca a `AWSSupport-ConnectivityTroubleshooter` automação.

- Verificando o ambiente Amazon MWAA (bucket do Amazon S3):

  Verifica se o bucket Amazon S3 do ambiente Amazon MWAA `Block Public Access` foi ativado e também analisa as configurações do Amazon S3 Block Public Access da conta.

- Verificar os CloudWatch registros do ambiente Amazon MWAA agrupa erros:

  Analisa os grupos de CloudWatch log existentes do ambiente Amazon MWAA para localizar erros.



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

Neptune

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Neptune. Para obter mais informações sobre runbooks, consulte Trabalhando com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableNeptuneDbAuditLogsToCloudWatch
- AWS-EnableNeptuneDbBackupRetentionPeriod
- AWS-EnableNeptuneClusterDeletionProtection

`AWS-EnableNeptuneDbAuditLogsToCloudWatch`

Descrição

O `AWS-EnableNeptuneDbAuditLogsToCloudWatch` runbook ajuda você a enviar registros de auditoria de um cluster de banco de dados Amazon Neptune para o Amazon Logs. CloudWatch

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DbClusterResourceId

  Tipo: string

  Descrição: (Obrigatório) O ID do recurso do cluster de banco de dados Neptune para o qual você deseja habilitar os registros de auditoria.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Retorna o ID do cluster de banco de dados Neptune.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Verifica se o tipo de mecanismo do Neptune DB é. `neptune`
- EnableNeptuneDbAuditLogs (`aws:executeAwsApi`) - Permite que os registros de auditoria do cluster de banco de dados Neptune recebam registros. CloudWatch
- VerifyNeptuneDbStatus (`aws:waitAwsResourceProperty`) - Verifica se o status do cluster de banco de dados Neptune é. `available`

- VerifyNeptuneDbAuditLogs (`aws:executeScript`) - Verifica se os registros de auditoria foram configurados com sucesso para serem enviados ao CloudWatch Logs.

AWS-EnableNeptuneDbBackupRetentionPeriod

Descrição

O `AWS-EnableNeptuneDbBackupRetentionPeriod` runbook ajuda você a habilitar backups automatizados com um período de retenção de backup entre 7 e 35 dias para um cluster de banco de dados Amazon Neptune.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DbClusterResourceId

  Tipo: string

  Descrição: (Obrigatório) O ID do recurso do cluster de banco de dados Neptune para o qual você deseja habilitar backups.

- BackupRetentionPeriod

  Tipo: inteiro

  Valores válidos: 7-35

  Descrição: (Obrigatório) O número de dias em que os backups são retidos.
- PreferredBackupWindow

  Tipo: string

  Descrição: (Opcional) Um período diário de pelo menos 30 minutos quando os backups são feitos. O valor deve estar em Tempo Universal Coordenado (UTC) e usar o formato:`hh24:mm-hh24:mm`. O período de retenção de backup não pode entrar em conflito com a janela de manutenção preferida.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Retorna o ID do cluster de banco de dados Neptune.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Verifica se o tipo de mecanismo do Neptune DB é. `neptune`
- VerifyNeptuneDbStatus (`aws:waitAwsResourceProperty`) - Verifica se o status do cluster de banco de dados Neptune é. `available`
- ModifyNeptuneDbRetentionPeriod (`aws:executeAwsApi`) - Define o período de retenção para o cluster de banco de dados Neptune.

- VerifyNeptuneDbBackupsEnabled (`aws:executeScript`) - Verifica se o período de retenção e a janela de backup foram definidos com sucesso.

AWS-EnableNeptuneClusterDeletionProtection

Descrição

O `AWS-EnableNeptuneClusterDeletionProtection` runbook permite a proteção contra exclusão do cluster Amazon Neptune que você especificar.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DbClusterResourceId

  Tipo: string

  Descrição: (Obrigatório) O ID do cluster Neptune no qual você deseja ativar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Retorna o ID do cluster de banco de dados Neptune.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Verifica se o tipo de mecanismo do cluster de banco de dados especificado é `neptune`.
- VerifyNeptuneStatus (`aws:waitForAwsResourceProperty`) - Verifica se o status do cluster é `available`.
- EnableNeptuneDbDeletionProtection (`aws:executeAwsApi`) - Ativa a proteção contra exclusão no cluster de banco de dados Neptune.
- VerifyNeptuneDbDeletionProtection (`aws:assertAwsResourceProperty`) - Verifica se a proteção contra exclusão está habilitada no cluster de banco de dados.

Saídas

- EnableNeptuneDbDeletionProtection. EnableNeptuneDbDeletionProtectionResponse - A saída da operação da API.

Amazon RDS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Relational Database Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-CreateEncryptedRdsSnapshot
- AWS-CreateRdsSnapshot
- AWSConfigRemediation-DeleteRDSCluster
- AWSConfigRemediation-DeleteRDSClusterSnapshot
- AWSConfigRemediation-DeleteRDSInstance
- AWSConfigRemediation-DeleteRDSInstanceSnapshot
- AWSConfigRemediation-DisablePublicAccessToRDSInstance
- AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster
- AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance
- AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance
- AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS
- AWSConfigRemediation-EnableMultiAZOnRDSInstance
- AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance
- AWSConfigRemediation-EnableRDSClusterDeletionProtection
- AWSConfigRemediation-EnableRDSInstanceBackup
- AWSConfigRemediation-EnableRDSInstanceDeletionProtection
- AWSConfigRemediation-ModifyRDSInstancePortNumber
- AWSSupport-ModifyRDSSnapshotPermission
- AWSPremiumSupport-PostgreSQLWorkloadReview
- AWS-RebootRdsInstance
- AWSSupport-ShareRDSSnapshot
- AWS-StartRdsInstance
- AWS-StartStopAuroraCluster
- AWS-StopRdsInstance
- AWSSupport-TroubleshootConnectivityToRDS
- AWSSupport-TroubleshootRDSIAMAuthentication
- AWSSupport-ValidateRdsNetworkConfiguration

AWS-CreateEncryptedRdsSnapshot

Descrição

O `AWS-CreateEncryptedRdsSnapshot` runbook cria um snapshot criptografado de uma instância não criptografada do Amazon Relational Database Service (Amazon RDS).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DBInstanceIdentificador

  Tipo: String

  Descrição: (Obrigatório) O ID da instância do Amazon RDS da qual você deseja criar um snapshot.
- DBSnapshotIdentificador

  Tipo: String

  Descrição: (Opcional) O modelo de nome para o snapshot do Amazon RDS. O modelo de nome padrão é*`DBInstanceIdentifier-yyyymmddhhmmss`*.
- DBSnapshotIdentificador criptografado

  Tipo: String

Descrição: (Opcional) O nome do instantâneo criptografado. O nome padrão é o valor que você especifica para o `DBSnapshotIdentifier` parâmetro anexado`-encrypted`.

- InstanceTags

  Tipo: String

  Descrição: (Opcional) Tags a serem adicionadas à instância de banco de dados. (Exemplo: key=tagKey1, value=tagValue1; key=tagKey2, value=tagValue2) '

- KmsKeyId

  Tipo: String

  Padrão: `alias/aws/rds`

  Descrição: (Opcional) O ARN, o ID da chave ou o alias da chave gerenciada pelo cliente que você deseja usar para criptografar o snapshot.

- SnapshotTags

  Tipo: String

  Descrição: (Opcional) Tags a serem adicionadas ao instantâneo. (Exemplo: key=tagKey1, value=tagValue1; key=tagKey2, value=tagValue2) '

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds:CreateDBSnapshot`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Etapas do documento

- `aws:executeScript`- Cria um instantâneo da instância de banco de dados que você especifica no `DBInstanceIdentifier` parâmetro.

- `aws:executeScript`- Verifica se o instantâneo criado na etapa anterior existe e é. `available`
- `aws:executeScript`- Copia o instantâneo criado anteriormente em um instantâneo criptografado.
- `aws:executeScript`- Verifica se o instantâneo criptografado criado na etapa anterior existe.

Saídas

CopyRdsSnapshotToEncryptedRdsSnapshot. EncryptedSnapshotId - O ID do snapshot criptografado do Amazon RDS.

AWS-CreateRdsSnapshot

Descrição

Criar um snapshot do Amazon Relational Database Service (Amazon RDS) para uma instância do Amazon RDS.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DBInstanceIdentificador

  Tipo: String

  Descrição: (Obrigatório) O DBInstance ID da instância do RDS a partir da qual criar o snapshot.
- DBSnapshotIdentificador

  Tipo: String

  Descrição: (Opcional) O ID do DBSnapshot identificador do instantâneo do RDS a ser criado.
- InstanceTags

  Tipo: String

  Descrição: (Opcional) tags a serem criadas para a instância.
- SnapshotTags

  Tipo: String

  Descrição: (Opcional) tags a serem criadas para o snapshot.

Etapas do documento

criar RDSSnapshot — Cria o instantâneo do RDS e retorna o ID do instantâneo.

verify RDSSnapshot — Verifica se o snapshot criado na etapa anterior existe.

Saídas

criarRDSSnapshot. SnapshotId — O ID do instantâneo criado.

AWSConfigRemediation-DeleteRDSCluster

Descrição

O `AWSConfigRemediation-DeleteRDSCluster` runbook exclui o cluster do Amazon Relational Database Service (Amazon RDS) que você especificar. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DBClusterIdentificação

  Tipo: String

  Descrição: (obrigatório) O identificador do recurso para o cluster de banco de dados no qual deseja habilitar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DeleteDBCluster`
- `rds:DeleteDBInstance`
- `rds:DescribeDBClusters`

Etapas do documento

- `aws:executeScript` :Exclui o cluster de banco de dados especificado no parâmetro `DBClusterId`.

AWSConfigRemediation-DeleteRDSClusterSnapshot

Descrição

O runbook `AWSConfigRemediation-DeleteRDSClusterSnapshot` exclui o snapshot do cluster do Amazon Relational Database Service (Amazon RDS) fornecido.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DBClusterSnapshotId

  Tipo: String

  Descrição: (obrigatório) O identificador de snapshot do cluster do Amazon RDS a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DeleteDBClusterSnapshot
- rds:DescribeDBClusterSnapshots

Etapas do documento

- aws:branch :Verifica se o snapshot do cluster está no estado available. Se não estiver disponível, o fluxo termina.
- aws:executeAwsApi :Exclui o snapshot do cluster Amazon RDS fornecido usando o identificador de snapshot do cluster do banco de dados (DB).
- aws:executeScript :Verifica se o snapshot de cluster do Amazon RDS fornecido foi excluído.

AWSConfigRemediation-DeleteRDSInstance

Descrição

O runbook AWSConfigRemediation-DeleteRDSInstance exclui a instância do Amazon Relational Database Service (Amazon RDS) especificada. Quando uma instância de banco de dados (BD) é excluída, todas as cópias de segurança automatizadas para essa instância são excluídas e não podem ser recuperadas. Os snapshots manuais do BD não são excluídos. Se a instância de banco de dados que deseja excluir estiver no estado failed, incompatible-network ou incompatible-restore, o parâmetro SkipFinalSnapshot deverá ser definido como true.

> **Note**
>
> Se a instância de banco de dados que você deseja excluir estiver em um cluster de banco de dados Amazon Aurora, o runbook não excluirá a instância de banco de dados se ela for uma réplica de leitura e a única instância no cluster de banco de dados.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbiResourceId

  Tipo: String

  Descrição: (obrigatório) O identificador de recurso da instância de banco de dados a ser excluída.
- SkipFinalSnapshot

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definido como `true`, um snapshot final não é criado antes que a instância de banco de dados seja excluída.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBInstance`
- `rds:DescribeDBInstances`

Etapas do documento

- `aws:executeAwsApi` :Reúne o nome da instância de banco de dados a partir do valor que você especifica no parâmetro `DbiResourceId`.
- `aws:branch` :Ramifica com base no valor especificado para o parâmetro `SkipFinalSnapshot`.
- `aws:executeAwsApi` :Exclui a instância de banco de dados especificada no parâmetro `DbiResourceId`.
- `aws:executeAwsApi` :Exclui a instância de banco de dados que você especifica no parâmetro `DbiResourceId` após a criação do snapshot final.
- `aws:assertAwsResourceProperty` :Verifica se a instância de banco de dados foi excluída.

AWSConfigRemediation-DeleteRDSInstanceSnapshot

Descrição

O runbook `AWSConfigRemediation-DeleteRDSInstanceSnapshot` exclui o snapshot da instância do Amazon Relational Database Service (Amazon RDS) especificado. Somente os snapshots no estado `available` são excluídos. Este runbook não oferece suporte à exclusão de snapshots das instâncias do banco de dados Amazon Aurora.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- DbSnapshotId

  Tipo: String

  Descrição: (obrigatório) O ID do snapshot a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

Etapas do documento

- `aws:executeAwsApi` :Reúne o estado do snapshot especificado no parâmetro `DbSnapshotId`.
- `aws:assertAwsResourceProperty` :Confirma o estado do snapshot como `available`.
- `aws:executeAwsApi` :Exclui o snapshot especificado no parâmetro `DbSnapshotId`.
- `aws:executeScript` :Verifica se o snapshot foi excluído.

AWSConfigRemediation-DisablePublicAccessToRDSInstance

Descrição

O runbook `AWSConfigRemediation-DisablePublicAccessToRDSInstance` desabilita a acessibilidade pública da instância de banco de dados (DB) do Amazon Relational Database Service (Amazon RDS) especificada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbiResourceId

  Tipo: String

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados para a qual deseja desabilitar a acessibilidade pública.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Verifica se as instâncias de banco de dados estão no estado `AVAILABLE`.
- `aws:executeAwsApi` :Desabilita a acessibilidade pública em sua instância de banco de dados.
- `aws:waitForAwsResourceProperty` :Espera que a instância de banco de dados mude para o estado `MODIFYING`.

- `aws:waitForAwsResourceProperty` :Espera que a instância de banco de dados mude para o estado `AVAILABLE`.
- `aws:assertAwsResourceProperty` :Confirma que a acessibilidade pública está desabilitada na instância de banco de dados.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

Descrição

O runbook `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` habilita a definição `CopyTagsToSnapshot` no cluster do Amazon Relational Database Service (Amazon RDS) especificado. Habilitar essa definição copia todas as tags do cluster do banco de dados para snapshots desse cluster. O padrão é não copiá-los. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` for especificado para esse parâmetro, as modificações feitas nesta solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona

assim que possível, independentemente da definição `PreferredMaintenanceWindow` do cluster de banco de dados.

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- DbClusterResourceId

  Tipo: String

  Descrição: (obrigatório) O identificador do recurso para o cluster do banco de dados no qual deseja habilitar a definição `CopyTagsToSnapshot`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador do cluster de banco de dados a partir do identificador de recursos do cluster de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que o cluster de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Ativa a definição `CopyTagsToSnapshot` em seu cluster de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a definição `CopyTagsToSnapshot` está habilitada no cluster de banco de dados.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

Descrição

O runbook `AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance` habilita a definição `CopyTagsToSnapshot` na instância do Amazon Relational Database Service (Amazon RDS) especificada. Habilitar essa configuração copia todas as tags da instância do banco de dados para snapshots dessa instância. O padrão é não copiá-los. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` é especificado para esse parâmetro, as modificações feitas nessa solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona logo que possível, independentemente da configuração de `PreferredMaintenanceWindow` da instância de banco de dados.
- AutomationAssumeRole

  Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- DbiResourceId

  Tipo: String

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja habilitar a definição `CopyTagsToSnapshot`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a instância de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Ativa a definição `CopyTagsToSnapshot` em sua instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a configuração `CopyTagsToSnapshot` está habilitada na instância de banco de dados.

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

Descrição

O runbook `AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance` permite o monitoramento avançado na instância de banco de dados do Amazon RDS especificada. Para obter informações sobre o monitoramento avançado, consulte Monitoramento avançado no Guia do usuário do Amazon RDS.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- MonitoringInterval

  Tipo: inteiro

  Valores válidos: 1 | 5 | 10 | 15 | 30 | 60

  Descrição: (obrigatório) O intervalo em segundos quando as métricas de monitoramento avançado são coletadas da instância de banco de dados.
- MonitoringRoleArn

  Tipo: String

  Descrição: (Obrigatório) O nome de recurso da Amazon (ARN) da função do IAM que permite que o Amazon RDS envie métricas de monitoramento aprimorado para o Amazon Logs. CloudWatch

- ResourceId

  Tipo: String

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja habilitar o Enhanced Monitoring.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a instância de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Permite o monitoramento avançado na instância de banco de dados.
- `aws:executeScript` :Confirma que o monitoramento avançado está habilitado na instância de banco de dados.

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

Descrição

O runbook `AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS` habilita a definição `AutoMinorVersionUpgrade` na instância de banco de dados do Amazon RDS especificada. Habilitar essa configuração significa que as atualizações secundárias das versões serão aplicadas automaticamente à instância de banco de dados durante a janela de manutenção.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbiResourceId

  Tipo: String

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja a definição `AutoMinorVersionUpgrade`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.

- `aws:assertAwsResourceProperty` :Confirma que a instância de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Ativa a definição `AutoMinorVersionUpgrade` em sua instância de banco de dados.
- `aws:executeScript` :Confirma se a definição `AutoMinorVersionUpgrade` está habilitada na sua instância de banco de dados.

AWSConfigRemediation-EnableMultiAZOnRDSInstance

Descrição

O runbook `AWSConfigRemediation-EnableMultiAZOnRDSInstance` transforma a instância de banco de dados (DB) do Amazon Relational Database Service (Amazon RDS) para uma implantação Multi-AZ. Alterar essa configuração não resultará em uma interrupção. A alteração será aplicada durante a próxima janela de manutenção, a menos que o parâmetro `ApplyImmediately` seja definido como `true`.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` é especificado para esse parâmetro, as modificações feitas nessa solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona

logo que possível, independentemente da configuração de `PreferredMaintenanceWindow` da instância de banco de dados.

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- DbiResourceId

  Tipo: String

  Descrição: (Obrigatório) O identificador Região da AWS exclusivo e imutável da instância de banco de dados para habilitar a configuração. `MultiAZ`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Etapas do documento

- `aws:executeAwsApi` :Recupera o nome da instância de banco de dados usando o valor fornecido no parâmetro `DBInstanceId`.
- `aws:executeAwsApi` :Verifica se `DBInstanceStatus` é `available`.
- `aws:branch` :Verifica se a `MultiAZ` já está definida como `true` na instância de banco de dados especificada no parâmetro `DbiResourceId`.
- `aws:executeAwsApi` :Altera a definição `MultiAZ` para `true` na instância de banco de dados especificada no parâmetro `DbiResourceId`.
- `aws:assertAwsResourceProperty` :Verifica se a `MultiAZ` está definida como `true` na instância de banco de dados especificada no parâmetro `DbiResourceId`.

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

Descrição

O runbook `AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance` habilita o Performance Insights na instância de banco de dados Amazon RDS especificada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbiResourceId

  Tipo: String

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja habilitar o Performance Insights.
- PerformanceInsightsKMSKeyIdentificação

  Tipo: String

  Padrão: `alias/aws/rds`

Descrição: (Opcional) O nome de recurso da Amazon (ARN), o ID da chave ou o alias da chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente que você deseja que o Performance Insights use para criptografar todos os dados potencialmente confidenciais. Prefixe o valor com **alias/** se for inserir o alias da chave para esse parâmetro. Se você não especificar um valor para esse parâmetro, o Chave gerenciada pela AWS será usado.

- PerformanceInsightsRetentionPeriod

  Tipo: inteiro

  Valores válidos: 7, 731

  Padrão: 7

  Descrição: (opcional) O número de dias para reter dados do Performance Insights.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que o status da instância de banco de dados é `available`.
- `aws:executeAwsApi`- Reúne o ARN da chave gerenciada AWS KMS pelo cliente especificada no `PerformanceInsightsKMSKeyId` parâmetro.
- `aws:branch` :Verifica se um valor já está atribuído à propriedade do `PerformanceInsightsKMSKeyId` da instância de banco de dados.

- `aws:executeAwsApi` :Habilita o Performance Insights na instância de banco de dados especificada no parâmetro `DbiResourceId`.
- `aws:assertAwsResourceProperty` :Confirma que o valor especificado para o parâmetro `PerformanceInsightsKMSKeyId` foi usado para habilitar a criptografia para o Performance Insights na instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que o Performance Insights está habilitado na instância de banco de dados.

AWSConfigRemediation-EnableRDSClusterDeletionProtection

Descrição

O `AWSConfigRemediation-EnableRDSClusterDeletionProtection` runbook permite a proteção contra exclusão no cluster Amazon Relational Database Service (Amazon RDS) que você especificar. AWS Config deve estar habilitado no Região da AWS local em que você executa essa automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterId

Tipo: String

Descrição: (obrigatório) O identificador do recurso para o cluster de banco de dados no qual deseja habilitar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

Etapas do documento

- `aws:executeAwsApi` :Reúne o nome do cluster de banco de dados a partir do identificador de recursos do cluster de banco de dados.
- `aws:assertAwsResourceProperty` :Verifica se o status do cluster de banco de dados é `available`.
- `aws:executeAwsApi` :Ativa a proteção contra exclusão no cluster de banco de dados especificada no parâmetro `ClusterId`.
- `aws:assertAwsResourceProperty` :Verifica se a proteção contra exclusão foi habilitada no cluster de banco de dados.

AWSConfigRemediation-EnableRDSInstanceBackup

Descrição

O runbook `AWSConfigRemediation-EnableRDSInstanceBackup` habilita backups para a instância de banco de dados do Amazon Relational Database Service (Amazon RDS) especificada. Este runbook não oferece suporte à habilitação de backups para instâncias de banco de dados Amazon Aurora.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` é especificado para esse parâmetro, as modificações feitas nessa solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona logo que possível, independentemente da configuração de `PreferredMaintenanceWindow` da instância de banco de dados.
- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- BackupRetentionPeriod

  Tipo: inteiro

  Valores válidos: 1 a 35

  Descrição: (obrigatório) O número de dias que os backups são retidos.
- DbiResourceId

  Tipo: String

Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados para a qual deseja habilitar backups.

- PreferredBackupWindow

  Tipo: String

  Descrição: (opcional) O intervalo de tempo diário (em UTC) durante o qual os backups são criados.

  Restrições:

  - Deve estar no formato `hh24:mi-hh24:mi`
  - Deve estar expresso no Tempo Universal Coordenado (Coordinated Universal Time, UTC)
  - Não pode entrar em conflito com a janela de manutenção preferencial
  - Deve ser, pelo menos, 30 minutos

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeScript` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados. Habilita backups para a instância de banco de dados. Confirma que backups estão habilitados na instância de banco de dados.

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

Descrição

O runbook `AWSConfigRemediation-EnableRDSInstanceDeletionProtection` habilita a proteção contra exclusão na instância de banco de dados do Amazon RDS especificada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- ApplyImmediately

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se o valor `true` é especificado para esse parâmetro, as modificações feitas nessa solicitação e todas as modificações pendentes serão aplicadas de maneira assíncrona logo que possível, independentemente da configuração de `PreferredMaintenanceWindow` da instância de banco de dados.
- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DbInstanceResourceId

  Tipo: String

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados na qual deseja habilitar a proteção contra exclusão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:executeAwsApi` :Habilita a proteção contra exclusão na instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a proteção contra exclusão está habilitada na instância de banco de dados.

AWSConfigRemediation-ModifyRDSInstancePortNumber

Descrição

O runbook `AWSConfigRemediation-ModifyRDSInstancePortNumber` modifica o número da porta na qual a instância do Amazon Relational Database Service (Amazon RDS) aceita conexões. A execução dessa automação reiniciará o banco de dados.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- PortNumber

  Tipo: String

  Descrição: (opcional) O número da porta na qual deseja que a instância de banco de dados aceite conexões.

- RDSDBInstanceResourceId

  Tipo: String

  Descrição: (obrigatório) O identificador do recurso para a instância de banco de dados cujo número da porta de entrada deseja modificar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

Etapas do documento

- `aws:executeAwsApi` :Reúne o identificador da instância de banco de dados a partir do identificador de recursos da instância de banco de dados.
- `aws:assertAwsResourceProperty` :Confirma que a instância de banco de dados está no estado `AVAILABLE`.
- `aws:executeAwsApi` :Modifica o número da porta de entrada na qual sua instância de banco de dados aceita conexões.

- `aws:waitForAwsResourceProperty` :Espera que a instância de banco de dados mude para o estado `MODIFYING`.
- `aws:waitForAwsResourceProperty` :Espera que a instância de banco de dados mude para o estado `AVAILABLE`.

AWSSupport-ModifyRDSSnapshotPermission

Descrição

O runbook `AWSSupport-ModifyRDSSnapshotPermission` ajuda a modificar permissões para vários snapshots do Amazon Relational Database Service (Amazon RDS). Usando este runbook, você pode criar snapshots `Public` ou `Private` e compartilhá-los com outras Contas da AWS. Os snapshots criptografados com uma chave KMS padrão não podem ser compartilhados com outras contas usando este runbook.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AccountIds

Tipo: StringList

Padrão: nenhum

Descrição: (Opcional) A IDs das contas com as quais você deseja compartilhar instantâneos. Esse parâmetro será necessário se um valor `No` for especificado para o parâmetro `Private`.

- AccountPermissionOperation

  Tipo: String

  Valores válidos: add | remove

  Padrão: nenhum

  Descrição: (opcional) O tipo de operação a ser executada.

- Privado

  Tipo: String

  Valores válidos: sim | não

  Descrição: (obrigatório) Insira o valor `No` se quiser compartilhar snapshots com contas específicas.

- SnapshotIdentifiers

  Tipo: StringList

  Descrição: (obrigatório) Os nomes dos snapshots do Amazon RDS cuja permissão deseja modificar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`
- `rds:ModifyDBSnapshotAttribute`

Etapas do documento

1. `aws:executeScript`- Verifica IDs os instantâneos fornecidos no `SnapshotIdentifiers` parâmetro. Depois de verificar o IDs, o script verifica se há instantâneos criptografados e gera uma lista, se alguma for encontrada.
2. `aws:branch` :Ramifica a automação com base no valor inserido para o parâmetro `Private`.
3. `aws:executeScript` :Modifica as permissões dos snapshots especificados para compartilhá-los com as contas especificadas.
4. `aws:executeScript` :Modifica as permissões dos snapshots para alterá-los de `Public` para `Private`.

Saídas

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Resultado

MakePrivate.Resultado

MakePrivate.Comandos

AWSPremiumSupport-PostgreSQLWorkloadReview

Descrição

O runbook `AWSPremiumSupport-PostgreSQLWorkloadReview` captura vários snapshots das estatísticas de uso do banco de dados PostgreSQL do Amazon Relational Database Service (Amazon RDS). As estatísticas capturadas são necessárias para que um especialista em Serviços Suporte Proativos realize uma análise operacional. As estatísticas são coletadas usando um conjunto de scripts SQL e shell personalizados. Esses scripts são baixados para uma instância temporária do Amazon Elastic Compute Cloud (Amazon EC2) na sua Conta da AWS , criada por este runbook. O runbook exige o fornecimento de credenciais usando um segredo do AWS Secrets Manager contendo um par de valores-chave de nome de usuário e senha. O nome de usuário deve ter permissões para consultar as visualizações e funções de estatísticas padrão do PostgreSQL.

Esse runbook cria automaticamente os seguintes AWS recursos em você Conta da AWS usando uma AWS CloudFormation pilha. Você pode monitorar a criação da pilha usando o console AWS CloudFormation .

- Uma nuvem privada virtual (VPC) e uma EC2 instância da Amazon lançadas em uma sub-rede privada da VPC com conectividade opcional à Internet usando um gateway NAT.
- Uma função AWS Identity and Access Management (IAM) anexada à EC2 instância temporária da Amazon com permissões para recuperar o valor secreto do Secrets Manager. A função também fornece permissões para fazer upload de arquivos para um bucket do Amazon Simple Storage Service (Amazon S3) de sua escolha e, opcionalmente, para um caso. Suporte
- Uma conexão de emparelhamento de VPC para permitir a conectividade entre sua instância de banco de dados e a instância temporária da Amazon. EC2
- Os endpoints da VPC, do Systems Manager, do Secrets Manager e do Amazon S3 que estão anexados à VPC temporária.
- Uma janela de manutenção com tarefas registradas que iniciam e interrompem periodicamente a EC2 instância temporária da Amazon, executam scripts de coleta de dados e carregam arquivos em um bucket do Amazon S3. Um perfil do IAM também é criado para a janela de manutenção que fornece permissões para realizar as tarefas registradas.

Quando o runbook é concluído, a AWS CloudFormation pilha usada para criar os AWS recursos necessários é excluída e o relatório é carregado no bucket Amazon S3 de sua escolha e, opcionalmente, em um caso. Suporte

> **Note**
>
> Por padrão, o volume raiz do Amazon EBS da EC2 instância temporária da Amazon é preservado. Você pode substituir essa opção configurando o parâmetro `EbsVolumeDeleteOnTermination` como `true`.

Pré-requisitos

- Assinatura do Enterprise Support Este runbook e os diagnósticos e análises da workload do Proactive Services exigem uma assinatura do Enterprise Support. Antes de usar este runbook, entre em contato com seu gerente técnico de contas (TAM) ou com o TAM especializado (STAM) para obter instruções. Para obter mais informações, consulte Proactive Services do Suporte.
- Conta e Região da AWS cotas Certifique-se de não ter atingido o número máximo de EC2 instâncias da Amazon ou de poder criar em sua conta e região em VPCs que você usa este runbook. Para solicitar um aumento de limite, use o Formulário de aumento de limite de serviço.
- Configuração do banco de dados

1. O banco de dados especificado no parâmetro `DatabaseName` deve ter a extensão `pg_stat_statements` configurada. Se `pg_stat_statements` não estiver configurado na `shared_preload_libraries`, o valor no grupo de parâmetros do banco de dados deverá ser editado e as alterações aplicadas. As alterações no parâmetro `shared_preload_libraries` exigem que você reinicie sua instância de banco de dados. Para obter mais informações, consulte Trabalhar com grupos de parâmetros. Adicionar `pg_stat_statements` a `shared_preload_libraries` adicionará alguma sobrecarga de desempenho. No entanto, isso é útil para monitorar o desempenho de instruções individuais. Para obter mais informações sobre a extensão `pg_stat_statements`, consulte a documentação do PostgreSQL. Se a extensão `pg_stat_statements` não for configurada ou se a extensão não estiver presente no banco de dados que está sendo usado para coleta de estatísticas, a análise em nível de instrução não será apresentada na revisão operacional.
2. Verifique se os parâmetros `track_counts` e `track_activities` não estão desativados. Se esses parâmetros estiverem desativados no grupo de parâmetros do banco de dados, nenhuma estatística significativa estará disponível. A alteração desses parâmetros exigirá a reinicialização da sua instância de banco de dados. Para mais informações, consulte Trabalhar com parâmetros na instância de banco de dados do Amazon RDS para PostgreSQL.
3. Se o `track_io_timing` parâmetro estiver desativado, as estatísticas de I/O nível não serão incluídas na análise operacional. A alteração de `track_io_timing` exigirá a reinicialização da sua instância de banco de dados e incorrerá em sobrecarga adicional de desempenho, dependendo da workload da instância de banco de dados. Apesar da sobrecarga de desempenho para cargas de trabalho críticas, esse parâmetro fornece informações úteis relacionadas ao I/O tempo por consulta.

Cobrança e cobranças Você Conta da AWS será cobrado pelos custos associados à EC2 instância temporária da Amazon, ao volume associado do Amazon EBS, ao gateway NAT e aos dados transferidos durante a execução dessa automação. Por padrão, esse runbook cria uma instância `t3.micro` do Amazon Linux 2 para coletar as estatísticas. O runbook inicia e interrompe a instância entre as etapas para reduzir custos.

Segurança e governança de dados Este runbook coleta estatísticas consultando as visualizações e funções de estatísticas do PostgreSQL. Verifique se as credenciais fornecidas no parâmetro `SecretId` permitem somente permissões de leitura para as visualizações e funções de estatísticas. Como parte da automação, os scripts de coleta são carregados em seu bucket do Amazon S3 e podem ser localizados em `s3://`*`amzn-s3-demo-bucket`*`/`*`automation execution id`*`/queries/`.

Esses scripts coletam dados que são usados por um AWS especialista para revisar os principais indicadores de desempenho no nível do objeto. O script coleta informações como nome da tabela, nome do esquema e nome do índice. Se alguma dessas informações contiver informações confidenciais, como indicadores de receita, nome de usuário, endereço de e-mail ou qualquer outra informação de identificação pessoal, recomendamos que essa análise da workload seja interrompida. Entre em contato com seu AWS TAM para discutir uma abordagem alternativa para a análise da carga de trabalho.

Certifique-se de ter a aprovação e a autorização necessárias para compartilhar as estatísticas e os metadados coletados por essa automação. AWS

Considerações de segurança Se você definir o `UpdateRdsSecurityGroup` parâmetro como`yes`, o runbook atualizará o grupo de segurança associado à sua instância de banco de dados para permitir o tráfego de entrada do endereço IP privado da EC2 instância temporária da Amazon.

Se você definir o `UpdateRdsRouteTable` parâmetro como`yes`, o runbook atualizará a tabela de rotas associada à sub-rede em que sua instância de banco de dados está sendo executada para permitir o tráfego para a instância temporária da Amazon por meio da conexão de EC2 emparelhamento de VPC.

Criação de usuário Para permitir que o script de coleta se conecte ao seu banco de dados do Amazon RDS, deve ser configurado um usuário com permissões para ler as visualizações estatísticas. Em seguida, as credenciais devem ser armazenadas no Secrets Manager. Recomendamos criar um novo usuário dedicado para essa automação. A criação de um usuário separado permite auditar e rastrear as atividades realizadas por essa automação.

1. Criar um novo usuário.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "CREATE USER <user_name> PASSWORD '<password>';"
```

2. Garantir que esse usuário possa fazer conexões somente para leitura.

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "ALTER USER <user_name> SET default_transaction_read_only=true;"
```

3. Definir limites de nível de usuário.

```
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. Conceder permissões de `pg_monitor` ao novo usuário para que ele possa acessar as estatísticas do banco de dados. (O perfil `pg_monitor` é membro de `pg_read_all_settings`, `pg_read_all_stats` e `pg_stat_scan_table`.)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

Permissões adicionadas ao perfil de EC2 instância temporária da Amazon por este Systems Manager Automation As seguintes permissões são adicionadas à função do IAM associada à EC2 instância temporária da Amazon. A política `AmazonSSMManagedInstanceCore` gerenciada também está associada à função do IAM para permitir que a EC2 instância da Amazon seja gerenciada pelo Systems Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeTags"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:PutObject"
```

```
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/automation execution id/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:region:account id:secret:secret id",
            "Effect": "Allow"
        },
        {
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:DescribeCases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Permissões adicionadas à janela de manutenção temporária por essa automação do Systems Manager Automation As seguintes permissões são adicionadas automaticamente ao perfil do IAM associada às tarefas do Maintenance Windows. As tarefas de manutenção do Windows iniciam, param e enviam comandos para a EC2 instância temporária da Amazon.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:ListCommands",
                "ssm:ListCommandInvocations",
                "ssm:GetCommandInvocation",
                "ssm:GetCalendarState",
                "ssm:CancelCommand",
                "ec2:DescribeInstanceStatus"
            ],
            "Resource": "*",
            "Effect": "Allow"
```

```
        },
        {
            "Action": [
                "ssm:SendCommand",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ec2:region:account id:instance/temporary instance id",
                "arn:aws:ssm:*:*:document/AWS-RunShellScript",
                "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:$DEFAULT",
                "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:$DEFAULT"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                },
                "ArnLike": {
                    "iam:AssociatedResourceARN": "arn:aws:ssm:*:*:automation-
definition/AWS-*"
                }
            },
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account id:role/SSM-*",
            "Effect": "Allow"
        }
    ]
}
```

[Executar esta automação (console)]

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DBInstanceIdentificador

  Tipo: String

  Descrição: (obrigatório) O ID de sua instância de banco de dados.

- DatabaseName

  Tipo: String

  Descrição: (obrigatório) O nome do banco de dados hospedado na instância de banco de dados.

- SecretId

  Tipo: String

  Descrição: (obrigatório) O ARN do segredo do Secrets Manager que contém o par de valores-chave de nome de usuário e senha. A AWS CloudFormation pilha cria uma política do IAM com permissões para a `GetSecretValue` operação desse ARN. As credenciais são usadas para permitir que a instância temporária colete as estatísticas do banco de dados. Entre em contato com seu TAM ou STAM para discutir as permissões mínimas necessárias.

- Reconhecer

  Tipo: String

  Descrição: (obrigatório) Digite **`yes`** para confirmar que esse runbook crie recursos temporários em sua conta para coletar estatísticas da sua instância de banco de dados. Recomendamos entrar em contato com seu TAM ou STAM antes de executar essa automação.

- SupportCase

Tipo: String

Descrição: (Opcional) O número do Suporte caso fornecido pelo seu TAM ou STAM. Se fornecido, o runbook atualiza o caso e anexa os dados coletados. Essa opção exige que a EC2 instância temporária da Amazon tenha conectividade com a Internet para acessar o endpoint da Suporte API. O parâmetro `AllowVpcInternetAccess` deve ser definido como `true`. O assunto do caso deve conter a frase `AWSPremiumSupport-PostgreSQLWorkloadReview`.

- S3 BucketName

  Tipo: String

  Descrição: (obrigatório) O nome do bucket do Amazon S3 na conta para a qual deseja fazer o upload dos dados coletados pela automação. Verificar se a política do bucket não concede permissões desnecessárias de leitura ou gravação às entidades principais que não precisam acessar o conteúdo do bucket. Recomendamos criar um novo bucket temporário do Amazon S3 para fins dessa automação. O runbook fornece permissões para a operação da `s3:PutObject` API para a função do IAM anexada à EC2 instância temporária da Amazon. Os arquivos enviados estarão localizados em `s3://`*`bucket name`*`/`*`automation execution id`*`/`.

- InstanceType

  Tipo: String

  Descrição: (Opcional) O tipo da EC2 instância temporária da Amazon que executará os scripts SQL e shell personalizados.

  Valores válidos: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

  Padrão: t3.micro

- VpcCidr

  Tipo: String

  Descrição: (opcional) O intervalo de endereço IP na notação CIDR para a nova VPC (por exemplo, `172.31.0.0/16`). Verificar se selecionou um CIDR que não se sobreponha ou corresponda a nenhuma VPC existente com conectividade com a instância de banco de dados. A menor VPC que você pode criar usa uma máscara de sub-rede /28 e a maior VPC usa uma máscara de sub-rede /16.

Padrão: 172.31.0.0/16

- StackResourcesNamePrefix

  Tipo: String

  Descrição: (Opcional) O prefixo e a tag do nome dos recursos da AWS CloudFormation pilha. O runbook cria os recursos da AWS CloudFormation pilha usando esse prefixo como parte do nome e da tag aplicados aos recursos. A estrutura do par chave/valor da tag é *`StackResourcesNamePrefix`*`:{{automation:EXECUTION_ID}}`.

  Padrão: AWSPostgre SQLWorkload Revisão

- Programação

  Tipo: String

  Descrição: (opcional) O cronograma da janela de manutenção. Especifica com que frequência a janela de manutenção executa as tarefas. O valor padrão é a cada `1 hour`.

  Valores válidos: 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 12 hours | 1 day | 2 days | 4 days

  Padrão: 1 hour

- Duração

  Tipo: Inteiro

  Descrição: (opcional) A duração máxima, em minutos, que deseja permitir que a automação seja executada. A duração máxima suportada é de 8.640 minutos (seis dias). O valor padrão é de 4.320 minutos (três dias).

  Valores válidos: 30 a 8640

  Padrão: 4320

- UpdateRdsRouteTable

  Tipo: String

  Descrição: (opcional) Se definido como `true`, o runbook atualiza a tabela de rotas associada à sub-rede em que a instância de banco de dados é executada. Uma IPv4 rota é adicionada para

rotear o tráfego para o IPV4 endereço privado temporário da EC2 instância Amazon por meio da conexão de emparelhamento de VPC recém-criada.

Valores válidos: True | False

Padrão: False

- AllowVpcInternetAccess

  Tipo: String

  Descrição: (Opcional) Se definido como`true`, o runbook cria um gateway NAT para fornecer conectividade com a Internet à EC2 instância temporária da Amazon para se comunicar com o endpoint da Suporte API. Você pode deixar esse parâmetro como `false` se quiser apenas que o runbook faça o upload da saída para o seu bucket do Amazon S3.

  Valores válidos: true | false

  Padrão: False

- UpdateRdsSecurityGroup

  Tipo: String

  Descrição: (opcional) Se definido como `true`, o runbook atualiza o grupo de segurança associado à sua instância de banco de dados para permitir o tráfego do endereço IP privado da instância temporária.

  Valores válidos: false | true

  Padrão: False

- EbsVolumeDeleteOnTermination

  Tipo: String

  Descrição: (Opcional) Se definido como`true`, o volume raiz da EC2 instância temporária da Amazon é excluído após a conclusão do runbook e a exclusão da pilha. AWS CloudFormation

  Valores válidos: false | true

  Padrão: False

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

1. aws:assertAwsResourceProperty - confirma que a instância de banco de dados está no estado available.
2. aws:executeAwsApi - reúne detalhes sobre a instância de banco de dados.
3. aws:executeScript - verifica se o bucket do Amazon S3 especificado em S3BucketName concede permissões de acesso anônimo ou público de leitura ou gravação.

4. `aws:executeScript`- Obtém o conteúdo do AWS CloudFormation modelo do anexo do Automation runbook que é usado para criar os AWS recursos temporários em seu Conta da AWS.
5. `aws:createStack`- Cria os recursos da AWS CloudFormation pilha.
6. `aws:waitForAwsResourceProperty`- Espera até que a EC2 instância da Amazon criada pelo AWS CloudFormation modelo esteja em execução.
7. `aws:executeAwsApi`- Obtém a IDs para a EC2 instância temporária da Amazon e a conexão de emparelhamento VPC criada por. AWS CloudFormation
8. `aws:executeAwsApi`- Obtém o endereço IP da EC2 instância temporária da Amazon para configurar a conectividade com sua instância de banco de dados.
9. `aws:executeAwsApi`- Marca o volume do Amazon EBS anexado à EC2 instância temporária da Amazon.
10. `aws:waitForAwsResourceProperty`- Espera até que a EC2 instância temporária da Amazon passe nas verificações de status.
11. `aws:waitForAwsResourceProperty`- Espera até que a EC2 instância temporária da Amazon seja gerenciada pelo Systems Manager. Se essa etapa expirar ou falhar, o runbook reinicializa a instância.
    a. `aws:executeAwsApi`- Reinicializa a EC2 instância temporária da Amazon se a etapa anterior falhar ou atingir o tempo limite.
    b. `aws:waitForAwsResourceProperty`- Espera até que a EC2 instância temporária da Amazon seja gerenciada pelo Systems Manager após a reinicialização.
12. `aws:runCommand`- Instala os requisitos do aplicativo coletor de metadados na instância temporária da Amazon. EC2
13. `aws:runCommand`- Configura o acesso à sua instância de banco de dados criando um arquivo de configuração na EC2 instância temporária da Amazon.
14. `aws:executeAwsApi` - Cria uma janela de manutenção para executar periodicamente o aplicativo coletor de metadados usando o comando Executar. A janela de manutenção inicia e interrompe a instância entre os comandos.
15. `aws:waitForAwsResourceProperty`- Espera até que a janela de manutenção criada pelo AWS CloudFormation modelo esteja pronta.
16. `aws:executeAwsApi`- Obtém IDs a janela de manutenção e o calendário de alterações criados por AWS CloudFormation.
17. `aws:sleep` - espera até a data de término da janela de manutenção.
18. `aws:executeAwsApi` - desliga a janela de manutenção.

19. `aws:executeScript` - obtém os resultados das tarefas executadas durante a janela de manutenção.
20. `aws:waitForAwsResourceProperty` - espera que a janela de manutenção conclua a última tarefa antes de continuar.
21. `aws:branch` - ramifica o fluxo de trabalho com base no fato de ter fornecido um valor para o parâmetro `SupportCase`.
    a. `aws:changeInstanceState`- Inicia a EC2 instância temporária da Amazon e aguarda a aprovação das verificações de status antes de fazer o upload do relatório.
    b. `aws:waitForAwsResourceProperty`- Espera até que a EC2 instância temporária da Amazon seja gerenciada pelo Systems Manager. Se essa etapa atingir o tempo limite ou falhar, o runbook reinicializa a instância.
        i. `aws:executeAwsApi`- Reinicializa a EC2 instância temporária da Amazon se a etapa anterior falhar ou atingir o tempo limite.
        ii. `aws:waitForAwsResourceProperty`- Espera até que a EC2 instância temporária da Amazon seja gerenciada pelo Systems Manager após a reinicialização.
    c. `aws:runCommand` - anexa o relatório de metadados ao caso do Suporte se foi fornecido um valor para o parâmetro `SupportCase`. O script compacta e divide o relatório em arquivos de 5 MB. O número máximo de arquivos que o script anexa a um caso do Suporte é 12.
22. `aws:changeInstanceState`- Interrompe a EC2 instância temporária da Amazon caso a AWS CloudFormation pilha não seja excluída.
23. `aws:executeAwsApi`- Descreve os eventos da AWS CloudFormation pilha se os runbooks falharem em criar ou atualizar a AWS CloudFormation pilha.
24. `aws:waitForAwsResourceProperty`- Espera até que a AWS CloudFormation pilha esteja em um status de terminal antes de excluí-la.
25. `aws:executeAwsApi`- Exclui a AWS CloudFormation pilha, excluindo a janela de manutenção. O volume raiz do Amazon EBS associado à EC2 instância temporária da Amazon é preservado se o valor do `EbsVolumeDeleteOnTermination` parâmetro tiver sido definido como. `false`

AWS-RebootRdsInstance

Descrição

O runbook `AWS-RebootRdsInstance` reinicializa uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS), caso esta ainda não esteja sendo reinicializada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: String

  Descrição: (obrigatório) O ID da instância de banco de dados do Amazon RDS que você deseja reinicializar.

Etapas do documento

RebootInstance - Reinicializa a instância de banco de dados se ela ainda não estiver sendo reinicializada.

WaitForAvailableState - Espera que a instância de banco de dados conclua o processo de reinicialização.

Saídas

Essa automação não tem saídas.

AWSSupport-ShareRDSSnapshot

Descrição

O runbook `AWSSupport-ShareRDSSnapshot` fornece uma solução automatizada para o procedimento descrito no artigo do centro de conhecimentos Como posso compartilhar um snapshot criptografado do banco de dados do Amazon RDS com outra conta? Se seu snapshot do Amazon Relational Database Service (Amazon RDS) foi criptografado usando o Chave gerenciada pela AWS padrão, você não poderá compartilhar o snapshot. Nesse caso, o snapshot deve ser copiado usando uma chave gerenciada pelo cliente para, em seguida, compartilhá-lo com a conta de destino. Essa automação executa essas etapas usando o valor especificado no parâmetro `SnapshotName` ou o último snapshot encontrado para o cluster ou instância de banco de dados selecionado do Amazon RDS.

> **Note**
>
> Se você não especificar um valor para o `KMSKey` parâmetro, a automação cria uma nova chave gerenciada pelo AWS KMS cliente em sua conta que é usada para criptografar o instantâneo.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AccountIds

Tipo: StringList

Descrição: (Obrigatório) Lista de contas separada por vírgulas IDs com a qual compartilhar o instantâneo.

- AutomationAssumeRole

  Tipo: string

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Banco de dados

  Tipo: string

  Descrição: (obrigatório) O nome do cluster ou instância de banco de dados do Amazon RDS cujo snapshot deseja compartilhar. Esse parâmetro será necessário se for especificado um valor para o parâmetro `SnapshotName`.

- KMSKey

  Tipo: string

  Descrição: (opcional) O nome do recurso da Amazon (ARN) completo da chave gerenciada pelo cliente do AWS KMS a ser usada para criptografar o snapshot.

- SnapshotName

  Tipo: string

  Descrição: (opcional) O ID do snapshot do cluster ou instância de banco de dados que deseja usar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBInstances`

- `rds:DescribeDBSnapshots`
- `rds:CopyDBSnapshot`
- `rds:ModifyDBSnapshotAttribute`

O `AutomationAssumeRole` requer as seguintes ações para iniciar com êxito o runbook de um cluster de banco de dados.

- `ssm:StartAutomationExecution`
- `rds:DescribeDBClusters`
- `rds:DescribeDBClusterSnapshots`
- `rds:CopyDBClusterSnapshot`
- `rds:ModifyDBClusterSnapshotAttribute`

O perfil do IAM usado para executar a automação deve ser adicionado como um usuário chave para usar a chave KMS especificada no parâmetro `ARNKmsKey`. Para obter informações sobre como adicionar usuários de chave à uma chave KMS, consulte Alterar uma política de chaves no Guia do desenvolvedor do AWS Key Management Service .

O `AutomationAssumeRole` requer as seguintes ações adicionais para iniciar com êxito o runbook se não for especificado um valor para o parâmetro de `KMSKey`.

- `kms:CreateKey`
- `kms:ScheduleKeyDeletion`
- `kms:CreateGrant`
- `kms:DescribeKey`

Etapas do documento

1. `aws:executeScript`- Verifica se um valor foi fornecido para o `KMSKey` parâmetro e cria uma chave gerenciada pelo AWS KMS cliente se nenhum valor for encontrado.
2. `aws:branch` :Verifica se um valor foi fornecido para o parâmetro de `SnapshotName` e ramifica de acordo.
3. `aws:executeAwsApi` :Verifica se o snapshot fornecido é de uma instância de banco de dados.

4. `aws:executeScript` :Formata o parâmetro de `SnapshotName` substituindo dois pontos por um hífen.
5. `aws:executeAwsApi` :Copia o snapshot usando a `KMSKey` especificada.
6. `aws:waitForAwsResourceProperty` :Aguarda a conclusão da operação de cópia do snapshot.
7. `aws:executeAwsApi` :Compartilha o novo snapshot com o `AccountIds` especificado.
8. `aws:executeAwsApi` :Verifica se o snapshot fornecido é de um cluster de banco de dados.
9. `aws:executeScript` :Formata o parâmetro de `SnapshotName` substituindo dois pontos por um hífen.
10. `aws:executeAwsApi` :Copia o snapshot usando a `KMSKey` especificada.
11. `aws:waitForAwsResourceProperty` :Aguarda a conclusão da operação de cópia do snapshot.
12. `aws:executeAwsApi` :Compartilha o novo snapshot com o `AccountIds` especificado.
13. `aws:executeAwsApi` :Verifica se o valor fornecido para o parâmetro do `Database` é uma instância de banco de dados.
14. `aws:executeAwsApi` :Verifica se o valor fornecido para o parâmetro do `Database` é um cluster de banco de dados.
15. `aws:executeAwsApi` :Recupera uma lista de snapshots para o `Database` especificado.
16. `aws:executeScript` :Determina o último snapshot disponível na lista montada na etapa anterior.
17. `aws:executeAwsApi` :Copia o snapshot da instância de banco de dados usando a `KMSKey` especificada.
18. `aws:waitForAwsResourceProperty` :Aguarda a conclusão da operação de cópia do snapshot.
19. `aws:executeAwsApi` :Compartilha o novo snapshot com o `AccountIds` especificado.
20. `aws:executeAwsApi` :Recupera uma lista de snapshots para o `Database` especificado.
21. `aws:executeScript` :Determina o último snapshot disponível na lista montada na etapa anterior.
22. `aws:executeAwsApi` :Copia o snapshot da instância de banco de dados usando a `KMSKey` especificada.
23. `aws:waitForAwsResourceProperty` :Aguarda a conclusão da operação de cópia do snapshot.

24. `aws:executeAwsApi` :Compartilha o novo snapshot com o `AccountIds` especificado.
25. `aws:executeScript`- Exclui a chave gerenciada pelo AWS KMS cliente criada pela automação se você não especificar um valor para o `KMSKey` parâmetro e a automação falhar.

AWS-StartRdsInstance

Descrição

Iniciar uma instância do Amazon Relational Database Service (Amazon RDS)

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: String

  Descrição: (obrigatório) O ID da instância do Amazon RDS a ser iniciado.

AWS-StartStopAuroraCluster

Descrição

Esse runbook inicia ou interrompe um cluster Amazon Aurora.

> **Note**
>
> Para iniciar um cluster, ele deve estar em um `stopped` status. Para parar um cluster, ele deve estar em um `available` status. Esse runbook não pode ser usado para iniciar ou interromper um cluster que seja um cluster Aurora Serverless, um cluster multimaster do Aurora, parte de um banco de dados global do Aurora ou um cluster que usa a consulta paralela do Aurora.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- ClusterName

  Tipo: String

Descrição: (Obrigatório) O nome do cluster Aurora que você deseja interromper ou iniciar.

- Ação

  Tipo: String

  Valores válidos: Iniciar | Parar

  Padrão: Iniciar

  Descrição: (Obrigatório) O nome do cluster Aurora que você deseja interromper ou iniciar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `rds:DescribeDBClusters`
- `rds:StartDBCluster`
- `rds:StopDBCluster`

Etapas do documento

- `aws:executeScript`- Inicia ou interrompe o cluster com base nos valores que você especifica para o.

Saídas

StartStopAuroraCluster. ClusterName - O nome do cluster Aurora

StartStopAuroraCluster. CurrentStatus - O status atual do cluster Aurora

StartStopAuroraCluster.Message - Detalhes da automação

AWS-StopRdsInstance

Descrição

Interrompa uma instância do Amazon Relational Database Service (Amazon RDS).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: String

  Descrição: ID (obrigatório) da instância do Amazon RDS a ser interrompida.

AWSSupport-TroubleshootConnectivityToRDS

Descrição

O `AWSSupport-TroubleshootConnectivityToRDS` runbook diagnostica problemas de conectividade entre uma EC2 instância e uma instância do Amazon Relational Database Service. A automação garante que a instância de banco de dados esteja disponível e, em seguida, verifica as regras do grupo de segurança, as listas de controle de acesso à rede (rede ACLs) e as tabelas de rotas associadas em busca de possíveis problemas de conectividade.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DBInstanceIdentificador

  Tipo: String

  Descrição: (obrigatória) o ID da instância de banco de dados com a qual testar a conectividade.
- SourceInstance

  Tipo: String

  Padrão permitido: ^i-[a-z0-9]{8,17}$

  Descrição: (Obrigatório) O ID da EC2 instância a partir da qual testar a conectividade.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`

- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma que o status da instância de banco de dados é `available`.
- `aws:executeAwsApi` :Obtém informações resumidas sobre a instância do banco de dados.
- `aws:executeAwsApi`- Obtém informações sobre a rede da instância de banco de dados ACLs.
- `aws:executeAwsApi` :Obtém o CIDR da sub-rede da instância de banco de dados.
- `aws:executeAwsApi`- Obtém informações sobre a EC2 instância.
- `aws:executeAwsApi`- Obtém informações sobre a rede da EC2 instância ACLs.
- `aws:executeAwsApi`- Obtém informações sobre os grupos de segurança associados à EC2 instância.
- `aws:executeAwsApi` :Obtém informações sobre os grupos de segurança associados à instância do banco de dados.
- `aws:executeAwsApi`- Obtém informações sobre as tabelas de rotas associadas à EC2 instância.
- `aws:executeAwsApi`- Obtém informações sobre a tabela de rotas principal associada à Amazon VPC para a EC2 instância.
- `aws:executeAwsApi` :Obtém informações sobre as tabelas de rotas associadas à instância do banco de dados.
- `aws:executeAwsApi` :Obtém informações sobre a tabela de rotas principal associada à Amazon VPC para a instância do banco de dados.
- `aws:executeScript`: avalia as regras do grupo de segurança.
- `aws:executeScript`- Avalia a rede ACLs.
- `aws:executeScript` :Avalia as tabelas de rotas.
- `aws:sleep` :Encerra a automação.

Saídas

obtenha RDSInstance propriedades. DBInstanceIdentificador - A instância de banco de dados usada na automação.

obtenha RDSInstance propriedades. DBInstanceStatus - O status atual do DBInstance.

evalSecurityGroupRegras. SecurityGroupEvaluation - Resultados da comparação das regras do grupo `SourceInstance` de segurança com as regras do grupo de segurança da instância de banco de dados.

evalNetworkAclRegras. NetworkAclEvaluation - Resultados da comparação da rede com ACLs a `SourceInstance` rede da instância de banco de dados ACLs.

evalRouteTableInscrições. RouteTableEvaluation - Resultados da comparação da tabela de `SourceInstance` rotas com as rotas da instância de banco de dados.

AWSSupport-TroubleshootRDSIAMAuthentication

Descrição

`AWSSupport-TroubleshootRDSIAMAuthentication`Isso ajuda a solucionar problemas de autenticação AWS Identity and Access Management (IAM) para instâncias do Amazon RDS para PostgreSQL, Amazon RDS para MySQL, Amazon RDS para MariaDB, Amazon Aurora PostgreSQL e Amazon Aurora MySQL. Use esse runbook para verificar a configuração necessária para a autenticação do IAM com uma instância do Amazon RDS ou Aurora Cluster. Ele também fornece etapas para corrigir os problemas de conectividade com a Instância do Amazon RDS ou o Aurora Cluster.

> **Important**
>
> Este runbook não é compatível com Amazon RDS para Oracle ou Amazon RDS para Microsoft SQL Server.

> **Important**
>
> Se uma EC2 instância Amazon de origem for fornecida e o banco de dados de destino for o Amazon RDS, uma automação secundária `AWSSupport-TroubleshootConnectivityToRDS` será invocada para solucionar problemas de conectividade TCP. A saída também fornece comandos que você pode executar na sua EC2 instância ou máquina de origem da Amazon para se conectar às instâncias do Amazon RDS usando a autenticação do IAM.

Como funciona?

Este runbook consiste em seis etapas:

- Etapa 1: ValidateInputs: valida as entradas para a automação.
- Etapa 2: branchOnSource EC2 fornecida: verifica se um ID de EC2 instância Amazon de origem é fornecido nos parâmetros de entrada.
- Etapa 3: validarRDSConnectivity: valida a conectividade do Amazon RDS a partir da EC2 instância Amazon de origem, se fornecida.
- Etapa 4: validarRDSIAMAuthentication: valida se o recurso de autenticação do IAM está ativado.
- Etapa 5: validarIAMPolicies: verifica se as permissões necessárias do IAM estão presentes no usuário/função do IAM fornecido.
- Etapa 6: Gerar relatório: gera um relatório dos resultados das etapas executadas anteriormente.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- RDSType

  Tipo: string

Descrição: (Obrigatório): Selecione o tipo de banco de dados relacional ao qual você está tentando se conectar e autenticar.

Valores permitidos: `Amazon RDS` ou `Amazon Aurora Cluster.`

- DBInstanceIdentificador

  Tipo: string

  Descrição: (Obrigatório) O identificador da instância de banco de dados Amazon RDS de destino ou do cluster de banco de dados Aurora.

  Allowed-pattern: `^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

  Número máximo de caracteres: 63

- SourceEc2InstanceIdentifier

  Tipo: `AWS::EC2::Instance::Id`

  Descrição: (Opcional) O ID da EC2 instância da Amazon se você estiver se conectando à instância de banco de dados do Amazon RDS a partir de uma EC2 instância da Amazon em execução na mesma conta e região. Não especifique esse parâmetro se a origem não for uma EC2 instância da Amazon ou se o tipo de destino do Amazon RDS for um cluster de banco de dados Aurora.

  Padrão: ""

- DBIAMRoleNome

  Tipo: string

  Descrição: (Opcional) O nome da função do IAM que está sendo usado para autenticação baseada em IAM. Forneça somente se o parâmetro não `DBIAMUserName` for fornecido, caso contrário, deixe-o vazio. `DBIAMRoleName`Ou `DBIAMUserName` deve ser fornecido.

  Allowed-pattern: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  Número máximo de caracteres: 64

  Padrão: ""

- DBIAMUserNome

  Tipo: string

Descrição: (Opcional) O nome de usuário do IAM usado para autenticação baseada em IAM. Forneça somente se o `DBIAMRoleName` parâmetro não for fornecido, caso contrário, deixe-o vazio. `DBIAMRoleNameOu DBIAMUserName` deve ser fornecido.

Allowed-pattern: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

Número máximo de caracteres: 64

Padrão: `""`

- DBUserNome

  Tipo: string

  Descrição: (Opcional) O nome de usuário do banco de dados mapeado para uma função/usuário do IAM para autenticação baseada em IAM no banco de dados. A opção padrão `*` avalia se a `rds-db:connect` permissão é permitida para todos os usuários no banco de dados.

  Allowed-pattern: `^[a-zA-Z0-9+=,.@*_-]{1,64}$`

  Número máximo de caracteres: 64

  Padrão: `*`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Instruções

1. Navegue até o AWSSupport-TroubleshootRDSIAMAuthenticationno AWS Systems Manager console.
2. Selecione Executar automação.
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole(Opcional):

     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - RDSType(Obrigatório):

     Selecione o tipo de Amazon RDS ao qual você está tentando se conectar e autenticar. Escolha entre os dois valores permitidos: `Amazon RDS` ou `Amazon Aurora Cluster.`
   - DBInstanceIdentificador (obrigatório):

     Insira o identificador da Instância de Banco de Dados Amazon RDS de destino ou do Aurora Cluster ao qual você está tentando se conectar e usar as credenciais do IAM para autenticação.
   - SourceEc2 InstanceIdentifier (opcional):

     Forneça o ID da EC2 instância da Amazon se você estiver se conectando à instância de banco de dados do Amazon RDS a partir de uma EC2 instância da Amazon presente na mesma conta e região. Deixe em branco se a origem não for a Amazon EC2 ou se o tipo de Amazon RDS de destino for um Aurora Cluster.

- DBIAMRoleNome (opcional):

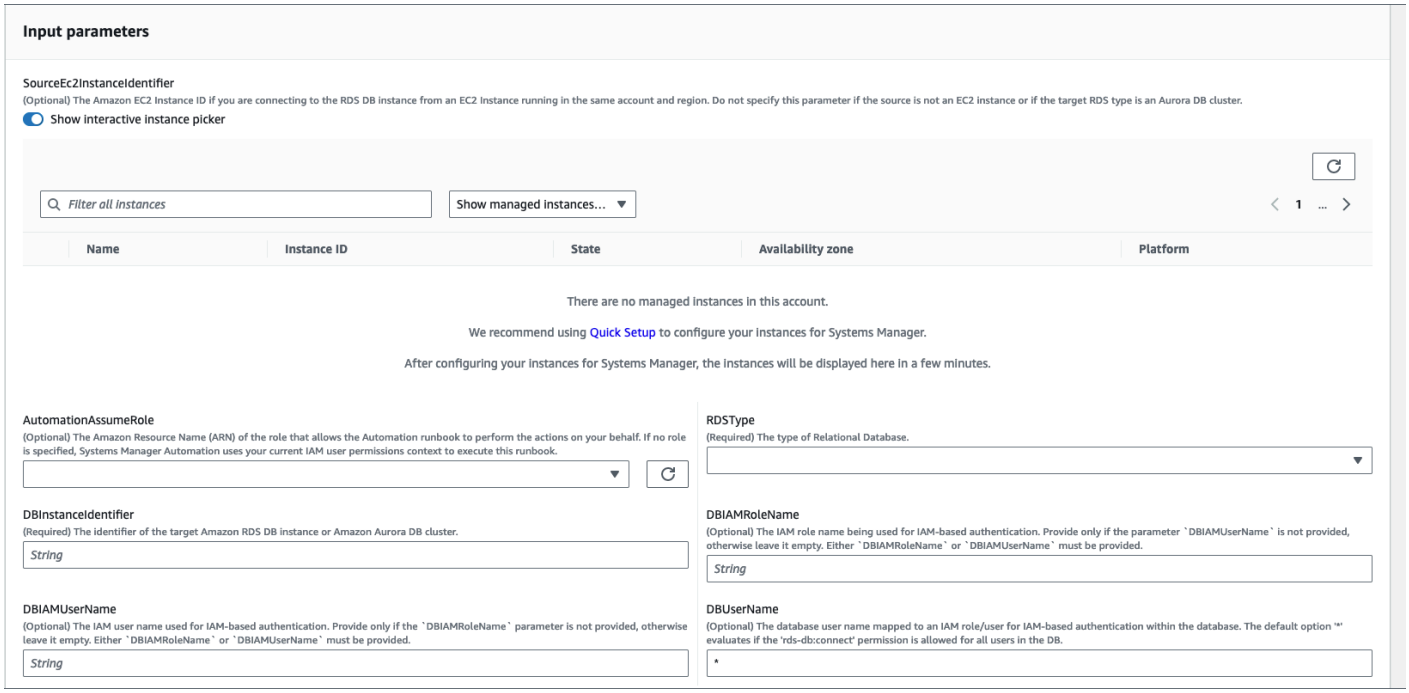
  Insira o nome da função do IAM usado para autenticação baseada em IAM. Forneça somente se não `DBIAMUserName` for fornecido; caso contrário, deixe em branco. `DBIAMRoleName`Ou `DBIAMUserName` deve ser fornecido.

- DBIAMUserNome (opcional):

  Insira o usuário do IAM usado para a autenticação baseada em IAM. Forneça somente se não `DBIAMRoleName` for fornecido, caso contrário, deixe em branco. `DBIAMRoleName`Ou `DBIAMUserName` deve ser fornecido.

- DBUserNome (opcional):

  Insira o usuário do banco de dados mapeado para uma função/usuário do IAM para autenticação baseada em IAM no banco de dados. A opção padrão * é usada para avaliar; nada é fornecido nesse campo.



4. Selecione Executar.
5. Observe que a automação é iniciada.
6. O bucket realiza as seguintes etapas:

   - Etapa 1: validar as entradas:

     Valida as entradas para a automação - `SourceEC2InstanceIdentifier` (opcional), `DBInstanceIdentifier` ou`ClusterID`, e `DBIAMRoleName` ou. `DBIAMUserName` Ele

verifica se os parâmetros de entrada inseridos estão presentes em sua conta e região. Ele também verifica se o usuário inseriu um dos parâmetros do IAM (por exemplo, `DBIAMRoleName` ou`DBIAMUserName`). Além disso, ele executa outras verificações, como se o banco de dados mencionado estiver no status Disponível.

- Etapa 2: branchOnSource EC2 Fornecido:

  Verifica se a fonte Amazon EC2 é fornecida nos parâmetros de entrada e se o banco de dados é Amazon RDS. Se sim, prossegue para a etapa 3. Caso contrário, ele pula a etapa 3, que é a validação da conectividade Amazon EC2 -Amazon RDS, e prossegue para a etapa 4.

- Etapa 3: validarRDSConnectivity:

  Se a Amazon de origem EC2 for fornecida nos parâmetros de entrada e o banco de dados for o Amazon RDS, a etapa 2 iniciará a etapa 3. Nesta etapa, a automação secundária `AWSSupport-TroubleshootConnectivityToRDS` é invocada para validar a conectividade do Amazon RDS da Amazon de origem. EC2 O runbook de automação infantil `AWSSupport-TroubleshootConnectivityToRDS` verifica se as configurações de rede necessárias (Amazon Virtual Private Cloud [Amazon VPC], grupos de segurança, lista de controle de acesso à rede [NACL], disponibilidade do Amazon RDS) estão em vigor para que você possa se conectar da instância da Amazon à instância do Amazon RDS. EC2

- Etapa 4: validarRDSIAMAuthentication:

  Valida se o recurso de autenticação do IAM está ativado na instância do Amazon RDS ou no Aurora Cluster.

- Etapa 5: validarIAMPolicies:

  Verifica se as permissões necessárias do IAM estão presentes no usuário/função do IAM passado para permitir que as credenciais do IAM sejam autenticadas na instância do Amazon RDS para o usuário de banco de dados especificado (se houver).

- Etapa 6: Gerar relatório:

  Obtém todas as informações das etapas anteriores e imprime o resultado ou a saída de cada etapa. Ele também lista as etapas a serem consultadas e executadas para se conectar à instância do Amazon RDS usando as credenciais do IAM.

7. Quando a automação estiver concluída, revise a seção Saídas para obter os resultados detalhados:

   - Verificando a permissão de usuário/função do IAM para se conectar ao banco de dados:

Verifica se as permissões necessárias do IAM estão presentes no usuário/função do IAM passado para permitir que as credenciais do IAM sejam autenticadas na instância do Amazon RDS para o usuário de banco de dados especificado (se houver).

- Verificando o atributo de autenticação baseado em IAM para o banco de dados:

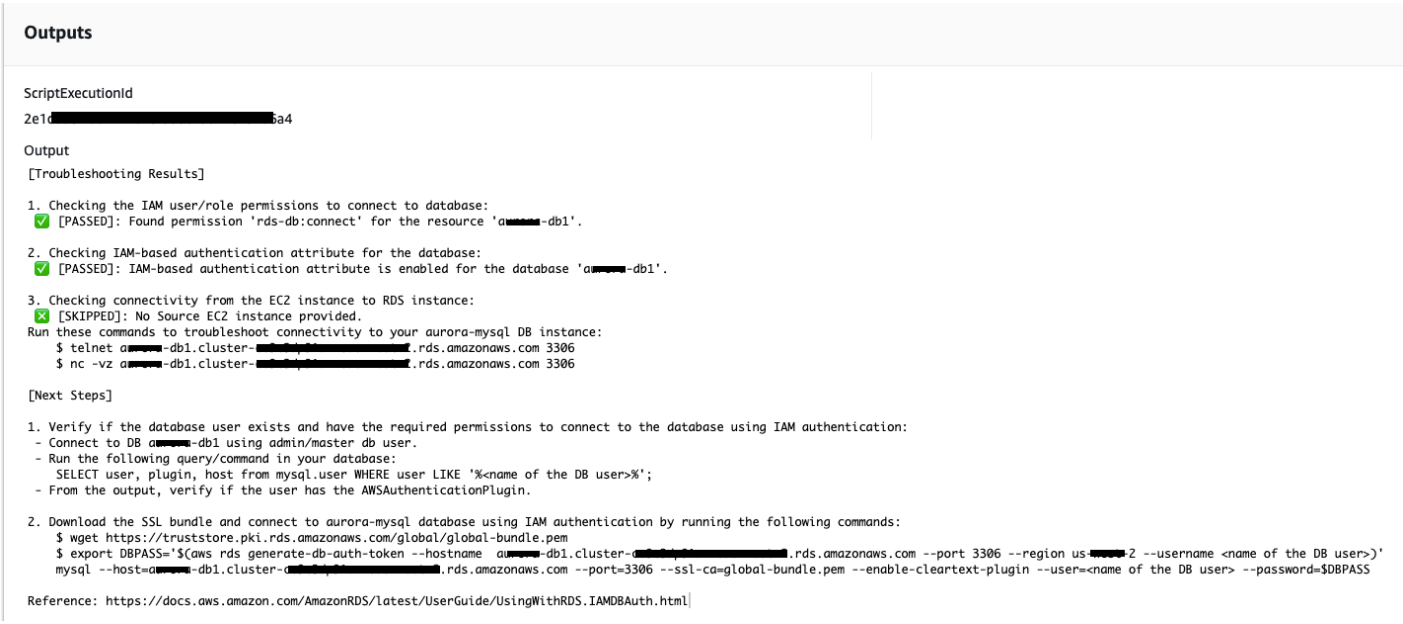
  Verifica se o recurso da autenticação do IAM está habilitado para o banco de dados Amazon RDS/cluster Aurora especificado.

- Verificando a conectividade da EC2 instância da Amazon com a instância do Amazon RDS:

  Verifica se as configurações de rede necessárias (Amazon VPC, grupos de segurança, NACL, disponibilidade do Amazon RDS) estão em vigor para que você possa se conectar da instância da Amazon à instância EC2 do Amazon RDS.

- Próximas etapas:

  Lista os comandos e as etapas a serem consultados e executados para se conectar à instância do Amazon RDS usando as credenciais do IAM.



Outputs

ScriptExecutionId

2e1d[redacted]6a4

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
```

Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação

- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSSupport-ValidateRdsNetworkConfiguration

Descrição

`AWSSupport-ValidateRdsNetworkConfiguration`a automação ajuda a evitar um estado de rede incompatível para sua instância existente do Amazon Relational Database Service (Amazon RDS) /Amazon Aurora /Amazon DocumentDB antes de você executar ou operar. `ModifyDBInstance` `StartDBInstance` Se a instância já estiver em um estado de rede incompatível, o runbook fornecerá o motivo.

Como funciona?

Este runbook determina se sua instância de banco de dados do Amazon RDS entrará em um estado de rede incompatível ou, se estiver, determina o motivo pelo qual está em um estado de rede incompatível.

O runbook executa as seguintes verificações em sua instância de banco de dados Amazon RDS:

- Cota da Amazon Elastic Network Interface (ENI) por região.
- Todas as sub-redes no grupo de sub-redes do banco de dados existem.
- Há endereços IP gratuitos suficientes disponíveis para a (s) sub-rede (s).
- (Para instâncias do Amazon RDS acessíveis publicamente) Configurações de atributos de VPC `enableDnsSupport` (`enableDnsHostnamese`).

> **Important**
>
> Ao usar este documento em clusters Amazon Aurora/Amazon DocumentDB, certifique-se de usar em vez de. `DBInstanceIdentifier` `ClusterIdentifier` Caso contrário, o documento falhará na primeira etapa.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `rds:DescribeDBInstances`
- `servicequotas:GetServiceQuota`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeSubnets`

Exemplo de política:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ValidateRdsNetwork",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances",
                "servicequotas:GetServiceQuota",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "arn:aws:rds:{Region}:{Account}:db:{DbInstanceName}"
            ]
        }
    ]
```

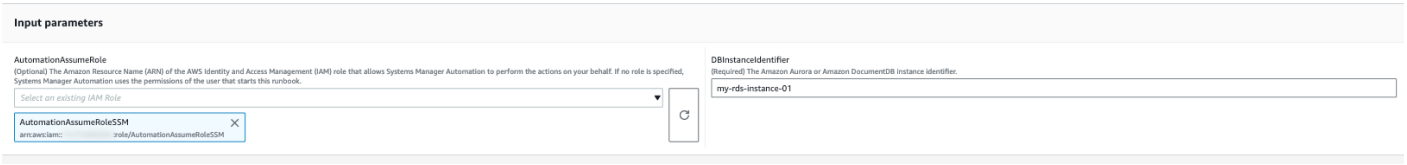
```
        }
```

Instruções

1. Navegue até o AWSSupport-ValidateRdsNetworkConfigurationno AWS Systems Manager console.
2. Selecione Executar automação.
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole(Opcional):

     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - DBInstanceIdentificador (obrigatório):

     Insira o identificador de instância do Amazon Relational Database Service.



4. Selecione Executar.
5. Observe que a automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - Etapa 1 assertRdsState:

     Verifica se o identificador de instância fornecido existe e tem algum dos seguintes estados:`available`,`stopped`, ou`incompatible-network`.
   - Etapa 2 gatherRdsInformation:

     Coleta as informações necessárias sobre a instância do Amazon RDS para uso posterior na automação.
   - Etapa 3 checkEniQuota:

     Verifica a cota atual disponível do Amazon ENI para a região.
   - Etapa 4 validateVpcAttributes:

Valida se os parâmetros de DNS (`enableDnsSupporteenableDnsHostnames`) da Amazon VPC estão definidos como verdadeiros (ou não, se a instância do Amazon RDS estiver). `PubliclyAccessible`

- Etapa 5 validateSubnetAttributes:

  Valida a existência de sub-redes no `DBSubnetGroup` e verifica se há disponibilidade IPs para cada sub-rede.

- Etapa 6: Gerar relatório:

  Obtém todas as informações das etapas anteriores e imprime o resultado ou a saída de cada etapa. Ele também lista as etapas a serem consultadas e executadas para se conectar à instância do Amazon RDS usando as credenciais do IAM.

7. Quando a automação estiver concluída, revise a seção Saídas para obter os resultados detalhados:

   Instância do Amazon RDS com configuração de rede 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 Existance Check: ✅ [PASSED]
     ii. Available IP Check: ✅ [PASSED]
  * Availability Zone: ap-south-1a
      i. Subnet Existance Check: ✅ [PASSED]
     ii. Available IP Check: ✅ [PASSED]

### [Next Steps]

✅ All the checks has passed so the RDS Network configuration is correct.

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.
```

Instância do Amazon RDS com configuração de rede incorreta (o enableDnsHostnames atributo VPC está definido como false):

Outputs

generateReport.Report

```
# AWS RDS Network Configuration Checks: test-fail-sazrds-vpcattrs (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 Existance 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 opeartion 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.
```

Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- Como resolvo problemas com um banco de dados do Amazon RDS que está em um estado de rede incompatível?
- Como resolvo problemas com uma instância do Amazon DocumentDB que está em um estado de rede incompatível?

Amazon Redshift

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Redshift. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-DeleteRedshiftCluster
- AWSConfigRemediation-DisablePublicAccessToRedshiftCluster
- AWSConfigRemediation-EnableRedshiftClusterAuditLogging
- AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot
- AWSConfigRemediation-EnableRedshiftClusterEncryption
- AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting
- AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster
- AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings
- AWSConfigRemediation-ModifyRedshiftClusterNodeType

`AWSConfigRemediation-DeleteRedshiftCluster`

Descrição

O runbook `AWSConfigRemediation-DeleteRedshiftCluster` exclui o cluster do Amazon Redshift especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterIdentifier

  Tipo: String

  Descrição: (obrigatório) O ID do cluster do Amazon Redshift que deseja excluir.
- SkipFinalClusterSnapshot

  Tipo: booliano

  Padrão: False

  Descrição: (opcional) Se definida como `false`, a automação cria um snapshot antes de excluir o cluster do Amazon Redshift. Se definido como `true`, um snapshot final do cluster não será criado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DeleteCluster`
- `redshift:DescribeClusters`

Etapas do documento

- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `SkipFinalClusterSnapshot`.
- `aws:executeAwsApi` :Exclui o cluster do Amazon Redshift especificado no parâmetro `ClusterIdentifier`.

- `aws:assertAwsResourceProperty` :Verifica se o cluster do Amazon Redshift foi excluído.

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

Descrição

O runbook `AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` desabilita a acessibilidade pública para o cluster do Amazon Redshift especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterIdentifier

  Tipo: String

  Descrição: (obrigatório) O identificador exclusivo do cluster para o qual deseja desabilitar a acessibilidade pública.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Desabilita a acessibilidade pública para o cluster especificado no parâmetro `ClusterIdentifier`.
- `aws:waitForAwsResourceProperty` :Espera que o estado do cluster mude para `available`.
- `aws:assertAwsResourceProperty` :Confirma que a definição de acessibilidade pública está desabilitada no cluster.

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

Descrição

O runbook `AWSConfigRemediation-EnableRedshiftClusterAuditLogging` habilita o log de auditoria para o cluster do Amazon Redshift especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- BucketName

  Tipo: String

  Descrição: (obrigatório) O nome do bucket do Amazon Simple Storage Service (Amazon S3) para o qual deseja fazer upload de logs.

- ClusterIdentifier

  Tipo: String

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual deseja habilitar o log de auditoria.

- S3 KeyPrefix

  Tipo: String

  Descrição: (opcional) O prefixo de chave (subpasta) do Amazon S3 para o qual deseja fazer o upload dos logs.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

Etapas do documento

- `aws:branch` :Ramifica com base no fato de um valor ter sido especificado para o parâmetro `S3KeyPrefix`.
- `aws:executeAwsApi` :Permite o log de auditoria no cluster especificado no `ClusterIdentifier` parâmetro.
- `aws:assertAwsResourceProperty` :Verifica se o log de auditoria foi habilitado no cluster.

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

Descrição

O runbook `AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` habilita snapshots automatizados para o cluster do Amazon Redshift especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- AutomatedSnapshotRetentionPeriod

  Tipo: inteiro

Valores válidos: 1 a 35

Descrição: (obrigatório) O número de dias que os snapshots automatizados são retidos.

- ClusterIdentifier

  Tipo: String

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual você deseja ativar os snapshots automatizados

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Habilita snapshots de automação no cluster especificado no parâmetro `ClusterIdentifier`.
- `aws:waitForAwsResourceProperty` :Espera que o estado do cluster mude para `available`.
- `aws:executeScript` :Confirma que os snapshots automatizados foram habilitados no cluster.

AWSConfigRemediation-EnableRedshiftClusterEncryption

Descrição

O `AWSConfigRemediation-EnableRedshiftClusterEncryption` runbook permite a criptografia no cluster do Amazon Redshift que você especifica usando AWS Key Management Service uma chave AWS KMS() gerenciada pelo cliente. Esse runbook só deve ser usado como uma linha de base para garantir que os clusters do Amazon Redshift sejam criptografados de acordo com as melhores práticas de segurança mínimas recomendadas. Recomendamos criptografar vários clusters com diferentes chaves gerenciadas pelo cliente. Esse runbook não pode alterar a

chave gerenciada pelo AWS KMS cliente usada em um cluster já criptografado. Para alterar a chave gerenciada pelo AWS KMS cliente usada para criptografar um cluster, primeiro você deve desativar a criptografia no cluster.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterIdentifier

  Tipo: String

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual você deseja habilitar a criptografia.
- KMSKeyARN

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) da chave gerenciada pelo cliente do AWS KMS que deseja usar para criptografar os dados do cluster.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Habilita a criptografia no cluster do Amazon Redshift especificado no parâmetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty` :Verifica se a criptografia foi habilitada no cluster.

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

Descrição

O runbook `AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` habilita um roteamento avançado da nuvem privada virtual (VPC) para o cluster do Amazon Redshift especificado. Para obter mais informações sobre o roteamento avançado da Amazon VPC, consulte Roteamento avançado da VPC do Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- ClusterIdentifier

  Tipo: String

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual deseja habilitar o roteamento avançado da VPC.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Habilita o roteamento avançado da VPC no cluster especificado no parâmetro `ClusterIdentifier`.
- `assertAwsResourceProperty` :Confirma que o roteamento avançado da VPC foi habilitado no cluster.

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

Descrição

O runbook `AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` exige que as conexões de entrada usem SSL para o cluster do Amazon Redshift especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- ClusterIdentifier

  Tipo: String

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual deseja habilitar o roteamento avançado da VPC.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

Etapas do documento

- `aws:executeAwsApi` :Reúne os detalhes dos parâmetros do cluster especificado no parâmetro `ClusterIdentifier`.
- `aws:executeAwsApi`: Habilita a definição de `require_ssl` no cluster especificado no parâmetro `ClusterIdentifier`.
- `aws:assertAwsResourceProperty` :Confirma que a definição de `require_ssl` está habilitada no cluster .
- `aws:executeScript` :Verifica a definição de `require_ssl` do cluster.

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

Descrição

O runbook `AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` modifica as definições de manutenção do cluster Amazon Redshift especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AllowVersionUpgrade

  Tipo: booliano

  Descrição: (obrigatório) Se definido como `true`, as atualizações da versão principal serão aplicadas automaticamente ao cluster durante a janela de manutenção.
- AutomationAssumeRole

Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- AutomatedSnapshotRetentionPeriod

  Tipo: inteiro

  Valores válidos: 1 a 35

  Descrição: (obrigatório) O número de dias que os snapshots automatizados são retidos.
- ClusterIdentifier

  Tipo: String

  Descrição: (obrigatório) O identificador exclusivo do cluster no qual deseja habilitar o roteamento avançado da VPC.
- PreferredMaintenanceWindow

  Tipo: String

  Descrição: (obrigatório) O intervalo de tempo semanal (em UTC) durante o qual pode ocorrer manutenção do sistema.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

Etapas do documento

- `aws:executeAwsApi` :Modifica as definições de manutenção do cluster especificado no parâmetro `ClusterIdentifier`.

- `aws:assertAwsResourceProperty` :Confirma que as definições de manutenção modificadas foram configuradas para o cluster.

AWSConfigRemediation-ModifyRedshiftClusterNodeType

Descrição

O runbook `AWSConfigRemediation-ModifyRedshiftClusterNodeType` modifica o tipo de nó e o número de nós para o cluster do Amazon Redshift especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Bancos de dados

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- Clássica

  Tipo: Booliano

  Descrição: (opcional) Se definida como `true`, a operação de redimensionamento usa o processo de redimensionamento clássico.
- ClusterIdentifier

  Tipo: String

Descrição: (obrigatório) O identificador exclusivo do cluster cujo tipo de nó deseja modificar.

- ClusterType

  Tipo: String

  Valores válidos: single-node | multi-node

  Descrição: (obrigatório) O tipo de cluster que deseja atribuir ao seu cluster.

- NodeType

  Tipo: String

  Valores válidos: ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

  Descrição: (obrigatório) O tipo de nó que você deseja atribuir ao seu cluster.

- NumberOfNodes

  Tipo: inteiro

  Valores válidos: 2 a 100

  Descrição: (opcional) O número de nós que deseja atribuir ao seu cluster. Se o cluster for do tipo `single-node`, não especifique um valor para esse parâmetro.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

Etapas do documento

- `aws:executeScript` :Modifica o tipo de nó e o número de nós do cluster especificado no parâmetro `ClusterIdentifier`.

Amazon S3

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Simple Storage Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-ArchiveS3BucketToIntelligentTiering
- AWS-ConfigureS3BucketLogging
- AWS-ConfigureS3BucketVersioning
- AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock
- AWSConfigRemediation-ConfigureS3PublicAccessBlock
- AWS-CreateS3PolicyToExpireMultipartUploads
- AWS-DisableS3BucketPublicReadWrite
- AWS-EnableS3BucketEncryption
- AWS-EnableS3BucketKeys
- AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy
- AWSConfigRemediation-RestrictBucketSSLRequestsOnly
- AWSSupport-TroubleshootS3PublicRead
- AWSSupport-EmptyS3Bucket
- AWSSupport-TroubleshootS3EventNotifications
- AWSSupport-ContainS3Resource

`AWS-ArchiveS3BucketToIntelligentTiering`

Descrição

O `AWS-ArchiveS3BucketToIntelligentTiering` runbook cria ou substitui uma configuração de classificação por níveis inteligente para o bucket do Amazon Simple Storage Service (Amazon S3) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: String

  Descrição: (Obrigatório) O nome do bucket do S3 para o qual você deseja criar uma configuração de hierarquização inteligente.
- ConfigurationId

  Tipo: String

  Descrição: (Obrigatório) O ID da configuração inteligente de camadas. Isso pode ser um novo ID de configuração ou o ID de uma configuração existente.
- NumberOfDaysToArchive

  Tipo: String

  Valores válidos: 90-730

  Descrição: (Obrigatório) O número de dias consecutivos após um objeto em seu bucket estar qualificado para ser transferido para o nível Archive Access.
- NumberOfDaysToDeepArchive

Tipo: String

Valores válidos: 180-730

Descrição: (Obrigatório) O número de dias consecutivos após um objeto em seu bucket estar qualificado para ser transferido para o nível de acesso ao Deep Archive.

- S3Prefix

  Tipo: String

  Descrição: (Opcional) O prefixo do nome da chave dos objetos aos quais você deseja aplicar a configuração.

- Tags

  Tipo: MapList

  Descrição: (Opcional) Metadados atribuídos aos objetos aos quais você deseja aplicar a configuração. As tags consistem em uma chave e um valor definidos pelo usuário.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`
- `s3:PutIntelligentTieringConfiguration`

Etapas do documento

- PutsBucketIntelligentTieringConfiguration (aws:ExecuteScript) — Cria ou atualiza uma configuração do Amazon S3 Intelligent-Tiering para o bucket especificado.
- VerifyBucketIntelligentTieringConfiguration(aws: assertAwsResource Property) - Verifica se a configuração inteligente do bucket do S3 foi aplicada ao bucket especificado.

AWS-ConfigureS3BucketLogging

Descrição

Habilitar o log do bucket do Amazon Simple Storage Service (Amazon S3).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: String

  Descrição: (obrigatório) O nome do bucket do Amazon S3 para o qual você deseja configurar o log.
- GrantedPermission

  Tipo: String

  Valores permitidos: FULL_CONTROL | READ | WRITE

  Descrição: (obrigatório) Registrar permissões atribuídas ao usuário autorizado para o bucket.

- GranteeEmailAddress

  Tipo: String

  (Opcional) O endereço de e-mail do favorecido.

- GranteeId

  Tipo: String

  Descrição: (opcional) O ID de usuário canônico do favorecido.

- GranteeType

  Tipo: String

  Valores válidos: CanonicalUser | AmazonCustomerByEmail | Grupo

  Descrição: (obrigatório) Tipo de favorecido.

- GranteeUri

  Tipo: String

  Descrição: (opcional) URI do grupo de favorecidos.

- TargetBucket

  Tipo: String

  Descrição: (obrigatório) Especifica o bucket em que você deseja que o Amazon S3 armazene os logs de acesso do servidor. Os logs podem ser entregues em qualquer bucket de sua propriedade. Você também pode configurar vários buckets para entregar seus logs para o mesmo bucket de destino. Nesse caso, você deve escolher um diferente TargetPrefix para cada bucket de origem para que os arquivos de log entregues possam ser diferenciados por chave.

- TargetPrefix

  Tipo: String

  Padrão: /

  Descrição: (opcional) Especifica um prefixo para as chaves em que os arquivos de log serão armazenados.

AWS-ConfigureS3BucketVersioning

Descrição

Configurar o versionamento de um bucket do Amazon Simple Storage Service (Amazon S3).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: String

  Descrição: (obrigatório) O nome do bucket do Amazon S3 para o qual você deseja configurar o versionamento.
- VersioningState

  Tipo: String

  Valores permitidos: Enabled | Suspended

Padrão: Habilitado

Descrição: (Opcional) Aplicada ao VersioningConfiguration .Status. Quando definido como "Enabled", esse processo permite o versionamento de objetos no bucket; todos os objetos adicionados ao bucket recebem um ID de versão exclusivo. Quando definido como `Suspended`, esse processo desabilita o versionamento dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão `null`.

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Descrição

O runbook `AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock` define as configurações do bloco de acesso público do Amazon Simple Storage Service (Amazon S3) para um bucket do Amazon S3 com base nos valores especificados nos parâmetros do runbook.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- BlockPublicAcls

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Se definido como`true`, o Amazon S3 bloqueia listas públicas de controle de acesso (ACLs) para o bucket S3 e objetos armazenados no bucket S3 que você especificar no parâmetro. `BucketName`

- BlockPublicPolicy

  Tipo: booleano

  Padrão: True

  Descrição: (opcional) Se definido como `true`, o Amazon S3 bloqueia políticas públicas de bucket para o bucket S3 especificado no parâmetro `BucketName`.

- BucketName

  Tipo: String

  Descrição: (obrigatória) O nome do bucket do S3 onde você deseja configurar.

- IgnorePublicAcls

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Se definido como`true`, o Amazon S3 ignora todos os públicos ACLs do bucket do S3 que você especificar no parâmetro. `BucketName`

- RestrictPublicBuckets

  Tipo: booleano

  Padrão: True

  Descrição: (opcional) Se definido como `true`, o Amazon S3 restringe as políticas públicas de bucket para o bucket do S3 especificado no parâmetro `BucketName`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

Etapas do documento

- `aws:executeAwsApi` :Cria ou modifica a configuração de `PublicAccessBlock` do bucket do S3 especificado no parâmetro `BucketName`.
- `aws:executeScript` :Retorna a configuração de `PublicAccessBlock` do bucket do S3 especificado no parâmetro `BucketName` e verifica se as alterações foram feitas com sucesso com base nos valores especificados nos parâmetros do runbook.

`AWSConfigRemediation-ConfigureS3PublicAccessBlock`

Descrição

O `AWSConfigRemediation-ConfigureS3PublicAccessBlock` runbook configura as configurações de um bloco de acesso público do Conta da AWS Amazon Simple Storage Service (Amazon S3) com base nos valores que você especifica nos parâmetros do runbook.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AccountId

  Tipo: String

  Descrição: (Obrigatório) O ID do proprietário do bucket S3 Conta da AWS que você está configurando.

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- BlockPublicAcls

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Se definido como`true`, o Amazon S3 bloqueia listas públicas de controle de acesso (ACLs) para buckets do S3 pertencentes ao Conta da AWS que você especificou no parâmetro. `AccountId`

- BlockPublicPolicy

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Se definido como`true`, o Amazon S3 bloqueia políticas públicas de bucket para buckets do S3 de propriedade do Conta da AWS que você especifica no parâmetro. `AccountId`

- IgnorePublicAcls

  Tipo: booleano

  Padrão: verdadeiro

Descrição: (Opcional) Se definido como`true`, o Amazon S3 ignora todos os buckets públicos ACLs do S3 pertencentes ao que Conta da AWS você especificou no parâmetro. `AccountId`

- RestrictPublicBuckets

  Tipo: booleano

  Padrão: verdadeiro

  Descrição: (Opcional) Se definido como`true`, o Amazon S3 restringe as políticas públicas de bucket para buckets do S3 de propriedade do que Conta da AWS você especifica no parâmetro. `AccountId`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

Etapas do documento

- `aws:executeAwsApi` :Cria ou modifica a configuração `PublicAccessBlock` para a Conta da AWS especificada no parâmetro `AccountId`.
- `aws:executeScript`- Retorna a `PublicAccessBlock` configuração Conta da AWS especificada no `AccountId` parâmetro e verifica se as alterações foram feitas com sucesso com base nos valores especificados nos parâmetros do runbook.

AWS-CreateS3PolicyToExpireMultipartUploads

Descrição

O `AWS-CreateS3PolicyToExpireMultipartUploads` runbook cria uma política de ciclo de vida para um bucket específico que expira os uploads incompletos de várias partes em andamento após

um número definido de dias. Esse runbook mescla a nova política de ciclo de vida com qualquer política de bucket de ciclo de vida existente que já exista.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: String

  Descrição: (obrigatória) O nome do bucket do S3 onde você deseja configurar.
- DaysUntilExpire

  Tipo: inteiro

  Descrição: (Obrigatório) O número de dias que o Amazon S3 espera antes de remover permanentemente todas as partes do upload.
- RuleId

  Tipo: String

Descrição: (Obrigatório) O ID usado para identificar a regra do intervalo de ciclo de vida. Esse deve ser um valor exclusivo.

- S3Prefix

  Tipo: String

  Descrição: (Opcional) O prefixo do nome da chave dos objetos aos quais você deseja aplicar a configuração.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

Etapas do documento

- ConfigureExpireMultipartUploads (aws:ExecuteScript) — Configura a política de ciclo de vida do bucket.
- VerifyExpireMultipartUploads (aws:ExecuteScript) — Verifica se a política de ciclo de vida foi configurada para o bucket.

Saídas

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

AWS-DisableS3BucketPublicReadWrite

Descrição

Usar o `Block Public Access` do Amazon Simple Storage Service (Amazon S3) para desabilitar o acesso de leitura e gravação para um bucket público do S3. Para obter mais informações, consulte

Usar o bloqueio de acesso público do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- S3 BucketName

  Tipo: String

  Descrição: (obrigatória) o bucket do S3 no qual você deseja restringir o acesso.

AWS-EnableS3BucketEncryption

Descrição

Configura o bucket Amazon Simple Storage Service (Amazon S3) para criptografia padrão.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: String

  Descrição: (obrigatória) o nome do bucket do S3 onde você deseja criptografar o conteúdo.
- SSEAlgorithm

  Tipo: String

  Padrão: AES256

  Descrição: (Opcional) Algoritmo de criptografia do lado do servidor a ser usado para a criptografia padrão.

AWS-EnableS3BucketKeys

Descrição

O `AWS-EnableS3BucketKeys` runbook habilita Bucket Keys no bucket do Amazon Simple Storage Service (Amazon S3) especificado por você. Essa chave em nível de bucket cria chaves de dados

para novos objetos durante seu ciclo de vida. Se você não especificar um valor para o `KmsKeyId` parâmetro, a criptografia do lado do servidor usando as chaves gerenciadas do Amazon S3 (SSE-S3) será usada para a configuração de criptografia padrão.

> **Note**
>
> As chaves de bucket do Amazon S3 não são compatíveis com criptografia de duas camadas no lado do servidor com AWS Key Management Service chaves () (DSSE-KMS).AWS KMS

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BucketName

  Tipo: String

  Descrição: (Obrigatório) O nome do bucket do S3 para o qual você deseja habilitar o Bucket Keys.
- KMSKeyIdentificação

Tipo: String

Descrição: (Opcional) O nome de recurso da Amazon (ARN), o ID da chave ou o alias da chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente que você deseja usar para criptografia no lado do servidor.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

Etapas do documento

- ChooseEncryptionType (aws:branch) - Avalia o valor fornecido para o `KmsKeyId` parâmetro para determinar se SSE-S3 (AES256) ou SSE-KMS serão usados.
- PutBucketKeysKMS (aws:executeAwsApi) - Define a `BucketKeyEnabled` propriedade `true` para o bucket S3 especificado usando o especificado. `KmsKeyId`
- PutBucketKeysAES256 (aws:executeAwsApi) - Define a `BucketKeyEnabled` propriedade `true` para o bucket S3 especificado com AES256 criptografia.
- VerifyS3 BucketKeysEnabled (aws: assertAwsResource Property) - Verifica se as chaves de bucket estão habilitadas no bucket S3 de destino.

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

Descrição

O runbook `AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy` remove as instruções de política da entidade principal que têm curingas (`Principal: *` ou `Principal: "AWS": *`) para ações de `Allow` de sua política de bucket do Amazon Simple Storage Service (Amazon S3). As instruções de política com condições também são removidas.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- BucketName

  Tipo: String

  Descrição: (obrigatório) O nome do bucket do Amazon S3 cuja política deseja modificar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

Etapas do documento

- `aws:executeScript` :Modifica a política do bucket e verifica se as instruções de política da entidade principal com curingas foram removidas do bucket do Amazon S3 especificado no parâmetro `BucketName`.

`AWSConfigRemediation-RestrictBucketSSLRequestsOnly`

Descrição

O runbook `AWSConfigRemediation-RestrictBucketSSLRequestsOnly` cria uma instrução de política de bucket do Amazon Simple Storage Service (Amazon S3) que nega explicitamente solicitações HTTP para o bucket do Amazon S3 especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- BucketName

  Tipo: String

  Descrição: (obrigatório) O nome do bucket do S3 cujas solicitações HTTP serão negadas.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutEncryptionConfiguration`
- `s3:PutBucketPolicy`

Etapas do documento

- `aws:executeScript` :Cria uma política de bucket para o bucket do S3 especificado no parâmetro `BucketName` que nega explicitamente as solicitações HTTP.

AWSSupport-TroubleshootS3PublicRead

Descrição

O runbook `AWSSupport-TroubleshootS3PublicRead` diagnostica problemas de leitura de objetos do bucket público do Amazon Simple Storage Service (Amazon S3) especificado no parâmetro `S3BucketName`. Um subconjunto de definições também é analisado para objetos no bucket do S3.

Executar esta automação (console)

Limitações

- Essa automação não verifica os pontos de acesso que permitem o acesso público aos objetos.
- Essa automação não avalia as chaves de condição na política de bucket do S3.
- Se você estiver usando AWS Organizations, essa automação não avalia as políticas de controle de serviços para confirmar se o acesso ao Amazon S3 é permitido.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- CloudWatchLogGroupName

  Tipo: String

  Descrição: (Opcional) O grupo de CloudWatch registros do Amazon Logs para o qual você deseja enviar a saída de automação. Se não for encontrado um grupo de logs que corresponda ao valor especificado, a automação criará um grupo de logs usando esse valor de parâmetro. O período de retenção do grupo de logs criado por essa automação é de 14 dias.
- CloudWatchLogStreamName

  Tipo: String

  Descrição: (Opcional) O fluxo de CloudWatch registros para o qual você deseja enviar a saída de automação. Se não for encontrado um fluxo de logs que corresponda ao valor especificado, a automação criará um fluxo de logs usando esse valor de parâmetro. Se um valor para esse parâmetro não for especificado, a automação usará o `ExecutionId` para o nome do fluxo de logs.
- HttpGet

  Tipo: booliano

  Valores válidos: True | False

Padrão: True

Descrição: (opcional) Se esse parâmetro for definido como `true`, a automação fará uma solicitação HTTP parcial aos objetos do `S3BucketName` que forem especificados. Somente o primeiro byte do objeto é retornado usando o cabeçalho HTTP Range.

- IgnoreBlockPublicAccess

  Tipo: booliano

  Valores válidos: True | False

  Padrão: False

  Descrição: (opcional) Se esse parâmetro for definido como `true`, a automação ignorará as definições do bloco de acesso público do bucket do S3 especificado no parâmetro `S3BucketName`. Não é recomendável alterar o valor do este parâmetro padrão.

- MaxObjects

  Tipo: inteiro

  Valores válidos: 1 a 25

  Padrão: 5

  Descrição: (opcional) O número de objetos a serem analisados no bucket do S3 especificado no parâmetro `S3BucketName`.

- S3 BucketName

  Tipo: String

  Descrição: (obrigatória) O ID do bucket do S3 para solução de problemas.

- S3 PrefixName

  Tipo: String

  Descrição: (opcional) O prefixo do nome da chave dos objetos que você quer analisar em seu bucket do S3. Para ter mais informações, consulte Chaves do objeto no Guia do usuário do Amazon Simple Storage Service.

- StartAfter

Tipo: String

Descrição: (opcional) O nome da chave do objeto em que a automação deve começar a analisar os objetos em seu bucket do S3.

- ResourcePartition

  Tipo: String

  Valores válidos: `aws` | `aws-us-gov` | `aws-cn`

  Padrão: `aws`

  Descrição: (obrigatório) A partição em que o bucket do S3 está localizado.

- Detalhado

  Tipo: Booliano

  Valores válidos: True | False

  Padrão: False

  Descrição: (opcional) Para retornar informações mais detalhadas durante a automação, defina esse parâmetro como `true`. Somente mensagens de aviso e erro serão retornadas se o parâmetro estiver definido como `false`.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

As `logs:PutLogEvents` permissões `logs:CreateLogGrouplogs:CreateLogStream`, e só são necessárias se você quiser que a automação envie dados de registro para o CloudWatch Logs.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:SimulateCustomPolicy",
                "iam:GetContextKeysForCustomPolicy",
                "s3:ListAllMyBuckets",
                "logs:CreateLogGroup",
```

```
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy",
                "s3:GetAccountPublicAccessBlock"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging"
            ],
            "Resource": "arn:aws:s3:::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"
        }
    ]
}
```

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma que o bucket do S3 existe e está acessível.
- `aws:executeScript` :Retorna a localização do bucket do S3 e seu ID de usuário canônico.
- `aws:executeScript` :Retorna as definições do bloco de acesso público de sua conta e do bucket do S3.
- `aws:assertAwsResourceProperty` :Confirma que o pagador do bucket do S3 está configurado como `BucketOwner`. Se `Requester Pays` estiver habilitado no bucket do S3, a automação será encerrada.

- `aws:executeScript` :Retorna o status da política do bucket do S3 e determina se ela é considerada pública. Para obter mais informações sobre buckets públicos do S3, consulte O significado de "público" no Guia do desenvolvedor do Amazon Simple Storage Service.
- `aws:executeAwsApi` :Retorna a política de bucket do S3.
- `aws:executeAwsApi` :Retorna todas as chaves de contexto encontradas na política de bucket do S3.
- `aws:assertAwsResourceProperty` :Confirma se há uma negação explícita na política de bucket do S3 para a ação `GetObject` da API.
- `aws:executeAwsApi` :Retorna a lista de controle de acesso (ACL) do bucket do S3.
- `aws:executeScript`- Cria um grupo de CloudWatch registros e um fluxo de registros se você especificar um valor para o `CloudWatchLogGroupName` parâmetro.
- `aws:executeScript` :Com base nos valores especificados nos parâmetros de entrada do runbook, avalia se alguma das definições do bucket do S3 coletadas durante a automação está impedindo que os objetos sejam acessados pelo público. Esse script executa as seguintes funções:
  - Avalia as definições de bloqueio de acesso público
  - Retorna objetos do bucket do S3 com base nos valores especificados nos parâmetros `MaxObjects`, `S3PrefixName` e `StartAfter`.
  - Retorna a política do bucket do S3 para simular uma política do IAM personalizada para os objetos retornados do bucket do S3.
  - Executa uma solicitação HTTP parcial para os objetos retornados se o parâmetro `HttpGet` estiver definido como `true`. Somente o primeiro byte do objeto é retornado usando o cabeçalho HTTP Range.
  - Verifica o nome da chave do objeto retornado para confirmar se ele termina com um ou dois pontos. Os nomes de chaves de objetos que terminam em pontos não podem ser baixados do console do Amazon S3.
  - Verifica se o proprietário do objeto retornado corresponde ao proprietário do bucket do S3.
  - Verifica se a ACL do objeto concede permissões de `READ` ou `FULL_CONTROL` a usuários anônimos.
  - Retorna tags associadas ao objeto.
  - Usa a política do IAM simulada para confirmar se há uma negação explícita desse objeto na política de bucket do S3 para a ação `GetObject` da API.
  - Retorna os metadados do objeto para confirmar que a classe de armazenamento é compatível.

- Verifica as configurações de criptografia do lado do servidor do objeto para confirmar se o objeto está criptografado usando uma chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente.

Saídas

AnalyzeObjects.balde

AnalyzeObjects.objeto

AWSSupport-EmptyS3Bucket

Descrição

O runbook de `AWSSupport-EmptyS3Bucket` automação esvazia um bucket existente do Amazon Simple Storage Service (Amazon S3) usando uma regra de configuração de expiração do ciclo de vida.

> **Important**
>
> - Os buckets do Amazon S3 com autenticação multifator (MFA) ativada não são suportados.
> - As regras de ciclo de vida modificadas por esse runbook excluem permanentemente todos os objetos e suas versões no bucket do Amazon S3 especificado. Você não pode recuperar objetos excluídos permanentemente. Para obter mais informações, consulte Expiring Objects.

Como funciona?

O runbook `AWSSupport-EmptyS3Bucket` executa as seguintes etapas de alto nível:

- Suspende o controle de versão do bucket, se ativado.
- Atualiza a política do bucket para negar qualquer chamada de `s3:PutObject` API (para evitar novos uploads enquanto ela está sendo esvaziada).
- Atualiza as regras do ciclo de vida para excluir todos os objetos de acordo com os dias de expiração especificados nos parâmetros de entrada.

> **Note**
>
> - As versões de objetos protegidas com o Amazon S3 Object Lock não são excluídas nem substituídas pelas configurações do ciclo de vida.
> - O processo de exclusão é assíncrono e pode levar algum tempo para ser concluído após o término da execução do runbook.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

/

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

O AutomationAssumeRole parâmetro requer as seguintes ações para usar o runbook com êxito:

- sms: DescribeAutomationExecutions
- sms: GetAutomationExecution
- s3: GetBucketVersioning
- s3: PutBucketVersioning
- s3: GetBucketPolicy
- s3: GetBucketLifecycleConfiguration
- s3: GetLifecycleConfiguration
- s3: PutBucketPolicy
- s3: PutBucketLifecycleConfiguration
- s3: PutLifecycleConfiguration

- s3: DeleteBucketPolicy
- s3: DeleteBucketLifecycle

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-EmptyS3Bucketem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - S3: BucketName

     O nome do bucket do Amazon S3 que você deseja esvaziar.
   - SNSTopicBraço:

     Forneça o ARN do tópico do Amazon SNS para notificação de aprovação. Esse tópico do Amazon SNS é usado para enviar notificações de aprovação quando necessário durante a execução da automação.
   - Aprovação:

     Forneça uma lista de diretores autenticados pela AWS que possam aprovar ou rejeitar a ação. O número máximo de aprovadores é10. Você pode especificar os principais usando qualquer um desses formatos, um nome de usuário AWS Identity and Access Management (IAM), um ARN de usuário do IAM, um ARN de função do IAM ou um ARN de usuário da função assumida pelo IAM.
   - MinimumRequiredApprovals (Opcional):

     O número mínimo de aprovações necessárias para retomar a automação. Se você não especificar um valor, o sistema usará como padrão. 1 O valor desse parâmetro deve ser um número positivo. O valor desse parâmetro não pode exceder o número de aprovadores definido pelo parâmetro ApproveRiam.

- NoncurrentVersionExpirationDays (Opcional):

  Especifique o número de dias em que as versões não atuais do objeto expiram. Após a expiração, o Amazon S3 exclui permanentemente as versões de objetos não atuais.

  - Padrão: 1
  - Valor máximo: 365

- ExpirationDays (Opcional):

  Especifique a expiração do ciclo de vida do objeto no formato dias.

  - Padrão: 1
  - Valor máximo: 365

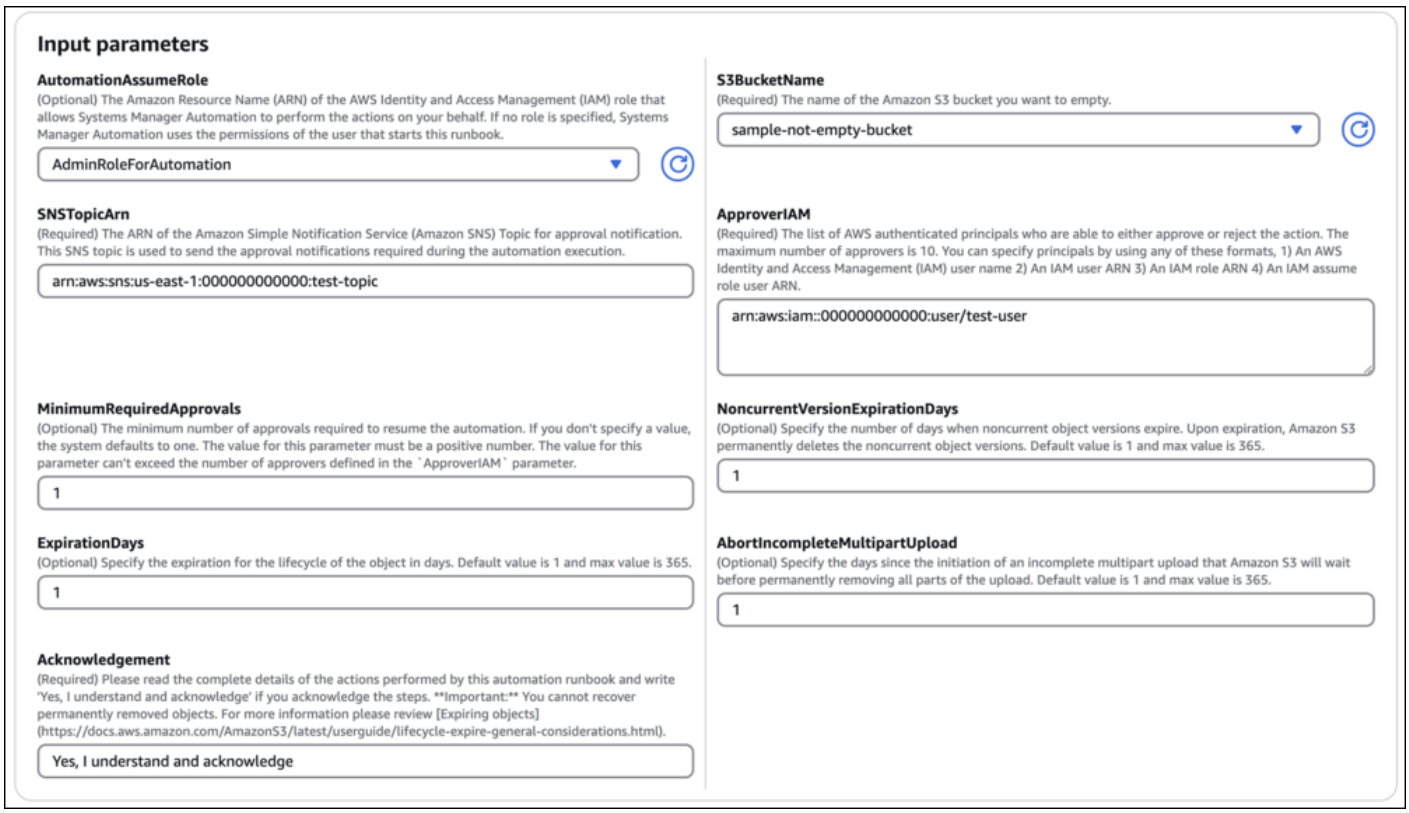
- AbortIncompleteMultipartUpload (Opcional):

  Especifique os dias, desde o início de um upload incompleto de várias partes, que o Amazon S3 aguardará antes de remover permanentemente todas as partes do upload.

  - Padrão: 1
  - Valor máximo: 365

- Reconhecimento:

  Leia os detalhes completos das ações realizadas por este runbook de automação e forneça consentimento `Yes, I understand and acknowledge` se você reconhecer as etapas.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - **`checkConcurrency`**:

     Garante que haja apenas uma execução desse runbook direcionada ao bucket especificado do Amazon S3. Se o runbook encontrar outra execução em andamento com o mesmo nome de bucket, ele retornará um erro e terminará.
   - **`getBucketVersioningConfiguration`**:

     Busca o status de versionamento do bucket Amazon S3 especificado.
   - **`branchOnStoppingIfMFADeleteEnabled`**(condicional):

     Interrompe a automação se a Autenticação Multifator (MFA) estiver habilitada no bucket do Amazon S3 especificado.
   - **`approvalToMakeChangesToTheProvidedS3Bucket`**:

Aguarda a aprovação dos diretores designados para desativar o controle de versão do bucket e atualizar a política do bucket e a configuração das regras de ciclo de vida do bucket Amazon S3 especificado.

- **`branchOnBucketVersioningStatus`**(condicional):

  Se o controle de versão estiver ativado no bucket do Amazon S3 especificado, desative-o, caso contrário, continue atualizando a política do bucket e a configuração do ciclo de vida.

- **`suspendBucketVersioning`**:

  Suspende o estado de versionamento do bucket Amazon S3 especificado.

- **`updateBucketPolicyAndLifeCycleConfiguration`**:

  Adiciona ou atualiza a política do bucket para negar todas as `s3:PutObject` solicitações e atualiza a configuração do ciclo de vida para expirar objetos com base nos parâmetros de entrada fornecidos pelo usuário.

- **`branchOnFailingIfBucketPropertiesNotUpdated`**(condicional):

  Verifica o status da `updateBucketPolicyAndLifeCycleConfiguration` etapa e tenta reverter o estado de versionamento original do bucket se alterado pela automação.

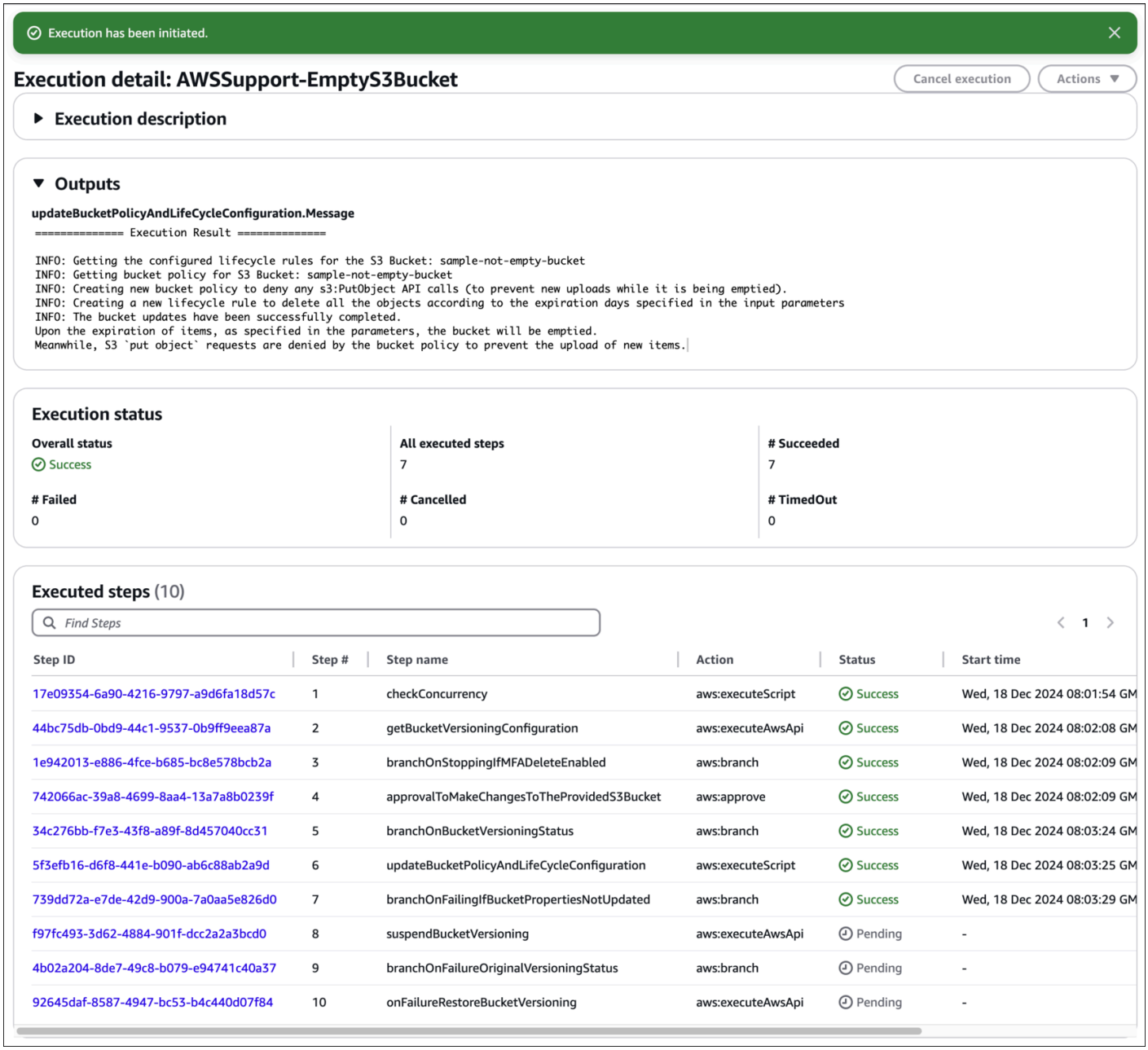
- **`branchOnFailureOriginalVersioningStatus`**(condicional):

  Em caso de falha, ramifica para determinar o status original do controle de versão. Se foi ativado e suspenso por essa automação, tenta habilitá-la novamente.

- **`onFailureRestoreBucketVersioning`**

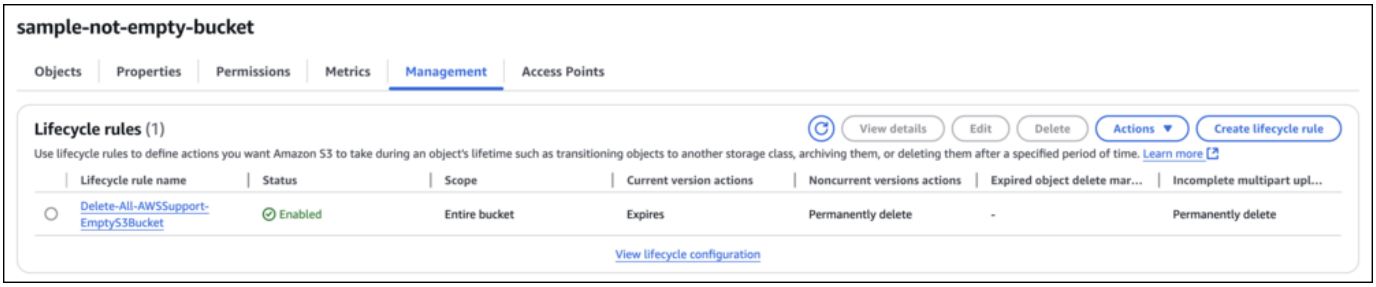
  Restaura o estado de versionamento ativado do bucket Amazon S3 especificado.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:



- Execução bem-sucedida

  Esse fluxo de trabalho atualiza a regra de ciclo de vida do bucket. Os objetos serão excluídos de acordo com a política de `Delete-All-AWSSupport-EmptyS3-Bucket` ciclo de vida.



- Falha na execução

  A exclusão parcial não será executada. Se a execução falhar, o ciclo de vida e outras configurações do bucket serão revertidas.

Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Fluxos de trabalho de automação de suporte

Para obter mais informações sobre o gerenciamento de buckets e objetos do Amazon S3, consulte Esvaziar um bucket.

AWSSupport-TroubleshootS3EventNotifications

Descrição

O runbook de `AWSSupport-TroubleshootS3EventNotifications` AWS Systems Manager automação ajuda a solucionar problemas de notificações de eventos de bucket do Amazon Simple Storage Service (Amazon S3) configuradas com AWS Lambda Functions, Amazon Simple Notification Service (Amazon SNS) Topics ou Amazon Simple Queue Service (Amazon SQS) Queues. Ele fornece um relatório de configurações dos diferentes recursos configurados com o Amazon S3 Bucket como uma notificação de evento de destino.

Como funciona?

O runbook executa as seguintes etapas:

- Verifica se o Amazon S3 Bucket existe na mesma conta em que `AWSSupport-TroubleshootS3EventNotifications` é executado.
- Busca os recursos de destino (AWS Lambda função, tópico do Amazon SNS ou fila do Amazon SQS) configurados como notificações de eventos para o bucket do Amazon S3 usando a API. GetBucketNotificationConfiguration
- Valida a existência do recurso de destino e, em seguida, analisa a política baseada em recursos dos recursos de destino para determinar se o Amazon S3 tem permissão para publicar no destino.
- Se você criptografou o destino com uma chave AWS Key Management Service (AWS KMS), a política de chaves é verificada para determinar se o acesso ao Amazon S3 é permitido.
- Gera um relatório de todas as verificações de recursos de destino.

> **Important**
>
> - Esse runbook só pode avaliar as configurações de notificação de eventos se o proprietário do bucket do Amazon S3 for o mesmo proprietário em que Conta da AWS o runbook de automação está sendo executado.
> - Além disso, esse runbook não pode avaliar políticas em recursos de destino hospedados em outro Conta da AWS.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- S3 BucketName

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

  Descrição: (Obrigatório) O nome do bucket Amazon S3 configurado com notificação (ões) de eventos.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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`

Exemplo de política do IAM para a função Automation Assume

```
                    {
                        "Version": "2012-10-17",
                        "Statement": [
                            {
                                "Sid": "S3Permission",
                                "Effect": "Allow",
                                "Action": [
                                    "s3:GetBucketLocation",
                                    "s3:ListAllMyBuckets"
                                ],
                                "Resource": "*"
                            },
                            {
                                "Sid": "S3PermissionGetBucketNotification",
                                "Effect": "Allow",
                                "Action": [
                                    "s3:GetBucketNotification"
                                ],
                                "Resource": "arn:aws:s3::::<bucket-name>"
                            },
                            {
                                "Sid": "SQSPermission",
                                "Effect": "Allow",
                                "Action": [
                                    "sqs:GetQueueAttributes",
                                    "sqs:GetQueueUrl"
                                ],
                                "Resource": "arn:aws:sqs:<region>:123456789012:*"
                            },
                            {
                                "Sid": "SNSPermission",
                                "Effect": "Allow",
                                "Action": [
                                    "sns:GetTopicAttributes"
                                ],
                                "Resource": "arn:aws:sns:<region>:123456789012:*"
                            },
                            {
                            "Sid": "KMSPermission",
                                "Effect": "Allow",
                                "Action": [
                                    "kms:GetKeyPolicy",
                                    "kms:DescribeKey",
                                    "kms:ListAliases"
```

```
                                ],
                                "Resource": "arn:aws:kms:<region>:123456789012:key/
<key-id>"
                            },
                            {
                                "Sid": "LambdaPermission",
                                "Effect": "Allow",
                                "Action": [
                                    "lambda:GetPolicy",
                                    "lambda:GetFunction"
                                ],
                                "Resource":
 "arn:aws:lambda:<region>:123456789012:function:*"
                            },
                            {
                                "Sid": "IAMPermission",
                                "Effect": "Allow",
                                "Action": [
                                    "iam:GetContextKeysForCustomPolicy",
                                    "iam:SimulateCustomPolicy",
                                    "iam:ListRoles"
                                ],
                                "Resource": "*"
                            },
                            {
                                "Sid": "SSMPermission",
                                "Effect": "Allow",
                                "Action": [
                                    "ssm:DescribeAutomationStepExecutions"
                                ],
                                "Resource": "*"
                            }
                        ]
                    }
```

Instruções

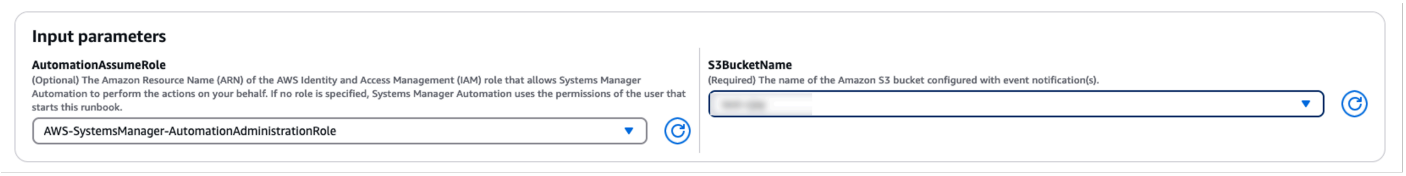
Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-TroubleshootS3EventNotificationsem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).

3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - S3 BucketName (obrigatório):

     O nome do bucket do Amazon S3 configurado com notificação (ões) de eventos.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - ValidateInputs

     Valida que o bucket Amazon S3 fornecido pertence à mesma conta em que a automação é executada e busca a região em que o bucket está hospedado.
   - GetBucketNotificationConfiguration

     Chama a `GetBucketNotificationConfiguration` API para revisar as notificações de eventos configuradas com o bucket do Amazon S3 e formata a saída.
   - BranchOnSQSResourcePolítica

     Define se há recursos do Amazon SQS nas notificações de eventos.
   - Validar política SQSResource

     Valida a política de recursos nos atributos do Amazon SQS Queue que `sqs:SendMessage` tem permissão para o Amazon S3. Se o recurso Amazon SQS estiver criptografado, verifica se a criptografia não está usando a AWS KMS chave padrão, ou seja, `aws/sqs` e verifica se a política de AWS KMS chaves tem permissões para o Amazon S3.
   - BranchOnSNSResourcePolítica

     Define se há recursos do Amazon SNS nas notificações de eventos.

- Validar política SNSResource

  Valida a política de recursos no Amazon SNS. Os atributos de tópico `sns:Publish` têm permissão para o Amazon S3. Se o recurso do Amazon SNS estiver criptografado, verifica se a criptografia não está usando a AWS KMS chave padrão, ou seja, `aws/sns` e verifica se a política de AWS KMS chaves tem permissões para o Amazon S3.

- BranchOnLambdaFunctionResourcePolicy

  Explica se há AWS Lambda funções nas notificações de eventos.

- ValidateLambdaFunctionResourcePolicy

  Valida a política de recursos se AWS Lambda a função tem `lambda:InvokeFunction` permissão para o Amazon S3.

- GenerateReport

  Retorna detalhes das etapas, saídas e recomendações do runbook para resolver qualquer problema com as notificações de eventos configuradas com o bucket do Amazon S3.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:

   - Notificações de eventos do Amazon SQS

     Se houver notificações de destino do Amazon SQS configuradas com o bucket do Amazon S3, uma lista das filas do Amazon SQS será exibida junto com os resultados das verificações. O relatório inclui verificação de recursos do Amazon SQS, verificação da política de acesso do Amazon SQS, verificação da chave AWS KMS , verificação do status da chave AWS KMS e verificação da política da chave. AWS KMS

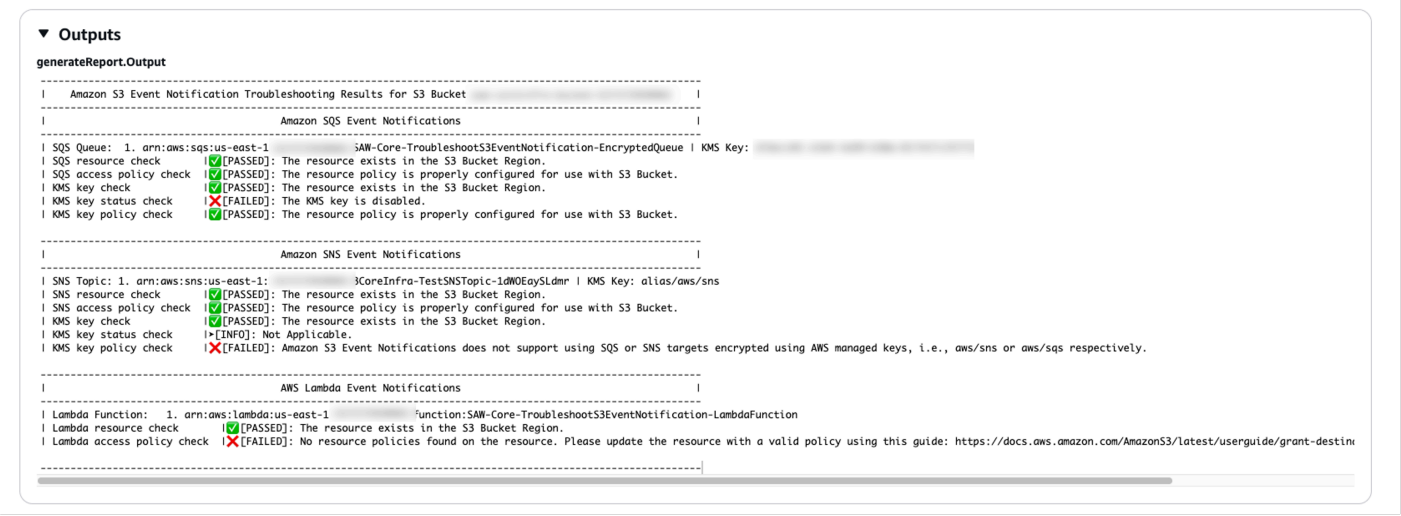
   - Notificações de eventos do Amazon SNS

     Se houver notificações de destino do Amazon SNS configuradas com o bucket do Amazon S3, uma lista dos tópicos do Amazon SNS será exibida junto com os resultados das verificações. O relatório inclui verificação de recursos do Amazon SNS, verificação da política de acesso do Amazon SNS, verificação da chave AWS KMS , verificação do status da chave AWS KMS e verificação da política da chave. AWS KMS

   - AWS Lambda Notificações de eventos

     Se houver notificações de AWS Lambda destino configuradas com o bucket do Amazon S3, uma lista das funções do Lambda será exibida junto com os resultados das verificações. O

relatório inclui a verificação de recursos do Lambda e a verificação da política de acesso do Lambda.



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSSupport-ContainS3Resource

Descrição

O `AWSSupport-ContainS3Resource` runbook fornece uma solução automatizada para o procedimento descrito no artigo Support Automation Workflow (SAW) Runbook: Contain a compromised Amazon AWS S3 Bucket

> **Important**
>
> - Esse runbook executa várias operações que exigem privilégios elevados, como modificar políticas de bucket, tags e configurações de acesso público do Amazon S3. Essas ações podem potencialmente levar à escalação de privilégios ou impactar outras cargas de trabalho que dependem do bucket do Amazon S3 de destino. Você deve analisar as

permissões concedidas à função especificada pelo `AutomationAssumeRole` parâmetro e garantir que elas sejam apropriadas para o caso de uso pretendido. Você pode consultar a AWS documentação a seguir para obter mais informações sobre as permissões do IAM: `Identity and Access Management (IAM) PermissionsAWS AWS Systems Manager Automation Permissions`.

- Esse runbook executa ações mutativas que podem causar indisponibilidade ou interrupção em suas cargas de trabalho. Especificamente, a `Contain` ação bloqueia todo o acesso ao bucket especificado do Amazon S3, exceto as funções especificadas no `SecureRoles` parâmetro. Isso pode afetar qualquer aplicativo ou serviço que dependa do bucket Amazon S3 de destino.
- Durante a `Contain` ação, esse runbook pode criar um bucket adicional do Amazon S3 (especificado pelo `BackupS3BucketName` parâmetro) para armazenar o backup da configuração do bucket original, caso ela ainda não exista.
- Se o `Action` parâmetro estiver definido como`Restore`, esse runbook tentará restaurar a configuração do bucket do Amazon S3 para seu estado original com base no backup armazenado no `BackupS3BucketName` bucket. No entanto, existe o risco de que o processo de restauração falhe, deixando o bucket do Amazon S3 em um estado inconsistente. O runbook fornece instruções para restauração manual em caso de falhas desse tipo, mas você deve estar preparado para lidar com possíveis problemas durante o processo de restauração.

É recomendável revisar o runbook minuciosamente, entender seus possíveis impactos e testá-lo em um ambiente que não seja de produção antes de executá-lo em seu ambiente de produção.

Como funciona?

Esse runbook opera de forma diferente com base no tipo de recurso e na ação:

- Para Amazon S3 General Purpose Bucket`Containment`: a automação bloqueia o acesso público ao bucket, desativa a configuração da ACL, impõe a propriedade do Bucket Owner Object e impõe uma política restritiva de bucket negando todas as ações do Amazon S3 ao bucket, exceto para permitir funções do IAM listadas.
- Para o objeto de uso geral do Amazon S3`Containment`: a automação bloqueia o acesso público ao bucket, desativa a configuração da ACL, impõe a propriedade do objeto do proprietário do

bucket e impõe uma política restritiva de bucket negando todas as ações do Amazon S3 no objeto, exceto as funções do IAM listadas como permitidas.

- Para o Amazon S3 Directory Bucket`Containment`: a automação coloca uma política restritiva de bucket negando todas as ações do Amazon S3 ao bucket, exceto as funções do IAM listadas como permitidas.
- Para o Amazon S3 General Purpose Bucket`Restore`: a automação restaura a configuração de acesso público do bloco, a configuração da ACL do bucket, a propriedade do objeto do proprietário do bucket e a política do bucket para a configuração inicial antes da contenção.
- Para o objeto de uso geral do Amazon S3`Restore`: a automação restaura a configuração de acesso público do bloco, a configuração da ACL do bucket, a configuração da ACL do objeto, a propriedade do objeto do proprietário do bucket e a política do bucket para a configuração inicial antes da contenção.
- Para o Amazon S3 Directory Bucket`Restore`: a automação restaura a política do bucket para a configuração inicial antes da contenção.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataforma

/

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- s3: CreateBucket
- s3: DeleteBucketPolicy
- s3: DeleteObjectTagging
- s3: GetAccountPublicAccessBlock
- s3: GetBucketAcl

- s3: GetBucketLocation
- s3: GetBucketOwnershipControls
- s3: GetBucketPolicy
- s3: GetBucketPolicyStatus
- s3: GetBucketTagging
- s3: GetEncryptionConfiguration
- s3: GetObject
- s3: GetObjectAcl
- s3: GetObjectTagging
- s3: GetReplicationConfiguration
- s3: ListBucket
- s3: PutAccountPublicAccessBlock
- s3: ACL PutBucket
- s3: PutBucketOwnershipControls
- s3: PutBucketPolicy
- s3: PutBucketPublicAccessBlock
- s3: PutBucketTagging
- s3: PutBucketVersioning
- s3: PutObject
- s3: PutObjectAcl
- s3 express diz: CreateSession
- s3 express diz: DeleteBucketPolicy
- s3 express diz: GetBucketPolicy
- s3 express diz: PutBucketPolicy
- sms: DescribeAutomationExecutions

Aqui está um exemplo de uma política do IAM que concede as permissões necessárias para`AutomationAssumeRole`:

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

```
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucketPolicy",
                "s3:DeleteObjectTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketOwnershipControls",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:GetReplicationConfiguration",
                "s3:ListBucket",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketACL",
                "s3:PutBucketOwnershipControls",
                "s3:PutBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutBucketTagging",
                "s3:PutBucketVersioning",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3ExpressPermissions",
            "Effect": "Allow",
            "Action": [
                "s3express:CreateSession",
                "s3express:DeleteBucketPolicy",
                "s3express:GetBucketPolicy",
                "s3express:PutBucketPolicy"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "SSMPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAutomationExecutions"
            ],
            "Resource": "*"
        }
    ]
}
```

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-ContainS3Resourceem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - BucketName (Obrigatório):
     - Descrição: (Obrigatório) O nome do bucket do Amazon S3.
     - Tipo: `AWS::S3::Bucket::Name`
   - Ação (obrigatória):
     - Descrição: (Obrigatório) Selecione `Contain` para isolar o recurso Amazon S3 `Restore` ou tentar restaurar a configuração do recurso ao seu estado original a partir de um backup anterior.
     - Tipo: String
     - Valores permitidos: `Contain|Restore`
   - DryRun (Opcional):
     - Descrição: (Opcional) Quando definida como verdadeira, a automação não fará nenhuma alteração no recurso de destino do Amazon S3; em vez disso, ela exibirá o que teria tentado alterar. Valor padrão: true.
     - Tipo: booliano
     - Valores permitidos: `true|false`
   - BucketKeyName (Opcional):
     - Descrição: (Opcional) A chave do objeto Amazon S3 que você deseja conter ou restaurar. Usado durante a contenção em nível de objeto.
     - Tipo: String

  - Allowed-pattern: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$`
- BucketRestrictAccess (Condicional):
  - Descrição: (Condicional) O ARN dos usuários ou funções do IAM que terão acesso ao recurso de destino do Amazon S3 após a execução das ações de contenção. Esse parâmetro é necessário quando `Action` definido como`Contain`.
  - Tipo: StringList
  - Allowed-pattern: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
- TagIdentifier (Opcional):
  - Descrição: (Opcional) Uma tag no formato Key=BatchId, Value=78925 que será adicionada aos recursos criados ou modificados por esse runbook durante o fluxo de trabalho de contenção.
  - Tipo: String
  - Allowed-pattern: `^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\/@a-zA-Z0-9]{0,128}$`
- Backups 3 BucketName (condicionais):
  - Descrição: (Condicional) O bucket do Amazon S3 para fazer backup da configuração do recurso de destino quando definido como ou `Contain` para restaurar `Action` a configuração a partir `Action` do momento em que está definido. `Restore`
  - Tipo: `AWS::S3::Bucket::Name`
- Backups 3 KeyName (condicionais):
  - Descrição: (Condicional) Se `Action` estiver definido como`Restore`, isso especifica a chave do Amazon S3 que a automação usará para tentar restaurar a configuração do recurso de destino.
  - Tipo: String
  - Allowed-pattern: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$`
- Backups 3 BucketAccess (condicionais):
  - Descrição: (Condicional) O ARN dos usuários ou funções do IAM que terão acesso ao bucket de backup do Amazon S3 após a execução das ações de contenção. Esse parâmetro é necessário quando `Action` é`Contain`.
  - Tipo: StringList

    - Allowed-pattern: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
- AutomationAssumeRole (Opcional):
    - Descrição: (Opcional) O Amazon Resource Name (ARN) da função do IAM que permite que o Systems Manager Automation execute as ações em seu nome.
    - Tipo: `AWS::IAM::Role::Arn`

4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
    - validateRequiredInputs

      Valida os parâmetros de entrada de automação necessários com base na Ação especificada.
    - assertBucketExists

      Verifica se o bucket de destino do Amazon S3 existe e está acessível.
    - backupBucketPreCheques

      Verifica se o bucket de backup do Amazon S3 potencialmente concede acesso público de leitura ou gravação a seus objetos.
    - backupTargetBucketMetadados

      Descreve a configuração atual do bucket do Amazon S3 de destino e carrega o backup para o bucket de backup especificado do Amazon S3.
    - Contenha um balde

      Executa operações em nível de bucket para conter o bucket de destino do Amazon S3.
    - BranchOnActionAndMode

      Ramifica a automação com base nos parâmetros de entrada Action DryRun e.
    - RestoreInstanceConfiguration

      Restaura a configuração do bucket do Amazon S3 a partir do backup.
    - containFinalOutput

      Consolida a atividade de contenção em formato legível.
    - ReportContain

Produz detalhes de funcionamento a seco para as ações de contenção.

- ReportRestore

  Produz detalhes de funcionamento a seco para as ações de restauração.

- ReportRestoreFailure

  Fornece instruções para restaurar a configuração original do bucket do Amazon S3 durante um cenário de falha no fluxo de trabalho de restauração.

- ReportContainmentFailure

  Fornece instruções para restaurar a configuração original do bucket Amazon S3 durante um cenário de falha no fluxo de trabalho de contenção.

- FinalOutput

  Exibe os detalhes das ações de contenção.

7. Após a conclusão da execução, revise a seção Saídas para obter os resultados detalhados da execução:

   - ContainFinalOutput.Saída

     Exibe os detalhes das ações de contenção realizadas por esse runbook quando `DryRun` está definido como False.

   - RestoreFinalOutput.Saída

     Exibe os detalhes das ações de restauração executadas por esse runbook quando `DryRun` está definido como False.

   - Contém 3. Saída ResourceDryRun

     Exibe os detalhes das ações de contenção realizadas por esse runbook quando `DryRun` está definido como True.

   - Restore S3. Saída ResourceDryRun

     Exibe os detalhes das ações de restauração executadas por esse runbook quando `DryRun` está definido como True.

   - ReportContainmentFailure.Saída

     Fornece instruções para restaurar a configuração original do recurso Amazon S3 de destino durante um cenário de falha no fluxo de trabalho de contenção.

- ReportRestoreFailure.Saída

  Fornece instruções para restaurar a configuração original do recurso Amazon S3 de destino durante um cenário de falha no fluxo de trabalho de restauração.

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Fluxos de trabalho de automação de suporte

Amazon SES

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Simple Email Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSSupport-AnalyzeSESMessageSendingStatus

`AWSSupport-AnalyzeSESMessageSendingStatus`

Descrição

O runbook de `AWSSupport-AnalyzeSESMessageSendingStatus` automação resume o status de entrega de e-mail de mensagens de e-mail não entregues e fornece conselhos para resolver o motivo pelo qual elas não foram entregues. O runbook recupera eventos de envio de e-mail do Amazon Simple Email Service (Amazon SES) armazenados em um grupo Amazon CloudWatch Logs publicado pelo Amazon SES. Para obter detalhes sobre a publicação de eventos do Amazon SES, consulte Monitoramento usando a publicação de eventos do Amazon Simple Email Service. O runbook também fornece um resumo e o cronograma das entregas de e-mail, bem como recomendações que podem afetar potencialmente as mensagens de e-mail não entregues. Você

pode encontrar essas mensagens na seção de saída de cada execução. Observe que esse runbook só pode solucionar os eventos após a implantação do repositório de eventos.

Como funciona?

O runbook executa as seguintes etapas:

- Verifica as execuções simultâneas de automação para o mesmo grupo de CloudWatch registros.
- Analise os eventos do Amazon SES correspondentes à mensagem IDs fornecida pelo parâmetro de automação.
- Resumos de entrega de saída para a seção de saída da execução da automação.

> **Important**
>
> - Antes de executar esse runbook, você precisa armazenar eventos publicados do Amazon SES em um grupo de CloudWatch logs de registros especificado pelo parâmetro de automação. Esse runbook analisa somente os eventos do Amazon SES armazenados no grupo de registros.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `logs:StartQuery`
- `logs:GetQueryResults`
- `ses:GetIdentityMailFromDomainAttributes`
- `ses:GetSendQuota`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Instruções

Siga estas etapas para configurar a automação:

1. Navegue até AWSSupport-AnalyzeSESMessageSendingStatusem Systems Manager em Documentos.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhuma função for especificada, o Systems Manager Automation usa as permissões do usuário que inicia esse runbook.
   - MessageIds (Obrigatório)

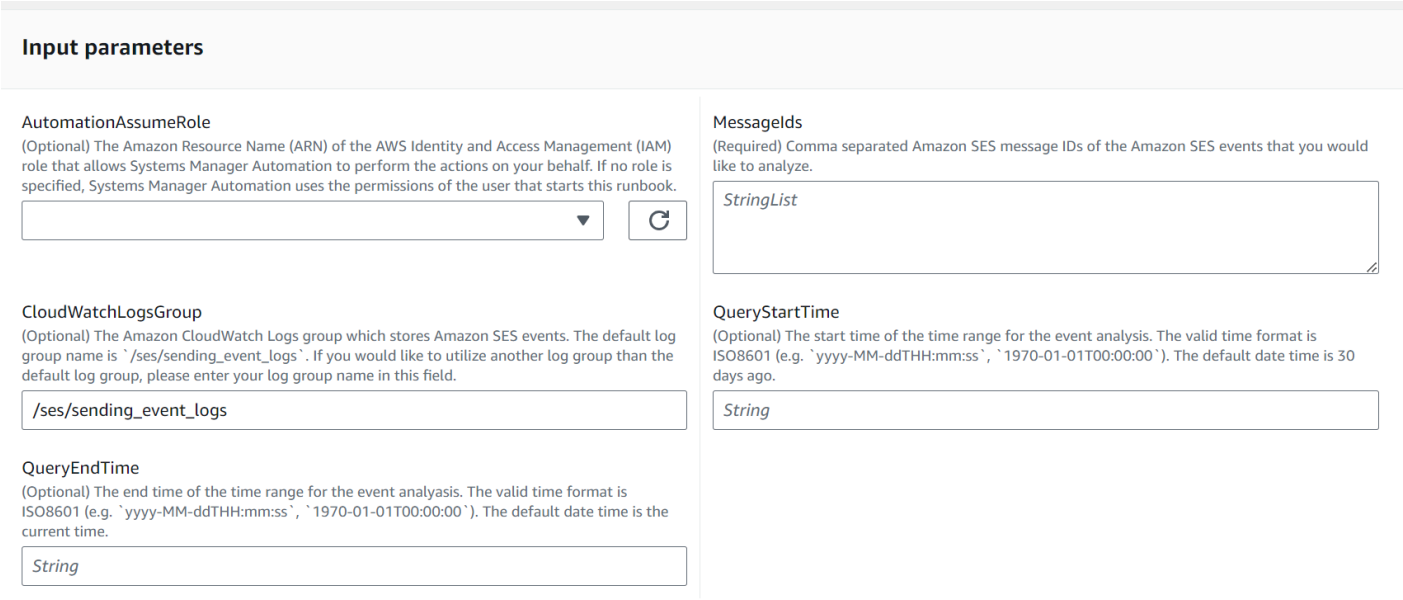
     Mensagem separada por vírgula do Amazon Simple Email Service IDs dos eventos do Amazon Simple Email Service que você gostaria de analisar.
   - CloudWatchLogsGroup (Opcional)

     O grupo Amazon CloudWatch Logs que armazena eventos do Amazon Simple Email Service. O nome padrão do grupo de registros é `/ses/sending_event_logs`. Se você quiser utilizar outro grupo de registros que não seja o grupo de registros padrão, insira o nome do grupo de registros nesse campo. “,
   - QueryStartTime (Opcional)

     A hora de início do intervalo de tempo para a análise do evento. O formato de hora válido é ISO86 01 (por exemplo, `YYYY-MM-DDTHH:mm:ss`, `1970-01-01T 00:00:00 `). A data e hora padrão é de 30 dias atrás.

- QueryEndTime (Opcional)

  A hora final do intervalo de tempo para a análise do evento. O formato de hora válido é ISO8601 (por exemplo, `YYYY-MM-DDTHH:mm:ss`, `1970-01-01T 00:00:00 `). A data e hora padrão é a hora atual.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - **`CheckConcurrency:`**

     Garante que haja apenas uma execução desse runbook direcionada ao grupo Amazon CloudWatch Logs. Se o runbook encontrar outra execução direcionada ao mesmo grupo de registros, ele retornará um erro e terminará.
   - **`AnalyzeSesEvents:`**

     Analise os eventos do Amazon Simple Email Service armazenados no grupo Amazon CloudWatch Logs especificado pelo parâmetro de automação.
   - **`OutputFailureReason:`**

     Envie mensagens de falha da etapa de execução quando a `AnalyzeSESMessageSendingStatus` etapa falhou.
7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:
   - Resultado da análise de uma mensagem de e-mail não entregue devido a uma rejeição

Saída de uma execução de automação para uma mensagem de e-mail que não chegou à caixa de correio de destino devido a uma rejeição.

Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

SageMaker IA

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon SageMaker AI. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-DisableSageMakerNotebookRootAccess

`AWS-DisableSageMakerNotebookRootAccess`

Descrição

O `AWS-DisableSageMakerNotebookRootAccess` runbook desativa o acesso root em uma instância de notebook Amazon SageMaker AI. Durante a automação, a instância do notebook é interrompida para fazer as alterações necessárias. SageMaker As instâncias do notebook AI Studio não são suportadas.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- NotebookInstanceName

  Tipo: String

  Descrição: (Obrigatório) O nome da instância do notebook SageMaker AI na qual desabilitar o acesso root.

- StartInstanceAfterUpdate

  Tipo: booleano

  Padrão: verdadeiro

Descrição: (Opcional) Determina se a instância do notebook é iniciada após a desativação do acesso root. A configuração padrão para esse parâmetro é`true`. Se definido como`true`, a instância será iniciada após a desativação do acesso root. Se definido como`false`, a instância permanece no `stopped` estado após a desativação do acesso root.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

Etapas do documento

- CheckNotebookInstanceStatus (aws:executeAwsApi): Verifica o status atual da instância do notebook.
- StopOrUpdateNotebookInstance (aws:branch): ramificações com base no status da instância do notebook.
- StopNotebookInstance (aws:executeAwsApi): inicia a instância se o status for`stopped`.
- WaitForInstanceToStop (aws: waitForAwsResourceProperty): Verifica se a instância é`stopped`.
- UpdateNotebookInstance (aws:executeAwsApi): desativa o acesso root na instância do notebook.
- WaitForNotebookUpdate (aws: waitForAwsResourceProperty): Verifica se o acesso root foi desativado e se a instância tem um `stopped` status.
- ChooseInstanceStart (aws:branch): ramificação com base na necessidade de iniciar a instância.
- StartNotebookInstance (aws:executeAwsApi): inicia a instância do notebook.
- VerifyNotebookInstanceStatus (aws: waitForAwsResourceProperty): Verifica se a instância está `available` antes de desativar o acesso root.
- VerifyNotebookInstanceRootAccess (aws: assertAwsResource Propriedade): Verifica se a configuração de acesso raiz da instância do notebook foi desativada com sucesso.

Secrets Manager

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Secrets Manager Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-DeleteSecret
- AWSConfigRemediation-RotateSecret

`AWSConfigRemediation-DeleteSecret`

Descrição

O `AWSConfigRemediation-DeleteSecret` runbook exclui um segredo e todas as versões armazenadas nele. AWS Secrets Manager Opcionalmente, você pode especificar a janela de recuperação durante a qual o segredo pode ser restaurado. Se não for especificado um valor para o parâmetro `RecoveryWindowInDays`, o padrão da operação será 30 dias.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- RecoveryWindowInDays

  Tipo: Inteiro

  Valores válidos: 7 a 30

  Padrão: 30

  Descrição: (opcional) O número de dias em que você pode restaurar o segredo.

- SecretId

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do segredo que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager:DeleteSecret`
- `secretsmanager:DescribeSecret`

Etapas do documento

- `aws:executeAwsApi` :Exclui o segredo especificado no parâmetro `SecretId`.
- `aws:executeScript` :Verifica se o segredo foi agendado para exclusão.

AWSConfigRemediation-RotateSecret

Descrição

O `AWSConfigRemediation-RotateSecret` runbook gira um segredo armazenado em. AWS Secrets Manager

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- RotationInterval

  Tipo: Intervalo

  Valores válidos: 1 a 365

  Descrição: (obrigatório) O número de dias entre as alternâncias do segredo.
- RotationLambdaArn

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) da função AWS Lambda que pode alternar o segredo.
- SecretId

  Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do segredo que deseja alternar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

Etapas do documento

- `aws:executeAwsApi` :Alterna o segredo especificado no parâmetro `SecretId`.
- `aws:executeScript` :Verifica se a rotação foi habilitada no segredo.

Security Hub

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Security Hub Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-EnableSecurityHub

`AWSConfigRemediation-EnableSecurityHub`

Descrição

O `AWSConfigRemediation-EnableSecurityHub` runbook habilita AWS Security Hub (Security Hub) para Conta da AWS e Região da AWS onde você executa a automação. Para obter informações sobre o Security Hub, consulte O que é AWS Security Hub? no Guia do AWS Security Hub usuário.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- EnableDefaultStandards

  Tipo: booleano

  Padrão: True

  Descrição: (obrigatório) Se definido como `true`, os padrões de segurança padrão designados pelo Security Hub serão habilitados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

Etapas do documento

- `aws:executeAwsApi` :Habilita o Security Hub na região e na conta atual.
- `aws:executeAwsApi` :Verifica se o Security Hub foi habilitado.

AWS Shield

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS Shield Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSPremiumSupport-DDoSResiliencyAssessment

`AWSPremiumSupport-DDoSResiliencyAssessment`

Descrição

O `AWSPremiumSupport-DDoSResiliencyAssessment` runbook de AWS Systems Manager automação ajuda você a verificar DDo as vulnerabilidades do S e a configuração dos recursos de acordo com a AWS Shield Advanced proteção de sua. Conta da AWS Ele fornece um relatório de configurações para recursos vulneráveis a ataques distribuídos de negação de serviço (DDoS). Ele é usado para coletar, analisar e avaliar os seguintes recursos: Amazon Route 53, Amazon Load Balancers, Amazon CloudFront distributions AWS Global Accelerator e AWS Elastic IPs para suas configurações de acordo com as melhores práticas recomendadas de proteção. AWS Shield Advanced O relatório de configuração final está disponível em um bucket do Amazon S3 de sua escolha como um arquivo HTML.

Como funciona?

Este runbook contém uma série de verificações dos vários tipos de recursos que estão habilitados para acesso público e se eles têm proteções configuradas de acordo com as recomendações do Documento Técnico de Boas Práticas de AWS DDo S. O runbook executa o seguinte:

- Verifica se a assinatura do AWS Shield Advanced está habilitada.
- Se ativada, ele descobre se há algum recurso protegido do Shield Advanced.
- Ele encontra todos os recursos globais e regionais na Conta da AWS e verifica se eles estão protegidos pelo Shield.

- Ela exige os parâmetros do tipo de recurso para avaliação, o nome do bucket do Amazon S3 e o ID do Conta da AWS bucket do Amazon S3 (S3). BucketOwner
- Ele retorna as descobertas como um relatório HTML armazenado no bucket do Amazon S3 fornecido.

O `AssessmentType` dos parâmetros de entrada decide se as verificações em todos os recursos serão realizadas. Por padrão, o runbook verifica todos os tipos de recursos. Somente se o parâmetro `GlobalResources` ou `RegionalResources` for selecionado, o runbook executará verificações somente nos tipos de recursos selecionados.

> **Important**
>
> - O acesso aos runbooks `AWSPremiumSupport-*` requer uma assinatura do Enterprise ou Business Support. Para obter mais informações, consulte Comparar os planos do Suporte.
> - Este runbook requer uma assinatura `ACTIVE` do AWS Shield Advanced.

Execute esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- AssessmentType

  Tipo: String

  Descrição: (Opcional) Determina o tipo de recursos a serem avaliados para a avaliação de resiliência DDo S. Por padrão, o runbook avaliará os recursos globais e regionais. Para recursos regionais, o runbook descreve todos os balanceadores de carga de aplicativo (ALB) e rede (NLB), bem como todo o grupo do Auto Scaling em sua Conta da AWS/região.

  Valores válidos: `['Global Resources', 'Regional Resources', 'Global and Regional Resources']`

  Padrão: recursos globais e regionais

- S3 BucketName

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

  Descrição: (obrigatório) o nome do bucket do Amazon S3 onde o relatório será carregado.

  Allowed-pattern: `^[0-9a-z][a-z0-9\-\.]{3,63}$`

- S3 BucketOwnerAccount

  Tipo: String

  Descrição: (Opcional) O Conta da AWS proprietário do bucket Amazon S3. Especifique esse parâmetro se o bucket do Amazon S3 pertencer a outro Conta da AWS, caso contrário, você pode deixar esse parâmetro vazio.

  Allowed-pattern: `^$|^[0-9]{12,13}$`

- S3 BucketOwnerRoleArn

  Tipo: `AWS::IAM::Role::Arn`

  Descrição: (Opcional) O ARN de uma função do IAM com permissões para descrever o bucket do Amazon S3 Conta da AWS e bloquear a configuração de acesso público se o bucket estiver em outro. Conta da AWS Se esse parâmetro não for especificado, o runbook usa o `AutomationAssumeRole` ou o usuário do IAM que inicia esse runbook (se

AutomationAssumeRole não for especificado). Consulte a seção de permissões necessárias na descrição do runbook.

Allowed-pattern: ^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$

- S3 BucketPrefix

  Tipo: String

  Descrição: (opcional) o prefixo do caminho dentro do Amazon S3 para armazenar os resultados.

  Allowed-pattern: ^[a-zA-Z0-9][-./a-zA-Z0-9]{0,255}$|^$

Permissões obrigatórias do IAM

O parâmetro AutomationAssumeRole requer as seguintes ações para usar o runbook com êxito.

- 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

Exemplo de política do IAM para a função Automation Assume

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Action": [
                    "s3:ListBucket",
                    "s3:GetBucketAcl",
                    "s3:GetAccountPublicAccessBlock"
                ],
                "Resource": "*",
                "Effect": "Allow"
            },
            {
                "Action": [
                    "s3:ListBucket",
                    "s3:GetBucketAcl",
                    "s3:GetBucketLocation",
                    "s3:GetBucketPublicAccessBlock",
                    "s3:GetBucketPolicyStatus",
```

```
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": "arn:aws:s3:::<bucket-name>",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::<bucket-name>/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "cloudfront:ListDistributions",
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:DescribeNetworkAcls",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "globalaccelerator:ListAccelerators",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "route53:ListHostedZones",
                "route53:GetHealthCheck",
                "shield:ListProtections",
                "shield:GetSubscriptionState",
                "shield:DescribeSubscription",
                "shield:DescribeEmergencyContactSettings",
                "shield:DescribeDRTAccess",
                "waf:GetWebACL",
                "waf:GetRateBasedRule",
                "wafv2:GetWebACL",
                "wafv2:GetWebACLForResource",
                "waf-regional:GetWebACLForResource",
                "waf-regional:GetWebACL"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "iam:PassRole",
```

```
                                "Resource": "arn:aws:iam::123456789012:role/
<AutomationAssumeRole-Name>",
                                "Effect": "Allow"
                            }
                        ]
                    }
```

Instruções

1. Navegue até o AWSPremiumSupport-DDoSResiliencyAssessmentno AWS Systems Manager console.
2. Selecione Executar automação.
3. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole(Opcional):

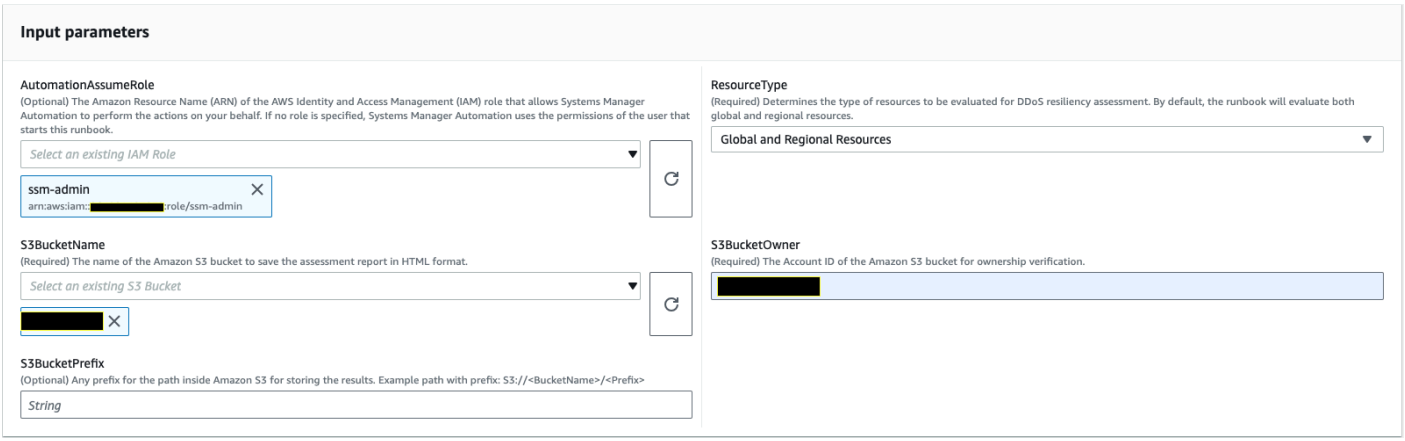
     O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - AssessmentType(Opcional):

     Determina o tipo de recursos a serem DDo avaliados para a avaliação de resiliência S. Por padrão, o runbook avalia os recursos globais e regionais.
   - S3 BucketName (obrigatório):

     O nome do bucket do Amazon S3 para salvar o relatório de avaliação no formato HTML.
   - S3 BucketOwner (opcional):

     O Conta da AWS ID do bucket Amazon S3 para verificação de propriedade. O Conta da AWS ID é obrigatório se o relatório precisar ser publicado em um bucket do Amazon S3 com várias contas e opcional se o bucket do Amazon S3 estiver no mesmo nível do início da Conta da AWS automação.
   - S3 BucketPrefix (opcional):

     Qualquer prefixo do caminho dentro do Amazon S3 para armazenar os resultados.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - CheckShieldAdvancedState:

     Verifica se o Conta da AWS está inscrito AWS Shield Advanced e se o runbook tem acesso ao bucket do Amazon S3.
   - S3: BucketSecurityChecks

     Verifica se o bucket do Amazon S3 especificado no “S3BucketName” permite permissões de acesso anônimo ou público de leitura ou gravação, se o bucket tem a criptografia em repouso ativada e se o Conta da AWS ID fornecido no “S3BucketOwner” é o proprietário do bucket do Amazon S3.
   - BranchOnShieldAdvancedStatus:

     Ramifica etapas do documento com base no status da assinatura do AWS Shield Advanced e/ou no status de propriedade do Amazon S3 Bucket.
   - ShieldAdvancedConfigurationReview:

     Analisa as configurações do Shield Advanced para garantir que os detalhes mínimos necessários estejam presentes. Por exemplo: IAM Access for AWS Shield Response Team Team (SRT), detalhes da lista de contatos e status de engajamento proativo do SRT.
   - ListShieldAdvancedProtections:

     Lista os recursos protegidos pelo Shield e cria um grupo de recursos protegidos para cada serviço.
   - BranchOnResourceTypeAndCount:

Ramifica etapas do documento com base no valor do parâmetro Tipo de recurso e no número de recursos globais protegidos pelo Shield.

- ReviewGlobalResources:

  Analisa os recursos globais protegidos pelo Shield Advanced, como zonas hospedadas, CloudFront distribuições e aceleradores globais do Route 53.

- BranchOnResourceType:

  Ramifica etapas do documento com base nas seleções do tipo de recurso, se global, regional ou ambas.

- ReviewRegionalResources:

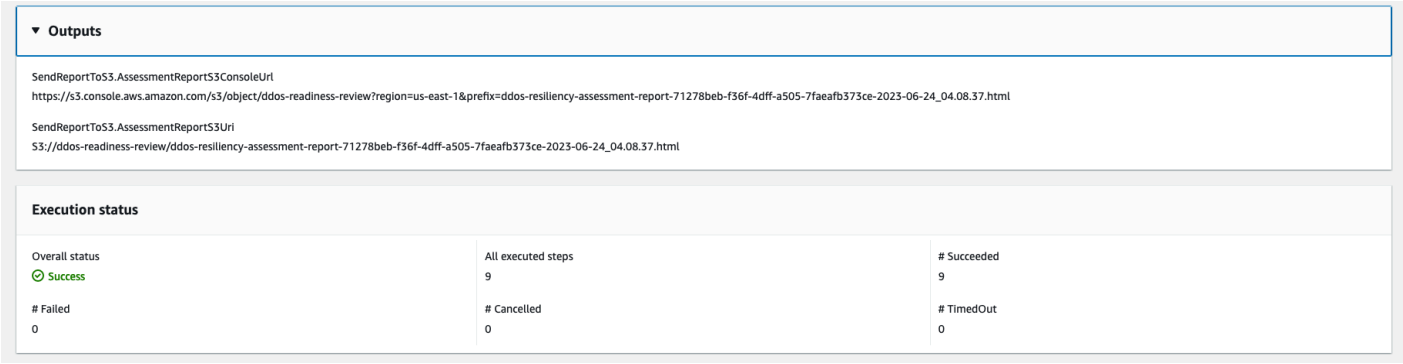
  Analisa os recursos regionais protegidos pelo Shield Advanced, como Application Load Balancers, Network Load Balancers, Classic Load Balancers, Amazon Elastic Compute Cloud (Amazon EC2) Instances (Elastic). IPs

- SendReportToS3:

  Carrega os detalhes do DDo S Assessment Report no bucket do Amazon S3.

7. Depois de concluído, o URI do arquivo HTML do relatório de avaliação é fornecido no bucket do Amazon S3:

   Link do console S3 e URI do Amazon S3 para o relatório sobre a execução bem-sucedida do runbook



Referências

Automação do Systems Manager

- Execute esta automação (console)

- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- AWS Shield Advanced

Amazon SNS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Simple Notification Service. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableSNSTopicDeliveryStatusLogging
- AWSConfigRemediation-EncryptSNSTopic
- AWS-PublishSNSNotification

AWS-EnableSNSTopicDeliveryStatusLogging

Descrição

O `AWS-EnableSNSTopicDeliveryStatusLogging` runbook configura o registro do status de entrega para um `HTTP` endpoint Amazon Data Firehose, Lambda ou Amazon Simple `Platform application` Queue Service (Amazon SQS). Isso permite que o Amazon SNS registre alertas com falha e uma porcentagem amostral de notificações de alerta bem-sucedidas na Amazon. CloudWatch Se o registro do status de entrega já estiver configurado para o tópico, o runbook substituirá a configuração existente pelos novos valores que você especificar para os parâmetros de entrada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- EndpointType

  Tipo: String

  Valores válidos:
  - HTTP
  - Firehose
  - Lambda
  - Aplicação
  - SQS

  Descrição: (Obrigatório) O tipo de endpoint de tópico do Amazon SNS para o qual você deseja registrar as mensagens de notificação de status de entrega.
- TopicArn

  Tipo: String

  Descrição: (Obrigatório) O ARN do tópico do Amazon SNS para o qual você deseja configurar o registro do status de entrega.
- SuccessFeedbackRoleArn

  Tipo: String

Descrição: (Obrigatório) O ARN da função do IAM que o Amazon SNS usa para enviar registros de mensagens de notificação bem-sucedidas. CloudWatch

- SuccessFeedbackSampleRate

  Tipo: String

  Valores válidos: 0-100

  Descrição: (Obrigatório) A porcentagem de mensagens bem-sucedidas a serem amostradas para o tópico especificado do Amazon SNS.

- FailureFeedbackRoleArn

  Tipo: String

  Descrição: (Obrigatório) O ARN da função do IAM que o Amazon SNS usa para enviar registros de mensagens de notificação de falha. CloudWatch

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Etapas do documento

- `aws:executeAwsApi`- Aplica o valor do `SuccessFeedbackRoleArn` parâmetro ao tópico do Amazon SNS.
- `aws:executeAwsApi`- Aplica o valor do `SuccessFeedbackSampleRate` parâmetro ao tópico do Amazon SNS.
- `aws:executeAwsApi`- Aplica o valor do `FailureFeedbackRoleArn` parâmetro ao tópico do Amazon SNS.

- `aws:executeScript`- Confirma que o registro do status de entrega está ativado no tópico Amazon SNS.

Saídas

VerifyDeliveryStatusLoggingEnabled. GetTopicAttributesResponse - Resposta das operações `GetTopicAttributes` da API.

VerifyDeliveryStatusLoggingEnabled. VerifyDeliveryStatusLoggingEnabled - Mensagem indicando a verificação bem-sucedida do registro do status de entrega.

`AWSConfigRemediation-EncryptSNSTopic`

Descrição

O `AWSConfigRemediation-EncryptSNSTopic` runbook permite a criptografia no tópico do Amazon Simple Notification Service (Amazon SNS) que você especifica usando uma chave AWS Key Management Service (AWS KMS) gerenciada pelo cliente. Esse runbook só deve ser usado como uma linha de base para garantir que os tópicos do Amazon SNS sejam criptografados de acordo com as melhores práticas de segurança mínimas recomendadas. Recomendamos criptografar vários tópicos com diferentes chaves gerenciadas pelo cliente.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- KmsKeyArn

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) da chave gerenciada pelo cliente do AWS KMS que deseja usar para criptografar o tópico do Amazon SNS.

- TopicArn

  Tipo: String

  Descrição: (obrigatório) O ARN do tópico do Amazon SNS a ser criptografado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

Etapas do documento

- `aws:executeAwsApi` :Criptografa o tópico do Amazon SNS especificado no parâmetro `TopicArn`.
- `aws:assertAwsResourceProperty` :Confirma que a criptografia está habilitada no tópico do Amazon SNS.

AWS-PublishSNSNotification

Descrição

Publicar uma notificação no Amazon SNS.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Mensagem

  Tipo: String

  Descrição: (obrigatório) A mensagem a ser incluída na notificação do SNS.
- TopicArn

  Tipo: String

  Descrição: (obrigatório) O ARN do tópico do SNS no qual publicar a notificação.

Amazon SQS

AWS Systems Manager A automação fornece runbooks predefinidos para o Amazon Simple Queue Service (Amazon SQS). Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableSQSEncryption

AWS-EnableSQSEncryption

Descrição

O `AWS-EnableSQSEncryption` runbook permite a criptografia em repouso para uma fila do Amazon Simple Queue Service (Amazon SQS). Uma fila do Amazon SQS pode ser criptografada com chaves gerenciadas do Amazon SQS (SSE-SQS) ou com AWS Key Management Service () chaves gerenciadas (SSE-KMS).AWS KMS A chave que você atribui à sua fila deve ter uma política de chaves que inclua permissões para todos os diretores autorizados a usar a fila. Com a criptografia ativada, as `ReceiveMessage` solicitações anônimas `SendMessage` e para a fila criptografada são rejeitadas.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- QueueUrl

  Tipo: string

  Descrição: (Obrigatório) A URL da fila do Amazon SQS na qual você deseja habilitar a criptografia.

- KmsKeyId

  Tipo: string

  Descrição: (Opcional) A AWS KMS chave a ser usada para criptografia. Esse valor pode ser um identificador global exclusivo, um ARN para um alias ou uma chave ou um nome de alias prefixado por “alias/”. Você também pode usar a chave AWS gerenciada especificando o alias aws/sqs.

- KmsDataKeyReusePeriodSeconds

  Tipo: string

  Valores válidos: 60-86400

  Padrão: 300

  Descrição: (Opcional) O período de tempo, em segundos, em que uma fila do Amazon SQS pode reutilizar uma chave de dados para criptografar ou descriptografar mensagens antes de ligar novamente. AWS KMS

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

Etapas do documento

- SelectKeyType (`aws:branch`): Ramificações com base na chave especificada.
- PutAttributeSseKms (`aws:executeAwsApi`) - Atualiza a fila do Amazon SQS para usar a AWS KMS chave especificada para criptografia.

- PutAttributeSseSqs (`aws:executeAwsApi`) - Atualiza a fila do Amazon SQS para usar a chave padrão para criptografia.
- VerifySqsEncryptionKms (`aws:assertAwsResourceProperty`) - Verifica se a criptografia está ativada na fila do Amazon SQS.
- VerifySqsEncryptionDefault (`aws:assertAwsResourceProperty`) - Verifica se a criptografia está ativada na fila do Amazon SQS.

Step Functions

AWS Systems Manager A automação fornece runbooks predefinidos para AWS Step Functions (Step Functions). Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-EnableStepFunctionsStateMachineLogging

`AWS-EnableStepFunctionsStateMachineLogging`

Descrição

O `AWS-EnableStepFunctionsStateMachineLogging` runbook ativa ou atualiza o registro na máquina de AWS Step Functions estado que você especificar. O nível mínimo de registro deve ser definido como`ALL`,`ERROR`, ou`FATAL`.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Nível

  Tipo: string

  Valores válidos: ALL | ERROR | FATAL

  Descrição: (Obrigatório) A URL da fila do Amazon SQS na qual você deseja habilitar a criptografia.

- LogGroupArn

  Tipo: string

  Descrição: (Obrigatório) O ARN do grupo de CloudWatch logs do Amazon Logs para o qual você deseja enviar os registros da máquina de estado.

- StateMachineArn

  Tipo: string

  Descrição: (Obrigatório) O ARN da máquina de estado na qual você deseja ativar o login.

- IncludeExecutionData

  Tipo: booliano

  Padrão: False

  Descrição: (Opcional) Determina se os dados de execução estão incluídos nos registros.

- TracingConfiguration

  Tipo: booliano

  Padrão: False

Descrição: (Opcional) Determina se AWS X-Ray o rastreamento está ativado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `states:DescribeStateMachine`
- `states:UpdateStateMachine`

Etapas do documento

- `EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)`- Atualiza a máquina de estado especificada com a configuração de registro especificada.
- `VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)`- Verifica se o registro foi ativado para a máquina de estado especificada.

Saídas

- EnableStepFunctionsStateMachineLogging.Response - Resposta da chamada da UpdateStateMachine API.

Systems Manager

AWS Systems Manager A automação fornece runbooks predefinidos para o Systems Manager. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- 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

Descrição

O runbook `AWS-BulkDeleteAssociation` ajuda você a excluir até 50 associações do State Manager do Systems Manager por vez.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- AssociationIds

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas IDs das associações que você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:DeleteAssociation`

Etapas do documento

- `aws:executeScript` :Exclui as associações especificadas no parâmetro `AssociationIds`.

AWS-BulkEditOpsItems

Descrição

O `AWS-BulkEditOpsItems` runbook ajuda você a editar o status, a gravidade, a categoria ou a prioridade do AWS Systems Manager OpsItems. Essa automação pode editar OpsItems no máximo 50 por vez.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Categoria

  Tipo: String

  Valores válidos:
  - Disponibilidade
  - Custo
  - Nenhuma alteração
  - Performance
  - Recuperação
  - Segurança

  Padrão: No change

  Descrição: (Opcional) A nova categoria que você deseja especificar para os editados OpsItems.
- OpsItemIds

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas OpsItems IDs que você deseja editar (por exemplo, OI-xxxxxxxxxxxx, OI-xxxxxxxxxxxx).
- Prioridade

  Tipo: String

  Valores válidos:
  - Nenhuma alteração

- 1
- 2
- 3
- 4
- 5

Padrão: No change

Descrição: (Opcional) A importância do editado OpsItems em relação aos outros OpsItems no sistema.

- Gravidade

  Tipo: String

  Valores válidos:

  - Nenhuma alteração
  - 1
  - 2
  - 3
  - 4

  Padrão: No change

  Descrição: (Opcional) A severidade da edição OpsItems.

- WaitTimeBetweenEditsInSecs

  Tipo: String

  Valores válidos: 0,0 a 2,0

  Padrão: 0.8

  Descrição: (opcional) O tempo que a automação espera entre chamar a operação de `UpdateOpsItems`.

- Status

  Tipo: String

Valores válidos:

- InProgress
- Nenhuma alteração
- Abra o
- Resolvido

Padrão: No change

Descrição: (Opcional) O novo status do editado OpsItems.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

Etapas do documento

- `aws:executeScript`- Edita o OpsItems que você especificou no `OpsItemIds` parâmetro com base nos valores que você especifica para os `Status` parâmetros `Category` `PrioritySeverity`,, e.

AWS-BulkResolveOpsItems

Descrição

O `AWS-BulkResolveOpsItems` runbook resolve o AWS Systems Manager OpsItems que corresponde ao filtro que você especificou. Você também pode especificar um OpsItemId para adicionar ao resolvido OpsItems usando o `OpsInsightsId` parâmetro. Se um valor para o parâmetro `S3BucketName` for especificado, um resumo do resultado será enviado para o bucket do Amazon Simple Storage Service (Amazon S3). Para receber uma notificação após o envio do resumo do resultado para o bucket do Amazon S3, especifique um valor para o parâmetro `SnsTopicArn`. Essa automação resolverá OpsItems no máximo 1.000 por vez.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Filtros

  Tipo: String

  Descrição: (Obrigatório) Os pares de filtros de valores-chave para retornar o OpsItems que você deseja resolver. Por exemplo, `[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`. Para saber mais sobre as opções disponíveis para filtrar OpsItems respostas, consulte OpsItemFiltersa Referência da AWS Systems Manager API.
- OpsInsightId

  Tipo: String

  Descrição: (Opcional) O identificador de recurso relacionado que você deseja adicionar ao resolvido OpsItems.
- S3 BucketName

  Tipo: String

Descrição: (opcional) O nome do bucket do Amazon S3 para o qual deseja enviar o resumo do resultado.

- SnsMessage

  Tipo: String

  Descrição: (opcional) A notificação que o Amazon Simple Notification Service (Amazon SNS) deverá enviar quando a automação for concluída.

- SnsTopicArn

  Tipo: String

  Descrição: (opcional) O ARN do tópico do Amazon SNS que deseja notificar quando o resumo do resultado for enviado para o Amazon S3.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `s3:GetBucketAcl`
- `s3:PutObject`
- `sns:Publish`
- `ssm:DescribeOpsItems`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

Etapas do documento

- `aws:executeScript`- Reúne e resolve o problema OpsItems com base nos filtros que você especifica. Se um valor para o parâmetro `OpsInsightId` for especificado, o valor será adicionado como um recurso relacionado.
- `aws:executeScript` - Se você especificar um valor para o parâmetro `S3BucketName`, um resumo do resultado será enviado para o bucket do Amazon Simple Storage Service (Amazon S3).

- `aws:executeScript` :Se um valor para o parâmetro `SnsTopicArn` for especificado, uma notificação será enviada ao tópico do Amazon SNS após o envio do resumo do resultado para o Amazon S3, incluindo o valor do parâmetro `SnsMessage`, se especificado.

AWS-ConfigureMaintenanceWindows

Descrição

O runbook `AWS-ConfigureMaintenanceWindows` ajuda a habilitar ou desabilitar várias janelas de manutenção do Systems Manager.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- MaintenanceWindows

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas IDs das janelas de manutenção que você deseja ativar ou desativar.

- MaintenanceWindowsStatus

  Tipo: String

  Valores válidos: True | False

  Padrão: "False"

  Descrição: (obrigatório) Determina se as janelas de manutenção estão habilitadas ou desabilitadas. Especifique “True” para habilitar as janelas de manutenção e “False” para desabilitá-las.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

Etapas do documento

- `aws:executeScript` :Reúne o status das janelas de manutenção especificadas no parâmetro `MaintenanceWindows` e habilita ou desabilita as janelas de manutenção.

AWS-CreateManagedLinuxInstance

Descrição

Crie uma EC2 instância para Linux configurada para Systems Manager.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux

Parâmetros

- AmiId

  Tipo: String

  Descrição: (obrigatório) ID da AMI a ser usada para iniciar a instância.

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- GroupName

  Tipo: String

  Padrão: SSMSecurity GroupForLinuxInstances

  Descrição: (obrigatório) Nome do grupo de segurança a ser criado.

- HttpTokens

  Tipo: String

  Valores válidos: optional | required

  Padrão: Optional

  Descrição: (Opcional) IMDSv2 usa sessões baseadas em tokens. Defina o uso de tokens HTTP como `optional` ou `required` para determinar se IMDSv2 é opcional ou obrigatório.

- InstanceType

  Tipo: String

  Padrão: t2.medium

  Descrição: (obrigatório) Tipo de instância a ser executada. O padrão é t2.medium.

- KeyPairName

  Tipo: String

  Descrição: (obrigatório) Par de chaves a ser usado ao criar a instância.

- RemoteAccessCidr

  Tipo: String

  Padrão: 0.0.0.0/0

  Descrição: (Obrigatório) Cria um grupo de segurança com porta para SSH (intervalo de portas 22) aberta IPs conforme especificado pelo CIDR (o padrão é 0.0.0.0/0). Se o grupo de segurança já existe, ele não será modificado e regras não serão alteradas.

- RoleName

  Tipo: String

  Padrão: SSMManaged InstanceProfileRole

  Descrição: (obrigatório) Nome da função a ser criada.

- StackName

  Tipo: String

  Padrão: CreateManagedInstanceStack {{automation:execution_id}}

  Descrição: (opcional) Especificar o nome da pilha usado por este runbook

- SubnetId

  Tipo: String

  Padrão: Default

  Descrição: (obrigatório) A nova instância será implantada nessa sub-rede ou na sub-rede padrão se não for especificada.

- VpcId

  Tipo: String

  Padrão: Default

Descrição: (obrigatório) A nova instância será implantada nessa Amazon Virtual Private Cloud (Amazon VPC) ou na Amazon VPC padrão se não for especificada.

AWS-CreateManagedWindowsInstance

Descrição

Crie uma EC2 instância para uma Windows Server que esteja configurada para Systems Manager.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Windows

Parâmetros

Parâmetros

- AmiId

  Tipo: String

  Padrão: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

  Descrição: (obrigatório) ID da AMI a ser usada para iniciar a instância.
- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- GroupName

  Tipo: String

  Padrão: SSMSecurity GroupForLinuxInstances

  Descrição: (obrigatório) Nome do grupo de segurança a ser criado.

- HttpTokens

  Tipo: String

  Valores válidos: optional | required

  Padrão: Optional

  Descrição: (Opcional) IMDSv2 usa sessões baseadas em tokens. Defina o uso de tokens HTTP como `optional` ou `required` para determinar se IMDSv2 é opcional ou obrigatório.

- InstanceType

  Tipo: String

  Padrão: t2.medium

  Descrição: (obrigatório) Tipo de instância a ser executada. O padrão é t2.medium.

- KeyPairName

  Tipo: String

  Descrição: (obrigatório) Par de chaves a ser usado ao criar a instância.

- RemoteAccessCidr

  Tipo: String

  Padrão: 0.0.0.0/0

  Descrição: (Obrigatório) Cria um grupo de segurança com porta para RDP (intervalo de portas 3389) aberta IPs conforme especificado pelo CIDR (o padrão é 0.0.0.0/0). Se o grupo de segurança já existe, ele não será modificado e regras não serão alteradas.

- RoleName

  Tipo: String

  Padrão: SSMManaged InstanceProfileRole

  Descrição: (obrigatório) Nome da função a ser criada.
- StackName

  Tipo: String

  Padrão: CreateManagedInstanceStack {{automation:execution_id}}

  Descrição: (opcional) Especificar o nome da pilha usado por este runbook
- SubnetId

  Tipo: String

  Padrão: Default

  Descrição: (obrigatório) A nova instância será implantada nessa sub-rede ou na sub-rede padrão se não for especificada.
- VpcId

  Tipo: String

  Padrão: Default

  Descrição: (obrigatório) A nova instância será implantada nessa Amazon Virtual Private Cloud (Amazon VPC) ou na Amazon VPC padrão se não for especificada.

AWSConfigRemediation-EnableCWLoggingForSessionManager

Descrição

O `AWSConfigRemediation-EnableCWLoggingForSessionManager` runbook permite que as sessões do AWS Systems Manager Session Manager (Session Manager) armazenem os registros de saída em um grupo de registros da Amazon CloudWatch (CloudWatch).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DestinationLogGroup

  Tipo: String

  Descrição: (Obrigatório) O nome do grupo de CloudWatch registros.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetDocument`
- `ssm:UpdateDocument`
- `ssm:CreateDocument`
- `ssm:UpdateDefaultDocumentVersion`
- `ssm:DescribeDocument`

Etapas do documento

- `aws:executeScript`- Aceita o grupo de CloudWatch registros para atualizar o documento que armazena as preferências de registros de saída da sessão do Gerenciador de Sessões ou cria um caso ele não exista.

AWS-ExportOpsDataToS3

Descrição

Esse runbook recupera uma lista de OpsData resumos no AWS Systems Manager Explorer e os exporta para um objeto em um bucket específico do Amazon Simple Storage Service (Amazon S3).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- columnFields

  Tipo: StringList

  Descrição: (Obrigatório) campos de coluna a serem gravados no arquivo de saída.
- filtros

Tipo: String

Descrição: (Opcional) Filtros para a getOpsSummary solicitação.

- resultAttribute

  Tipo: String

  Descrição: (Opcional) O atributo de resultado da getOpsSummary solicitação.

- s3 BucketName

  Tipo: String

  Descrição: (obrigatória) o bucket do S3 onde deseja fazer download do arquivo de saída.

- snsSuccessMessage

  Tipo: String

  Descrição: (opcional) Mensagem a ser enviada quando o runbook terminar.

- snsTopicArn

  Tipo: String

  Descrição: (obrigatório) ARN do tópico do Amazon Simple Notification Service (Amazon SNS) a ser notificado quando o download for concluído.

- syncName

  Tipo: String

  Descrição: (Opcional) o nome da sincronização de dados do recurso.

Etapas do documento

getOpsSummaryEtapa — Recupera até 5.000 resumos de operações para exportar em um arquivo CSV agora.

Saídas

OpsData object — Se o runbook for executado com êxito, você encontrará o OpsData objeto exportado no bucket do S3 de destino.

AWS-ExportPatchReportToS3

Descrição

Esse runbook recupera listas de dados de resumo de patches e detalhes de patches no Patch Manager do AWS Systems Manager e as exporta para arquivos .csv em um bucket específico do Amazon Simple Storage Service (Amazon S3).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- assumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhuma função for especificada, a Automação do Systems Manager usará as permissões do usuário que executar esse documento.
- s3 BucketName

  Tipo: String

  Descrição: (obrigatório) O bucket do S3 onde deseja fazer download do arquivo de saída.
- snsTopicArn

  Tipo: String

  Descrição: (opcional) O nome do recurso da Amazon (ARN) do tópico do Amazon Simple Notification Service (Amazon SNS) a ser notificado quando o download for concluído.

- snsSuccessMessage

  Tipo: String

  Descrição: (opcional) Texto da mensagem a ser enviada quando o runbook terminar.
- destinos

  Tipo: String

  Descrição: (obrigatório) O ID da instância ou um caractere curinga (*) para indicar se os dados de patch devem ser reportados para uma instância específica ou para todas as instâncias.

Etapas do documento

ExportReportStep — A ação dessa etapa depende do valor do `targets` parâmetro. Se os `targets` estiverem no formato de `instanceids=*`, a etapa recupera até 10.000 resumos de patches para instâncias em sua conta e exporta os dados para um arquivo .csv.

Se os `targets` estiverem no formato `instanceids=<instance-id>`, a etapa recupera o resumo do patch e todos os patches da instância especificada em sua conta e os exporta para um arquivo .csv.

Saídas

PatchSummaryObjeto /Patches — Se o runbook for executado com êxito, o objeto do relatório de patch exportado será baixado para o bucket do S3 de destino.

`AWS-SetupInventory`

Descrição

Criar uma associação de inventário do Systems Manager Inventory para uma ou mais instâncias gerenciadas. O sistema coleta metadados de suas instâncias de acordo com a programação na associação. Para obter mais informações, consulte AWS Systems Manager Inventário.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- Aplicações

  Tipo: String

  Padrão: Habilitado

  Descrição: (Opcional) Colete metadados sobre aplicativos instalados.
- AssociatedDocName

  Tipo: String

  Padrão: `AWS-GatherSoftwareInventory`

  Descrição: (opcional) O nome do runbook do SSM usado para coletar o inventário da instância gerenciada.
- AssociationName

  Tipo: String

  Descrição: (Opcional) Um nome para a associação de Inventário que será atribuído à instância.
- AssocWaitTime

  Tipo: String

  Padrão: PT5 M

  Descrição: (Opcional) A quantidade de tempo que deve pausar a coleta de inventário quando o horário de início da associação de Inventário for atingido. O tempo usa o formato ISO 8601.
- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- `AwsComponents`

  Tipo: String

  Padrão: Habilitado

  Descrição: (Opcional) Colete metadados para AWS componentes como amazon-ssm-agent.

- CustomInventory

  Tipo: String

  Padrão: Habilitado

  Descrição: (Opcional) Colete metadados de inventário personalizados.

- Arquivos

  Tipo: String

  Descrição: (Opcional) Colete metadados sobre arquivos em suas instâncias. Para obter mais informações sobre como coletar esse tipo de dados de inventário, consulte Trabalhando com arquivo e inventário de registro do Windows. Requer o SSMAgent versão 2.2.64.0 ou posterior. Exemplo do Linux: `[{"Path":"/usr/bin", "Pattern": ["aws*", "*ssm*"],"Recursive":false},{"Path":"/var/log", "Pattern": ["amazon*.*"], "Recursive":true, "DirScanLimit":1000}]` Windows example: `[{"Path":"%PROGRAMFILES%", "Pattern":["*.exe"],"Recursive":true}]`

- InstanceDetailedInformation

  Tipo: String

  Padrão: Habilitado

  Descrição: (Opcional) Colete informações adicionais sobre a instância, incluindo o modelo da CPU, velocidade e o número de núcleos, entre outros.

- InstanceIds

  Tipo: String

  Padrão: *

Descrição: EC2 instâncias (obrigatórias) que você deseja inventariar.

- LambdaAssumeRole

  Tipo: String

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.

- NetworkConfig

  Tipo: String

  Padrão: Habilitado

  Descrição: (Opcional) Colete metadados sobre configurações de rede.

- Saídas 3 BucketName

  Tipo: String

  Descrição: (opcional) O nome de um bucket Amazon S3 em que você deseja gravar dados de log de inventário.

- Saídas 3 KeyPrefix

  Tipo: String

  Descrição: (opcional) Um prefixo de chaves do Amazon S3 (subpasta) em que você deseja gravar dados de log de inventário.

- OutputS3Region

  Tipo: String

  Descrição: (Opcional) O nome do Região da AWS local onde o Amazon S3 existe.

- Programação

  Tipo: String

  Padrão: cron(0 */30 * * * ? *)

Descrição: (Opcional) Uma expressão cron para a programação da associação de inventário. O padrão é a cada 30 minutos.

- Serviços

  Tipo: String

  Padrão: Habilitado

  Descrição: (Opcional, somente o sistema operacional Windows, requer a SSMAgent versão 2.2.64.0 e superior) Colete dados para configurações de serviço.

- WindowsRegistry

  Tipo: String

  Descrição: (Opcional) Colete metadados sobre as chaves de registro do Microsoft Windows. Para obter mais informações sobre como coletar esse tipo de dados de inventário, consulte Trabalhando com arquivo e inventário de registro do Windows. Requer SSM Agent versão 2.2.64.0 ou posterior. Exemplo: [{"Path” :"HKEY_CURRENT_CONFIG\ System”, "Recursive” :true}, {"Path” :"HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\ “," “: [” “]}] MachineImage ValueNames AMIName

- WindowsRoles

  Tipo: String

  Padrão: Habilitado

  Descrição: (Opcional) Colete informações sobre funções do Windows na instância. Aplica-se apenas a sistemas operacionais Windows. Requer o SSMAgent versão 2.2.64.0 ou posterior.

- WindowsUpdates

  Tipo: String

  Padrão: Habilitado

  Descrição: (Opcional) Colete dados sobre todas as atualizações do Windows na instância.

AWS-SetupManagedInstance

Descrição

Configure uma instância com uma função AWS Identity and Access Management (IAM) para acesso ao Systems Manager.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: String

  Descrição: ID (obrigatório) da EC2 instância a ser configurada
- LambdaAssumeRole

  Tipo: String

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.

- RoleName

  Tipo: String

  Padrão: SSMRole ForManagedInstance

  Descrição: (Opcional) O nome da função do IAM para a EC2 instância. Se essa função não existir, ela será criada. Ao especificar esse valor, verifique se a função contém a Amazon SSMManaged InstanceCore Managed Policy.

AWS-SetupManagedRoleOnEC2Instance

Descrição

Configure uma instância com a função SSMRole ForManagedInstance gerenciada do IAM para acesso ao Systems Manager.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- InstanceId

  Tipo: String

  Descrição: ID (obrigatório) da EC2 instância a ser configurada

- LambdaAssumeRole

  Tipo: String

  Descrição: (opcional) o ARN da função que permite que a Lambda criada por Automação realize ações em seu nome. Se não for especificado, uma função transitória será criada para executar a função Lambda.

- RoleName

  Tipo: String

  Padrão: SSMRole ForManagedInstance

  Descrição: (Opcional) O nome da função do IAM para a EC2 instância. Se essa função não existir, ela será criada. Ao especificar esse valor, verifique se a função contém a Amazon SSMManaged InstanceCore Managed Policy.

`AWSSupport-TroubleshootManagedInstance`

Descrição

O `AWSSupport-TroubleshootManagedInstance` runbook ajuda você a determinar por que uma instância do Amazon Elastic Compute Cloud EC2 (Amazon) não é reportada como gerenciada por. AWS Systems Manager Este runbook analisa a configuração da VPC para a instância, incluindo regras de grupo de segurança, endpoints da VPC, regras de lista de controle de acesso (ACL) à rede e tabelas de rotas. Também confirma que um perfil de instância AWS Identity and Access Management (IAM) que contém as permissões necessárias está anexado à instância.

> **Important**
>
> Esse runbook de automação não avalia IPv6 as regras.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: string

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon que não está reportando como gerenciada pelo Systems Manager.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- aws:executeScript :Reúne o PingStatus da instância.
- aws:branch :Ramifica com base no fato de a instância já estar reportando conforme gerenciado pelo Systems Manager.
- aws:executeAwsApi :Reúne detalhes sobre a instância, incluindo a configuração da VPC.
- aws:executeScript :Se aplicável, reúne detalhes adicionais relacionados aos endpoints da VPC que foram implantados para uso com o Systems Manager e confirma que os grupos de segurança anexados ao endpoint da VPC permitem tráfego de entrada na porta TCP 443 da instância.
- aws:executeScript :Verifica se a tabela de rotas permite tráfego para o endpoint da VPC ou endpoints públicos do Systems Manager.
- aws:executeScript :Verifica se as regras de network ACL permite tráfego para o endpoint da VPC ou endpoints públicos do Systems Manager.
- aws:executeScript :Verifica se o tráfego de saída para o endpoint da VPC ou para os endpoints públicos do Systems Manager é permitido pelo grupo de segurança associado à instância.
- aws:executeScript :Verifica se o perfil de instância anexado à instância inclui uma política gerenciada que fornece as permissões necessárias.
- aws:branch :Ramifica com base no sistema operacional da instância.

- `aws:executeScript` :Fornece referência ao shell script do `ssmagent-toolkit-linux`.
- `aws:executeScript`- Fornece referência ao `ssmagent-toolkit-windows` PowerShell script.
- `aws:executeScript` :Gera a saída final para a automação.
- `aws:executeScript` :Se o `PingStatus` da instância for `Online`, retorna que a instância já é gerenciada pelo Systems Manager.

AWSSupport-TroubleshootPatchManagerLinux

Descrição

O `AWSSupport-TroubleshootPatchManagerLinux` runbook soluciona problemas comuns que podem causar uma falha de patch em nós gerenciados baseados em Linux usando o Patch Manager, uma ferramenta do. AWS Systems Manager O objetivo principal desse runbook é identificar a causa raiz da falha do comando de patch e sugerir um plano de correção.

Como funciona?

O `AWSSupport-TroubleshootPatchManagerLinux` runbook considera o ID da instância/ID do comando do casal fornecido por você para a solução de problemas. Se nenhum ID de comando for fornecido, ele selecionará o último comando de patch com falha nos últimos 30 dias na instância fornecida. Depois de verificar o status do comando, o cumprimento dos pré-requisitos e a distribuição do sistema operacional, o runbook baixa e executa um pacote de análise de log. A saída inclui a causa raiz do problema, bem como a ação necessária para corrigir o problema.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

- Amazon Linux 2 e AL2 023
- Red Hat Enterprise Linux 8.X e 9.X
- Centos 8.X e 9.X
- USO 15.X

Parâmetros

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

Instruções

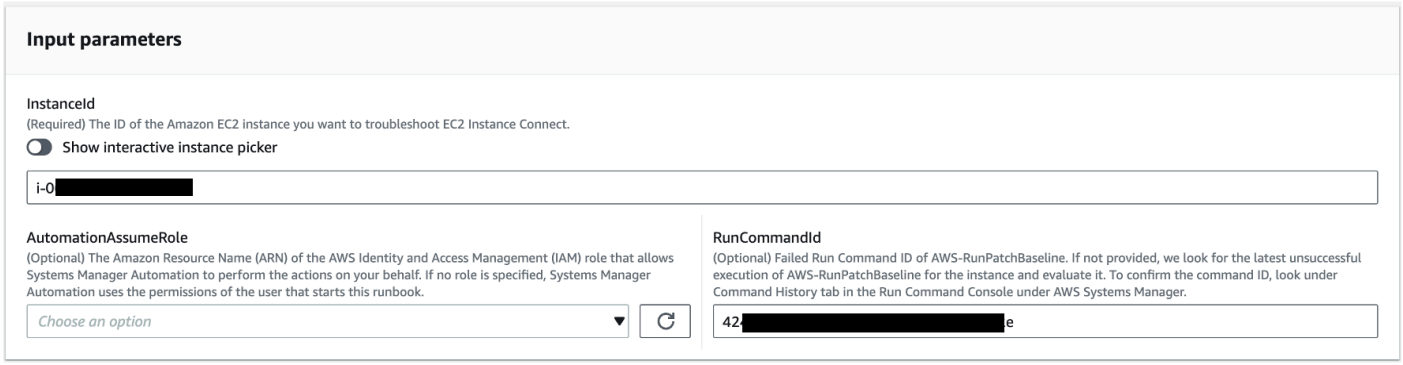
Siga estas etapas para configurar a automação:

1. Navegue até o `AWSSupport-TroubleshootPatchManagerLinux`no AWS Systems Manager console.
2. Selecione Execute automation (Executar automação).
3. Para os parâmetros de entrada, insira o seguinte:
   - InstanceId (Obrigatório):

     Use o seletor de instância interativo para escolher o ID do nó gerenciado SSM baseado em Linux (Amazon Elastic Compute Cloud (Amazon EC2) ou servidor Hybrid Activated) no qual o comando patch falhou, ou insira manualmente o ID da instância gerenciada do SSM.
   - AutomationAssumeRole (Opcional):

     Insira o ARN da função do IAM que permite que a Automation execute ações em seu nome. Se uma função não for especificada, a automação usa as permissões do usuário que inicia esse runbook.
   - RunCommandId (Opcional):

Insira o ID do comando Failed Run do `AWS-RunPatchBaseline` documento. Se você não fornecer uma ID de comando, o runbook procurará o comando de patch com falha mais recente nos últimos 30 dias na instância selecionada.



4. Selecione Executar.
5. A automação é iniciada.
6. O bucket realiza as seguintes etapas:
   - CheckConcurrency:

     Garante que haja apenas uma execução desse runbook direcionada à mesma instância. Se o runbook encontrar outra execução em andamento visando a mesma instância, ele retornará um erro e terminará.
   - ValidateCommandID:

     Valida se o ID do comando fornecido, como parâmetro de entrada, foi executado para o documento `AWS-RunPatchBaseline` SSM. Se nenhum ID de comando for fornecido, o runbook considerará a última falha de execução dos `AWS-RunPatchBaseline` últimos 30 dias na instância selecionada.
   - BranchOnCommandStatus:

     Confirma que o status do comando fornecido falhou. Caso contrário, o runbook encerra a execução e gera um relatório informando que o comando fornecido foi executado com sucesso.
   - VerifyPrerequistes:

     Confirma que os pré-requisitos mencionados acima foram cumpridos.
   - GetPlatformDetails:

     Recupera a distribuição e a versão do sistema operacional (OS).
   - GetDownloadURL:

Recupera a URL de download do pacote PatchManager Log Analyzer.

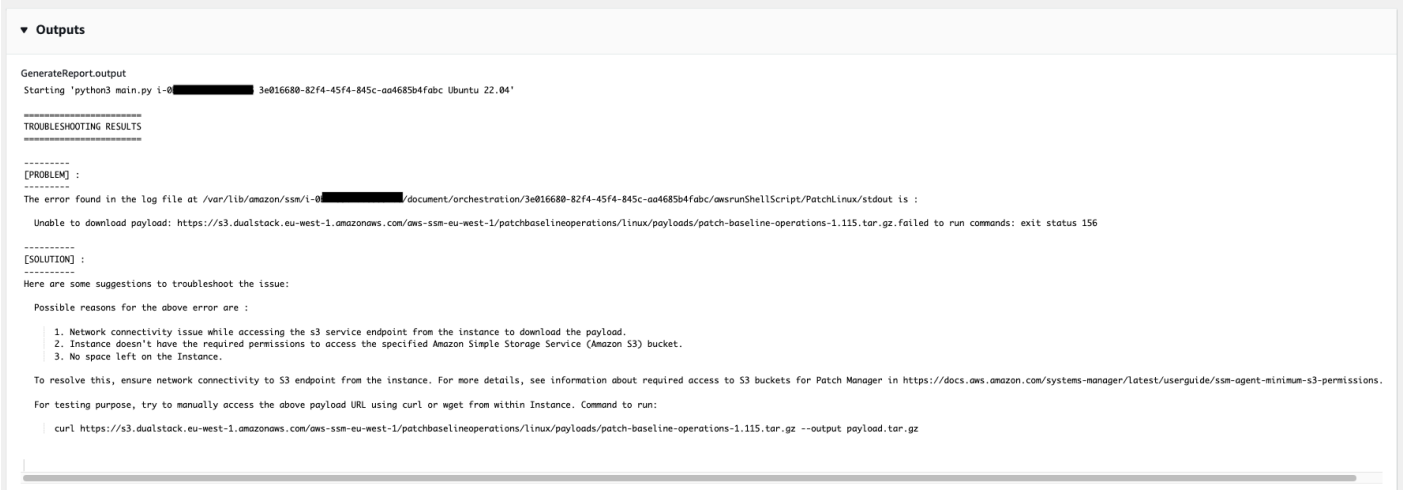
- EvaluatePatchManagerLogs:

  Faz o download e executa o pacote python do PatchManager Log Analyzer na instância para avaliar o arquivo de log.

- GenerateReport:

  Gera um relatório final da execução do runbook que inclui o problema identificado e a solução sugerida.

7. Depois de concluído, revise a seção Saídas para obter os resultados detalhados da execução:



Referências

Automação do Systems Manager

- Executar esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWSSupport-TroubleshootSessionManager

Descrição

O `AWSSupport-TroubleshootSessionManager` runbook ajuda você a solucionar problemas comuns que impedem a conexão com instâncias gerenciadas do Amazon Elastic Compute Cloud

(Amazon EC2) usando o Session Manager. O Gerenciador de Sessões é uma ferramenta em AWS Systems Manager. Este runbook verifica o seguinte:

- Verifica se a instância está sendo executada e reportada como gerenciada pelo Systems Manager.
- Executa o runbook `AWSSupport-TroubleshootManagedInstance` se a instância não estiver reportando como gerenciada pelo Systems Manager.
- Verifica a versão do SSM Agent instalado na instância.
- Verifica se um perfil de instância contendo uma política recomendada AWS Identity and Access Management (IAM) para o Session Manager está anexado à EC2 instância da Amazon.
- Coleta os logs do SSM Agent da instância.
- Analisa suas preferências do Session Manager.
- Executa o `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` runbook para analisar a conectividade da instância com os endpoints do Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service (Amazon S3) e Amazon CloudWatch Logs (Logs). CloudWatch

Considerações

- Não há suporte para nós gerenciados híbridos.
- Esse runbook só verifica se uma política do IAM gerenciada recomendada está anexada ao perfil de instância. Ele não analisa o IAM nem as permissões do AWS KMS contidas no perfil de instância.

> **Important**
>
> O runbook `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` usa o VPC Reachability Analyzer para analisar a conectividade de rede entre uma fonte e um endpoint de serviço. Você é cobrado por análise executada entre a origem e o destino. Para obter mais detalhes, consulte Preço da Amazon VPC.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- InstanceId

  Tipo: String

  Descrição: (Obrigatório) O ID da EC2 instância da Amazon à qual você não consegue se conectar usando o Gerenciador de Sessões.
- SessionPreferenceDocument

  Tipo: String

  Padrão: SSM- SessionManagerRunShell

  Descrição: (opcional) O nome do seu documento de preferências de sessão. Se não for especificado um documento de preferências de sessão personalizado ao iniciar sessões, use o valor padrão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

1. `aws:waitForAwsResourceProperty`: espera até 6 minutos para que sua instância de destino passe pelas verificações de status.
2. `aws:executeScript`: analisa o documento de preferência da sessão.
3. `aws:executeAwsApi`: obtém o ARN do perfil de instância anexado à sua instância.
4. `aws:executeAwsApi`: verifica se a instância está sendo executada e reportada como gerenciada pelo Systems Manager.
5. `aws:branch`: ramifica com base no fato de sua instância estar reportando como sendo gerenciada pelo Systems Manager.
6. `aws:executeScript`: verifica se o SSM agent instalado na sua instância é compatível com o Session Manager.
7. `aws:branch`: ramifica com base na plataforma da sua instância para coletar logs da `ssm-cli`.
8. `aws:runCommand`: coleta a saída de logs da `ssm-cli` de uma instância do Linux or macOS.
9. `aws:runCommand`: coleta a saída de logs da `ssm-cli` de uma instância do Windows.
10. `aws:executeScript`: analisa os logs da `ssm-cli` .
11. `aws:executeScript`: Esse runbook só verifica se uma política do IAM gerenciada recomendada está anexada ao perfil de instância.
12. `aws:branch`: determina se a conectividade do endpoint do `ssmmessages` deve ser avaliada com base nos logs da `ssm-cli`.
13. `aws:executeAutomation`: avalia se a instância pode se conectar a um endpoint do `ssmmessages`.
14. `aws:branch`: determina se a conectividade do endpoint Amazon S3 deve ser avaliada com base nos logs da `ssm-cli` e nas suas preferências de sessão.
15. `aws:executeAutomation`: avalia se a instância pode se conectar a um endpoint do Amazon S3.
16. `aws:branch`: determina se a conectividade do AWS KMS endpoint deve ser avaliada com base nos `ssm-cli` registros e nas suas preferências de sessão.
17. `aws:executeAutomation`: avalia se a instância pode se conectar a um AWS KMS endpoint.
18. `aws:branch`: determina se a conectividade do endpoint do CloudWatch Logs deve ser avaliada com base nos `ssm-cli` registros e nas suas preferências de sessão.
19. `aws:executeAutomation`: avalia se a instância pode se conectar a um endpoint do CloudWatch Logs.

20 `aws:executeAutomation`: executa o runbook `AWSSupport-TroubleshootManagedInstance`.

21 `aws:executeScript`: compila a saída das etapas anteriores e gera um relatório.

Saídas

- `generateReport.EvalReport` :Os resultados das verificações realizadas pelo runbook em texto simples.

Terceiros

AWS Systems Manager A automação fornece runbooks predefinidos para produtos e serviços de terceiros. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-CreateJiraIssue
- AWS-CreateServiceNowIncident
- AWS-RunPacker

`AWS-CreateJiraIssue`

Descrição

Cria um problema no Jira.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AssigneeName

  Tipo: String

  Descrição: (opcional) O nome de usuário da pessoa à qual o problema deve ser atribuído.
- DueDate

  Tipo: String

  Descrição: (Opcional) A data de vencimento da edição em yyyy-mm-dd formato.
- IssueDescription

  Tipo: String

  Descrição: (obrigatório) Uma descrição detalhada do problema.
- IssueSummary

  Tipo: String

  Descrição: (obrigatório) Um breve resumo do problema.
- IssueTypeName

  Tipo: String

  Descrição: (obrigatório) O nome do tipo do problema que você deseja criar (por exemplo, Tarefa, Subtarefa, Bug, etc.).
- JiraURL

  Tipo: String

  Descrição: (obrigatório) O URL da instância do Jira.
- JiraUsername

  Tipo: String

  Descrição: (obrigatório) O nome do usuário com o qual o problema será criado.
- PriorityName

Tipo: String

Descrição: (opcional) O nome da prioridade do problema.

- ProjectKey

  Tipo: String

  Descrição: (obrigatório) A chave do projeto no qual o problema deve ser criado.

- SSMParameterNome

  Tipo: String

  Descrição: (obrigatório) O nome de um parâmetro do SSM criptografado que contém a chave de API ou senha do usuário do Jira.

Etapas do documento

`aws:createStack`- Crie uma CloudFormation pilha para criar a função e a função do Lambda IAM.

`aws:invokeLambdaFunction` :Invocar a função do Lambda para criar o problema do Jira

`aws:deleteStack`- Exclua a CloudFormation pilha criada.

Saídas

IssueId: ID da edição recém-criada do Jira

AWS-CreateServiceNowIncident

Descrição

Crie um incidente na tabela de ServiceNow incidentes.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Categoria

  Tipo: String

  Descrição: (opcional) a categoria do incidente.

  Valores válidos: Nenhum | | Software Inquiry/Help | Hardware | Rede | Banco de dados

  Valor padrão: None
- Descrição

  Tipo: String

  Descrição: (obrigatório) uma explicação detalhada sobre o incidente.
- Impacto

  Tipo: String

  Descrição: (opcional) o efeito que um incidente tem sobre os negócios.

  Valores válidos: High | Medium | Low

  Valor padrão: Low
- ServiceNowInstanceUsername

  Tipo: String

Descrição: (obrigatório) o nome do usuário com o qual o incidente será criado.

- ServiceNowInstancePassword

  Tipo: String

  Descrição: (Obrigatório) O nome de um parâmetro SSM criptografado contendo a senha do ServiceNow usuário.

- ServiceNowInstanceURL

  Tipo: String

  Descrição: (Obrigatório) O URL da ServiceNow instância

- ShortDescription

  Tipo: String

  Descrição: (obrigatório) uma breve descrição do incidente.

- Subcategory

  Tipo: String

  Descrição: (opcional) a subcategoria do incidente.

  Valores válidos: Nenhum | Antivírus | E-mail | Aplicativo interno | Sistema operacional | CPU | Disco | Teclado | Hardware | Memória | Monitor | Mouse | DHCP | DNS | Endereço IP | VPN | Sem fio | DB2 | MS SQL Server | Oracle

  Valor padrão: None

Etapas do documento

Push_incident — Envia as informações do incidente para. ServiceNow

Saídas

Push_incident.incidentID :O ID de incidente criado.

AWS-RunPacker

Descrição

Esse runbook usa a ferramenta HashiCorp Packer para validar, corrigir ou criar modelos de empacotador que são usados para criar imagens de máquina. Este runbook está usando o Packer v1.7.2.

> **Note**
>
> Se você especificar um valor de `vpc_id`, especifique também o valor de `subnet_id` de uma sub-rede pública. A menos que você modifique o atributo de endereçamento IPv4 público da sub-rede, você também deve `associate_public_ip_address` definir como verdadeiro.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Force

  Tipo: Booliano

  Descrição: uma opção da Packer para forçar um compilador a ser executado quando artefatos de uma compilação anterior impedirem que uma compilação seja executada.

- Modo

  Tipo: String

  Descrição: o modo, ou comando, no qual usar o Packer ao validar em relação ao modelo. As opções incluem `Build`, `Validate` e `Fix`.
- TemplateFileName

  Tipo: String

  Descrição: o nome ou a chave do arquivo de modelo no bucket do S3.
- Templates3 BucketName

  Tipo: String

  Descrição: o nome do bucket do S3 que contém o modelo do empacotador.

Etapas do documento

RunPackerProcessTemplate — Executa o modo selecionado em relação ao modelo usando a ferramenta Packer.

Saídas

RunPackerProcessTemplate.output — O stdout da ferramenta Packer.

RunPackerProcessTemplate.fixed_template_key — O nome do modelo armazenado em um bucket do S3 para ser usado somente quando executado no modo “Fix”.

RunPackerProcessTemplate.s3_bucket — O nome do bucket do S3 que contém o modelo fixo a ser usado somente quando executado no modo “Fix”.

Amazon VPC

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon Virtual Private Cloud. Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- 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

Descrição

Esse runbook remove todas as regras de entrada e saída do grupo de segurança especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- SecurityGroupId

  Tipo: String

  Descrição: (Obrigatório) O ID do grupo de segurança que você deseja fechar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Etapas do documento

- `aws:executeScript`- Remove todas as regras de entrada e saída do grupo de segurança especificado no `SecurityGroupId` parâmetro.

AWSSupport-ConfigureDNSQueryLogging

Descrição

O runbook `AWSSupport-ConfigureDNSQueryLogging` configura o registro em log para consultas ao DNS que se originam em sua nuvem privada virtual (VPC) ou em zonas hospedadas do Amazon Route 53. Você pode optar por publicar registros de consulta no Amazon CloudWatch Logs, no Amazon Simple Storage Service (Amazon S3) ou no Amazon Data Firehose. Para obter mais informações sobre logs de consultas e logs de consultas do resolvedor, consulte log público de consultas ao DNS e log de consultas do resolvedor.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LogDestinationArn

  Tipo: String

  Descrição: (Opcional) O ARN do grupo CloudWatch Logs, bucket do Amazon S3 ou stream do Firehose para o qual você deseja enviar registros de consulta. Observe que o registro de

consultas DNS públicas do Route 53 só oferece suporte a grupos de CloudWatch registros. Se você não especificar um valor para esse parâmetro, a automação cria um grupo de CloudWatch registros com o formato `AWSSupport-ConfigureDNSQueryLogging-{automation:EXECUTION_ID}` e uma política de recursos do IAM para publicar os registros de consulta. O grupo de CloudWatch registros criado pela automação tem um período de retenção de 14 dias.

- QueryLogType

  Tipo: String

  Descrição: (opcional) Os tipos de consultas que deseja fazer o log.

  Valores válidos: Public | Resolver/Private

  Padrão: Public

- ResourceId

  Tipo: String

  Descrição: (obrigatório) O ID do recurso cujas consultas deseja fazer o log. Se `Public` for especificado para o parâmetro `QueryLogType`, o recurso deverá ser o ID de uma zona hospedada privada do Route 53. Se você especificar `Resolver/Private` para o parâmetro `QueryLogType`, o recurso deverá ser o ID de uma VPC.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `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

Etapas do documento

- `aws:executeScript` :Verifica se o recurso especificado para o parâmetro `ResourceId` existe e se o tipo de recurso corresponde à opção `QueryLogType` obrigatória.
- `aws:executeScript` :Verifica se o valor especificado para o parâmetro `LogDestinationArn` corresponde ao `QueryLogType` obrigatório.
- `aws:executeScript`- Verifica as permissões necessárias para o Route 53 publicar registros no grupo de CloudWatch registros de registros e cria a política de recursos do IAM necessária, caso ela não exista.
- `aws:executeScript` :Habilita o log de consultas ao DNS no destino selecionado.

AWSSupport-ConfigureTrafficMirroring

Descrição

O `AWSSupport-ConfigureTrafficMirroring` runbook configura o espelhamento de tráfego para ajudá-lo a solucionar problemas de conectividade entre um balanceador de carga e instâncias do Amazon Elastic Compute Cloud (Amazon). EC2 O espelhamento de tráfego copia o tráfego de entrada e saída das interfaces de rede anexadas às suas instâncias. Para configurar o espelhamento de tráfego, esse runbook cria os destinos, filtros e sessões obrigatórios. Por padrão, o runbook configura o espelhamento para todo o tráfego de entrada e saída de todos os protocolos, exceto o Amazon DNS. Se quiser espelhar o tráfego de origens e destinos específicos, você pode modificar as regras de entrada e saída depois da conclusão da automação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- SourceENI

  Tipo: String

  Descrição: (obrigatório) A interface de rede elástica para a qual deseja configurar o espelhamento de tráfego.

- Alvo

  Tipo: String

  Descrição: (obrigatório) O destino do tráfego espelhado. Você deve especificar o ID de uma interface de rede, um Network Load Balancer ou um endpoint do balanceador de carga de gateway. Se um Network Load Balancer for especificado, deverá haver receptores UDP na porta 4789.

- SessionNumber

  Tipo: String

  Valores válidos: 1 a 32766

  Descrição: (obrigatório) O número de sessão do espelho que deseja usar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:CreateTrafficMirrorTarget`
- `ec2:CreateTrafficMirrorFilter`
- `ec2:CreateTrafficMirrorFilterRule`
- `ec2:CreateTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorFilter`

- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilterRule
- iam:ListRoles
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

Etapas do documento

- aws:executeScript :Executa um script para criar um destino.
- aws:executeAwsApi :Cria uma regra de filtro.
- aws:executeAwsApi :Cria uma regra de filtro do espelho para todo o tráfego de entrada.
- aws:executeAwsApi :Cria uma regra de filtro do espelho para todo o tráfego de saída.
- aws:executeAwsApi :Cria uma sessão do espelho de tráfego.
- aws:executeAwsApi :Exclui o filtro se a criação do filtro ou da sessão falhar.
- aws:executeAwsApi :Exclui o destino se a criação do filtro ou da sessão falhar.

Saídas

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget.Alvo IDOutput

AWSSupport-ConnectivityTroubleshooter

Descrição

O runbook AWSSupport-ConnectivityTroubleshooter diagnostica problemas de conectividade entre os seguintes:

- AWS recursos em uma Amazon Virtual Private Cloud (Amazon VPC)
- AWS recursos em diferentes Amazon VPCs dentro da mesma Região da AWS que estão conectados usando emparelhamento de VPC
- AWS recursos em uma Amazon VPC e um recurso da Internet usando um gateway da Internet

- AWS recursos em uma Amazon VPC e um recurso da Internet usando um gateway de tradução de endereços de rede (NAT)

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- DestinationIP

  Tipo: String

  Descrição: (Obrigatório) O IPv4 endereço do recurso ao qual você deseja se conectar.
- DestinationPort

  Tipo: String

  Padrão: True

  Descrição: (obrigatório) O número da porta à qual deseja se conectar no recurso de destino.
- DestinationVpc

Tipo: String

Padrão: All

Descrição: (opcional) O ID da Amazon VPC com o qual deseja testar a conectividade.

- SourceIP

  Tipo: String

  Descrição: (Obrigatório) O IPv4 endereço privado do AWS recurso em sua Amazon VPC a partir do qual você deseja testar a conectividade.

- SourcePortRange

  Tipo: String

  Descrição: (Opcional) O intervalo de portas usado pelo AWS recurso em sua Amazon VPC a partir do qual você deseja testar a conectividade.

- SourceVpc

  Tipo: String

  Padrão: All

  Descrição: (opcional) O ID da Amazon VPC do qual deseja testar a conectividade.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcPeeringConnections`

Etapas do documento

- `aws:executeScript`- Reúne detalhes sobre o AWS recurso que você especifica no `SourceIP` parâmetro.
- `aws:executeScript`- Determina o destino do tráfego de rede do AWS recurso usando as rotas coletadas na etapa anterior.
- `aws:branch` :Ramifica com base no destino do tráfego de rede.
- `aws:executeAwsApi` :Reúne detalhes sobre o recurso de destino.
- `aws:executeScript` :Confirma se o ID retornado para a Amazon VPC de destino corresponde ao valor especificado, se houver, no parâmetro `DestinationVpc`.
- `aws:executeAwsApi` :Reúne as regras de grupo de segurança para os recursos de origem e destino.
- `aws:executeScript` :Confirma se as regras de grupo de segurança permitem o tráfego necessário entre os recursos de origem e destino.
- `aws:executeAwsApi`- Reúne as listas de controle de acesso à rede (NACLs) associadas às sub-redes para os recursos de origem e destino.
- `aws:executeScript`- Confirma se eles NACLs permitem o tráfego necessário entre os recursos de origem e destino.
- `aws:executeScript` :Confirma se a fonte tem um endereço IP público associado ao recurso, se o destino da rota for um gateway da internet.
- `aws:executeAwsApi` :Reúne as regras de grupo de segurança para os recursos de origem.
- `aws:executeScript` :Confirma se as regras de grupo de segurança permitem o tráfego necessário do recurso de origem para o destino.
- `aws:executeAwsApi`- Reúne o NACLs associado à sub-rede para o recurso de origem.
- `aws:executeScript`- Confirma se eles NACLs permitem o tráfego necessário do recurso de origem.
- `aws:executeAwsApi` :Reúne detalhes sobre o gateway NAT.
- `aws:executeAwsApi`- Reúne o NACLs associado à sub-rede do gateway NAT.
- `aws:executeScript`- Confirma se eles NACLs permitem o tráfego necessário da sub-rede para o gateway NAT.
- `aws:executeScript` :Reúne as rotas associadas à sub-rede para o gateway NAT.
- `aws:executeScript` :Confirma se o gateway NAT tem uma rota para um gateway da Internet.
- `aws:executeAwsApi` :Reúne detalhes sobre a conexão de emparelhamento da VPC.

- `aws:executeScript`- Confirma que ambos VPCs estão na mesma região e que o ID retornado para a VPC de destino corresponde ao valor especificado, se houver, no `DestinationVpc` parâmetro.
- `aws:executeAwsApi` :Retorna a sub-rede do recurso de destino.
- `aws:executeScript` :Reúne as rotas associadas à sub-rede para a VPC emparelhada.
- `aws:executeScript` :Confirma se a VPC emparelhada tem uma rota para a conexão de emparelhamento.
- `aws:executeScript` :Confirma se o tráfego é permitido a partir do recurso de origem se o destino não for suportado pela automação.

AWSSupport-TroubleshootVPN

Descrição

O `AWSSupport-TroubleshootVPN` runbook ajuda você a rastrear e resolver erros em uma AWS Site-to-Site VPN conexão. A automação inclui várias verificações automatizadas projetadas para rastrear `IKEv1` `IKEv2` erros relacionados aos túneis de AWS Site-to-Site VPN conexão. A automação tenta combinar erros específicos e sua resolução correspondente forma uma lista de problemas comuns.

Observação: esta automação não corrige os erros. Ele é executado no intervalo de tempo mencionado e verifica o grupo de registros em busca de erros no grupo de CloudWatch registros de VPN.

Como funciona?

O runbook executa uma validação de parâmetros para confirmar se o grupo de CloudWatch log da Amazon incluído no parâmetro de entrada existe, se há algum fluxo de log no grupo de log que corresponde ao registro de túneis VPN, se o ID de conexão VPN existe e se o endereço IP do túnel existe. Ele faz chamadas à API Logs Insights em seu grupo de CloudWatch registros que estão configuradas para registro de VPN.

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- LogGroupName

  Tipo: string

  Descrição: (Obrigatório) O nome do grupo de CloudWatch log da Amazon configurado para registro de AWS Site-to-Site VPN conexão

  Allowed-pattern: `^[\.\-_/#A-Za-z0-9]{1,512}`
- VpnConnectionId

  Tipo: string

  Descrição: (Obrigatório) O ID de AWS Site-to-Site VPN conexão a ser solucionado.

  Allowed-pattern: `^vpn-[0-9a-f]{8,17}$`
- Túnel AIPAddress

  Tipo: string

  Descrição: (Obrigatório) O IPv4 endereço do túnel número 1 associado ao seu AWS Site-to-Site VPN.

  Allowed-pattern: `^((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: string

Descrição: (Opcional) O IPv4 endereço do túnel número 2 associado ao seu AWS Site-to-Site VPN.

Allowed-pattern: `^((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: string

  Descrição: (obrigatório) selecione a versão do IKE que você está usando. Valores permitidos: IKEv1, IKEv2

  Valores válidos: `['IKEv1', 'IKEv2']`

- StartTimeinEpoch

  Tipo: string

  Descrição: (opcional) horário de início da análise de logs. Você pode usar StartTimeinEpoch/EndTimeinEpoch ou LookBackPeriod para análise de registros

  Allowed-pattern: `^\d{10}|^$`

- EndTimeinEpoch

  Tipo: string

  Descrição: (opcional) horário de término da análise de logs. Você pode usar StartTimeinEpoch/EndTimeinEpoch ou LookBackPeriod para análise de registros. Se for fornecido tanto StartTimeinEpoch/EndTimeinEpoch quanto LookBackPeriod , em seguida, LookBackPeriod tem precedência

  Allowed-pattern: `^\d{10}|^$`

- LookBackPeriod

  Tipo: string

  Descrição: (opcional) tempo de dois dígitos em horas para analisar o log. Intervalo válido: de 01 a 99 Esse valor tem precedência se você também fornecer StartTimeinEpoch e EndTime

  Allowed-pattern: `^(\d?[1-9]|[1-9]0)|^$`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`
- `ec2:DescribeVpnConnections`

Instruções

Observação: essa automação funciona nos grupos de CloudWatch registros configurados para o registro de túneis VPN, quando o formato de saída do registro é JSON.

Siga estas etapas para configurar a automação:

1. Navegue até o AWSSupport-TroubleshootVPNno AWS Systems Manager console.
2. Você pode usar os seguintes parâmetros de entrada:
   - AutomationAssumeRole (Opcional):

     O Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation execute as ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
   - LogGroupName (Obrigatório):

     O nome do grupo de CloudWatch registros da Amazon a ser validado. Esse deve ser o grupo de CloudWatch registros configurado para o envio de registros pela VPN.
   - VpnConnectionId (Obrigatório):

     O ID de AWS Site-to-Site VPN conexão cujo grupo de registros é rastreado em busca de erro de VPN.
   - Túnel AIPAddress (obrigatório):

     O túnel Um endereço IP associado à sua AWS Site-to-Site VPN conexão.
   - Túnel BIPAddress (opcional):

O endereço IP do túnel B associado à sua AWS Site-to-Site VPN conexão.

- IKEVersion (Obrigatório):

  Selecione o que IKEversion você está usando. Valores permitidos: IKEv1, IKEv2.

- StartTimeinEpoch (Opcional):

  O início do intervalo de tempo a ser consultado em busca de erros. O intervalo é inclusivo, portanto, o horário de início especificado é incluído na consulta. Especificado como horário epoch, o número de segundos desde 1º de janeiro de 1970, 00:00:00 UTC.

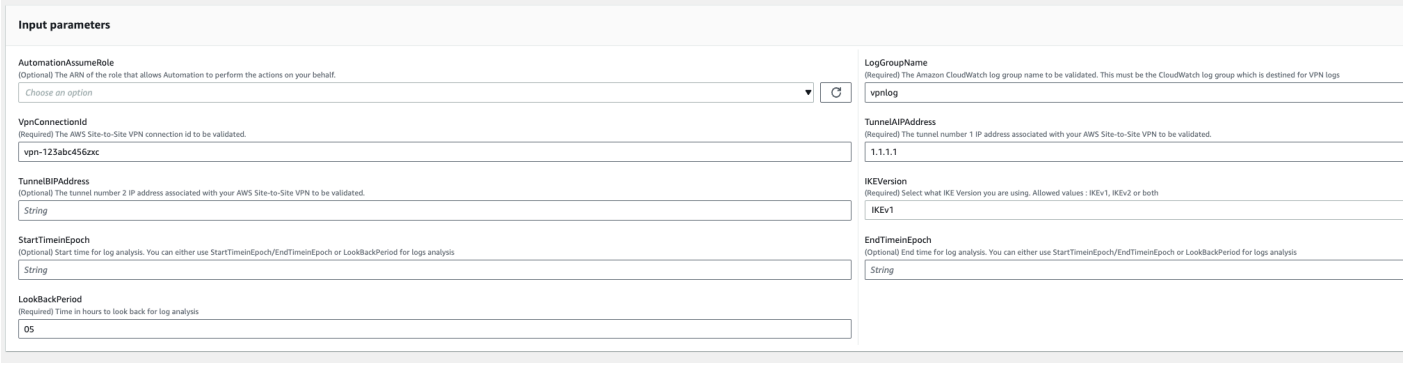
- EndTimeinEpoch (Opcional):

  O final do intervalo de tempo a ser consultado em busca de erros. O intervalo é inclusivo, portanto, o horário final especificado é incluído na consulta. Especificado como horário epoch, o número de segundos desde 1º de janeiro de 1970, 00:00:00 UTC.

- LookBackPeriod (Obrigatório):

  Tempo em horas para analisar a consulta em busca de erros.

Nota: Configure um StartTimeinEpoch, EndTimeinEpoch, ou LookBackPeriod para fixar o intervalo de tempo para análise de log. Forneça um número de dois dígitos em horas para verificar se há erros no passado a partir do horário de início da automação. Ou, se o erro estiver no passado dentro de um intervalo de tempo específico, inclua StartTimeinEpoch e EndTimeinEpoch, em vez de LookBackPeriod.



3. Selecione Executar.
4. A automação é iniciada.
5. O runbook de automação realiza as seguintes etapas:

   - parameterValidation:

Executa uma série de validações nos parâmetros de entrada incluídos na automação.

- branchOnValidationOfLogGroup:

  Verifica se o grupo de logs mencionado no parâmetro é válido. Se inválido, ele interrompe o início adicional das etapas de automação.

- branchOnValidationOfLogStream:

  Verifica se o fluxo de log existe no grupo de CloudWatch log incluído. Se inválido, ele interrompe o início adicional das etapas de automação.

- branchOnValidationOfVpnConnectionId:

  Verifica se o ID de conexão VPN incluído no parâmetro é válido. Se inválido, ele interrompe o início adicional das etapas de automação.

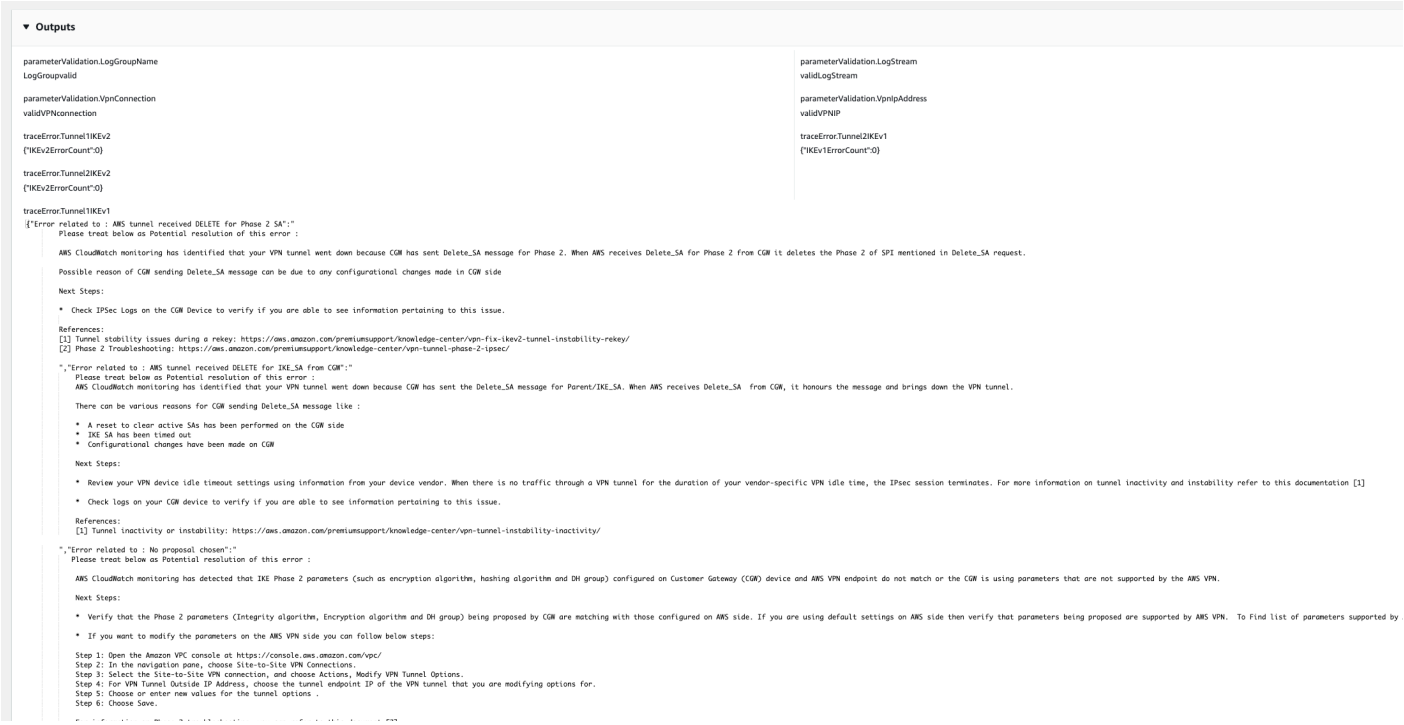
- branchOnValidationOfVpnIp:

  Verifica se o endereço IP do túnel mencionado no parâmetro é válido ou não. Se inválido, ele interrompe a execução adicional das etapas de automação.

- traceError:

  Faz uma chamada à API Logs Insight em seu grupo de registros incluído CloudWatch e pesquisa o erro relacionado a IKEv1/IKEv2 junto com uma sugestão de resolução relacionada.

6. Depois de concluído, revise a seção Outputs para obter os resultados detalhados da execução.



Referências

Automação do Systems Manager

- Execute esta automação (console)
- Executar uma automação
- Configurar a automação
- Página inicial dos fluxos de trabalho de automação

AWS documentação de serviço

- Conteúdo dos registros de Site-to-Site VPN

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

Descrição

O runbook `AWSConfigRemediation-DeleteEgressOnlyInternetGateway` exclui o gateway da Internet somente de saída especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- EgressOnlyInternetGatewayId

  Tipo: String

  Descrição: (obrigatório) O ID do Gateway da Internet somente de saída que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteEgressOnlyInternetGateway`
- `ec2:DescribeEgressOnlyInternetGateways`

Etapas do documento

- `aws:executeScript` - Exclui o gateway da Internet de somente saída especificado no parâmetro `EgressOnlyInternetGatewayId`.

- `aws:executeScript` :Verifica se o gateway da Internet somente de saída foi excluído.

AWSConfigRemediation-DeleteUnusedENI

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedENI` exclui uma interface de rede elástica (ENI) que tem o status de anexo como `detached`.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- NetworkInterfaceId

  Tipo: String

  Descrição: (obrigatório) O ID do ENI que você deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

Etapas do documento

- `aws:executeAwsApi` :Exclui a ENI especificada no parâmetro de `NetworkInterfaceId`.
- `aws:executeScript` - Verifica se o ENI foi excluído.

AWSConfigRemediation-DeleteUnusedSecurityGroup

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedSecurityGroup` exclui o grupo de segurança especificado no parâmetro `GroupId`. Se você tentar excluir um grupo de segurança associado a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou referenciado por outro grupo de segurança, a automação falhará. Essa automação não exclui um grupo de segurança padrão.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- GroupId

  Tipo: String

  Descrição: (obrigatório) O ID do grupo de segurança que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

Etapas do documento

- `aws:executeAwsApi` :Retorna o nome do grupo de segurança usando o valor fornecido no parâmetro `GroupId`.
- `aws:branch` :Confirma que o nome do grupo não é “padrão”.
- `aws:executeAwsApi` - O runbook exclui o grupo de segurança especificado no parâmetro `GroupId`.
- `aws:executeScript` :Confirma que o grupo de segurança foi excluído.

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

Descrição

O runbook `AWSConfigRemediation-DeleteUnusedVPCNetworkACL` exclui uma lista de controle de acesso (ACL) de rede que não está associada a uma sub-rede.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- NetworkAclId

  Tipo: String

  Descrição: (obrigatório) O ID da ACL de rede que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

Etapas do documento

- `aws:executeAwsApi` :Exclui a ACL de rede especificada no parâmetro `NetworkAclId`.
- `aws:executeScript`: confirma a rede ACL de rede especificada no parâmetro `NetworkAclId`.

AWSConfigRemediation-DeleteVPCFlowLog

Descrição

O runbook `AWSConfigRemediation-DeleteVPCFlowLog` exclui o log de fluxo da nuvem privada virtual (VPC) especificado.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- FlowLogId

  Tipo: String

  Descrição: (obrigatório) O ID do log do fluxo que você deseja reinicializar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

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

- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Etapas do documento

- `aws:executeAwsApi` :Exclui o log de fluxo especificado no parâmetro `FlowLogId`.
- `aws:executeScript`- Verifica se o log de fluxo foi excluído.

AWSConfigRemediation-DetachAndDeleteInternetGateway

Descrição

O runbook `AWSConfigRemediation-DetachAndDeleteInternetGateway` separa e exclui o gateway da internet especificado. Se alguma EC2 instância da Amazon em sua nuvem privada virtual (VPC) tiver endereços IP elásticos ou IPv4 endereços públicos associados a ela, o runbook falhará.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- InternetGatewayId

Tipo: String

Descrição: (obrigatório) O ID do gateway da Internet que deseja excluir.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

Etapas do documento

- `aws:waitForAwsResourceProperty` :Aceita a ID do gateway privado virtual e espera até que a propriedade de estado do gateway privado virtual mude para `available` ou expire o tempo limite.
- `aws:executeAwsApi` :Recupera uma configuração de gateway privado virtual especificada.
- `aws:branch`- Ramificações com base no valor do VpcAttachments parâmetro.state.

- `aws:waitForAwsResourceProperty`- Aceita a ID do gateway privado virtual e espera até que a VpcAttachments propriedade.state do gateway privado virtual mude para `attached` ou expire.
- `aws:executeAwsApi` :Aceita o ID do gateway privado virtual e o ID da Amazon VPC como entrada e separa o gateway privado virtual da Amazon VPC.
- `aws:waitForAwsResourceProperty`- Aceita a ID do gateway privado virtual e espera até que a VpcAttachments propriedade.state do gateway privado virtual mude para `detached` ou expire.

- `aws:executeAwsApi` :Aceita o ID do gateway privado virtual como entrada e o exclui.

- `aws:waitForAwsResourceProperty` :Aceita o ID do gateway privado virtual como entrada e verifica sua exclusão.

  `aws:executeAwsApi` :Reúne a ID da VPC a partir da ID do gateway da Internet.

- `aws:executeAwsApi` :Separa o ID do gateway da internet da VPC.
- `aws:executeAwsApi` :Exclui o gateway da Internet.

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

Descrição

O `AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` runbook separa e exclui um determinado gateway privado virtual da Amazon Elastic Compute Cloud (Amazon EC2) conectado a uma nuvem privada virtual (VPC) criada com a Amazon Virtual Private Cloud (Amazon VPC).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- VpnGatewayId

  Tipo: String

  Descrição: (obrigatório) O ID do gateway privado virtual a ser excluído.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteVpnGateway`
- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

Etapas do documento

- `aws:waitForAwsResourceProperty` :Aceita a ID do gateway privado virtual e espera até que a propriedade de estado do gateway privado virtual mude para `available` ou expire o tempo limite.
- `aws:executeAwsApi` :Recupera uma configuração de gateway privado virtual especificada.
- `aws:branch`- Ramificações com base no valor do VpcAttachments parâmetro.state.

- `aws:waitForAwsResourceProperty`- Aceita a ID do gateway privado virtual e espera até que a VpcAttachments propriedade.state do gateway privado virtual mude para `attached` ou expire.
- `aws:executeAwsApi` :Aceita o ID do gateway privado virtual e o ID da Amazon VPC como entrada e separa o gateway privado virtual da Amazon VPC.
- `aws:waitForAwsResourceProperty`- Aceita a ID do gateway privado virtual e espera até que a VpcAttachments propriedade.state do gateway privado virtual mude para `detached` ou expire.

- `aws:executeAwsApi` :Aceita o ID do gateway privado virtual como entrada e o exclui.

- `aws:waitForAwsResourceProperty` :Aceita o ID do gateway privado virtual como entrada e verifica sua exclusão.

AWS-DisableIncomingSSHOnPort22

Descrição

O `AWS-DisableIncomingSSHOnPort22` runbook remove regras que permitem tráfego SSH de entrada irrestrito na porta TCP 22 para grupos de segurança.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- SecurityGroupIds

  Tipo: String

  Descrição: (Obrigatório) Uma lista separada por vírgulas dos grupos IDs de segurança para os quais você deseja restringir o tráfego SSH.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Etapas do documento

- `aws:executeAwsApi`- Remove todas as regras que permitem o tráfego SSH de entrada na porta TCP 22 dos grupos de segurança que você especifica no parâmetro. `SecurityGroupIds`

Saídas

DisableIncomingSSHTemplate. RestrictedSecurityGroupIds - Uma lista dos grupos IDs de segurança que tiveram as regras SSH de entrada removidas.

`AWS-DisablePublicAccessForSecurityGroup`

Descrição

Esse runbook desabilita as portas SSH e RDP padrão que são abertas para todos os endereços IP.

> **Important**
>
> Este runbook falha com um "InvalidPermission. NotFound"erro para grupos de segurança que atendem aos dois critérios a seguir: 1) O grupo de segurança está localizado em uma VPC não padrão; e 2) As regras de entrada do grupo de segurança não especificam portas abertas usando todos os quatro padrões a seguir:
>
> - `0.0.0.0/0`
> - `::/0`
> - `SSH or RDP port + 0.0.0.0/0`
> - `SSH or RDP port + ::/0`

> **Note**
>
> Este runbook não está disponível na Regiões da AWS China.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- GroupId

  Tipo: String

  Descrição: (obrigatório) O ID do grupo de segurança para o qual as portas devem ser desabilitadas.
- IpAddressToBlock

  Tipo: String

  Descrição: (Opcional) IPv4 Endereços adicionais dos quais o acesso deve ser bloqueado, no formato`1.2.3.4/32`.

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

Descrição

O `AWSConfigRemediation-DisableSubnetAutoAssignPublicIP` runbook desativa o atributo de endereçamento IPv4 público para a sub-rede que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- SubnetId

  Tipo: String

  Descrição: (Obrigatório) O ID da sub-rede na qual você deseja desativar o atributo de IPv4 endereço público de atribuição automática.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

Etapas do documento

- `aws:executeAwsApi`- Desativa o atributo de IPv4 endereço público de atribuição automática para a sub-rede especificada no parâmetro. `SubnetId`
- `aws:assertAwsResourceProperty` :Verifica se o atributo foi desabilitado.

AWSSupport-EnableVPCFlowLogs

Descrição

O AWSSupport-EnableVPCFlowLogs runbook cria registros de fluxo da Amazon Virtual Private Cloud (Amazon VPC) para sub-redes, interfaces de rede e no seu. VPCs Conta da AWS Se você criar um log de fluxo para uma sub-rede ou VPC, toda interface de rede na sub-rede ou Amazon VPC será monitorada. Os dados do log de fluxo são publicados no grupo de CloudWatch logs Amazon Logs ou no bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Para obter mais informações sobre logs de fluxo, consulte Logs de fluxo no Guia do usuário da Amazon VPC.

Important

As taxas de ingestão e arquivamento de dados para registros vendidos se aplicam quando você publica registros de fluxo no Logs ou no CloudWatch Amazon S3. Para obter mais informações, consulte Precificação de logs de fluxo do .

Executar esta automação (console)

Note

Ao selecionar s3 como destino do log, certifique-se de que a política do bucket permita que o serviço de entrega de log acesse o bucket. Para obter mais informações, consulte Permissões de bucket do Amazon S3 para registros de fluxo

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- DeliverLogsPermissionArn

  Tipo: string

  Descrição: (Opcional) O ARN para a função do IAM que permite que o Amazon Elastic Compute Cloud (EC2Amazon) publique registros de fluxo CloudWatch no grupo de registros de registros em sua conta. Se especificar `s3` para o parâmetro `LogDestinationType`, não forneça um valor para esse parâmetro. Para obter mais informações, consulte Publicar registros de fluxo em CloudWatch registros no Guia do usuário da Amazon VPC.

- LogDestinationARN

  Tipo: string

  Descrição: (opcional) O ARN do recurso no qual os dados de log de fluxo são publicados. Se `cloud-watch-logs` for especificado para o `LogDestinationType` parâmetro, forneça o ARN do grupo de CloudWatch registros no qual você deseja publicar os dados do registro de fluxo. Como alternativa, use `LogGroupName`. Se `s3` for especificado para o parâmetro `LogDestinationType`, você deverá especificar o ARN do bucket do Amazon S3 no qual deseja publicar dados de log de fluxo para esse parâmetro. Você também pode especificar uma pasta no bucket.

  > **Important**
  >
  > Ao escolher `s3` como o, `LogDestinationType` você deve garantir que o bucket selecionado siga as melhores práticas de segurança do Amazon S3 Bucket e que você siga as leis de privacidade de dados da sua organização e região geográfica.

- LogDestinationType

  Tipo: string

Valores válidos: cloud-watch-logs | s3

Descrição: (obrigatório) Determina onde os dados do log de fluxo são publicados. Se você especificar `LogDestinationType` como `s3`, não especifique `DeliverLogsPermissionArn` ou `LogGroupName`.

- LogFormat

  Tipo: string

  Descrição: (opcional) os campos a serem incluídos no log de fluxo e a ordem na qual eles devem aparecer no registro. Para obter uma lista de campos disponíveis, consulte Registros de logs de fluxo no Guia do usuário da Amazon VPC. Se não fornecer um valor para esse parâmetro, o log de fluxo será criado usando o formato padrão. Se você especificar esse parâmetro, deverá especificar pelo menos um campo.

- LogGroupName

  Tipo: string

  Descrição: (Opcional) O nome do grupo de registros de CloudWatch registros em que os dados do registro de fluxo são publicados. Se especificar `s3` para o parâmetro `LogDestinationType`, não forneça um valor para esse parâmetro.

- ResourceIds

  Tipo: StringList

  Descrição: (Obrigatório) Uma lista separada por vírgulas das IDs sub-redes, interfaces de rede elástica ou VPC para as quais você deseja criar um log de fluxo.

- TrafficType

  Tipo: string

  Valores válidos: ACCEPT | REJECT | ALL

  Descrição: (obrigatório) O tipo de tráfego para o log. Você pode registrar em log o tráfego que o recurso aceita ou rejeita ou todo o tráfego.

Permissões obrigatórias do IAM

O parâmetro AutomationAssumeRole requer as seguintes ações para usar o runbook com êxito.

- 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

Política de amostra

```
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "SSM Execution Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "ssm:StartAutomationExecution",
                        "ssm:GetAutomationExecution"
                    ],
                    "Resource": "*"
                },
                {
                    "Sid": "EC2 FlowLogs Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "ec2:CreateFlowLogs",
                        "ec2:DeleteFlowLogs",
                        "ec2:DescribeFlowLogs"
                    ],
                    "Resource": "arn:{partition}:ec2:{region}:{account-id}:{instance|
subnet|vpc|transit-gateway|transit-gateway-attachment}/{resource ID}"
                },
                {
                    "Sid": "IAM CreateRole Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "iam:AttachRolePolicy",
                        "iam:CreateRole",
                        "iam:CreatePolicy",
                        "iam:DeletePolicy",
                        "iam:DeleteRole",
                        "iam:DeleteRolePolicy",
                        "iam:GetPolicy",
                        "iam:GetRole",
```

```
                        "iam:TagRole",
                        "iam:PassRole",
                        "iam:PutRolePolicy",
                        "iam:UpdateRole"
                    ],
                    "Resource": [
                        "arn:{partition}:iam::{account-id}:role/{role name}",
                        "arn:{partition}:iam::{account-id}:role/
AWSSupportCreateFlowLogsRole"
                    ]
                },
                {
                    "Sid": "CloudWatch Logs Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "logs:CreateLogDelivery",
                        "logs:CreateLogGroup",
                        "logs:DeleteLogDelivery",
                        "logs:DeleteLogGroup",
                        "logs:DescribeLogGroups",
                        "logs:DescribeLogStreams"
                    ],
                    "Resource": [
                        "arn:{partition}:logs:{region}:{account-id}:log-group:{log
 group name}",
                        "arn:{partition}:logs:{region}:{account-id}:log-group:{log
 group name}:*"
                    ]
                },
                {
                    "Sid": "S3 Permissions",
                    "Effect": "Allow",
                    "Action": [
                        "s3:GetBucketLocation",
                        "s3:GetBucketPublicAccessBlock",
                        "s3:GetAccountPublicAccessBlock",
                        "s3:GetBucketPolicyStatus",
                        "s3:GetBucketAcl",
                        "s3:ListBucket",
                        "s3:PutObject"
                    ],
                    "Resource": [
                        "arn:{partition}:s3:::{bucket name}",
                        "arn:{partition}:s3:::{bucket name}/*"
```

```
                ]
            }
        ]
    }
```

Etapas do documento

- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `LogDestinationType`.
- `aws:executeScript`- Verifica se o Amazon Simple Storage Service (Amazon S3) de destino potencialmente concede acesso de leitura ou `public` gravação a seus objetos.
- `aws:executeScript` :Cria um grupo de logs se nenhum valor for especificado para o parâmetro `LogDestinationARN` e for especificado `cloud-watch-logs` para o parâmetro `LogDestinationType`.
- `aws:executeScript` :Cria logs de fluxo com base nos valores especificados nos parâmetros do runbook.

`AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch`

Descrição

O `AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch` runbook substitui um log de fluxo existente do Amazon VPC que publica dados do log de fluxo no Amazon Simple Storage Service (Amazon S3) por um log de fluxo que publica dados do log de fluxo no grupo de log Amazon CloudWatch Logs (Logs) que você especificar. CloudWatch

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

- DestinationLogGroup

  Tipo: String

  Descrição: (Obrigatório) O nome do grupo de CloudWatch registros de registros no qual você deseja publicar os dados do registro de fluxo.

- DeliverLogsPermissionArn

  Tipo: String

  Descrição: (Obrigatório) O ARN da função AWS Identity and Access Management (IAM) que você deseja usar e que fornece ao Amazon Elastic Compute Cloud (Amazon EC2) as permissões necessárias para publicar dados de log de fluxo no Logs. CloudWatch

- FlowLogId

  Tipo: String

  Descrição: (obrigatório) O ID do log de fluxo publicado no Amazon S3 que deseja substituir.

- MaxAggregationInterval

  Tipo: inteiro

  Valores válidos: 60 | 600

  Descrição: (opcional) o intervalo máximo de tempo, em segundos, durante o qual um fluxo de pacotes é capturado e agregado em um registro de log de fluxo.

- TrafficType

  Tipo: String

Valores válidos: ACCEPT | REJECT | ALL

Descrição: (obrigatório) O tipo de dados de log de fluxo que deseja registrar e publicar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Etapas do documento

- `aws:executeAwsApi` :Reúne detalhes sobre sua VPC a partir do valor especificado no parâmetro `FlowLogId`.
- `aws:executeAwsApi` :Cria um log de fluxo com base nos valores que especificados para os parâmetros do runbook.
- `aws:assertAwsResourceProperty`- Verifica se o registro de fluxo recém-criado é publicado no Logs. CloudWatch
- `aws:executeAwsApi` :Exclui o log de fluxo para publicação no Amazon S3.
- `aws:executeScript` :Confirma que o log de fluxo publicado no Amazon S3 foi excluído.

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

Descrição

O `AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket` runbook substitui um log de fluxo existente da Amazon VPC que publica dados do log de fluxo no Amazon CloudWatch Logs (CloudWatch Logs) por um log de fluxo que publica dados do log de fluxo no bucket do Amazon Simple Storage Service (Amazon S3) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- Destinos 3 BucketArn

  Tipo: String

  Descrição: (obrigatório) O ARN do bucket do Amazon S3 no qual deseja publicar dados de log de fluxo.
- FlowLogId

  Tipo: String

  Descrição: (Obrigatório) O ID do registro de fluxo que é publicado nos CloudWatch registros que você deseja substituir.
- MaxAggregationInterval

  Tipo: inteiro

  Valores válidos: 60 | 600

  Descrição: (opcional) o intervalo máximo de tempo, em segundos, durante o qual um fluxo de pacotes é capturado e agregado em um registro de log de fluxo.

- TrafficType

  Tipo: String

  Valores válidos: ACCEPT | REJECT | ALL

  Descrição: (obrigatório) O tipo de dados de log de fluxo que deseja registrar e publicar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

Etapas do documento

- `aws:executeAwsApi` :Reúne detalhes sobre sua VPC a partir do valor especificado no parâmetro `FlowLogId`.
- `aws:executeAwsApi` :Cria um log de fluxo com base nos valores que especificados para os parâmetros do runbook.
- `aws:assertAwsResourceProperty` - Verifica se o log de fluxo recém-criado é publicado no Amazon S3.
- `aws:executeAwsApi`- Exclui o registro de fluxo que é publicado no Logs. CloudWatch
- `aws:executeScript`- Confirma que o registro de fluxo publicado no CloudWatch Logs foi excluído.

AWS-ReleaseElasticIP

Descrição

Libere o endereço IP elástico especificado usando o ID da alocação.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AllocationId

  Tipo: String

  Descrição: (obrigatório) O ID de alocação do endereço IP elástico.

AWS-RemoveNetworkACLUnrestrictedSSHRDP

Descrição

O `AWS-RemoveNetworkACLUnrestrictedSSHRDP` runbook remove todas as regras da lista de controle de acesso (ACL) de rede da ACL de rede especificada que permitem o tráfego de entrada de todos os endereços de origem para as portas SSH e RDP padrão. As regras que incluem intervalos de portas que se sobrepõem às portas SSH e RDP padrão não são removidas.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- NetworkAclId

  Tipo: String

  Descrição: (Obrigatório) A ID da ACL de rede da qual você deseja remover regras irrestritas que permitem o tráfego de entrada de todos os endereços de origem para as portas SSH e RDP padrão.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAclEntry`
- `ec2:DescribeNetworkAcls`

Etapas do documento

- `aws:executeScript` :Remove todas as regras de entrada que permitem o tráfego de todos os endereços de origem do grupo de segurança especificado no parâmetro `SecurityGroupId`.

Saídas

RemoveNaclEntriesAndVerify. VerificationMessage - Mensagens de verificação das regras de ACL de rede excluídas com sucesso.

RemoveNaclEntriesAndVerify. RulesDeletedAndApiResponses - As regras de ACL de rede que foram excluídas e as respostas da operação `DeleteNetworkAclEntry` da API.

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules

Descrição

O runbook `AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules` remove todas as regras de entrada do grupo de segurança especificado que permitem o tráfego de todos os endereços de origem.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- SecurityGroupId

Tipo: String

Descrição: (obrigatório) O ID do grupo de segurança do qual deseja remover as regras de entrada que permitem o tráfego de todos os endereços de origem.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

Etapas do documento

- `aws:executeScript` :Remove todas as regras de entrada que permitem o tráfego de todos os endereços de origem do grupo de segurança especificado no parâmetro `SecurityGroupId`.

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

Descrição

O runbook `AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` remove todas as regras do grupo de segurança padrão da nuvem privada virtual (VPC) especificada.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- GroupId

  Tipo: String

  Descrição: (obrigatório) O ID do grupo de segurança do qual deseja remover todas as regras.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

Etapas do documento

- `aws:assertAwsResourceProperty` :Confirma que o grupo de segurança especificado no parâmetro `GroupId` tem o nome padrão.
- `aws:executeScript`: remove todas as regras do grupo de segurança que você especificou no parâmetro `GroupId`.

AWSSupport-SetupIPMonitoringFromVPC

Descrição

`AWSSupport-SetupIPMonitoringFromVPC`cria uma instância do Amazon Elastic Compute Cloud (Amazon EC2) na sub-rede especificada e monitora o destino selecionado IPs (IPv4 ou

IPv6) executando continuamente testes de ping, MTR, traceroute e tracetcp. Os resultados são armazenados nos CloudWatch registros do Amazon Logs e filtros métricos são aplicados para visualizar rapidamente as estatísticas de latência e perda de pacotes em um painel. CloudWatch

Informações adicionais

Os dados de CloudWatch registros podem ser usados para solucionar problemas de rede e analisar se a pattern/trends. Additionally, you can configure CloudWatch alarms with Amazon SNS notifications when packet loss and/or latência atinge um limite. Os dados também podem ser usados ao abrir um caso com AWS Support, para ajudar a isolar um problema rapidamente e reduzir o tempo de resolução ao investigar um problema de rede.

> **Note**
>
> Para limpar os recursos criados pelo `AWSSupport-SetupIPMonitoringFromVPC`, é possível usar o runbook`AWSSupport-TerminateIPMonitoringFromVPC`. Para obter mais informações, consulte `AWSSupport-TerminateIPMonitoringFromVPC`.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- CloudWatchLogGroupNamePrefix

  Tipo: String

  Padrão: `/AWSSupport-SetupIPMonitoringFromVPC`

  Descrição: (Opcional) Prefixo usado para cada grupo de CloudWatch registros criado para os resultados do teste.

- CloudWatchLogGroupRetentionInDays

  Tipo: String

  Valores válidos: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

  Padrão: 7

  Descrição: (Opcional) O número de dias que você deseja manter os resultados de monitoramento de rede.

- InstanceType

  Tipo: String

  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

  Padrão: t3.micro

  Descrição: (Opcional) O tipo de EC2 instância da instância do EC2 Rescue. Tamanho recomendado: t3.micro.

- SubnetId

  Tipo: String

  Descrição: (Obrigatório) O ID de sub-rede para a instância do monitor. Lembre-se de que, se você especificar uma sub-rede privada, deverá garantir que haja acesso à Internet para permitir que a instância do monitor configure o teste (ou seja, instale o agente CloudWatch Logs, interaja com o Systems Manager e CloudWatch).

- Alvo IPs

Tipo: String

Descrição: (Obrigatório) Lista separada por vírgulas de IPv4s e/ou IPv6s para monitorar. Espaços não são permitidos. O tamanho máximo é de 255 caracteres. Lembre-se de que, se você fornecer um IP inválido, a automação falhará e reverterá a configuração de teste.

- TestInstanceSecurityGroupId

  Tipo: String

  Descrição: (Opcional) O ID do grupo de segurança da instância de teste. Se não for especificada, a automação cria uma durante a criação da instância. Certifique-se de que o grupo de segurança permita acesso externo ao monitoramento IPs.

- TestInstanceProfileName

  Tipo: String

  Descrição: (Opcional) O nome de um perfil de instância do IAM existente para a instância de teste. Se não for especificada, a automação cria uma durante a criação da instância. A função deve ter as seguintes permissões:`logs:CreateLogStream`,, `logs:DescribeLogGroupslogs:DescribeLogStreams`, `logs:PutLogEvents` e a AWS Managed Policy`AmazonSSMManagedInstanceCore`.

- TestInterval

  Tipo: String

  Descrição: (Opcional) O número de minutos entre os intervalos de teste. O valor padrão é 1 minuto e o máximo é `10` minutos.

- RetainDashboardAndLogsOnDeletion

  Tipo: String

  Descrição: (Opcional) Especifique `False` a exclusão do CloudWatch painel e dos registros da Amazon ao excluir a CloudFormation pilha da AWS. O valor padrão é `True`. Por padrão, o painel e os registros são mantidos e precisarão ser excluídos manualmente quando não forem mais necessários.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

> **Warning**
>
> É recomendável passar `TestInstanceProfileName` parâmetros ou garantir a existência de proteções de segurança para evitar o uso indevido de permissões mutáveis do IAM.

É recomendável que o usuário que executa a automação tenha a política gerenciada do Amazon SSMAutomation Role IAM anexada. Além disso, o usuário deve ter a política a seguir anexada à sua conta de usuário, grupo ou função:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreateInstanceProfile",
                "iam:GetRole",
                "iam:GetInstanceProfile",
                "iam:DetachRolePolicy",
                "iam:AttachRolePolicy",
                "iam:PassRole",
                "iam:AddRoleToInstanceProfile",
                "iam:GetRolePolicy",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:PutRolePolicy",
                "iam:TagRole"
            ],
            "Resource": [
                "arn:<partition>:iam::<account-id>:role/SetupIPMonitoringFromVPC*",
                "arn:<partition>:iam::<account-id>:instance-profile/
SetupIPMonitoringFromVPC*"
            ],
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateChangeSet",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudwatch:PutDashboard",
                "cloudwatch:DeleteDashboards",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:CreateSecurityGroup",
                "ec2:CreateLaunchTemplate",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcs",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteSecurityGroup",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:CreateTags",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeTags",
                "ec2:DescribeInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeLaunchTemplates",
                "ec2:RevokeSecurityGroupEgress",
                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:PutMetricFilter",
                "logs:PutRetentionPolicy",
                "logs:TagResource",
                "ssm:DescribeInstanceInformation",
                "ssm:GetParameter",
                "ssm:GetParameters",
                "ssm:SendCommand",
                "ssm:ListCommands",
                "ssm:ListCommandInvocations"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
```

```
        }
    ]
}
```

Se o `TestInstanceProfileName` parâmetro for fornecido, as seguintes permissões do IAM não serão necessárias para executar o runbook:

- objetivo: CreateRole
- objetivo: CreateInstanceProfile
- objetivo: DetachRolePolicy
- objetivo: AttachRolePolicy
- objetivo: AddRoleToInstanceProfile
- objetivo: RemoveRoleFromInstanceProfile
- objetivo: DeleteRole
- objetivo: DeleteRolePolicy
- objetivo: DeleteInstanceProfile

Etapas do documento

1. **`aws:executeAwsApi`** :descreve a sub-rede fornecida.
2. **`aws:branch`**- avalie a IPs entrada do Target.

   (IPv6) Se o Target IPs contiver um IPv6:

   `aws:assertAwsResourceProperty`- verifique se a sub-rede fornecida tem um IPv6 pool associado
3. **`aws:executeScript`** :obtenha a arquitetura do tipo de instância e do caminho do parâmetro público para o AMI do Amazon Linux 2 mais recente.
4. **`aws:executeAwsApi`** :obtenha o AMI do Amazon Linux 2 mais recente na Parameter Store.
5. **`aws:executeAwsApi`**: criar um grupo de segurança para o teste na VPC da sub-rede.

   (Limpeza) Se a criação do grupo de segurança falhar:

   `aws:executeAwsApi` - excluir o grupo de segurança criado pela automação, se existir.

6. **aws:executeAwsApi**: permitir a entrada de todo o tráfego de saída no grupo de segurança de teste.

   (Limpeza) Se a criação da regra de saída do grupo de segurança falhar:

   aws:executeAwsApi - excluir o grupo de segurança criado pela automação, se existir.

7. **aws:executeAwsApi**- criar uma função do IAM para a EC2 instância de teste

   (Limpeza) Se a criação da função falhar:

   a. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação, se existir.

   b. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

8. **aws:executeAwsApi**- anexar a política SSMManaged InstanceCore gerenciada da Amazon

   (Limpeza) Se a anexação da política falhar:

   a. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação, se anexada.

   b. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

   c. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

9. **aws:executeAwsApi**- anexe uma política embutida para permitir a configuração de retenções de grupos de CloudWatch registros e a criação de um painel CloudWatch

   (Limpeza) Se a anexação da política em linha falhar:

   a. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação, se criada.

   b. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

   c. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

   d. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

10. **aws:executeAwsApi**: criar um perfil de instância do IAM

    (Limpeza) Se a criação do perfil de instância falhar:

    a. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação, se existir.

    b. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

c. **aws:executeAwsApi**- exclua a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

d. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

e. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

11 **aws:executeAwsApi** - anexe o perfil de instância do IAM ao perfil do IAM.

(Limpeza) Se a associação do perfil de instância e da função falhar:

a. **aws:executeAwsApi** - remova o perfil de instância do IAM da função, se associado.

b. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

c. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

d. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

e. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

f. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

12 **aws:sleep** - aguarde que o perfil de instância fique disponível.

13 **aws:runInstances** - crie a instância de teste na sub-rede especificada e com o perfil de instância criada anteriormente anexado.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

14 **aws:branch**- avalie a IPs entrada do Target.

(IPv6) Se o Target IPs contiver um IPv6:

aws:executeAwsApi- IPv6 atribua um à instância de teste.

15. **aws:waitForAwsResourceProperty** :aguarde até que a instância de teste se torne uma instância gerenciada.

    (Limpeza) Se a etapa falhar:

    a. **aws:changeInstanceState** :encerre a instância de teste.

    b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

    c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

    d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

    e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

    f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

    g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

16. **aws:runCommand** :instale os pré-requisitos de teste:

    (Limpeza) Se a etapa falhar:

    a. **aws:changeInstanceState** :encerre a instância de teste.

    b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

    c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

    d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

    e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

    f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

    g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

17. **aws:runCommand**- valide se os endereços fornecidos IPs são sintaticamente corretos: IPv4 and/or IPv6

    (Limpeza) Se a etapa falhar:

    a. **aws:changeInstanceState** :encerre a instância de teste.

    b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

    c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

18 **aws:runCommand**- defina o teste MTR para cada um dos fornecidos IPs.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

19 **aws:runCommand**- defina o primeiro teste de ping para cada um dos fornecidos IPs.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

20 **aws:runCommand**- defina o segundo teste de ping para cada um dos fornecidos IPs.

(Limpeza) Se a etapa falhar:

a. **`aws:changeInstanceState`** :encerre a instância de teste.

b. **`aws:executeAwsApi`** - remover o perfil de instância do IAM da função.

c. **`aws:executeAwsApi`** - excluir o perfil de instância do IAM criado pela automação.

d. **`aws:executeAwsApi`**- exclua a política CloudWatch embutida da função criada pela automação.

e. **`aws:executeAwsApi`**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **`aws:executeAwsApi`** - excluir o perfil do IAM criado pela automação.

g. **`aws:executeAwsApi`** - excluir o grupo de segurança criado pela automação, se existir.

21. **`aws:runCommand`**- defina o teste de rastreamento para cada um dos fornecidos. IPs

(Limpeza) Se a etapa falhar:

a. **`aws:changeInstanceState`** :encerre a instância de teste.

b. **`aws:executeAwsApi`** - remover o perfil de instância do IAM da função.

c. **`aws:executeAwsApi`** - excluir o perfil de instância do IAM criado pela automação.

d. **`aws:executeAwsApi`**- exclua a política CloudWatch embutida da função criada pela automação.

e. **`aws:executeAwsApi`**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **`aws:executeAwsApi`** - excluir o perfil do IAM criado pela automação.

g. **`aws:executeAwsApi`** - excluir o grupo de segurança criado pela automação, se existir.

22. **`aws:runCommand`**- defina o teste de traceroute para cada um dos fornecidos. IPs

(Limpeza) Se a etapa falhar:

a. **`aws:changeInstanceState`** :encerre a instância de teste.

b. **`aws:executeAwsApi`** - remover o perfil de instância do IAM da função.

c. **`aws:executeAwsApi`** - excluir o perfil de instância do IAM criado pela automação.

d. **`aws:executeAwsApi`**- exclua a política CloudWatch embutida da função criada pela automação.

e. **`aws:executeAwsApi`**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **`aws:executeAwsApi`** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

23 **aws:runCommand**- configurar CloudWatch registros.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

24 **aws:runCommand** - programe cronjobs para executar cada teste a cada minuto.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

25 **aws:sleep** - aguarde até que os testes gerem alguns dados.

26 **aws:runCommand**- defina as retenções de grupos de CloudWatch registros desejadas.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

27 **aws:runCommand**- defina os filtros métricos do grupo de CloudWatch registros.

(Limpeza) Se a etapa falhar:

a. **aws:changeInstanceState** :encerre a instância de teste.

b. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

c. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

d. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

e. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

f. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

g. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

28 **aws:runCommand**- crie o CloudWatch painel.

(Limpeza) Se a etapa falhar:

a. **aws:executeAwsApi**- exclua o CloudWatch painel, se ele existir.

b. **aws:changeInstanceState** :encerre a instância de teste.

c. **aws:executeAwsApi** - remover o perfil de instância do IAM da função.

d. **aws:executeAwsApi** - excluir o perfil de instância do IAM criado pela automação.

e. **aws:executeAwsApi**- exclua a política CloudWatch embutida da função criada pela automação.

f. **aws:executeAwsApi**- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.

g. **aws:executeAwsApi** - excluir o perfil do IAM criado pela automação.

h. **aws:executeAwsApi** - excluir o grupo de segurança criado pela automação, se existir.

Saídas

createCloudWatchDashboards.Output - o URL do painel. CloudWatch

createManagedInstance. InstanceIds - o ID da instância de teste.

AWSSupport-TerminateIPMonitoringFromVPC

Descrição

O `AWSSupport-TerminateIPMonitoringFromVPC` encerra um teste de monitoramento de IP iniciado anteriormente pelo `AWSSupport-SetupIPMonitoringFromVPC`. Dados relacionados ao ID de teste especificado serão excluídos.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- AutomationExecutionId

  Tipo: String

Descrição: (obrigatório) O ID de execução da automação de quando o runbook `AWSSupport-SetupIPMonitoringFromVPC` foi executado anteriormente. Todos os recursos associados a essa ID de execução são excluídos.

- InstanceId

  Tipo: String

  Descrição: (Obrigatório) O ID de instância para a instância do monitor.

- SubnetId

  Tipo: String

  Descrição: (Obrigatório) O ID de sub-rede para a instância do monitor.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

É recomendável que o usuário que executa a automação tenha a política gerenciada do Amazon SSMAutomation Role IAM anexada. Além disso, o usuário deve ter a política a seguir anexada ao seu usuário, grupo ou função:

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Action": [
            "iam:DetachRolePolicy",
            "iam:RemoveRoleFromInstanceProfile",
            "iam:DeleteRole",
            "iam:DeleteInstanceProfile",
            "iam:DeleteRolePolicy"
        ],
        "Resource": [
            "arn:aws:iam::An-AWS-Account-ID:role/AWSSupport/
SetupIPMonitoringFromVPC_*",
            "arn:aws:iam::An-AWS-Account-ID:instance-profile/AWSSupport/
SetupIPMonitoringFromVPC_*"
        ],
        "Effect": "Allow"
    },
```

```
    {
        "Action": [
            "iam:DetachRolePolicy"
        ],
        "Resource": [
            "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "cloudwatch:DeleteDashboards"
        ],
        "Resource": [
            "*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ec2:DescribeTags",
            "ec2:DescribeInstances",
            "ec2:DescribeSecurityGroups",
            "ec2:DeleteSecurityGroup",
            "ec2:TerminateInstances",
            "ec2:DescribeInstanceStatus"
        ],
        "Resource": [
            "*"
        ],
        "Effect": "Allow"
    ]
}
```

Etapas do documento

1. `aws:assertAwsResourceProperty`- InstanceId verificam AutomationExecutionId e estão relacionados ao mesmo teste.
2. `aws:assertAwsResourceProperty`- InstanceId verificam SubnetId e estão relacionados ao mesmo teste.
3. `aws:executeAwsApi` :recupere o grupo de segurança do teste.
4. `aws:executeAwsApi`- exclua o CloudWatch painel.

5. `aws:changeInstanceState` :encerre a instância de teste.
6. `aws:executeAwsApi`: remover o perfil de instância do IAM da função.
7. `aws:executeAwsApi`: excluir o perfil de instância do IAM criado pela automação.
8. `aws:executeAwsApi`- exclua a política CloudWatch embutida da função criada pela automação.
9. `aws:executeAwsApi`- separe a política SSMManaged InstanceCore gerenciada da Amazon da função criada pela automação.
10. `aws:executeAwsApi`: excluir o perfil do IAM criado pela automação.
11. `aws:executeAwsApi`: excluir o grupo de segurança criado pela automação, se existir.

Saídas

Nenhum

AWS WAF

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS WAF Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl
- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

AWS-AddWAFRegionalRuleToRuleGroup

Descrição

O `AWS-AddWAFRegionalRuleToRuleGroup` runbook adiciona uma regra AWS WAF regional existente a um grupo de regras AWS WAF regionais. Somente grupos de regras regionais AWS WAF clássicos são suportados. AWS WAF Os grupos de regras regionais clássicos podem ter no máximo 10 regras.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- RuleGroupId

  Tipo: String

  Descrição: (Obrigatório) O ID do grupo de regras que você deseja atualizar.
- RulePriority

  Tipo: inteiro

  Descrição: (Obrigatório) A prioridade da nova regra. A prioridade da regra determina a ordem na qual as regras em um grupo regional são avaliadas. As regras com um valor menor têm maior prioridade do que as regras com um valor maior. O valor deve ser um inteiro exclusivo. Se você adicionar várias regras a um grupo de regras regional, os valores não precisarão ser consecutivos.
- RuleId

  Tipo: String

  Descrição: (Obrigatório) O ID da regra que você deseja adicionar ao seu grupo de regras regional.
- RuleAction

Tipo: String

Descrição: (Obrigatório) Especifica a ação que é AWS WAF executada quando uma solicitação da web corresponde às condições da regra.

Valores válidos: ALLOW | BLOCK | COUNT

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

Etapas do documento

- Get WAFChange Token (aws:executeAwsApi) - Recupera um token de AWS WAF alteração para garantir que o runbook não envie solicitações conflitantes ao serviço.
- Adicionar WAFRule a WAFRegional RuleGroup (aws:ExecuteScript) - Adiciona a regra especificada ao grupo de regras regional. AWS WAF
- VerifyChangeTokenPropagating (aws: waitForAwsResourceProperty) - Verifica se o token de alteração tem um status de `PENDING` ou`INSYNC`.
- VerifyRuleAddedToRuleGroup (aws:ExecuteScript) - Verifica se a AWS WAF regra especificada foi adicionada ao grupo de regras regionais de destino.

Saídas

- VerifyRuleAddedToRuleGroup. VerifyRuleAddedToRuleGroupResponse - Saída da etapa de verificação de que a nova regra foi adicionada ao grupo de regras regional.
- VerifyRuleAddedToRuleGroup. ListActivatedRulesInRuleGroupResponse - Saída da operação `ListActivatedRulesInRuleGroup` da API.

AWS-AddWAFRegionalRuleToWebAcl

Descrição

O AWS-AddWAFRegionalRuleToWebAcl runbook adiciona uma regra AWS WAF regional existente, um grupo de regras ou uma regra baseada em taxas a uma lista regional AWS WAF clássica de controle de acesso à web (ACL). Este runbook não atualiza as ACLs web regionais AWS WAF clássicas existentes que são gerenciadas pelo. AWS Firewall Manager

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- Web ACLId

  Tipo: String

  Descrição: (Obrigatório) O ID da ACL da web que você deseja atualizar.
- ActivatedRulePriority

  Tipo: inteiro

Descrição: (Obrigatório) A prioridade da nova regra. A prioridade da regra determina a ordem na qual as regras em uma ACL da web são avaliadas. As regras com um valor menor têm maior prioridade do que as regras com um valor maior. O valor deve ser um inteiro exclusivo. Se você adicionar várias regras a uma ACL da web regional, os valores não precisarão ser consecutivos.

- ActivatedRuleRuleId

  Tipo: String

  Descrição: (Obrigatório) O ID da regra regular, regra baseada em taxa ou grupo que você deseja adicionar à Web ACL.

- ActivatedRuleAction

  Tipo: String

  Valores válidos: ALLOW | BLOCK | COUNT

  Descrição: (Opcional) Especifica a ação que é AWS WAF executada quando uma solicitação da web corresponde às condições da regra.

- ActivatedRuleType

  Tipo: String

  Valores válidos: REGULAR | RATE_BASED | GROUP

  Padrão: REGULAR

  Descrição: (Opcional) O tipo de regra que você está adicionando à ACL da web. Embora esse campo seja opcional, observe que, se você tentar adicionar uma `RATE_BASED` regra a uma ACL da web sem definir o tipo, a solicitação falhará porque a solicitação usa como padrão uma regra. `REGULAR`

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`

- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

Etapas do documento

- DetermineWebACLNotEm FMSAnd RulePriority (aws:ExecuteScript) - Verifica se a ACL da AWS WAF web está em uma política de segurança do Firewall Manager e verifica se a ID de prioridade não está em conflito com uma ACL existente.
- AddRuleOrRuleGroupToWebACL (aws:ExecuteScript) - Adiciona a regra especificada à ACL da web. AWS WAF
- VerifyRuleOrRuleGroupAddedToWebAcl (aws:ExecuteScript) - Verifica se a AWS WAF regra especificada foi adicionada à ACL da web de destino.

Saídas

- DetermineWebACLNotDentro FMSAndRulePriority. PrereqResponse: Saída da `DetermineWebACLNotInFMSAndRulePriority` etapa.
- VerifyRuleOrRuleGroupAddedToWebAcl. VerifyRuleOrRuleGroupAddedToWebACLResponse: Saída da `AddRuleOrRuleGroupToWebACL` etapa.
- VerifyRuleOrRuleGroupAddedToWebAcl. ListActivatedRulesOrRuleGroupsInWebACLResponse: Saída da `VerifyRuleOrRuleGroupAddedToWebAcl` etapa.

AWSConfigRemediation-EnableWAFClassicLogging

Descrição

O `AWSConfigRemediation-EnableWAFClassicLogging` runbook permite registrar no Amazon Data Firehose (Firehose) a lista de controle de acesso AWS WAF à web (web ACL) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- DeliveryStreamName

  Tipo: String

  Descrição: (Obrigatório) O nome do stream de entrega do Firehose para o qual você deseja enviar registros.
- Web ACLId

  Tipo: String

  Descrição: (Obrigatório) A ID da ACL AWS WAF da web na qual você deseja ativar o login.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

Etapas do documento

- `aws:executeAwsApi` :Confirma que o fluxo de entrega especificado no `DeliveryStreamName` existe.
- `aws:executeAwsApi`- Reúne o ARN da ACL AWS WAF da web especificada no parâmetro. `WebACLId`
- `aws:executeAwsApi` :Habilita o log da ACL da web.
- `aws:assertAwsResourceProperty`- Verifica se o registro foi ativado na ACL da AWS WAF web.

`AWSConfigRemediation-EnableWAFClassicRegionalLogging`

Descrição

O `AWSConfigRemediation-EnableWAFClassicRegionalLogging` runbook permite registrar no Amazon Data Firehose (Firehose) a lista de controle de acesso AWS WAF à web (ACL) que você especificar.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LogDestinationConfigs

Tipo: String

Descrição: (Obrigatório) O Amazon Resource Name (ARN) do stream de entrega do Firehose para o qual você deseja enviar registros.

- Web ACLId

  Tipo: String

  Descrição: (Obrigatório) A ID da ACL AWS WAF da web na qual você deseja ativar o login.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

Etapas do documento

- `aws:executeAwsApi`- Reúne o ARN da ACL AWS WAF da web especificada no parâmetro. `WebACLId`
- `aws:executeAwsApi` :Habilita o log da ACL da web.
- `aws:assertAwsResourceProperty`- Verifica se o registro foi ativado na ACL da AWS WAF web.

AWSConfigRemediation-EnableWAFV2Logging

Descrição

O `AWSConfigRemediation-EnableWAFV2Logging` runbook permite o registro de uma lista de controle de acesso à web AWS WAF (Web ACL) (AWS WAF V2) com o stream de entrega especificado do Amazon Data Firehose (Firehose).

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- LogDestinationConfigs

  Tipo: String

  Descrição: (Obrigatório) O ARN do stream de entrega do Firehose que você deseja associar à Web ACL.

  > **Note**
  >
  > O ARN do stream de entrega do Firehose deve começar com o prefixo. `aws-waf-logs-` Por exemplo, `aws-waf-logs-us-east-2-analytics`. Para obter mais informações, consulte Amazon Data Firehose.

- WebAclArn

  Tipo: String

  Descrição: (obrigatório) ARN da ACL da web para a qual o log será habilitado.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

Etapas do documento

- `aws:executeScript`- Ativa o registro para a ACL da web AWS WAF V2 e verifica se o registro tem a configuração especificada.

Amazon WorkSpaces

AWS Systems Manager A automação fornece runbooks predefinidos para a Amazon. WorkSpaces Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWS-CreateWorkSpace
- AWSSupport-RecoverWorkSpace

`AWS-CreateWorkSpace`

Descrição

O `AWS-CreateWorkSpace` runbook cria um novo desktop WorkSpaces virtual da Amazon, conhecido como a WorkSpace, com base nos valores que você especifica para os parâmetros de entrada. Para obter informações sobre WorkSpaces, consulte O que é a Amazon WorkSpaces? no Guia de WorkSpaces administração da Amazon.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome. Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.
- BundleId

  Tipo: String

  Descrição: (Obrigatório) O ID do pacote a ser usado para o. WorkSpace
- ComputeTypeName

  Tipo: String

  Valores válidos: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

  Descrição: (Opcional) O tipo de computação para o seu WorkSpace.
- DirectoryId

  Tipo: String

  Descrição: (Obrigatório) O ID do diretório ao qual você WorkSpace deve ser adicionado.
- RootVolumeEncryptionEnabled

Tipo: booliano

Valores válidos: True | False

Padrão: False

Descrição: (Opcional) Determina se o volume raiz do WorkSpace está criptografado.

- RootVolumeSizeGib

  Tipo: inteiro

  Descrição: (Obrigatório) O tamanho do volume raiz do WorkSpace.

- RunningMode

  Tipo: String

  Valores válidos: ALWAYS_ON | AUTO_STOP

  Descrição: (Obrigatório) O modo de execução do WorkSpace.

- RunningModeAutoStopTimeoutInMinutes

  Tipo: inteiro

  Descrição: (Opcional) O tempo após o usuário se desconectar quando WorkSpaces ele para. Especifique um valor em intervalos de 60 minutos.

- Tags

  Tipo: String

  Descrição: (Opcional) Tags que você deseja aplicar ao WorkSpace.

- UserName

  Tipo: String

  Descrição: (Obrigatório) O nome de usuário a ser associado ao WorkSpace.

- UserVolumeEncryptionEnabled

  Tipo: booliano

  Valores válidos: True | False

Padrão: False

Descrição: (Opcional) Determina se o volume do usuário do WorkSpace está criptografado.

- UserVolumeSizeGib

  Tipo: inteiro

  Descrição: (Obrigatório) O tamanho do volume do usuário para WorkSpace o.

- VolumeEncryptionKey

  Tipo: String

  Descrição: (Opcional) A AWS Key Management Service chave simétrica que você deseja usar para criptografar dados armazenados no seu. WorkSpace

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

Etapas do documento

- `aws:executeScript`- Cria um WorkSpace com base nos valores que você especifica para os parâmetros de entrada.
- `aws:waitForAwsResourceProperty`- Verifica o estado do WorkSpace é`AVAILABLE`.

Saídas

`CreateWorkspace.WorkspaceId`

AWSSupport-RecoverWorkSpace

Descrição

O `AWSSupport-RecoverWorkSpace` runbook executa etapas de recuperação no desktop WorkSpaces virtual da Amazon, conhecido como WorkSpace, que você especifica. O runbook

reinicia o e WorkSpace, se o estado persistirUNHEALTHY, restaura ou reconstrói o WorkSpace com base nos valores que você especifica para os parâmetros de entrada. Antes de usar este runbook, recomendamos revisar a solução de WorkSpaces problemas no Guia de WorkSpaces administração da Amazon.

> **Important**
>
> Restaurar ou reconstruir um WorkSpace é uma ação potencialmente destrutiva que pode resultar na perda de dados. Isso ocorre porque o WorkSpace é restaurado a partir do último instantâneo disponível e os dados recuperados dos instantâneos podem ter até 12 horas. A opção de restauração recria o volume raiz e o volume do usuário com base nos snapshots mais recentes. A opção de reconstrução recria o volume do usuário a partir do snapshot mais recente e o recria da imagem associada ao pacote a WorkSpace partir do qual foi criado. WorkSpace Os aplicativos que foram instalados ou as configurações do sistema que foram alteradas após a WorkSpace criação são perdidos. Para obter mais informações sobre restauração e reconstrução WorkSpaces, consulte Restore a WorkSpace e Rebuild WorkSpace a no Amazon WorkSpaces Administration Guide.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (opcional) o nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.

Se nenhum perfil for especificado, o Systems Manager Automation usa as permissões do usuário que inicia este runbook.

- Reconhecer

  Tipo: String

  Valores válidos: yes

  Descrição: (Obrigatório) Digitar sim significa que você entende que as ações de restauração e reconstrução tentarão recuperar o WorkSpace do instantâneo mais recente e que os dados restaurados desses instantâneos podem ter até 12 horas.

- Reinicializar

  Tipo: String

  Valores válidos: sim | não

  Padrão: sim

  Descrição: (Obrigatório) Determina se o WorkSpace é reinicializado.

- Rebuild

  Tipo: String

  Valores válidos: sim | não

  Padrão: não

  Descrição: (Obrigatório) Determina WorkSpace se o foi reconstruído.

- Restaurar

  Tipo: String

  Valores válidos: sim | não

  Padrão: não

  Descrição: (Obrigatório) Determina se o WorkSpace é restaurado.

- WorkspaceId

  Tipo: String

Descrição: (Obrigatório) O ID do WorkSpace que você deseja recuperar.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

Etapas do documento

- `aws:executeAwsApi`- Reúne o estado do WorkSpace que você especifica no `WorkspaceId` parâmetro.
- `aws:assertAwsResourceProperty`- Verifica o estado do WorkSpace é`AVAILABLE`,`ERROR`, `IMPAIREDSTOPPED`, ou`UNHEALTHY`.
- `aws:branch`- Filiais com base no estado do WorkSpace.
- `aws:executeAwsApi`- Inicia WorkSpace o.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Action`.
- `aws:waitForAwsResourceProperty`- Aguarda o WorkSpace status após ser iniciado.
- `aws:waitForAwsResourceProperty`- Espera que o WorkSpace estado mude para`AVAILABLE`, `ERRORIMPAIRED`, ou `UNHEALTHY` depois de ser iniciado.
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após o início.
- `aws:branch`- Filiais com base no estado do WorkSpace após o início.
- `aws:executeAwsApi`- Reúne os instantâneos disponíveis para restaurar ou reconstruir o. WorkSpace
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Reboot`.

- `aws:executeAwsApi`- Reinicia o. WorkSpace
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após o início.
- `aws:waitForAwsResourceProperty`- Espera que o estado do mude WorkSpace para. `REBOOTING`
- `aws:waitForAwsResourceProperty`- Espera que o WorkSpace estado mude para `AVAILABLE`, `ERROR`, ou `UNHEALTHY` depois de ser reinicializado.
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após a reinicialização.
- `aws:branch`- Ramificações com base no estado WorkSpace após a reinicialização.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Restore`.
- `aws:executeAwsApi`- Restaura o. WorkSpace Se a restauração falhar, o runbook tentará reconstruir o. WorkSpace
- `aws:waitForAwsResourceProperty`- Espera que o estado do mude WorkSpace para. `RESTORING`
- `aws:waitForAwsResourceProperty`- Espera que o WorkSpace estado mude para `AVAILABLE`, `ERROR`, ou `UNHEALTHY` depois de ser restaurado.
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após ser restaurado.
- `aws:branch`- Filiais com base no estado da restauração WorkSpace após a restauração.
- `aws:branch` :Ramificações com base no valor especificado para o parâmetro `Rebuild`.
- `aws:executeAwsApi`- Reconstrói o. WorkSpace
- `aws:waitForAwsResourceProperty`- Espera que o estado do mude WorkSpace para. `REBUILDING`
- `aws:waitForAwsResourceProperty`- Espera que o WorkSpace estado mude para `AVAILABLE`, `ERROR`, ou `UNHEALTHY` depois de ser reconstruído.
- `aws:executeAwsApi`- Reúne o estado do WorkSpace após a reconstrução.
- `aws:assertAwsResourceProperty`- Confirma o estado do WorkSpace é`AVAILABLE`.

X-Ray

AWS Systems Manager A automação fornece runbooks predefinidos para. AWS X-Ray Para obter informações sobre como usar runbooks, consulte Trabalhado com runbooks. Para obter informações sobre como visualizar o conteúdo do runbook, consulte Exibir conteúdo do runbook.

Tópicos

- AWSConfigRemediation-UpdateXRayKMSKey

AWSConfigRemediation-UpdateXRayKMSKey

Descrição

O `AWSConfigRemediation-UpdateXRayKMSKey` runbook permite a criptografia em seus AWS X-Ray dados usando uma chave AWS Key Management Service (AWS KMS). Esse runbook só deve ser usado como base para garantir que seus AWS X-Ray dados sejam criptografados de acordo com as melhores práticas mínimas de segurança recomendadas. Recomendamos criptografar vários conjuntos de dados com chaves KMS diferentes.

Executar esta automação (console)

Tipo de documento

Automação

Proprietário

Amazon

Plataformas

Linux, macOS, Windows

Parâmetros

- AutomationAssumeRole

  Tipo: String

  Descrição: (obrigatório) O nome do recurso da Amazon (ARN) do perfil do AWS Identity and Access Management (IAM) que permite que o Systems Manager Automation realize ações em seu nome.
- KeyId

  Tipo: String

  Descrição: (Obrigatório) O nome de recurso da Amazon (ARN), o ID da chave ou o alias da chave KMS que você deseja usar AWS X-Ray para criptografar dados.

Permissões obrigatórias do IAM

O parâmetro `AutomationAssumeRole` requer as seguintes ações para usar o runbook com êxito.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

Etapas do documento

- `aws:executeAwsApi` :Habilita a criptografia em seus dados do X-Ray usando a chave do KMS especificada no parâmetro `KeyId`.
- `aws:waitForAwsResourceProperty` :Espera que o status da configuração da criptografia do X-Ray seja `ACTIVE`.
- `aws:executeAwsApi` :Reúne o ARN da chave especificada no parâmetro `KeyId`.
- `aws:assertAwsResourceProperty` :Verifica se a criptografia foi habilitada no seu X-Ray.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.