aws

ユーザーガイド

AWS Systems Manager 自動化ランブックリファレンス

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

AWS Systems Manager 自動化ランブックリファレンス: ユーザーガイド

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

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

オートメーションランブックリファレンス 1
ランブックの内容を表示する 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 17
AWSSupport-TroubleshootCFNCustomResource 20
AWS-UpdateCloudFormationStack 22
CloudFront 23
AWSConfigRemediation-EnableCloudFrontDefaultRootObject 23
AWSConfigRemediation-EnableCloudFrontAccessLogs 25
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity 27
AWSConfigRemediation-EnableCloudFrontOriginFailover 28
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS 30
CloudTrail 31
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail 32
AWS-EnableCloudTrail 34
AWS-EnableCloudTrailCloudWatchLogs 35
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS 36
AWS-EnableCloudTrailKmsEncryption 38
AWSConfigRemediation-EnableCloudTrailLogFileValidation 40
AWS-EnableCloudTrailLogFileValidation 41
AWS-QueryCloudTrailLogs 42
CloudWatch 44
AWS-ConfigureCloudWatchOnEC2Instance 45
AWS-EnableCWAlarm 46
AWSSupport-TroubleshootCloudWatchAlarm 48
Amazon DocumentDB 56

AWS-EnableDocDbClusterBackupRetentionPeriod 56
CodeBuild 58
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK 58
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject 60
AWS CodeDeploy 61
AWSSupport-TroubleshootCodeDeploy 62
AWS Config 64
AWSSupport-SetupConfig 64
Amazon Connect 67
AWSSupport-AssociatePhoneNumbersToConnectContactFlows 67
AWSSupport-CollectAmazonConnectContactFlowLog 75
AWS Directory Service 80
AWS-CreateDSManagementInstance 81
AWSSupport-TroubleshootADConnectorConnectivity 85
AWSSupport-TroubleshootDirectoryTrust 89
AWS AppSync 92
AWS-EnableAppSyncGraphQLApiLogging 93
Amazon Athena 95
AWS-EnableAthenaWorkGroupEncryptionAtRest 95
DynamoDB 97
AWS-ChangeDDBRWCapacityMode 98
AWS-CreateDynamoDBBackup 100
AWS-DeleteDynamoDbBackup 101
AWSConfigRemediation-DeleteDynamoDbTable 102
AWS-DeleteDynamoDbTableBackups 103
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable 105
AWSConfigRemediation-EnablePITRForDynamoDbTable 106
AWS-EnableDynamoDbAutoscaling 108
AWS-RestoreDynamoDBTable 111
AWS Database Migration Service 114
AWSSupport-TroubleshootDMSTableErrors 114
Amazon EBS 120
AWSSupport-AnalyzeEBSResourceUsage 120
AWS-ArchiveEBSSnapshots 127
AWS-AttachEBSVolume 129
AWSSupport-CalculateEBSPerformanceMetrics 130

AWS-CopySnapshot 137
AWS-CreateSnapshot 138
AWS-DeleteSnapshot 139
AWSConfigRemediation-DeleteUnusedEBSVolume 140
AWS-DeregisterAMIs 142
AWS-DetachEBSVolume 144
AWSConfigRemediation-EnableEbsEncryptionByDefault 145
AWS-ExtendEbsVolume 146
AWSSupport-ModifyEBSSnapshotPermission 148
AWSConfigRemediation-ModifyEBSVolumeType 150
Amazon EC2 152
AWS-ASGEnterStandby 154
AWS-ASGExitStandby 155
AWS-CreateImage 156
AWS-DeleteImage 158
AWS-PatchAsgInstance 159
AWS-PatchInstanceWithRollback 161
AWS-QuarantineEC2Instance 164
AWS-ResizeInstance 166
AWS-RestartEC2Instance 167
AWS-SetupJupyter 168
AWS-StartEC2Instance 171
AWS-StopEC2Instance 172
AWS-TerminateEC2Instance 173
AWS-UpdateLinuxAmi 174
AWS-UpdateWindowsAmi 177
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck 181
AWSConfigRemediation-EnforceEC2InstanceIMDSv2 182
AWSEC2-CloneInstanceAndUpgradeSQLServer 184
AWSEC2-CloneInstanceAndUpgradeWindows 188
AWSEC2-ConfigureSTIG 192
AWSEC2-PatchLoadBalancerInstance 228
AWSEC2-SQLServerDBRestore 229
AWSSupport-ActivateWindowsWithAmazonLicense 235
AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 238
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD 243

AWSSupport-CheckXenToNitroMigrationRequirements ... 249
AWSSupport-ConfigureEC2Metadata ... 252
AWSSupport-ContainEC2Instance ... 255
AWSSupport-CopyEC2Instance ... 266
AWSSupport-EnableWindowsEC2SerialConsole ... 272
AWSSupport-ExecuteEC2Rescue ... 280
AWSSupport-ListEC2Resources ... 283
AWSSupport-ManageRDPSettings ... 286
AWSSupport-ManageWindowsService ... 288
AWSSupport-MigrateEC2ClassicToVPC ... 290
AWSSupport-MigrateXenToNitroLinux ... 297
AWSSupport-ResetAccess ... 309
AWSSupport-ResetLinuxUserPassword ... 312
AWSPremiumSupport-ResizeNitroInstance ... 318
AWSSupport-RestoreEC2InstanceFromSnapshot ... 325
AWSSupport-SendLogBundleToS3Bucket ... 330
AWSSupport-StartEC2RescueWorkflow ... 332
AWSPremiumSupport-TroubleshootEC2DiskUsage ... 342
AWSSupport-TroubleshootEC2InstanceConnect ... 347
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs ... 353
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 ... 468
エラスティックロードバランシング ... 471
AWSConfigRemediation-DropInvalidHeadersForALB ... 472
AWS-EnableCLBAccessLogs ... 473
AWS-EnableCLBConnectionDraining ... 475
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing ... 477
AWSConfigRemediation-EnableELBDeletionProtection ... 478
AWSConfigRemediation-EnableLoggingForALBAndCLB ... 480
AWSSupport-TroubleshootCLBConnectivity ... 481
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing ... 484
AWS-UpdateALBDesyncMitigationMode ... 486
AWS-UpdateCLBDesyncMitigationMode ... 488
Amazon EMR ... 489
AWSSupport-AnalyzeEMRLogs ... 490
AWSSupport-DiagnoseEMRLogsWithAthena ... 496
Amazon OpenSearch Service ... 504
AWSConfigRemediation-DeleteOpenSearchDomain ... 505
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain ... 506
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups ... 507
AWSSupport-TroubleshootOpenSearchRedYellowCluster ... 509

AWSSupport-TroubleshootOpenSearchHighCPU 515
EventBridge 521
AWS-AddOpsItemDedupStringToEventBridgeRule 521
AWS-DisableEventBridgeRule 523
AWS Glue 524
AWSSupport-TroubleshootGlueConnection 524
Amazon FSx 535
AWSSupport-ValidateFSxWindowsADConfig 536
GuardDuty 550
AWSConfigRemediation-CreateGuardDutyDetector 550
IAM 551
AWSSupport-TroubleshootIAMAccessDeniedEvents 552
AWS-AttachIAMToInstance 559
AWS-DeleteIAMInlinePolicy 561
AWSConfigRemediation-DeleteIAMRole 562
AWSConfigRemediation-DeleteIAMUser 564
AWSConfigRemediation-DeleteUnusedIAMGroup 566
AWSConfigRemediation-DeleteUnusedIAMPolicy 567
AWSConfigRemediation-DetachIAMPolicy 569
AWSConfigRemediation-EnableAccountAccessAnalyzer 570
AWSSupport-GrantPermissionsToIAMUser 572
AWSConfigRemediation-RemoveUserPolicies 577
AWSConfigRemediation-ReplaceIAMInlinePolicy 578
AWSConfigRemediation-RevokeUnusedIAMUserCredentials 580
AWSConfigRemediation-SetIAMPasswordPolicy 582
AWSSupport-ContainIAMPrincipal 585
Amazon Kinesis Data Streams 599
AWS-EnableKinesisStreamEncryption 599
AWS KMS 601
AWSConfigRemediation-CancelKeyDeletion 602
AWSConfigRemediation-EnableKeyRotation 603
Lambda 604
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing 605
AWSConfigRemediation-DeleteLambdaFunction 606
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK 607
AWSConfigRemediation-MoveLambdaToVPC 609

AWSSupport-RemediateLambdaS3Event ... 611
AWSSupport-TroubleshootLambdaInternetAccess ... 613
AWSSupport-TroubleshootLambdaS3Event ... 617
Amazon Managed Workflows for Apache Airflow ... 619
AWSSupport-TroubleshootMWAAEnvironmentCreation ... 619
Neptune ... 626
AWS-EnableNeptuneDbAuditLogsToCloudWatch ... 626
AWS-EnableNeptuneDbBackupRetentionPeriod ... 628
AWS-EnableNeptuneClusterDeletionProtection ... 630
Amazon RDS ... 631
AWS-CreateEncryptedRdsSnapshot ... 632
AWS-CreateRdsSnapshot ... 635
AWSConfigRemediation-DeleteRDSCluster ... 636
AWSConfigRemediation-DeleteRDSClusterSnapshot ... 638
AWSConfigRemediation-DeleteRDSInstance ... 639
AWSConfigRemediation-DeleteRDSInstanceSnapshot ... 641
AWSConfigRemediation-DisablePublicAccessToRDSInstance ... 642
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster ... 644
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance ... 646
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance ... 647
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS ... 649
AWSConfigRemediation-EnableMultiAZOnRDSInstance ... 651
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance ... 652
AWSConfigRemediation-EnableRDSClusterDeletionProtection ... 655
AWSConfigRemediation-EnableRDSInstanceBackup ... 656
AWSConfigRemediation-EnableRDSInstanceDeletionProtection ... 658
AWSConfigRemediation-ModifyRDSInstancePortNumber ... 660
AWSSupport-ModifyRDSSnapshotPermission ... 661
AWSPremiumSupport-PostgreSQLWorkloadReview ... 664
AWS-RebootRdsInstance ... 680
AWSSupport-ShareRDSSnapshot ... 681
AWS-StartRdsInstance ... 685
AWS-StartStopAuroraCluster ... 686
AWS-StopRdsInstance ... 687
AWSSupport-TroubleshootConnectivityToRDS ... 688
AWSSupport-TroubleshootRDSIAMAuthentication ... 691

AWSSupport-ValidateRdsNetworkConfiguration 699
Amazon Redshift 704
AWSConfigRemediation-DeleteRedshiftCluster 704
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster 706
AWSConfigRemediation-EnableRedshiftClusterAuditLogging 707
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot 709
AWSConfigRemediation-EnableRedshiftClusterEncryption 710
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting 712
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster 713
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings 715
AWSConfigRemediation-ModifyRedshiftClusterNodeType 717
Amazon S3 719
AWS-ArchiveS3BucketToIntelligentTiering 719
AWS-ConfigureS3BucketLogging 721
AWS-ConfigureS3BucketVersioning 723
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock 724
AWSConfigRemediation-ConfigureS3PublicAccessBlock 727
AWS-CreateS3PolicyToExpireMultipartUploads 729
AWS-DisableS3BucketPublicReadWrite 731
AWS-EnableS3BucketEncryption 732
AWS-EnableS3BucketKeys 733
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy 735
AWSConfigRemediation-RestrictBucketSSLRequestsOnly 736
AWSSupport-TroubleshootS3PublicRead 737
AWSSupport-EmptyS3Bucket 743
AWSSupport-TroubleshootS3EventNotifications 750
AWSSupport-ContainS3Resource 757
Amazon SES 766
AWSSupport-AnalyzeSESMessageSendingStatus 766
SageMaker AI 770
AWS-DisableSageMakerNotebookRootAccess 770
Secrets Manager 773
AWSConfigRemediation-DeleteSecret 773
AWSConfigRemediation-RotateSecret 774
Security Hub 776
AWSConfigRemediation-EnableSecurityHub 776

AWS Shield 778
AWSPremiumSupport-DDoSResiliencyAssessment 778
Amazon SNS 787
AWS-EnableSNSTopicDeliveryStatusLogging 787
AWSConfigRemediation-EncryptSNSTopic 790
AWS-PublishSNSNotification 791
Amazon SQS 792
AWS-EnableSQSEncryption 792
Step Functions 795
AWS-EnableStepFunctionsStateMachineLogging 795
Systems Manager 797
AWS-BulkDeleteAssociation 798
AWS-BulkEditOpsItems 799
AWS-BulkResolveOpsItems 802
AWS-ConfigureMaintenanceWindows 804
AWS-CreateManagedLinuxInstance 806
AWS-CreateManagedWindowsInstance 808
AWSConfigRemediation-EnableCWLoggingForSessionManager 811
AWS-ExportOpsDataToS3 812
AWS-ExportPatchReportToS3 814
AWS-SetupInventory 816
AWS-SetupManagedInstance 820
AWS-SetupManagedRoleOnEC2Instance 821
AWSSupport-TroubleshootManagedInstance 823
AWSSupport-TroubleshootPatchManagerLinux 825
AWSSupport-TroubleshootSessionManager 829
Third-party 835
AWS-CreateJiraIssue 835
AWS-CreateServiceNowIncident 837
AWS-RunPacker 839
Amazon VPC 841
AWS-CloseSecurityGroup 842
AWSSupport-ConfigureDNSQueryLogging 843
AWSSupport-ConfigureTrafficMirroring 847
AWSSupport-ConnectivityTroubleshooter 849
AWSSupport-TroubleshootVPN 853

AWSConfigRemediation-DeleteEgressOnlyInternetGateway 859
AWSConfigRemediation-DeleteUnusedENI 860
AWSConfigRemediation-DeleteUnusedSecurityGroup 861
AWSConfigRemediation-DeleteUnusedVPCNetworkACL 863
AWSConfigRemediation-DeleteVPCFlowLog 864
AWSConfigRemediation-DetachAndDeleteInternetGateway 865
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway 867
AWS-DisableIncomingSSHOnPort22 869
AWS-DisablePublicAccessForSecurityGroup 870
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP 872
AWSSupport-EnableVPCFlowLogs 873
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch 880
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket 882
AWS-ReleaseElasticIP 884
AWS-RemoveNetworkACLUnrestrictedSSHRDP 885
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules 886
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules 887
AWSSupport-SetupIPMonitoringFromVPC 889
AWSSupport-TerminateIPMonitoringFromVPC 903
AWS WAF 906
AWS-AddWAFRegionalRuleToRuleGroup 907
AWS-AddWAFRegionalRuleToWebAcl 909
AWSConfigRemediation-EnableWAFClassicLogging 912
AWSConfigRemediation-EnableWAFClassicRegionalLogging 913
AWSConfigRemediation-EnableWAFV2Logging 915
Amazon WorkSpaces 916
AWS-CreateWorkSpace 917
AWSSupport-RecoverWorkSpace 920
X-Ray 924
AWSConfigRemediation-UpdateXRayKMSKey 924
..... cmxxvi

Systems Manager Automation ランブックのリファレンス

すぐに開始できるように、 は事前定義されたランブック AWS Systems Manager を提供します。これらのランブックは、Amazon Web Services AWS サポート、および によって管理されます AWS Config。ランブックリファレンスでは、Systems Manager が提供する事前定義された各ランブック サポート、および について説明します AWS Config。

> **Important**
>
> AWS Identity and Access Management (IAM) サービスロールを使用して他のサービスを呼び出す自動化ワークフローを実行する場合は、それらのサービスを呼び出すためのアクセス許可をサービスロールに設定する必要がある点に注意してください。この要件は、`AWS-ConfigureS3BucketLogging`、`AWS-CreateDynamoDBBackup`、`AWS-RestartEC2Instance` ランブックなど、すべての AWS オートメーションランブック (`AWS-*` ランブック) に適用されます。この要件は、他の AWS サービスを呼び出すアクションを使用して他の サービスを呼び出す、作成するカスタムオートメーションランブックにも適用されます。たとえば、`aws:executeAwsApi`、`aws:createStack`、または `aws:copyImage` などのアクションを使用する場合は、それらのサービスを呼び出すためのアクセス許可を持つサービスロールを設定する必要があります。ロールに IAM インラインポリシーを追加することで、他の AWS サービスへのアクセス許可を有効にできます。詳細については、「オートメーションインラインポリシーを追加して他の AWS サービスを呼び出す」を参照してください。

このリファレンスには、 AWS、 AWS サポート、 が所有する各 Systems Manager ランブックについて説明するトピックが含まれています AWS Config。ランブックは、関連する によって整理されます AWS のサービス。各ページには、ユーザーがランブックを使用する際に指定する、必須およびオプションのパラメータに関する個別の説明が記載されています。ランブック使用の手順に加え、該当するものがある場合は、オートメーションの出力に関する一覧も示されています。

このリファレンスには、`AWS-CreateManagedLinuxInstanceWithApproval` や `AWS-StopEC2InstanceWithApproval` ランブックなど、承認が必要なランブックの別のページは含まれていません。ランブックの名前に `WithApproval` が含まれている場合は、そのランブックに `aws:approve` アクションが含まれていることを意味します。このアクションでは、指定されたプリンシパルによってアクションか承認または拒否されるまで、一時的にオートメーションを停止します。必要な承認数が得られると、オートメーションが再開されます。

自動化の実行については、「オートメーションを実行する」を参照してください。複数のターゲットにおける自動化の実行については、「ターゲットとレート制御を使用してオートメーションを実行する」を参照してください。

トピック

- ランブックの内容を表示する
- 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
- エラスティックロードバランシング
- Amazon EMR
- Amazon OpenSearch Service

- 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 AI
- Secrets Manager
- Security Hub
- AWS Shield
- Amazon SNS
- Amazon SQS
- Step Functions
- Systems Manager
- Third-party
- Amazon VPC
- AWS WAF
- Amazon WorkSpaces
- X-Ray

ランブックの内容を表示する

Systems Manager コンソールでランブックの内容を表示できます。

ランブックの内容を表示するには

1. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。

   -または-

   AWS Systems Manager ホームページが最初に開いたら、メニューアイコン (☰) を選択してナビゲーションペインを開き、ナビゲーションペインでドキュメントを選択します。
3. [カテゴリ] セクションで、[自動化文書] を選択します。
4. ランブックを選択し、[詳細を表示] を選択します。
5. [Content] タブを選択します。

API Gateway

AWS Systems Manager Automation は、Amazon API Gateway 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

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

AWSConfigRemediation-DeleteAPIGatewayStage

説明

AWSConfigRemediation-DeleteAPIGatewayStage ランブックは、Amazon API Gateway (API Gateway) stage を削除します。このオートメーションを実行する AWS リージョン で有効に AWS Config する必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- StageArn

  タイプ: 文字列

  説明: (必須) 削除される API Gateway ステージの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeScript` - `StageArn` パラメータで指定された API Gateway ステージを削除します。

AWSConfigRemediation-EnableAPIGatewayTracing

説明

AWSConfigRemediation-EnableAPIGatewayTracing ランブックは、Amazon API Gateway (API Gateway) ステージでのトレースを有効にします。このオートメーションを実行する AWS リージョン で を有効にする AWS Config 必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- StageArn

  タイプ: 文字列

  説明: (必須) トレースを有効にする API Gateway ステージの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:GetAutomationExecution

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

ドキュメントステップ

- aws:executeScript - StageArn パラメータで指定された API Gateway ステージでトレースを有効にします。

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

説明

AWSConfigRemediation-UpdateAPIGatewayMethodCaching ランブックは、Amazon API Gateway ステージリソースのキャッシュメソッド設定を更新します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- CachingAuthorizedMethods

タイプ: StringList

説明: (必須) キャッシュを有効にすることを許可されたメソッド。リストは、DELETE、GET、HEAD、OPTIONS、PATCH、POST、PUT のうち、いくつかの組み合わせである必要があります。キャッシュは選択されたメソッドに対して有効になり、選択されていないメソッドでは無効になります。ANY が選択されている場合はすべてのメソッドでキャッシュが有効になり、NONE が選択されている場合はすべてのメソッドでキャッシュが無効になります。

- StageArn

  タイプ: 文字列

  説明: (必須) REST API の API Gateway ステージ ARN。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeScript - ステージリソース ID を入力として受け入れ、UpdateStage API アクションを使用して API Gateway ステージのキャッシュメソッド設定を更新し、更新を検証します。

AWS Batch

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Batch。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-TroubleshootAWSBatchJob

AWSSupport-TroubleshootAWSBatchJob

説明

AWSSupport-TroubleshootAWSBatchJob ランブックは、 AWS Batch ジョブが から STARTINGステータスRUNNABLEに進行するのを妨げる問題のトラブルシューティングに役立ちます。

動作の仕組み

このランブックは、次のチェックを実行します。

- コンピューティング環境が INVALIDまたは DISABLED状態の場合。
- コンピューティング環境の Max vCPUパラメータが、ジョブキュー内のジョブボリュームに対応するのに十分な大きさである場合。
- ジョブが、コンピューティング環境のインスタンスタイプが提供できるよりも多くの vCPUs またはメモリリソースを必要とする場合。
- ジョブを GPU ベースのインスタンスで実行する必要があるが、コンピューティング環境が GPU ベースのインスタンスを使用するように設定されていない場合。
- コンピューティング環境の Auto Scaling グループがインスタンスの起動に失敗した場合。
- 起動されたインスタンスが基盤となる Amazon Elastic Container Service (Amazon ECS) クラスターに参加できる場合、そうでない場合は、AWSSupport-TroubleshootECSContainerInstance ランブックを実行します。
- アクセス許可の問題により、ジョブの実行に必要な特定のアクションがブロックされている場合。

Important

- このランブックは、 RUNNABLEステータスでスタックしているジョブと同じ AWS リージョンで開始する必要があります。
- このランブックは、Amazon ECS AWS Fargate または Amazon Elastic Compute Cloud (Amazon EC2) インスタンスでスケジュールされた AWS Batch ジョブに対して開始できます。Amazon Elastic Kubernetes Service (Amazon EKS) で AWS Batch ジョブのオートメーションが開始されると、開始は停止します。

- インスタンスでジョブを実行できても Amazon ECS クラスターの登録に失敗した場合、このランブックはAWSSupport-TroubleshootECSContainerInstanceオートメーションランブックを開始して、その理由を判断します。詳細については、AWSSupport-TroubleshootECSContainerInstance ランブックを参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- JobId

  タイプ: 文字列

  説明: (必須) RUNNABLEステータスでスタックしている AWS Batch ジョブの ID。

  許可されたパターン: `^[a-f0-9]{8}(-[a-f0-9]{4}){3}-[a-f0-9]{12}(:[0-9]+)?(#[0-9]+)?$`

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

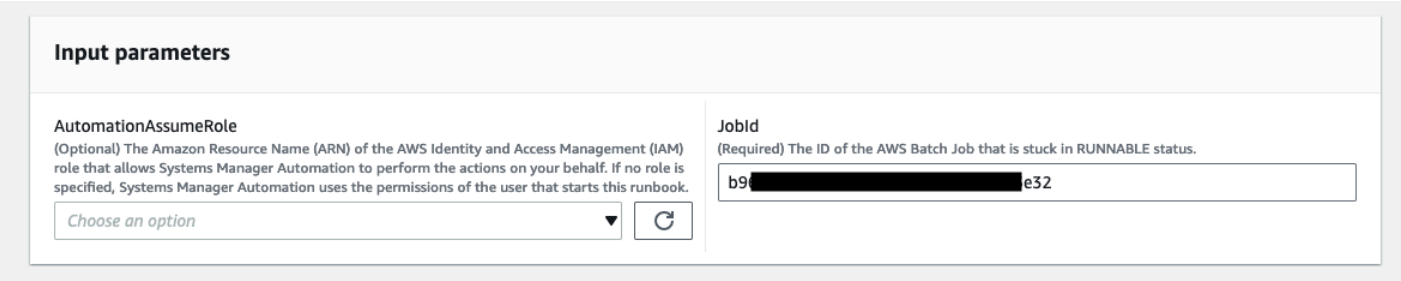
- iam:PassRole
- iam:SimulateCustomPolicy
- iam:SimulatePrincipalPolicy
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- sts:GetCallerIdentity

指示

1. コンソールで AWSSupport-TroubleshootAWSBatchJob AWS Systems Manager に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 次の入力パラメータを入力できます。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
   - JobId (必須):

     RUNNABLE ステータスでスタックしている AWS Batch ジョブの ID。



4. [実行] を選択します。
5. オートメーションが開始されることに注意してください。
6. ドキュメントは以下のステップを実行します。
   - PreflightPermissionChecks:

開始するユーザー/ロールに対してプリフライト IAM アクセス許可チェックを実行します。不足しているアクセス許可がある場合、このステップでは、グローバル出力セクションに欠落している API アクションが表示されます。

- ProceedOnlyIfUserHasPermission:

  ランブックに必要なすべてのアクションに対するアクセス許可があるかどうかに基づいて分岐します。

- AWSBatchJobEvaluation:

  AWS Batch ジョブに対してチェックを実行し、ジョブが存在し、 RUNNABLEステータスであることを確認します。

- ProceedOnlyIfBatchJobExistsAndIsinRunnableState:

  ジョブが存在し、 RUNNABLEステータスであるかどうかに基づいて分岐します。

- BatchComputeEnvironmentEvaluation:

  AWS Batch コンピューティング環境に対してチェックを実行します。

- ProceedOnlyIfComputeEnvironmentChecksAreOK:

  コンピューティング環境チェックが成功したかどうかに基づいて分岐します。

- UnderlyingInfraEvaluation:

  基盤となる Auto Scaling グループまたはスポットフリートリクエストに対してチェックを実行します。

- ProceedOnlyIfInstancesNotJoiningEcsCluster:

  Amazon ECS クラスターに参加していないインスタンスがあるかどうかに基づいて分岐します。

- EcsAutomationRunner:

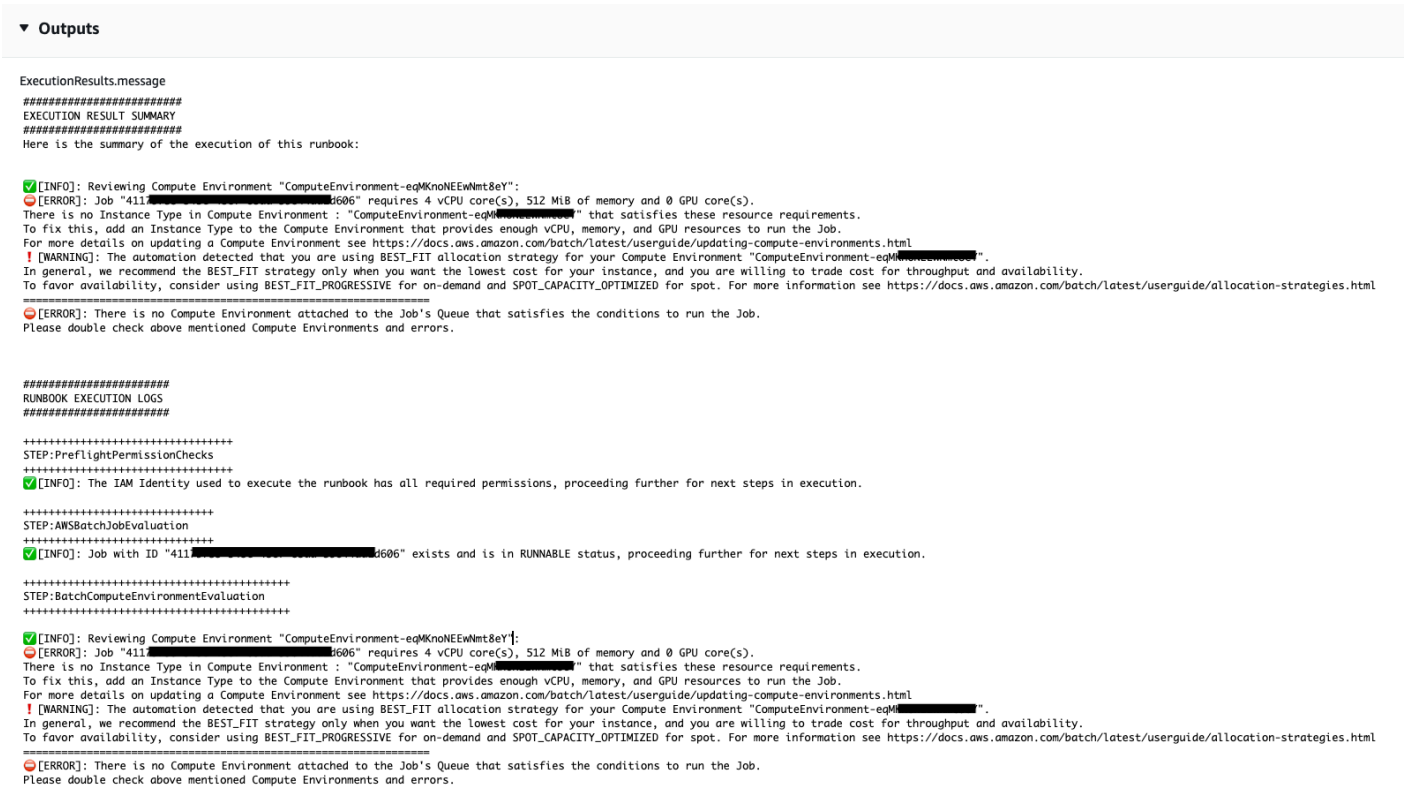
  クラスターに参加していないインスタンスの Amazon ECS オートメーションを実行します。

- ExecutionResults:

  前のステップに基づいて出力を生成します。

7. 完了すると、評価レポートの HTML ファイルの URI が提供されます。

   ランブックが正常に実行された場合のレポートの S3 コンソールリンクと Amazon S3 URI



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS CloudFormation

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS CloudFormation。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-DeleteCloudFormationStack
- AWS-EnableCloudFormationSNSNotification

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

AWS-DeleteCloudFormationStack

説明

AWS CloudFormation スタックを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- StackNameOrId

  タイプ: 文字列

  説明: (必須) 削除する CloudFormation スタックの名前または一意の ID

AWS-EnableCloudFormationSNSNotification

説明

AWS-EnableCloudFormationSNSNotification ランブックは、指定した () スタックの Amazon Simple Notification Service AWS CloudFormation (Amazon SNS AWS CloudFormation) 通知を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- StackArn

  タイプ: 文字列

  説明: (必須) Amazon SNS 通知を有効にする AWS CloudFormation スタックの ARN または名前。
- NotificationArn

  タイプ: 文字列

  説明: (必須) AWS CloudFormation スタックに関連付ける Amazon SNS トピックの ARN。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- CheckCfnSnsLimits (`aws:executeScript`) - 指定した AWS CloudFormation スタックに Amazon SNS トピックの最大数がまだ関連付けられていないことを確認します。
- EnableCfnSnsNotification (`aws:executeAwsApi`) - AWS CloudFormation スタックの Amazon SNS 通知を有効にします。
- VerificationCfnSnsNotification (`aws:executeScript`) - AWS CloudFormation スタックに対して Amazon SNS 通知が有効になっていることを確認します。

出力

CheckCfnSnsLimits.NotificationArnList - AWS CloudFormation スタックの Amazon SNS 通知を受信する ARNs のリスト。

VerificationCfnSnsNotification.VerifySnsTopicsResponse - AWS CloudFormation スタックに対して Amazon SNS 通知が有効になっていることを確認する API オペレーションからのレスポンス。

AWS-RunCfnLint

説明

このランブックでは、AWS CloudFormation Linter ( ) `cfn-python-lint` を使用して、AWS CloudFormation リソース仕様に対して YAML テンプレートと JSON テンプレートを

検証します。AWS-RunCfnLint ランブックでは、リソースプロパティに有効な値が入力されていることを確認するなど、追加のチェックが実行されます。検証が成功しなかった場合、RunCfnLintAgainstTemplate ステップは失敗し、linter ツールの出力がエラーメッセージに表示されます。このランブックは、cfn-lint v0.24.4 を使用しています。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ConfigureRuleFlag

  タイプ: 文字列

  説明: (オプション) --configure-rule パラメータに渡すルールの設定オプションです。

  例: E2001:strict=false、E3012:strict=false。

- FormatFlag

  タイプ: 文字列

  説明: (オプション) 出力形式を指定する --format パラメータに渡す値です。

有効な値: Default | quiet | parseable | json

デフォルト: Default

- IgnoreChecksFlag

  タイプ: 文字列

  説明: （オプション）--ignore-checks パラメータに渡すルールの ID です。これらのルールはチェックされません。

  例: E1001、E1003、W7001

- IncludeChecksFlag

  タイプ: 文字列

  説明: （オプション）`--include-checks` パラメータに渡すルールの ID です。これらのルールはチェックされます。

  例: E1001、E1003、W7001

- InfoFlag

  タイプ: 文字列

  説明: （オプション）`--info` パラメータのオプションです。テンプレート処理に関する追加のログ情報を有効にするオプションを含めます。

  デフォルト: false

- TemplateFileName

  タイプ: 文字列

  説明: S3 バケット内のテンプレートファイルの名前またはキー。

- TemplateS3BucketName

  タイプ: 文字列

  説明: Packer テンプレートを含む S3 バケットの名前です。

- RegionsFlag

  タイプ: 文字列

説明: (オプション) テンプレートを指定された に対してテストするために `--regions`パラメータの に渡す値 AWS リージョン。

例: us-east-1、us-west-1

ドキュメントステップ

RunCfnLintAgainstTemplate – 指定された AWS CloudFormation テンプレートに対して`cfn-python-lint`ツールを実行します。

出力

RunCfnLintAgainstTemplate.output – `cfn-python-lint` ツールからの stdout です。

AWSSupport-TroubleshootCFNCustomResource

説明

`AWSSupport-TroubleshootCFNCustomResource` ランブックは、 AWS CloudFormation スタックがカスタムリソースの作成、更新、削除に失敗した理由を診断するのに役立ちます。ランブックは、カスタムリソースに使用されたサービストークンと返されたエラーメッセージをチェックします。カスタムリソースの詳細を確認すると、ランブックの出力にはカスタムリソースのスタックの動作とトラブルシューティング手順の説明が表示されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- StackName

  タイプ: 文字列

  説明: (必須) カスタムリソースが失敗した AWS CloudFormation スタックの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- validateCloudFormationStack - AWS CloudFormation スタックが同じ AWS アカウント とに存在することを確認します AWS リージョン。
- checkCustomResource - AWS CloudFormation スタックを分析し、失敗したカスタムリソースをチェックし、失敗したカスタムリソースのトラブルシューティング方法に関する情報を出力します。

AWS-UpdateCloudFormationStack

説明

Amazon S3 バケットに保存されている AWS CloudFormation テンプレートを使用して AWS CloudFormation スタックを更新します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- LambdaAssumeRole

  タイプ: 文字列

  説明: (必須) Lambda によって継承されたロールの ARN
- StackNameOrId

  タイプ: 文字列

  説明: (必須) 更新する AWS CloudFormation スタックの名前または一意の ID

- TemplateUrl

  タイプ: 文字列

  説明: (必須) 更新された CloudFormation テンプレートを含む S3 バケットの場所 (例 `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`))

CloudFront

AWS Systems Manager Automation は、Amazon CloudFront 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

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

AWSConfigRemediation-EnableCloudFrontDefaultRootObject

説明

`AWSConfigRemediation-EnableCloudFrontDefaultRootObject` ランブックでは、指定した Amazon CloudFront (CloudFront) ディストリビューションのデフォルトのルートオブジェクトを設定します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- CloudFrontDistributionId

  タイプ: 文字列

  説明: (必須) デフォルトのルートオブジェクトを設定する CloudFront ディストリビューションの ID。
- DefaultRootObject

  タイプ: 文字列

  説明: (必須) ビューワーのリクエストがルート URL を指しているときに CloudFront が返すオブジェクト。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeScript` - `CloudFrontDistributionId` パラメータで指定した CloudFront ディストリビューションのデフォルトのルートオブジェクトを設定します。

AWSConfigRemediation-EnableCloudFrontAccessLogs

説明

AWSConfigRemediation-EnableCloudFrontAccessLogs ランブックでは、指定した Amazon CloudFront (CloudFront) ディストリビューションのアクセスログ記録を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- BucketName

  タイプ: 文字列

  説明: (必須) アクセスログを保存する Amazon Simple Storage Service (Amazon S3) バケットの名前。af-south-1、ap-east-1、eu-south-1、および me-south-1 AWS リージョン のバケットはサポートされていません。
- CloudFrontId

  タイプ: 文字列

  説明: (必須) アクセスログ記録を有効にする CloudFront ディストリビューションの ID。
- IncludeCookies

型: ブール値

有効な値: true | false

説明: (必須) アクセスログに Cookie `true` を含める場合は、このパラメータを に設定します。

- Prefix

  タイプ: 文字列

  説明: (オプション) CloudFront でこのディストリビューションのアクセスログの `filenames` にプレフィックスとして使用するオプションの文字列 (`myprefix/` など)。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

> **Note**
>
> `s3:GetBucketLocation` API は、同じアカウントの S3 バケットにのみ使用できます。クロスアカウント S3 バケットには使用できません。

ドキュメントステップ

- `aws:executeScript` - `CloudFrontDistributionId` パラメータで指定した CloudFront ディストリビューションのアクセスログ記録を有効にします。

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

説明

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity ランブックは、指定した Amazon CloudFront (CloudFront) ディストリビューションのオリジンアクセスアイデンティティを有効にします。このオートメーションにより、指定した CloudFront ディストリビューションのオリジンアクセスアイデンティティを含まない Amazon Simple Storage Service (Amazon S3) オリジンタイプのすべてのオリジンに対して、同じ CloudFront オリジンアクセスアイデンティティが割り当てられます。このオートメーションは、CloudFront が Amazon S3 バケット内のオブジェクトにアクセスするためのオリジンアクセスアイデンティティに読み取りアクセス許可を付与しません。アクセスを許可するには、Amazon S3 バケットのアクセス許可を更新する必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- CloudFrontDistributionId

  タイプ: 文字列

  説明: (必須) オリジンフェイルオーバーを有効にする CloudFront ディストリビューションの ID。

- OriginAccessIdentityId

  タイプ: 文字列

  説明: (必須) オリジンに関連付ける CloudFront オリジンアクセスアイデンティティの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeScript - CloudFrontDistributionId パラメータで指定した CloudFront ディストリビューションのオリジンアクセスアイデンティティを有効にし、オリジンアクセスアイデンティティが割り当てられていることを確認します。

AWSConfigRemediation-EnableCloudFrontOriginFailover

説明

AWSConfigRemediation-EnableCloudFrontOriginFailover ランブックは、指定した Amazon CloudFront (CloudFront) ディストリビューションのオリジンフェイルオーバーを有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- CloudFrontDistributionId

  タイプ: 文字列

  説明: (必須) オリジンフェイルオーバーを有効にする CloudFront ディストリビューションの ID。
- OriginGroupId

  タイプ: 文字列

  説明: (必須) オリジングループの ID。
- PrimaryOriginId

  タイプ: 文字列

  説明: (必須) オリジングループ内のプライマリオリジンの ID。
- SecondaryOriginId

  タイプ: 文字列

  説明: (必須) オリジングループ内のセカンダリオリジンの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

- cloudfront:GetDistributionConfig
- cloudfront:UpdateDistribution

ドキュメントステップ

- aws:executeScript - CloudFrontDistributionId パラメータで指定した CloudFront ディストリビューションのオリジンフェイルオーバーを有効にし、フェイルオーバーが有効であることを確認します。

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

説明

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS ランブックにより、指定した Amazon CloudFront (CloudFront) ディストリビューションのビューワープロトコルポリシーを有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- CloudFrontDistributionId

タイプ: 文字列

説明: (必須) ビューワープロトコルポリシーを有効にする CloudFront ディストリビューションの ID。

- ViewerProtocolPolicy

  タイプ: 文字列

  有効な値: https-only、redirect-to-https

  説明: (必須) ビューワーがオリジン内のファイルにアクセスするために使用できるプロトコル。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeScript - CloudFrontDistributionId パラメータで指定した CloudFront ディストリビューションのビューワープロトコルポリシーを有効にし、ポリシーが割り当てられたことを確認します。

CloudTrail

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS CloudTrail。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

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

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

説明

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail ランブックは、複数の AWS リージョン から任意の Amazon Simple Storage Service AWS CloudTrail (Amazon S3) バケットにログファイルを配信する (CloudTrail) 証跡を作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- BucketName

タイプ: 文字列

説明: (必須) ログをアップロードする Amazon S3 バケットの名前。

- keyPrefix

  タイプ: 文字列

  説明: (オプション) ログファイル配信用に指定したバケット名の後に付く Amazon S3 キープレフィックス。

- TrailName

  タイプ: 文字列

  説明: (必須) 作成する CloudTrail 証跡の名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeAwsApi - 証跡名と Amazon S3 バケット名を入力として受け入れ、CloudTrail 証跡を作成します。
- aws:executeAwsApi - 作成した証跡の口グ記録を有効にし、指定した Amazon S3 バケットへの口グ配信を開始します。

- `aws:assertAwsResourceProperty` - CloudTrail 証跡が作成されていることを検証します。

AWS-EnableCloudTrail

説明

AWS CloudTrail 証跡を作成し、S3 バケットへのログ記録を設定します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- S3BucketName

  タイプ: 文字列

  説明: (必須) ログファイルの発行用に指定された S3 バケットの名前。

> **Note**
>
> S3 バケットが存在し、バケットポリシーで CloudTrail にバケットへの書き込み権限を付与する必要があります。詳細については、「CloudTrail の Amazon S3 バケットポリシー」を参照してください。

- TrailName

  タイプ: 文字列

  説明: (必須) 新しい証跡の名前。

AWS-EnableCloudTrailCloudWatchLogs

説明

このランブックは、1 つ以上の AWS CloudTrail 証跡の設定を更新して、Amazon CloudWatch Logs ロググループにイベントを送信します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム

(ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- CloudWatchLogsLogGroupArn

  タイプ: 文字列

  説明: (必須) CloudTrail ログが配信される CloudWatch Logs ロググループの ARN。 CloudTrail

- CloudWatchLogsRoleArn

  タイプ: 文字列

  説明: (必須) CloudWatch Logs Logs が指定されたロググループに書き込むために引き受ける IAM ロールの ARN。

- TrailNames

  タイプ: StringList

  説明: (必須) CloudWatch Logs にイベントを送信する CloudTrail 証跡の名前のカンマ区切りリスト。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeScript` - 指定された CloudTrail 証跡を更新して、指定された CloudWatch Logs ロググループにイベントを配信します。

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

説明

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS ランブックは、指定した AWS CloudTrail () カスタマーマネージドキーを使用して AWS Key Management Service (CloudTrail AWS KMS) 証跡を暗号化します。このランブックは、推奨される最小限セキュリティのベストプラクティスに従って CloudTrail 証跡が暗号化されるようにするための、ベースラインとしてのみ使用するようにします。複数の証跡は、それぞれ異なる KMS キーを使用して暗号化することをお勧めします。CloudTrail ダイジェストファイルは暗号化されません。以前に証跡trueの EnableLogFileValidationパラメータを に設定したことがある場合は、AWS CloudTrail 「ユーザーガイド」のCloudTrail 予防セキュリティのベストプラクティス」トピックの AWS KMS 「マネージドキーによるサーバー側の暗号化の使用」セクションを参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- KMSKeyId

  タイプ: 文字列

  説明: (必須) TrailName パラメータで指定した証跡の暗号化に使用する、カスタマーマネージドキーの ARN、キー ID、またはキーエイリアス。
- TrailName

  タイプ: 文字列

説明:(必須) 更新して暗号化する証跡の ARN または名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeAwsApi - TrailName パラメータで指定された証跡の暗号化を有効にします。
- aws:executeAwsApi - KMSKeyId パラメータで指定したカスタマーマネージドキーの ARN を収集します。
- aws:assertAwsResourceProperty - CloudTrail 証跡で暗号化が有効になっているかを確認します。

AWS-EnableCloudTrailKmsEncryption

説明

このランブックは、 AWS Key Management Service （ AWS KMS) 暗号化を使用する 1 つ以上の AWS CloudTrail 証跡の設定を更新します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- KMSKeyId

  タイプ: 文字列

  説明: (必須) `TrailName`パラメータで指定した証跡の暗号化に使用するカスタマーマネージドキーの のキー ID。値には、「alias/」というプレフィックスが付いたエイリアス名、エイリアスに完全に指定された ARN、またはキーに完全に指定された ARN を使用できます。

- TrailNames

  タイプ: StringList

  説明: (必須) 更新する証跡のカンマ区切りリストを暗号化します。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeScript` - `TrailName`パラメータで指定した証跡で AWS KMS 暗号化を有効にします。

AWSConfigRemediation-EnableCloudTrailLogFileValidation

説明

AWSConfigRemediation-EnableCloudTrailLogFileValidation ランブックは、証 AWS CloudTrail 跡のログファイルの検証を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- TrailName

  タイプ: 文字列

  説明: (必須) ログの検証を有効化する証跡の名前または Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution

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

ドキュメントステップ

- aws:executeAwsApi - TrailName パラメータで指定する AWS CloudTrail 証跡のログ検証を有効化します。
- aws:assertAwsResourceProperty - 証跡についてのログ検証が有効になっていることを確認します。

AWS-EnableCloudTrailLogFileValidation

説明

AWS-EnableCloudTrailLogFileValidation ランブックは、指定した AWS CloudTrail 証跡のログファイルの検証を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム

(ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- TrailNames

  タイプ: StringList

  説明: (必須) ログ検証を有効にする CloudTrail 証跡の名前のカンマ区切りリスト。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeScript` - `TrailNames`パラメータで指定した AWS CloudTrail 証跡のログ検証を有効にします。

AWS-QueryCloudTrailLogs

説明

`AWS-QueryCloudTrailLogs` ランブックは、 AWS CloudTrail (CloudTrail) ログを含む任意の Amazon Simple Storage Service (Amazon S3) バケットから Amazon Athena テーブルを作成します。テーブルを作成すると、自動化は指定した SQL クエリを実行した後、テーブルを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- クエリ

  タイプ: 文字列

  説明: (必須) 実行する SQL クエリ。
- SourceBucketPath

  タイプ: 文字列

  説明: (必須) クエリする CloudTrail ログファイルを含む Amazon S3 バケットの名前。
- TableName

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Athena テーブルの名前。

  デフォルト: cloudtrail_logs

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `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

ドキュメントステップ

- aws:executeAwsApi - Athena テーブルを作成します。
- aws:executeAwsApi - Query パラメータで指定したクエリ文字列を実行します。
- aws:executeScript - ポーリングを行い、クエリが完了するのを待ちます。
- aws:executeAwsApi - クエリの結果を取得します。
- aws:executeAwsApi - 自動化によって作成されたテーブルを削除します。

CloudWatch

AWS Systems Manager 自動化は、Amazon CloudWatch 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

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

AWS-ConfigureCloudWatchOnEC2Instance

説明

マネージドインスタンスの Amazon CloudWatch の詳細なモニタリングを有効または無効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: 文字列

  説明: (必須) CloudWatch のモニタリングを有効にする Amazon EC2 インスタンスの ID。
- プロパティ

  タイプ: 文字列

  説明: (オプション) このパラメータはサポートされていません。下位互換性のためにここに記載されています。
- ステータス

有効な値: Enabled | Disabled

説明: (オプション) CloudWatch を有効、または無効にするかを指定します。

デフォルト: Enabled

ドキュメントステップ

configureCloudWatch - Amazon EC2 インスタンスで、指定されたステータスで CloudWatch を設定します。

出力

このオートメーションには出力はありません。

AWS-EnableCWAlarm

説明

AWS-EnableCWAlarm ランブックは、 にまだリソースがない AWS リソースに対して Amazon CloudWatch (CloudWatch) AWS アカウント アラームを作成します。CloudWatch アラームは、次の AWS リソースに対して作成されます。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンス
- Amazon Elastic Block Store (Amazon EBS) ボリューム
- Amazon Simple Storage Service (Amazon S3) の バケット
- Amazon Relational Database Service (Amazon RDS) クラスター

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ComparisonOperator

  タイプ: 文字列

  有効な値: GreaterThanOrEqualToThreshold | GreaterThanThreshold | GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpperThreshol | LessThanLowerThreshold | LessThanOrEqualToThreshold | LessThanThreshold

  説明: (必須) 指定された統計としきい値を比較するときに使用する算術演算。
- MetricName

  タイプ: 文字列

  説明: (必須) アラームに関連付けられたメトリクスの名前。
- 期間

  タイプ: 整数

  有効な値: 10 | 30 | 60 | 60 の倍数

  説明: (必須) 統計が適用される秒単位の期間。
- ResourceARNs

  タイプ: StringList

  説明: (必須) CloudWatch アラームを作成するリソースの ARNs のカンマ区切りリスト
- 統計

  タイプ: 文字列

有効な値: Average | Maximum | Minimum | SampleCount | Sum

説明: (必須) アラームに関連付けられたメトリクスの統計。

- Threshold

  タイプ: 整数

  説明: (必須) 指定された統計と比較する値。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- cloudwatch:PutMetricAlarm

ドキュメントステップ

- aws:executeScript - パラメータ で指定したリソースのランブックパラメータで指定された値に従って CloudWatch ResourceARNs アラームを作成します。

出力

EnableCWAlarm.FailedResources: CloudWatch アラームが作成されなかったリソース ARNs のマップリストと失敗の理由。

EnableCWAlarm.SuccessfulResources: CloudWatch アラームが正常に作成されたリソース ARNs のリスト。

AWSSupport-TroubleshootCloudWatchAlarm

説明

AWSSupport-TroubleshootCloudWatchAlarm ランブックは、設定ミスや問題のある Amazon CloudWatch (CloudWatch) アラームの問題を特定してトラブルシューティングするのに役立ちます。 AWS APIsと既知のアラーム評価ロジックを活用して、モニタリング対象メトリクスのデータポイントの遅延や欠落を検出します。これにより、アラームアクションの欠落や遅延が発生する可能性があります。このランブックは、Amazon CloudWatch (CloudWatch) アラーム関連の問題を調査して解決するための構造化されたアプローチを提供します。

動作の仕組み

ランブックは次のステップAWSSupport-TroubleshootCloudWatchAlarmを実行します。

- Amazon CloudWatch (CloudWatch) アラームの詳細と AlarmTriggerTimestampパラメータの値を検証して、2,592,000 秒 (30 日) 以内かどうかを確認します。
- アラームが Metric または Metric Math に基づいているか、または Anomaly Detector アラームであるかどうかを確認します。
- アラームのデータ不足がないかどうかを確認します。
- アラームで使用されるメトリクス (複数可) がListMetrics値と一致するかどうかを確認します。
- 特定のタイムスタンプでメトリクスにデータポイント (複数可) がないかどうかを確認します。
- 特定のタイムスタンプの最新の履歴を取得します。
- メトリクスの遅延または欠落 (複数可) が原因でアラームがトリガーされなかったかどうかを確認します。
- アラームの有効なアクション (複数可) が配信されたかどうかを確認します。
- すべての診断結果を組み合わせたトラブルシューティングレポートを生成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager AWSSupport-TroubleshootCloudWatchAlarmで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):
     - 型: String
     - 説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。

- CloudWatchMetricAlarmName (必須):
  - 型: String
  - 説明: (必須) トラブルシューティングする Amazon CloudWatch (CloudWatch) メトリクスアラームの名前。
  - 許可されたパターン: ^[a-zA-Z0-9.:;,\\-_&()]{1,255}$
- AlarmTriggerTimestamp (必須):
  - 型: String
  - 説明: (必須) アラームの問題が発生したときの UTC タイムスタンプ。この情報は、問題をトラブルシューティングし、発生したコンテキストを理解するために不可欠です。タイムスタンプ値は、今日から過去 30 日以内の時刻で、 の形式である必要がありますYYYY-MM-DDTHH:mm:ssZ。例: 2024-10-29T09:04:00Z
  - 許可されたパターン: ^(\\d{4})-(\\d{2})-(\\d{2})T(\\d{2}):(\\d{2}):(\\d{2})Z$

4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - **VerifyRunbookInputs**

     Amazon CloudWatch (CloudWatch) アラームの詳細と AlarmTriggerTimestampパラメータの値を検証して、2,592,000 秒 (30 日) 以内かどうかを確認します。
   - **UpdateSSMDocumentInputChecksVariable**

     VerifyRunbookInputs ステップSSMDocumentInputChecksの値SSMDocumentInputChecksで変数を更新します。
   - **BranchOnAlarmIsVerified**

     Runbook の入力検証AlarmTriggerTimestampと の分岐CloudWatchAlarmName。
   - **CheckMetricAlarmType**

     アラームが Metric または Metric Math に基づいているか、または Anomaly Detector アラームであるかどうかを確認します。
   - **CheckAlarmInInsufficientDataState**

     アラームのデータ不足がないかどうかを確認します。
   - **UpdateInsufficientDataChecksVariable**

CheckAlarmInInsufficientDataState ステップInsufficientDataChecksの値InsufficientDataChecksで変数を更新します。

- **BranchOnAlarmHasInsufficientData**

  CheckAlarmInInsufficientDataState ステップAlarmHasInsufficientDataの値の分岐。デフォルトのステップは ですCheckMetricMismatch。

- **CheckMetricMismatch**

  アラームで使用されるメトリクス (複数可) がListMetrics値と一致するかどうかを確認します。

- **UpdateMetricMismatchChecksVariable**

  CheckMetricMismatch ステップMetricMismatchChecksの値MetricMismatchChecksで変数を更新します。

- **BranchOnMetricsMatched**

  CheckMetricMismatch ステップMetricsMatchedの値の分岐。デフォルトのステップは ですCheckMissingDatapoint。

- **CheckMissingDatapoint**

  特定のタイムスタンプでメトリクスにデータポイント (複数可) がないかどうかを確認します。

- **UpdateMetricMissingDatapointsChecksVariable**

  CheckMissingDatapoint ステップMetricMissingDatapointsChecksの値MetricMissingDatapointsChecksで変数を更新します。

- **BranchOnMetricMissingDatapoint**

  CheckMissingDatapoint ステップMetricMissingDatapointの値の分岐。デフォルトのステップは ですGetAlarmHistoryDetails。

- **GetAlarmHistoryDetails**

  特定のタイムスタンプの最新の履歴を取得します。

- **UpdateAlarmHistoryChecksVariable**

  GetAlarmHistoryDetails ステップAlarmHistoryChecksの値AlarmHistoryChecksで変数を更新します。

- **BranchOnAlarmHistoryFound**

GetAlarmHistoryDetails ステップAlarmHistoryFoundの値の分岐。デフォルトのステップは ですCheckDelayedMetric。

- **CheckDelayedMetric**

  メトリクスの遅延または欠落 (複数可) が原因でアラームがトリガーされなかったかどうかを確認します。

- **UpdateDelayedMetricChecksVariable**

  CheckDelayedMetric ステップDelayedMetricChecksの値DelayedMetricChecksで変数を更新します。

- **BranchOnMetricDelayedAndDatapointsMeetThreshold**

  CheckDelayedMetric ステップの MetricDelayedおよび DatapointsMeetThreshold値のブランチ。デフォルトのステップは ですGenerateReport。

- **CheckActionDelivered**

  アラームの有効なアクション (複数可) が配信されたかどうかを確認します。

- **UpdateActionDeliveredChecksVariable**

  ActionDeliveredChecks CheckActionDelivered ステップからの出力ActionDeliveredChecksで変数を更新します。

- **GenerateReport**

  前のステップの出力をコンパイルし、レポートを出力します。

7. 実行が完了したら、出力セクションで実行の詳細な結果を確認します。

- GenerateReport.Report

  提供された Amazon CloudWatch (CloudWatch) メトリクスアラームのレポート。

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

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する

- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

Amazon DocumentDB

AWS Systems Manager Automation は、Amazon DocumentDB (MongoDB 互換) 用の事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-EnableDocDbClusterBackupRetentionPeriod

AWS-EnableDocDbClusterBackupRetentionPeriod

説明

AWS-EnableDocDbClusterBackupRetentionPeriod ランブックは、指定した Amazon DocumentDB クラスターのバックアップ保持期間を有効にします。この機能は、自動バックアップが保持される合計日数を設定します。クラスターを変更するには、クラスターが のエンジンタイプで使用可能な状態である必要がありますdocdb。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- DBClusterResourceId

  タイプ: 文字列

  説明: (必須) バックアップ保持期間を有効にする Amazon DocumentDB クラスターのリソース ID。

- BackupRetentionPeriod

  タイプ: 整数

  説明: (必須) 自動バックアップが保持される日数。7 ~ 35 日の値にする必要があります。

- PreferredBackupWindow

  タイプ: 文字列

  説明: (オプション) 協定世界時 (UTC) の 1 日あたりの時間範囲。形式は hh24:mm-hh24:mm、例えば 07:14-07:44 です。値は 30 分以上でなければならず、希望するメンテナンスウィンドウと競合することはできません。

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

ドキュメントステップ

- GetDocDbClusterIdentifier (`aws:executeAwsApi`) - 指定されたリソース ID を使用して Amazon DocumentDB クラスター識別子を返します。

- VerifyDocDbEngine (aws:assertAwsResourceProperty) - Amazon DocumentDB エンジンタイプが であることを確認しdocdb、他の Amazon RDS エンジンタイプの不注意による変更を防止します。
- VerifyDocDbStatus (aws:waitAwsResourceProperty) - Amazon DocumentDB クラスターのステータスが であることを確認しますavailable。
- ModifyDocDbRetentionPeriod (aws:executeAwsApi) - 指定された Amazon DocumentDB クラスターに指定された値を使用して保持期間を設定します。
- VerifyDocDbBackupsEnabled (aws:executeScript) - Amazon DocumentDB クラスターの保持期間と、指定された場合は優先バックアップウィンドウが正常に設定されていることを確認します。

出力

ModifyDocDbRetentionPeriod.ModifyDbClusterResponse - ModifyDBCluster API オペレーションからのレスポンス。

VerifyDocDbBackupsEnabled.VerifyDbClusterBackupsEnabledResponse - Amazon DocumentDB クラスターが正常に変更されたことを確認するVerifyDocDbBackupsEnabledステップからの出力。

CodeBuild

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS CodeBuild。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK
- AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK

説明

AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK ランブックは、指定した AWS CodeBuild () カスタマーマネージドキーを使用して AWS Key Management Service (CodeBuild AWS KMS) プロジェクトのビルドアーティファクトを暗号化します。このオートメーションを実行する AWS リージョン で を有効にする AWS Config 必要があります。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- KMSKeyId

  タイプ: 文字列

  説明: (必須) `ProjectId` パラメータで指定した CodeBuild プロジェクトの暗号化に使用する AWS KMS カスタマーマネージドキーの Amazon リソースネーム (ARN)。
- ProjectId

  タイプ: 文字列

  説明: (必須) ビルドアーティファクトを暗号化する CodeBuild プロジェクトの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

- codebuild:BatchGetProjects
- codebuild:UpdateProject
- config:GetResourceConfigHistory

ドキュメントステップ

- aws:executeAwsApi - プロジェクト ID から CodeBuild プロジェクトの名前を収集します。
- aws:executeAwsApi - ProjectId パラメータで指定された CodeBuild プロジェクトの暗号化を有効にします。
- aws:assertAwsResourceProperty - CodeBuild プロジェクトで暗号化が有効になっているかを確認します。

出力

UpdateLambdaConfig.UpdateFunctionConfigurationResponse - UpdateFunctionConfiguration API コールからの応答。

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

説明

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject ランブックは、指定した AWS CodeBuild (CodeBuild) プロジェクトから AWS_ACCESS_KEY_IDおよび AWS_SECRET_ACCESS_KEY環境変数を削除します。このオートメーションを実行する AWS リージョン で を有効にする AWS Config 必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- ResourceId

  タイプ: 文字列

  説明: (必須) アクセスキー環境変数が削除される CodeBuild プロジェクトの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeScript` - `ResourceId` パラメータで指定された CodeBuild プロジェクトのアクセスキー環境変数を削除します。

AWS CodeDeploy

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS CodeDeploy。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-TroubleshootCodeDeploy

AWSSupport-TroubleshootCodeDeploy

説明

AWSSupport-TroubleshootCodeDeploy ランブックは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで AWS CodeDeploy デプロイが失敗した理由を診断するのに役立ちます。ランブックは、問題の解決やさらなるトラブルシューティングに役立つ手順を出力します。将来、同様の問題を回避するのに役立つ CodeDeploy のベストプラクティスも提供されています。

このランブックは、以下の問題の解決に役立ちます。

- CodeDeploy エージェントは Amazon EC2 インスタンスにインストールされていないか、Amazon EC2 インスタンスで実行されていません。
- Amazon EC2 インスタンスに AWS Identity and Access Management (IAM) インスタンスプロファイルがアタッチされていません
- Amazon EC2 インスタンスにアタッチされた IAM インスタンスプロファイルには、必要な Amazon Simple Storage Service (Amazon S3) 権限がありません
- Amazon S3 に保存されているリビジョンがないか、 AWS リージョン に使用されている Amazon S3 バケットが Amazon EC2 インスタンスと異なります
- アプリケーション仕様 (AppSpec) ファイルの問題
- 「ファイルはすでにその口ケーションに存在します」というエラー
- 失敗した CodeDeploy マネージドライフサイクルイベントのフック
- 失敗したカスタマーマネージドライフサイクルイベントのフック
- デプロイ中のスケールインイベント

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- DeploymentId

  タイプ: 文字列

  説明: (必須) 失敗したデプロイの ID。
- InstanceId

  タイプ: 文字列

  説明: (必須) デプロイに失敗した Amazon EC2 インスタンスの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeAwsApi` - `DeploymentId` および `InstanceId` パラメータに指定された値を検証します。

- aws:executeScript - Amazon EC2 インスタンスから、インスタンスの状態や IAM インスタンスプロファイルの詳細などの情報を収集します。
- aws:executeScript - 指定されたデプロイを確認し、デプロイが失敗した理由に関する分析を返します。

AWS Config

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Config。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-SetupConfig

AWSSupport-SetupConfig

説明

AWSSupport-SetupConfig ランブックは、 AWS Identity and Access Management (IAM) サービスにリンクされたロール、 を使用する設定レコーダー AWS Config、および が設定スナップショットと設定履歴ファイル AWS Config を送信する Amazon Simple Storage Service (Amazon S3) バケットを持つ配信チャネルを作成します。AggregatorAccountId および AggregatorAccountRegionパラメータの値を指定すると、ランブックは、複数の AWS アカウント と複数の から AWS Config 設定およびコンプライアンスデータを収集するためのデータ集約の認可も作成します AWS リージョン。複数のアカウントおよびリージョンからのデータの集約の詳細については、AWS Config デベロッパーガイドの「複数アカウントのマルチリージョンでのデータ集約」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- AggregatorAccountId

  タイプ: 文字列

  説明: (オプション) 複数の アカウントおよび の設定 AWS Config およびコンプライアンスデータを集約するためにアグリゲータが追加され AWS アカウント る の ID AWS リージョン。このアカウントは、アグリゲータがソースアカウントを承認するためにも使用されます。

- AggregatorAccountRegion

  タイプ: 文字列

  説明: (オプション) 複数のアカウント AWS Config とリージョンの設定データとコンプライアンスデータを集約するためにアグリゲータが追加されるリージョン。

- IncludeGlobalResourcesRegion

  タイプ: 文字列

  デフォルト: us-east-1

  説明: (必須) 各リージョンでグローバルリソースデータが記録されるのを回避するには、グローバルリソースデータの記録元となるリージョンを 1 つ指定します。

- パーティション

  タイプ: 文字列

  デフォルト: aws

説明: (必須) AWS Config の設定およびコンプライアンスデータを収集するパーティション。

- S3BucketName

  タイプ: 文字列

  デフォルト: aws-config-delivery-channel

  説明: (オプション) 配信チャネル用に作成された Amazon S3 バケットに用いる名前。アカウント ID は名前の末尾に追加されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeScript - AWS Config のサービスにリンクされた IAM ロールがまだ存在しない場合は、そのロールを作成します。
- aws:executeScript - 設定レコーダーが存在しない場合は、設定レコーダーを作成します。

- aws:executeScript - 配信チャネルによって使用される Amazon S3 バケットが存在しない場合は、Amazon S3 バケットを作成します。
- aws:executeScript - ランブックによって作成されたリソースを使用して配信チャンネルを作成します。
- aws:executeAwsApi - 設定レコーダーを起動します。
- aws:executeScript - AggregatorAccountId パラメータと AggregatorAccountRegion パラメータの値を指定した場合、マルチアカウントおよびマルチリージョンデータ集約の承認が設定されます。

Amazon Connect

AWS Systems Manager Automation は、Amazon Connect 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-AssociatePhoneNumbersToConnectContactFlows
- AWSSupport-CollectAmazonConnectContactFlowLog

AWSSupport-AssociatePhoneNumbersToConnectContactFlows

説明

AWSSupport-AssociatePhoneNumbersToConnectContactFlows は、Amazon Connect インスタンスの問い合わせフローに電話番号を関連付けるのに役立ちます。電話番号と問い合わせフローのマッピングを入力カンマ区切り値 (CSV) ファイルに提供することで、ランブックは 14.5 分以内にできるだけ多くの電話番号を問い合わせフローに関連付けます。ランブックは、すべての電話番号と問い合わせフローペアの CSV ファイルを生成します。このファイルは、制限時間内に関連付けることができなかったため、次の実行で入力できます。

動作の仕組み

ランブックAWSSupport-AssociatePhoneNumbersToConnectContactFlowsは、Amazon Simple Storage Service (Amazon S3) バケットに保存されているマッピングデータの CSV ファイルを使用して、電話番号を Amazon Connect インスタンスの問い合わせフローに関連付けるのに役立ちます。Amazon S3 入力 CSV ファイルは、E.164 形式のPhoneNumber値で、次の形式と一致する必要があります。

入力 CSV ファイルの例

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

オートメーションランブックは、 DestinationFileBucketおよび で指定された送信先ロケーションに次のファイルも作成しますDestinationFilePath。

- **automation:EXECUTION_ID/ResourceIdList.csv**: AssociatePhoneNumberContactFlow API に必要な PhoneNumberIdと のContactFlowIdペアを含む一時ファイル。
- **automation:EXECUTION_ID/ErrorResourceList.csv**: のResourceNotFoundException形式など、エラーのために処理できなかった電話番号と問い合わせフローペアを含むファイルPhoneNumber,ContactFlowName,ErrorMessage。
- **automation:EXECUTION_ID/NonProcessedResourceList.csv**: 処理されなかった電話番号と問い合わせフローのペアを含むファイル。ランブックは、14.5 分以内に可能な限り多くの電話番号と問い合わせフローを処理しようとします (AWS Lambda 関数タイムアウトの 15 分 - バッファの 30 秒) 。時間制約のために処理できなかった電話番号/問い合わせフローがある場合、ランブックは次のランブック実行の入力として使用する CSV ファイルにそれらを含めます。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager [AWSSupport-AssociatePhoneNumbersToConnectContactFlows]で に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション)

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロール

が指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。

- ConnectInstanceId (必須)

  Amazon Connect インスタンスの ID。

- SourceFileBucket (必須)

  電話番号と問い合わせフローペアを含む CSV ファイルを保存する Amazon S3 バケット。

- SourceFilePath (必須)

  電話番号と問い合わせフローペアを含む CSV ファイルの Amazon S3 オブジェクトキー。例えば、`path/to/input.csv` と指定します。

- DestinationFileBucket (必須)

  オートメーションが中間ファイルと結果レポートを配置する Amazon S3 バケット。

- DestinationFilePath (オプション)

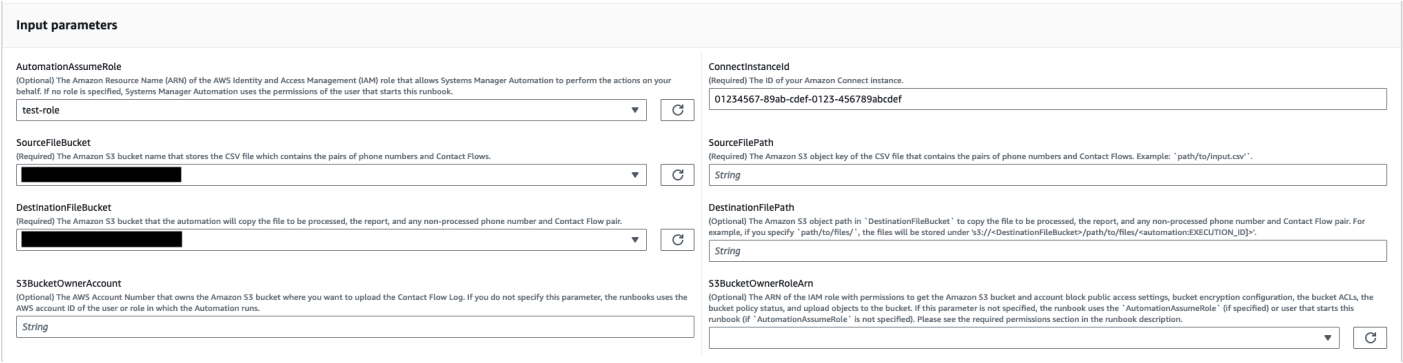
  `DestinationFileBucket` 中間ファイルと結果レポートを保存する Amazon S3 オブジェクトパス。たとえば、 を指定すると`path/to/files/`、ファイルは に保存されます`s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`。

- S3BucketOwnerAccount (オプション)

  問い合わせフローログをアップロードする Amazon S3 バケットを所有する AWS アカウント番号。このパラメータを指定しない場合、ランブックはオートメーションを実行するユーザーまたはロールの AWS アカウント ID を使用します。

- S3BucketOwnerRoleArn (オプション)

  Amazon S3 バケットとアカウントブロックのパブリックアクセス設定、バケット暗号化設定、バケット ACLs。このパラメータが指定されていない場合、ランブックは`AutomationAssumeRole`、このランブックを開始する (指定されている場合) または ユーザー (が指定され`AutomationAssumeRole`ていない場合) を使用します。ランブックの説明の「必要な権限」セクションを参照してください。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - CheckConnectInstanceExistance

     で指定された Amazon Connect インスタンスConnectInstanceIdが存在するかどうかを確認します。
   - CheckS3BucketPublicStatus

     で指定された Amazon S3 バケットをチェックSourceFileBucketし、匿名またはパブリックの読み取りまたは書き込みアクセス許可DestinationFileBucketを付与します。
   - CheckSourceFileExistenceAndSize

     で指定されたソース CSV ファイルSourceFilePathが存在するかどうか、およびファイルサイズが 25 MiB の制限を超えているかどうかを確認します。
   - GenerateResourceIdMap

     で指定されたソース CSV ファイルをダウンロードSourceFilePathし、リソースContactFlowIdごとに PhoneNumberIdと を識別します。完了すると、PhoneNumber、、、および を含む CSV ファイルがPhoneNumberIdContactFlowName、 で指定された送信先 Amazon S3 バケットにアップロードContactFlowIdされますDestinationFileBucket。特定の数値に対して が識別PhoneNumberIdできない場合、CSV ファイル内の ファイルは空になります。
   - AssociatePhoneNumbersToContactFlows

     AWS CloudFormation スタックを使用して アカウントに AWS Lambda 関数を作成します。 AWS Lambda 関数は、 SourceFileBucketおよび で指定されたソース CSV ファイルに記載されている問い合わせフローに各番号を関連付けSourceFilePath、 AWS

CloudFormation スタックは 関数を呼び出します。 AWS Lambda 関数は、タイムアウト (15 分) する前に、できるだけ多くの電話番号を問い合わせフローにマッピングします。エラーのために処理できなかった電話番号と問い合わせフローのリストは、 にアップロードされます[automation:EXECUTION_ID]/ErrorResourceList.csv。1 回の実行で処理できる電話番号の最大数を超えたために処理できなかった電話番号は、 にアップロードされます[automation:EXECUTION_ID]/NonProcessedResourceList.csv。このステップが失敗した場合、 AWS CloudFormation スタックイベントから失敗した理由を示すDescribeCloudFormationErrorFromStackEventsステップに進みます。

- WaitForPhoneNumberContactFlowAssociationCompletion

  電話番号を問い合わせフローにマッピングする AWS Lambda 関数が作成され、 AWS CloudFormation スタックが呼び出しを完了するまで待ちます。

- GenerateReport

  問い合わせフローにマッピングされた電話番号の数、エラーにより処理できなかった電話番号、および 1 回の実行で処理できる電話番号の最大数を超えたために処理できなかった電話番号を含むレポートを生成します。このレポートには、該当する場合[automation:EXECUTION_ID]/NonProcessedResourceList.csv、[automation:EXECUTION_ID]/ErrorResourceList.csvまたは の場所 (Amazon S3 URI と Amazon S3 コンソール URL) も表示されます。

- **DeleteCloudFormationStack**

  マッピング用の Lambda 関数を含む AWS CloudFormation スタックを削除します。

- **DescribeCloudFormationErrorFromStackEvent**

  AssociatePhoneNumbersToContactFlows ステップの AWS CloudFormation スタックからのエラーについて説明します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

   - GenerateReport.OutputPayload

     電話番号と問い合わせフローの関連付けの出力。このレポートには、次の情報が含まれています。

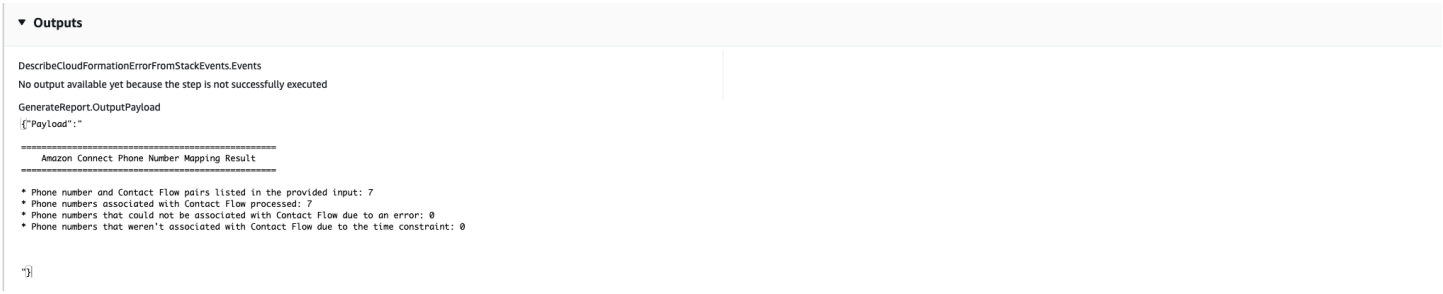
     - 入力 CSV ファイルに記載されている電話番号と問い合わせフローのペアの数
     - 入力 CSV ファイルで指定された問い合わせフローに関連付けられた電話番号の数
     - エラーにより問い合わせフローに関連付けられなかった電話番号の数
     - 時間的制約により問い合わせフローに関連付けられなかった電話番号の数

- エラーにより関連付けできなかった電話番号と問い合わせフローペアを含む CSV ファイルの場所 (Amazon S3 URI と Amazon S3 コンソール URL)
- 時刻の制約により関連付けられなかった電話番号と問い合わせフローペアを含む CSV ファイルの場所 (Amazon S3 URI と Amazon S3 コンソール URL)

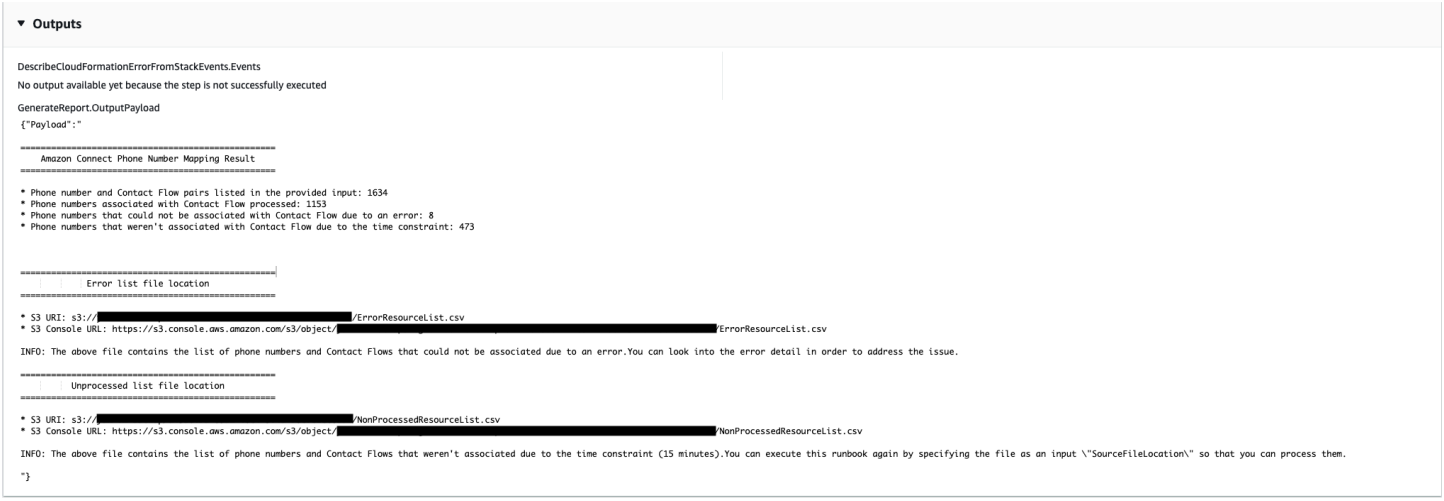
- DescribeCloudFormationErrorFromStackEvents.Events

  `AssociatePhoneNumbersToContactFlows` ステップが失敗した場合に AWS CloudFormation スタックイベントを表示する出力。

少数の電話番号と問い合わせフローを使用した実行の出力



エラーや時間の制約により関連付けられなかった多数の電話番号、問い合わせフロー、電話番号を含む実行の出力



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する

- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWSSupport-CollectAmazonConnectContactFlowLog

説明

AWSSupport-CollectAmazonConnectContactFlowLog オートメーションランブックは、特定の問い合わせ ID の Amazon Connect 問い合わせフローログを収集するために使用されます。Amazon Connect インスタンス ID と問い合わせ ID を指定することで、ランブックは Amazon CloudWatch ロググループから問い合わせフローログを検索し、リクエストパラメータで指定された Amazon Simple Storage Service (Amazon S3) バケットにアップロードします。ランブックは、ログをダウンロードするための Amazon S3 コンソール URL と AWS CLI コマンドを提供する出力を生成します。

動作の仕組み

AWSSupport-CollectAmazonConnectContactFlowLog オートメーションランブックは、設定された CloudWatch ロググループに保存されている特定の問い合わせ ID の Amazon Connect 問い合わせフローログを収集し、指定された Amazon S3 バケットにアップロードするのに役立ちます。Amazon Connect 問い合わせフローから収集されたログのセキュリティをサポートするために、オートメーションは Amazon S3 バケット設定を評価して、バケットがパブリックアクセス許可`read`または`write`アクセス許可を付与し、 `S3BucketOwnerAccountId`パラメータで指定された AWS アカウントによって所有されているかどうかを確認します。Amazon S3 バケットが AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS) を使用している場合は、このオートメーションを実行しているユーザーまたは AWS Identity and Access Management (IAM) ロールに AWS KMS キーに対する`kms:GenerateDataKey`アクセス許可があることを確認してください。Amazon Connect インスタンスによって生成されるログの詳細については、Amazon CloudWatch ロググループに保存されているフローログ」を参照してください。

> **Important**
>
> CloudWatch Logs Insights クエリには、クエリされたデータ量に基づいて料金が発生します。無料利用枠のお客様は、サービスクォータを超える使用に対してのみ料金が発生します。詳細については、「Amazon CloudWatch 料金表」をご覧ください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager AWSSupport-CollectAmazonConnectContactFlowLogで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - ConnectInstanceId (必須):

     Amazon Connect インスタンスの ID。
   - ContactId (必須):

     問い合わせフローログを収集する問い合わせの ID。
   - S3BucketName (必須):

     問い合わせフローログをアップロードするアカウントの Amazon S3 バケット名。バケットポリシーが、収集されたログへのアクセスを必要としない当事者に不要な読み取り/書き込みアクセス許可を付与していないことを確認してください。

- S3ObjectPrefix (オプション):

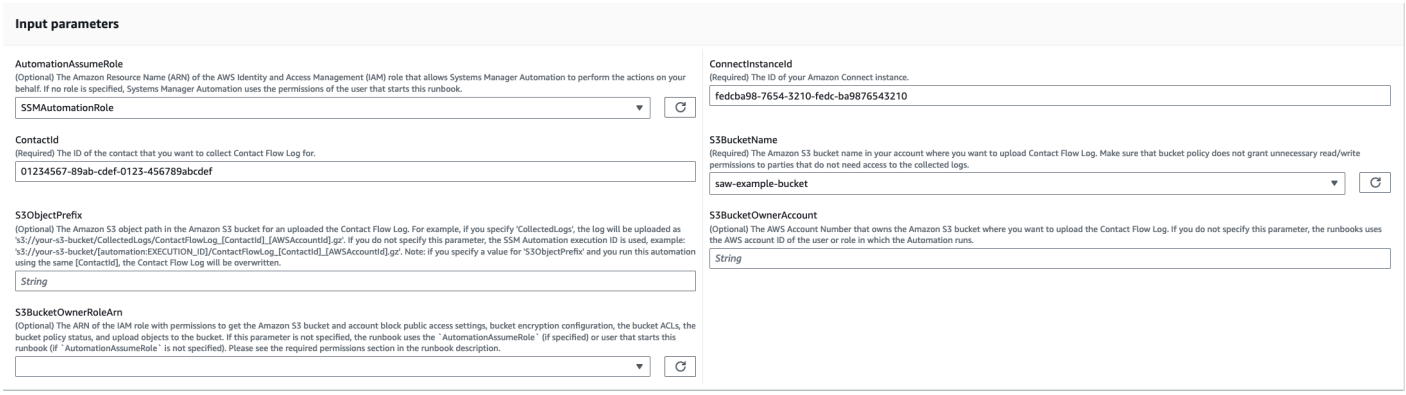
  アップロードされた問い合わせフローログの Amazon S3 バケット内の Amazon S3 オブジェクトパス。例えば、 を指定するとCollectedLogs、ログは としてアップロードされますs3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId]_[AWSAccountId].gz。このパラメータを指定しない場合、Systems Manager Automation の実行 ID が使用されます。例: s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz。注: の値を指定S3ObjectPrefixし、同じ [ContactId] を使用してこのオートメーションを実行すると、問い合わせフローログは上書きされます。

- S3BucketOwnerAccount (オプション):

  問い合わせフローログをアップロードする Amazon S3 バケットを所有する AWS アカウント番号。このパラメータを指定しない場合、ランブックはオートメーションを実行するユーザーまたはロールの AWS アカウント ID を使用します。

- S3BucketOwnerRoleArn (オプション):

  Amazon S3 バケットとアカウントブロックのパブリックアクセス設定、バケット暗号化設定、バケット ACLs。このパラメータが指定されていない場合、ランブックはAutomationAssumeRole、このランブックを開始する (指定されている場合) または ユーザー (が指定されAutomationAssumeRoleていない場合) を使用します。ランブックの説明の必要なアクセス許可セクションを参照してください。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。

   - CheckConnectInstanceExistance

で提供されている Amazon Connect インスタンスConnectInstanceIdが かどうかを確認しますACTIVE。

- CheckS3BucketPublicStatus

  で指定された Amazon S3 バケットが、匿名またはパブリックの読み取り/書き込みアクセス許可S3BucketNameを許可しているかどうかを確認します。

- GenerateLogSearchTimeRange

  に基づいてStartQueryステップEndTimeの StartTimeと InitiationTimestampを生成し、 DescribeContact API によってLastUpdateTimestamp返されます。 StartTime は 1 時間前InitiationTimestamp、 は 1 時間後EndTimeになりますLastUpdateTimestamp。

- StartQuery

  で提供される Amazon Connect インスタンスに関連付けられた ContactId CloudWatch Logs ロググループで提供される のクエリログを開始しますConnectInstanceId。クエリは 60 分のランタイム後にタイムアウトします。クエリがタイムアウトした場合は、検索する時間範囲を短くします。現在進行中のクエリと最近のクエリ履歴は、CloudWatch コンソールで表示できます。詳細については、「実行中のクエリまたはクエリ履歴を表示する」を参照してください。

- WaitForQueryCompletion

  指定された が完了するまで CloudWatch Logs クエリログContactIdを待ちます。クエリは 60 分のランタイム後にタイムアウトすることに注意してください。クエリがタイムアウトした場合は、検索する時間範囲を短くします。Amazon Connect コンソールで、現在進行中のクエリと最近のクエリ履歴を表示できます。詳細については、「実行中のクエリまたはクエリ履歴を表示する」を参照してください。

- UploadContactFlowLog

  クエリ結果を取得し、問い合わせフローログを で指定された Amazon S3 バケットにアップロードしますS3BucketName。

- GenerateReport

  問い合わせフローログがアップロードされた Amazon S3 AWS コンソール URL と、ログファイルのダウンロードに使用できる CLI コマンドの例を返します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

- GenerateReport.OutputPayload

ランブックが指定された問い合わせの問い合わせフローログを正常に取得したことを示す出力。このレポートには、ログファイルをダウンロードできるように、Amazon S3 コンソール URL AWS と CLI コマンドの例も含まれています。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS Directory Service

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Directory Service。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

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

AWS-CreateDSManagementInstance

説明

AWS-CreateDSManagementInstance ランブックは、 AWS Directory Service ディレクトリの管理に使用できる Amazon Elastic Compute Cloud (Amazon EC2) Windows インスタンスを作成します。管理インスタンスは AD Connector ディレクトリの管理には使用できません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- AmiID

  タイプ: 文字列

  デフォルト: {{ ssm:/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-Base }}

  説明: (必須) 管理インスタンスの起動に使用する Amazon Machine Image (AMI) の ID。

- DirectoryId

タイプ: 文字列

説明: (必須) 管理する AWS Directory Service ディレクトリの ID。インスタンスは指定したディレクトリに結合されます。

- IamInstanceProfileName

  タイプ: 文字列

  説明: (必須) 指定した名前は、自動化によって作成され、管理インスタンスにアタッチされる IAM インスタンスプロファイルに適用されます。

- InstanceType

  タイプ: 文字列

  デフォルト: t3.medium

  許可される値:

  - 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

  説明: (必須) 起動するインスタンスのタイプ。

- KeyPairName

タイプ: 文字列

説明: (オプション) インスタンスを作成するときに使用するキーペア。値を指定しないと、キーペアはインスタンスに関連付けられません。

- RemoteAccessCidr

  タイプ: 文字列

  説明: (必須) RDP トラフィック (ポート 3389) を許可する CIDR ブロック。指定した CIDR ブロックは、自動化によって作成されたセキュリティグループに追加されたインバウンドルールに適用されます。

- SecurityGroupName

  タイプ: 文字列

  説明: (必須) 指定した名前は、自動化によって作成され、管理インスタンスに関連付けられるセキュリティグループに適用されます。

- [タグ]

  タイプ: MapList

  説明: (オプション) 自動化によって作成されたリソースに適用するキーと値のペア。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeAwsApi - DirectoryId パラメータで指定されたディレクトリの詳細を収集します。
- aws:executeAwsApi - ディレクトリが起動された仮想プライベートクラウド (VPC) の CIDR ブロックを取得します。
- aws:executeAwsApi - SecurityGroupName パラメータに指定した値を使用してセキュリティグループを作成します。
- aws:executeAwsApi - RemoteAccessCidr パラメータで指定した CIDR からの RDP トラフィックを許可する、新しく作成したセキュリティグループのインバウンドルールを作成します。
- aws:executeAwsApi - IamInstanceProfileName パラメータで指定した値を使用して IAM ロールとインスタンスプロファイルを作成します。
- aws:executeAwsApi - ランブックパラメータで指定された値に基づいて Amazon EC2 インスタンスを起動します。
- aws:executeAwsApi - 新しく起動したインスタンスを ディレクトリに結合する AWS Systems Manager ドキュメントを作成します。
- aws:runCommand - 新しいインスタンスをディレクトリに結合します。
- aws:runCommand - 新しいインスタンスにリモートサーバー管理ツールをインストールします。

AWSSupport-TroubleshootADConnectorConnectivity

説明

AWSSupport-TroubleshootADConnectorConnectivity ランブックでは、AD Connector の以下の前提条件を確認します。

- 必要なトラフィックが、AD Connector に関連するセキュリティグループおよびネットワークアクセスコントロールリスト (ACL) ルールによって許可されているかどうかを確認します。
- AD Connector と同じ Virtual Private Cloud (VPC) に AWS Systems Manager、 AWS Security Token Service、、および Amazon CloudWatch インターフェイス VPC エンドポイントが存在するかどうかを確認します。

前提条件のチェックが正常に完了すると、ランブックは AD Connector と同じサブネットで 2 つの Amazon Elastic Compute Cloud (Amazon EC2) Linux t2.micro インスタンスを起動します。その後、`netcat` および `nslookup` ユーティリティを使用してネットワーク接続テストが実行されます。

このオートメーションを実行する (コンソール)

> **Important**
>
> このランブックを使用すると、Amazon EC2 インスタンス、Amazon Elastic Block Store ボリューム、およびオートメーション中に作成された Amazon Machine Image (AMI) AWS アカウント に対して、 に追加の料金が発生する場合があります。詳細については、「Amazon Elastic Compute クラウド料金表」と「Amazon Elastic Block Store 料金表」を参照してください。
>
> `aws:deletestack` ステップが失敗した場合は、 AWS CloudFormation コンソールに移動してスタックを手動で削除します。このランブックで作成されたスタック名は `AWSSupport-TroubleshootADConnectorConnectivity` で始まります。 AWS CloudFormation スタックの削除の詳細については、「 AWS CloudFormation ユーザーガイド」の「スタックの削除」を参照してください。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム

(ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- DirectoryId

  タイプ: 文字列

  説明: (必須) 接続のトラブルシューティングを行う AD Connector ディレクトリの ID。

- Ec2InstanceProfile

  タイプ: 文字列

  最大文字数: 128

  説明: (必須) 接続テストを実行するために起動されるインスタンスに割り当てるインスタンスプロファイルの名前。指定するインスタンスプロファイルには、AmazonSSMManagedInstanceCore ポリシーまたは同等の権限がアタッチされている必要があります。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:assertAwsResourceProperty - DirectoryId パラメータで指定されたディレクトリが AD Connector であることを確認します。
- aws:executeAwsApi - AD Connector に関する情報を収集します。
- aws:executeAwsApi - AD Connector に関連付けられているセキュリティグループに関する情報を収集します。
- aws:executeAwsApi - AD Connector のサブネットに関連付けられているネットワーク ACL ルールに関する情報を収集します。
- aws:executeScript - AD Connector セキュリティグループのルールを評価して、必要なアウトバウンドトラフィックが許可されていることを確認します。
- aws:executeScript - AD Connector ネットワーク ACL のルールを評価して、必要なアウトバウンドネットワークトラフィックとインバウンドネットワークトラフィックが許可されていることを確認します。
- aws:executeScript - AWS Systems Manager AWS Security Token Service および Amazon CloudWatch インターフェイスエンドポイントが AD Connector と同じ VPC に存在するかどうかを確認します。
- aws:executeScript - 前のステップで実行したチェックの出力をコンパイルします。
- aws:branch - 前のステップの出力に応じて自動化を分岐させます。セキュリティグループとネットワーク ACL に必要なアウトバウンドルールとインバウンドルールが欠落している場合、自動化はここで停止します。
- aws:createStack - AWS CloudFormation スタックを作成して Amazon EC2 インスタンスを起動し、接続テストを実行します。
- aws:executeAwsApi - 新しく起動した Amazon EC2 インスタンスの ID を収集します。

- aws:waitForAwsResourceProperty - 新しく起動された最初の Amazon EC2 インスタンスが AWS Systems Managerの管理対象としてレポートされるのを待ちます。
- aws:waitForAwsResourceProperty - 新しく起動された 2 番目の Amazon EC2 インスタンスが AWS Systems Managerの管理対象としてレポートされるのを待ちます。
- aws:runCommand - 最初の Amazon EC2 インスタンスからオンプレミス DNS サーバーの IP アドレスへのネットワーク接続テストを実行します。
- aws:runCommand - 2 番目の Amazon EC2 インスタンスからオンプレミス DNS サーバーの IP アドレスへのネットワーク接続テストを実行します。
- aws:changeInstanceState - 接続テストに使用した Amazon EC2 インスタンスを停止します。
- aws:deleteStack - AWS CloudFormation スタックを削除します。
- aws:executeScript - 自動化が AWS CloudFormation スタックの削除に失敗した場合にスタックを手動で削除する方法に関する指示を出力します。

AWSSupport-TroubleshootDirectoryTrust

説明

AWSSupport-TroubleshootDirectoryTrust ランブックは、 AWS Managed Microsoft AD と Microsoft Active Directory 間の信頼作成の問題を診断します。このオートメーションにより、ディレクトリタイプが信頼関係をサポートしていることが確認され、関連付けられているセキュリティグループのルール、ネットワークアクセスコントロールリスト (ネットワーク ACL)、ルートテーブルの潜在的な接続の問題がチェックされます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- DirectoryId

  タイプ: 文字列

  使用できるパターン: ^d-[a-z0-9]{10}$

  説明: (必須) トラブルシューティング AWS Managed Microsoft AD する の ID。

- RemoteDomainCidrs

  タイプ: StringList

  使用できるパターン: ^(([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]))$

  説明: (必須) 信頼関係を確立しようとしているリモートドメインの CIDR。カンマ区切り値を使用して、複数の CIDR を追加できます。例: 172.31.48.0/20, 192.168.1.10/32

- RemoteDomainName

  タイプ: 文字列

  説明: (必須) 信頼関係を確立しようとしているリモートドメインの完全修飾ドメイン名。

- RequiredTrafficACL

  タイプ: 文字列

  説明: (必須) のデフォルトのポート要件 AWS Managed Microsoft AD。ほとんどの場合、デフォルト値を変更する必要はありません。

  デフォルト: {"inbound":{"tcp":[[53,53],[88,88],[135,135],[389,389],[445,445],[464,464],[636,636],[1024,65535]],"udp":[[53,53],[88,88],[123.123],[138,138],[389,389],[445,445],[464,464]],"icmp":[[-1,-1]]},"outbound":{"-1":[[0,65535]]}}

- RequiredTrafficSG

タイプ: 文字列

説明: (必須) のデフォルトのポート要件 AWS Managed Microsoft AD。ほとんどの場合、デフォルト値を変更する必要はありません。

デフォルト: {"inbound":{"tcp":[[53,53],[88,88],[135,135],[389,389],[445,445],[464,464],[636,636],[1024,65535]],"udp":[[53,53],[88,88],[123.123],[138,138],[389,389],[445,445],[464,464]],"icmp":[[-1,-1]]},"outbound":{"-1":[[0,65535]]}}

- TrustId

タイプ: 文字列

説明: (オプション) トラブルシューティングを行う信頼関係の ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:assertAwsResourceProperty - ディレクトリタイプが AWS Managed Microsoft ADであることを確認します。
- aws:executeAwsApi - に関する情報を取得します AWS Managed Microsoft AD。
- aws:branch - TrustId 入力パラメータに値が指定されている場合にオートメーションを分岐させます。
- aws:executeAwsApi - 信頼関係に関する情報を取得します。

- aws:executeAwsApi - RemoteDomainName の条件付きフォワーダーの DNS の IP アドレスを取得します。
- aws:executeAwsApi - AWS Managed Microsoft ADに追加された IP ルートに関する情報を取得します。
- aws:executeAwsApi - AWS Managed Microsoft AD サブネットの CIDRs を取得します。
- aws:executeAwsApi - AWS Managed Microsoft ADに関連付けられているセキュリティグループに関する情報を取得します。
- aws:executeAwsApi - AWS Managed Microsoft ADに関連付けられているネットワーク ACL に関する情報を取得します。
- aws:executeScript - RemoteDomainCidrs の値が有効であることを確認します。に の条件付きフォワーダー AWS Managed Microsoft AD があり、 が RFC RemoteDomainCidrs 1918 以外の IP アドレス AWS Managed Microsoft AD である場合、必要な IP ルートRemoteDomainCidrsが に追加されていることを確認します。
- aws:executeScript - セキュリティグループのルールを評価します。
- aws:executeScript - ネットワーク ACL を評価します。

出力

evalDirectorySecurityGroup.output - に関連付けられたセキュリティグループルールが信頼の作成に必要なトラフィック AWS Managed Microsoft AD を許可しているかどうかを評価した結果。

evalAclEntries.output - に関連付けられたネットワーク ACLs が信頼の作成に必要なトラフィック AWS Managed Microsoft AD を許可しているかどうかを評価した結果。

evaluateRemoteDomainCidr.output - RemoteDomainCidrs が有効な値であるかどうかを評価した結果。に AWS Managed Microsoft AD の条件付きフォワーダーがあり、 が RFC RemoteDomainCidrs 1918 以外の IP アドレス AWS Managed Microsoft AD である場合、必要な IP ルートRemoteDomainCidrsが に追加されていることを確認します。

AWS AppSync

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS AppSync。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-EnableAppSyncGraphQLApiLogging

AWS-EnableAppSyncGraphQLApiLogging

説明

AWS-EnableAppSyncGraphQLApiLogging ランブックは、指定した AWS AppSync GraphQL API のフィールドレベルのログ記録とリクエストレベルのログ記録を有効にします。ランブックは、ログ記録がすでに有効になっている場合でも、指定された GraphQL API に変更を適用します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ApiId

  タイプ: 文字列

  説明: (必須) ログ記録を有効にする API の ID。

- FieldLogLevel

タイプ: 文字列

有効な値: ERROR | ALL

説明: (必須) フィールドのログ記録レベル。

- CloudWatchLogsRoleArn

  タイプ: 文字列

  説明: (必須) が Amazon CloudWatch Logs への発行を AWS AppSync 引き受けるサービスロールの ARN。

- ExcludeVerboseContent

  型: ブール値

  デフォルト: False

  説明: (オプション) ログ記録レベルに関係なく、ヘッダー、コンテキスト、評価されたマッピングテンプレートなどの情報を除外Trueするには、 に設定します。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeAwsApi - プライマリ認証タイプに関連する認証タイプと設定情報を収集します。
- aws:branch - 認証タイプに基づいて分岐します。
- aws:executeAwsApi - ランブックの入力パラメータに指定された値に基づいて、 AWS AppSync GraphQL API のログ記録設定を更新します。

出力

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: UpdateGraphqlApi呼び出しからのレスポンス。
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: UpdateGraphqlApi呼び出しからのレスポンス。
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: UpdateGraphqlApi呼び出しからのレスポンス。
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: UpdateGraphqlApi呼び出しからのレスポンス。

Amazon Athena

AWS Systems Manager Automation は、Amazon Athena 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-EnableAthenaWorkGroupEncryptionAtRest

AWS-EnableAthenaWorkGroupEncryptionAtRest

説明

`AWS-EnableAthenaWorkGroupEncryptionAtRest` ランブックは、指定した Amazon Athena ワークグループの保管時の暗号化を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- WorkGroup

  タイプ: 文字列

  説明: (必須) 保管時の暗号化を有効にするワークグループ。

- EncryptionOption

  タイプ: 文字列

  有効な値: SSE_S3 | SSE_KMS | CSE_KMS

  説明: (必須) 使用する暗号化オプションを指定します。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE_S3)、 AWS KMS マネージドキーによるサーバー側の暗号化 (SSE_KMS)、または AWS KMS マネージドキーによるクライアント側の暗号化 (CSE_KMS) を選択できます。

- KmsKeyId

  タイプ: 文字列

  説明: (オプション) AWS KMS 暗号化オプションを使用している場合は、使用するキーのキー ARN、キー ID、またはキーエイリアスを指定します。

- EnableMinimumEncryptionConfiguration

  型: ブール値

  デフォルト: True

  説明: (オプション) Amazon S3 に書き込まれるクエリおよび計算結果に対して、ワークグループの暗号化の最小レベルを適用します。有効にすると、ワークグループユーザーは、クエリの送信時に

管理者が設定した最小レベル以上にのみ暗号化を設定できます。この設定は、Spark 対応のワークグループには適用されません。

- EnforceWorkGroupConfiguration

  型: ブール値

  デフォルト: True

  説明: (オプション) に設定すると`True`、ワークグループの設定がクライアント側の設定よりも優先されます。に設定すると`False`、クライアント側の設定が使用されます。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:branch - `EncryptionOption`パラメータで指定された暗号化オプションに基づいて分岐します。
- aws:executeAwsApi - このステップでは、指定された暗号化設定で Athena ワークグループを更新します。
- aws:executeAwsApi - 指定された暗号化設定で Athena ワークグループを更新します。
- aws:assertAwsResourceProperty - ワークグループの暗号化が有効になっていることを確認します。

DynamoDB

AWS Systems Manager Automation は、Amazon DynamoDB 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

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

AWS-ChangeDDBRWCapacityMode

説明

AWS-ChangeDDBRWCapacityMode ランブックは、1 つ以上の Amazon DynamoDB (DynamoDB) テーブルの読み取り/書き込みキャパシティモードをオンデマンドモードまたはプロビジョンドモードに変更します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- CapacityMode

  タイプ: 文字列

  有効な値: PROVISIONED | PAY_PER_REQUEST

  説明: (必須) 必要な読み取り/書き込みキャパシティモード。オンデマンド (pay-per-requestからプロビジョンドキャパシティに切り替える場合は、プロビジョンドキャパシティの初期値を設定する必要があります。プロビジョニングされた初期容量値は、過去 30 分間にテーブルとグローバルセカンダリインデックスの消費された読み取りおよび書き込み容量に基づいて推定されます。

- ReadCapacityUnits

  タイプ: 整数

  デフォルト: 0

  説明: (オプション) DynamoDB がスロットリング例外を返すまでに 1 秒あたりに消費される強力な整合性のある読み込みの最大数。

- TableNames

  タイプ: 文字列

  説明: (必須) 読み取り/書き込みキャパシティモードを変更する DynamoDB テーブル名のカンマ区切りリスト。

- WriteCapacityUnits

  タイプ: 整数

  デフォルト: 0

  説明: (オプション) DynamoDB がスロットリング例外を返すまでに 1 秒あたりに消費される書き込みの最大数。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- dynamodb:DescribeTable
- dynamodb:UpdateTable

ドキュメントステップ

- aws:executeScript - TableNamesパラメータで指定された DynamoDB テーブルの読み取り/書き込みキャパシティモードを変更します。

出力

ChangeDDBRWCapacityMode.SuccessesTables - キャパシティモードが正常に変更された DynamoDB テーブル名のリスト

ChangeDDBRWCapacityMode.FailedTables - 容量モードの変更が失敗した DynamoDB テーブル名のマップリストと、失敗の理由。

AWS-CreateDynamoDBBackup

説明

Amazon DynamoDB テーブルのバックアップを作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- BackupName

  タイプ: 文字列

  説明: (必須) 作成するバックアップの名前。

- LambdaAssumeRole

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Lambda がユーザーに代わってアクションを実行できるようにするロールの ARN。指定されていない場合、Lambda 関数を実行するために一時的なロールが作成されます。

- TableName

  タイプ: 文字列

  説明: (必須) DynamoDB テーブルの名前。

AWS-DeleteDynamoDbBackup

説明

Amazon DynamoDB テーブルのバックアップを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- BackupArn

  タイプ: 文字列

  説明: (必須) 削除する DynamoDB テーブルのバックアップの ARN。

AWSConfigRemediation-DeleteDynamoDbTable

説明

AWSConfigRemediation-DeleteDynamoDbTable ランブックは、指定した Amazon DynamoDB (DynamoDB) テーブルを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- TableName

  タイプ: 文字列

  説明: (必須) 削除する DynamoDB テーブルの名前。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeScript` - `TableName` パラメータで指定された DynamoDB テーブルを削除します。
- `aws:executeScript` - DynamoDB テーブルが削除されたことを確認します。

AWS-DeleteDynamoDbTableBackups

説明

保持日数またはカウントに基づいて DynamoDB テーブルのバックアップを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- LambdaAssumeRole

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Lambda がユーザーに代わってアクションを実行できるようにするロールの ARN。指定されていない場合、Lambda 関数を実行するために一時的なロールが作成されます。
- RetentionCount

  タイプ: 文字列

  デフォルト: 10

  説明: (オプション) テーブルに保持するバックアップの数。指定した数を超えるバックアップが存在する場合は、超えた数の分の最も古いバックアップが削除されます。RetentionCount または RetentionDays のいずれかを使用できますが、両方を使用することはできません。
- RetentionDays

  タイプ: 文字列

  説明: (オプション) テーブルのバックアップを保持する日数。指定した日数より古いバックアップは削除されます。RetentionCount または RetentionDays のいずれかを使用できますが、両方を使用することはできません。

- TableName

  タイプ: 文字列

  説明: (必須) DynamoDB テーブルの名前。

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

説明

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable ランブックは、 KMSKeyIdパラメータに指定した AWS Key Management Service () カスタマーマネージドキーを使用して Amazon DynamoDB (DynamoDB AWS KMS) テーブルを暗号化します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- KMSKeyId

  タイプ: 文字列

  説明:(必須) TableName パラメータで指定した DynamoDB テーブルの暗号化に使用する、カスタマーマネージドキーの ARN。

- TableName

  タイプ: 文字列

  説明: (必須) 暗号化する DynamoDB テーブルの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeAwsApi - TableName パラメータで指定された DynamoDB テーブルを暗号化します。
- aws:waitForAwsResourceProperty - DynamoDB テーブルの SSESpecification での Enabled プロパティが true に設定されていることを確認します。
- aws:assertAwsResourceProperty - DynamoDB テーブルが、KMSKeyId パラメータで指定されたカスタマーマネージドキーで暗号化されていることを確認します。

AWSConfigRemediation-EnablePITRForDynamoDbTable

説明

AWSConfigRemediation-EnablePITRForDynamoDbTable ランブックは、ユーザーにより指定された Amazon DynamoDB テーブルで、ポイントインタイムリカバリ (PITR) を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- TableName

  タイプ: 文字列

  説明: (必須) ポイントインタイムリカバリを有効にする DynamoDB テーブルの名前。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeAwsApi` - `TableName` パラメータで指定された DynamoDB テーブルの、ポイントインタイムリカバリを有効にします。
- `aws:assertAwsResourceProperty` - DynamoDB テーブルでポイントインタイムリカバリが有効になっていることを確認します。

AWS-EnableDynamoDbAutoscaling

説明

AWS-EnableDynamoDbAutoscaling ランブックは、指定したプロビジョンドキャパシティの Amazon DynamoDB テーブルに対して Application Auto Scaling を有効にします。Application Auto Scaling は、トラフィックパターンに応じてプロビジョニングされたスループットキャパシティを動的に調整します。詳細については、「Amazon DynamoDB デベロッパーガイド」の「DynamoDB 自動スケーリングによるスループットキャパシティの自動管理」を参照してください。 DynamoDB

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- TableName

  タイプ: 文字列

  説明: (必須) Application Auto Scaling を有効にする DynamoDB テーブルの名前。

- MinReadCapacity

  タイプ: 整数

説明: (必須) DynamoDB テーブルのプロビジョニングされたスループット読み取りキャパシティユニットの最小数。

- MaxReadCapacity

  タイプ: 整数

  説明: (必須) DynamoDB テーブルのプロビジョニングされたスループット読み取りキャパシティユニットの最大数。

- TargetReadCapacityUtilization

  タイプ: 整数

  説明: (必須) 目的のターゲット読み取りキャパシティ使用率。ターゲット使用率は、ある時点で消費されたプロビジョンドスループットの割合です。自動スケーリングのターゲット使用率の値は 20 ~ 90% に設定できます。

- ReadScaleOutCooldown

  タイプ: 整数

  説明: (必須) 以前の読み込みキャパシティのスケールアウトアクティビティが有効になるまでの秒単位の待機時間。

- ReadScaleInCooldown

  タイプ: 整数

  説明: (必須) 読み込みキャパシティのスケールインアクティビティが完了してから、別のスケールインアクティビティを開始できるまでの秒単位の時間。

- MinWriteCapacity

  タイプ: 整数

  説明: (必須) DynamoDB テーブルのプロビジョニングされたスループット書き込みユニットの最小数。

- MaxWriteCapacity

  タイプ: 整数

  説明: (必須) DynamoDB テーブルのプロビジョニングされたスループット書き込みユニットの最大数。

- TargetWriteCapacityUtilization

  タイプ: 整数

  説明: (必須) 目的のターゲット書き込みキャパシティ使用率。ターゲット使用率は、ある時点で消費されたプロビジョンドスループットの割合です。自動スケーリングのターゲット使用率の値は 20 ~ 90% に設定できます。

- WriteScaleOutCooldown

  タイプ: 整数

  説明: (必須) 前の書き込みキャパシティのスケールアウトアクティビティが有効になるまでの秒単位の待機時間。

- WriteScaleInCooldown

  タイプ: 整数

  説明: (必須) 書き込みキャパシティのスケールインアクティビティが完了してから、別のスケールインアクティビティを開始できるまでの時間。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

- RegisterAppAutoscalingTargetWrite (aws:executeAwsApi) - 指定した DynamoDB テーブルで Application Auto Scaling を設定します。
- RegisterAppAutoscalingTargetWriteDelay (aws:sleep) - API スロットリングを避けるためにスリープします。

- PutScalingPolicyWrite (aws:executeAwsApi) - DynamoDB テーブルのターゲット書き込み容量使用率を設定します。
- PutScalingPolicyWriteDelay (aws:sleep) - API スロットリングを避けるためにスリープします。
- RegisterAppAutoscalingTargetRead (aws:executeAwsApi) - DynamoDB テーブルの最小読み取りキャパシティーユニットと最大読み取りキャパシティーユニットを設定します。
- RegisterAppAutoscalingTargetReadDelay (aws:sleep) - API スロットリングを避けるためにスリープします。
- PutScalingPolicyRead (aws:executeAwsApi) - DynamoDB テーブルのターゲット読み取りキャパシティ使用率を設定します。
- VerifyDynamoDbAutoscalingEnabled (aws:executeScript) - 指定した値に従って、DynamoDB テーブルで Application Auto Scaling が有効になっていることを確認します。

出力

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

AWS-RestoreDynamoDBTable

説明

AWS-RestoreDynamoDBTable ランブックは、ポイントインタイムリカバリ (PITR) を使用して指定した Amazon DynamoDB テーブルを復元します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- EnablePointInTimeRecoverAsNeeded

  型: ブール値

  デフォルト: true

  説明: (オプション) テーブルの復元に必要なポイントインタイムリカバリを自動化でオンにするかどうかを決定します。

- GlobalSecondaryIndexOverride

  タイプ: 文字列

  説明: (オプション) 新しいテーブルの既存のセカンダリインデックスを置き換える新しいグローバルセカンダリインデックス。

- LocalSecondaryIndexOverride

  タイプ: 文字列

  説明: (オプション) 新しいテーブルの既存のセカンダリインデックスを置き換える新しいローカルセカンダリインデックス。

- RestoreDateTime

  タイプ: 文字列

  説明: (必須) 過去 35 日間にテーブルを復元するポイントインタイムリカバリ。日付と時間は DD/MM/YYYY HH:MM:SS の形式で指定します。

- SourceTableArn

  タイプ: 文字列

  説明: (必須) 復元するテーブルの ARN。

- SseSpecificationOverride

  タイプ: 文字列

  説明: (オプション) 新しいテーブルに使用するサーバー側の暗号化設定。

- TargetTableName

  タイプ: 文字列

  説明: (必須) 復元するテーブルの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeScript - ポイントインタイムリカバリを使用して TargetTableName パラメータで指定された DynamoDB テーブルを復元します。

AWS Database Migration Service

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Database Migration Service。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-TroubleshootDMSTableErrors

AWSSupport-TroubleshootDMSTableErrors

説明

AWS Systems Manager AWSSuport-TroubleshootDMSTabelErrors 自動化ランブックは、データベース移行タスクまたはサーバーレスレプリケーションでTable errors見つかった のトラブルシューティングプロセスを自動化するのに役立ちます AWS Database Migration Service。これらのエラーは、データベース移行タスクまたは AWS DMS サービスで作成されたサーバーレスレプリケーションによって、テーブルがソースエンドポイント (ソースデータベース) からターゲットエンドポイント (ターゲットデータベース) に移行できない場合に発生します。このランブックは、CloudWatch ログからの署名エラーメッセージを分析し、特に従来のデータベース移行タスクのタスクログとサーバーレスレプリケーションのサーバーレスログに焦点を当てます。また、 AWS DMS 移行Table error中に で発生する一般的なエラーメッセージのターゲットを絞った提案と修復手順も提供します。

動作の仕組み

ランブックは次のステップを実行します。

- 提供された AWS DMS ARN に関する情報を取得します。これは、データベース移行タスクまたはサーバーレスレプリケーションのいずれかです。
- DescribeReplicationTasks API (データベース移行タスク用) および DescribeReplications API (サーバーレスレプリケーション用) レスポンスFreshStartDateの値をチェックして、提供された AWS DMS リソースが少なくとも 1 回起動されたかどうかを確認します。リソースが開始されていない場合、自動化によってエラーが発生します。
- リソースが開始された場合、オートメーションはTableStatistics情報を使用してTableError状態のテーブルをチェックします。エラーが見つからない場合、オートメーションは、指定されたデータベース移行タスクまたはサーバーレスレプリケーションでテーブルエラーが見つからなかったことを確認するメッセージを表示した後、ワークフローを終了します。

- TableError 状態のテーブルが見つかった場合、オートメーションは指定された AWS DMS リソースに対して CloudWatch ログ記録が有効になっているかどうかを確認します。ログ記録が有効になっていない場合、オートメーションはログ記録が有効になっていないことを示すメッセージを表示した後にワークフローを終了します。

  注: CloudWatch ログ記録は、自動化がこれらのログに依存して TableError状態のテーブルの問題を分析して特定するため、有効になると予想されます。
- ログ記録が有効になっている場合、自動化は CloudWatch ログを分析し、 TableError状態にある各テーブルのレポートを生成します。このレポートには、一般的なエラーメッセージの提案が含まれており、 AWS DMS ソースエンドポイントから AWS DMS ターゲットエンドポイントへのテーブル移行の成功を妨げる問題を特定して解決するための関連するエラーログを提供します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

/

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- DMSArn

  タイプ: 文字列

  説明: (必須) データベース移行タスクまたはサーバーレスレプリケーションの ARN

許可されたパターン: ^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

  タイプ: 文字列

  説明: (オプション) このパラメータは、指定されたデータベース移行タスクまたはサーバーレスレプリケーションの CloudWatch ログ分析の時間範囲の開始を定義します。指定した場合、この特定の時間以降に生成されたログのみが収集および分析されます。startDate と の間の時間範囲が長すぎると、ワークフローendDateがタイムアウトする可能性があります。値は ISO 6081 の日付時刻形式で指定する必要があります。

  許可されたパターン: ^$|^(\\d{4})-(\\d{2})-(\\d{2})T(\\d{2}):(\\d{2}):(\\d{2})\\.(\\d{3})Z$

- EndTimeRange

  タイプ: 文字列

  説明: (オプション) このパラメータは、指定されたデータベース移行タスクまたはサーバーレスレプリケーションの CloudWatch ログ分析の時間範囲の終了を設定します。指定した場合、この特定の時間までに生成されたログのみが収集および分析されます。startDate と の間の時間範囲が長すぎると、ワークフローendDateがタイムアウトする可能性があります。値は ISO 6081 の日付時刻形式で指定する必要があります。

  許可されたパターン: ^$|^(\\d{4})-(\\d{2})-(\\d{2})T(\\d{2}):(\\d{2}):(\\d{2})\\.(\\d{3})Z$

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- dms:DescribeReplicationTasks
- dms:DescribeReplications
- dms:DescribeEndpoints
- dms:DescribeReplicationConfigs
- dms:DescribeTableStatistics

- dms:DescribeReplicationTableStatistics
- logs:FilterLogEvents

自動化引き受けロールの IAM ポリシーの例

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

指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager AWSSupport-TroubleshootDMSTableErrorsで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロール

が指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。

- DMSArn

  テーブルエラーがあるデータベース移行タスクまたはサーバーレスレプリケーションの ARN。

- StartTimeRange

  (オプション) 特定のデータベース移行タスクまたはサーバーレスレプリケーションの CloudWatch ログを分析するための時間範囲の開始を定義する ISO 6081 日付時刻形式。

- EndTimeRange

  (オプション) 特定のデータベース移行タスクまたはサーバーレスレプリケーションの CloudWatch ログを分析するための時間範囲の終了を定義する ISO 6081 日付時刻形式。

4. ページの下部から実行ボタンを選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。

- validateDMSInputTypeAndGatherDetails

  指定された AWS DMS ARN 入力を検証し、次のステップで必要なデータベース移行タスクまたはサーバーレスレプリケーションの基本的な詳細を収集します。

- branchOnTableErrors

  上記のステップで見つかったテーブルエラーの数に基づいてワークフローを分岐します。カウントが 0 より大きい場合は、 - `branchOnCWLoggingStatus` ステップに進みます。それ以外の場合は、 - `outputNoTableErrors` ステップに進みます。

- outputNoTableErrors

  指定されたデータベース移行タスクまたはサーバーレスレプリケーションでテーブルエラーが見つからないことを示すメッセージを出力します。

- branchOnCWLoggingStatus

  上記のステップで見つかった CloudWatch ログ記録ステータスに基づいてワークフローを分岐します。有効にした場合、 - `gatherTableDetails` ステップに進みます。それ以外の場合は、 - `outputNoCWLoggingEnabled` ステップに進みます。

- outputNoCWLoggingEnabled

指定されたデータベース移行タスクまたはサーバーレスレプリケーションで CloudWatch ログ記録が有効になっていないことを示すメッセージを出力します。

- gatherTableDetails

  失敗したテーブルの`FullLoadEndTime`タイムスタンプを収集し、CloudWatch ログを分析するための時間範囲値を計算します。

- analyzeCloudWatchLogs

  署名エラーメッセージに基づいて CloudWatch ロググループで見つかったログを分析し、レポートをユーザーに返します。

7. 実行が完了したら、出力セクションで実行の詳細な結果を確認します。
   - テーブルなしエラーの出力

     提供されたデータベース移行タスクまたはサーバーレスレプリケーションにテーブルエラーが見つからない場合、自動化は同じことを示す出力を表示します。

   - CloudWatch ログインが有効になっていない場合の出力

     提供されたデータベース移行タスクまたはサーバーレスレプリケーションで CloudWatch ログ記録が有効になっていない場合、自動化は同じことを示す出力を表示し、ログ記録を有効にする手順を提供します。

   - Analysis レポートのログ記録

     提供されたデータベース移行タスクまたはサーバーレスレプリケーションから `Table error`状態のテーブルを識別し、エラータイプを区別し、発生したエラーメッセージを一覧表示し、識別された各テーブルに対して的を絞った修復ステップと提案を提供するレポートを出力します。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

Amazon EBS

AWS Systems Manager Automation は、Amazon Elastic Block Store 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- 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

説明

AWSSupport-AnalyzeEBSResourceUsage オートメーションランブックは、Amazon Elastic Block Store (Amazon EBS) のリソース使用状況を分析するために使用されます。ボリュームの使用状況を分析し、特定の AWS リージョンで中止されたボリューム、イメージ、スナップショットを識別します。

動作の仕組み

ランブックは次の 4 つのタスクを実行します。

1. Amazon Simple Storage Service (Amazon S3) バケットが存在することを確認するか、新しい Amazon S3 バケットを作成します。
2. 使用可能な状態のすべての Amazon EBS ボリュームを収集します。
3. ソースボリュームが削除されたすべての Amazon EBS スナップショットを収集します。
4. 終了されていない Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで使用されていないすべての Amazon マシンイメージ (AMIs) を収集します。

ランブックは CSV レポートを生成し、ユーザーが用意した Amazon S3 バケットに保存します。提供されたバケットは、最後に説明されているように、 AWS セキュリティのベストプラクティスに従って保護する必要があります。ユーザーが指定した Amazon S3 バケットがアカウントに存在しない場合、ランブックはカスタム AWS Key Management Service （ AWS KMS) キーで`<User-provided-name>-awssupport-YYYY-MM-DD`暗号化された名前形式 で新しい Amazon S3 バケットを作成し、オブジェクトのバージョニングが有効で、パブリックアクセスがブロックされ、SSL/TLS を使用するリクエストが必要です。

独自の Amazon S3 バケットを指定する場合は、次のベストプラクティスに従って設定されていることを確認してください。

- バケットへのパブリックアクセスをブロックします (`IsPublic`に設定`False`) 。
- Amazon S3 アクセスログ記録を有効にします。
- バケットへの SSL リクエストのみを許可します。
- オブジェクトのバージョニングを有効にします。
- AWS Key Management Service （ AWS KMS) キーを使用してバケットを暗号化します。

> **Important**
>
> このランブックを使用すると、Amazon S3 バケットとオブジェクトの作成に対してアカウントに対して追加料金が発生する場合があります。発生する可能性のある料金の詳細については、Amazon S3 の料金」を参照してください。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- S3BucketName

  型: `AWS::S3::Bucket::Name`

  説明: (必須) レポートをアップロードするアカウントの Amazon S3 バケット。バケットポリシーが、収集されたログへのアクセスを必要としない当事者に不要な読み取り/書き込みアクセス許可を付与していないことを確認します。指定されたバケットがアカウントに存在しない場合、自動化は、カスタム AWS KMS キーで<User-provided-name>-awssupport-YYYY-MM-DD暗号化された名前形式 で自動化が開始されるリージョンに新しいバケットを作成します。

  許可されたパターン: `$|^(?!(^(([0-9]{1,3}[.]){3}[0-9]{1,3}$)))^((?!xn—)(?!.*-s3alias))[a-z0-9][-.a-z0-9]{1,61}[a-z0-9]$`

- CustomerManagedKmsKeyArn

  タイプ: 文字列

  説明: (オプション) 指定されたバケットがアカウントに存在しない場合に が作成する新しい Amazon S3 バケットを暗号化するためのカスタム AWS KMS キー Amazon リソースネーム (ARN)。カスタム AWS KMS キー ARN を指定せずにバケットを作成しようとすると、自動化は失敗します。

  許可されたパターン: `(^$|^arn:aws:kms:[-a-z0-9]:[0-9]:key/[-a-z0-9]*$)`

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

このランブックを実行するために必要な最小限の IAM アクセス許可を持つポリシーの例：

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

指示

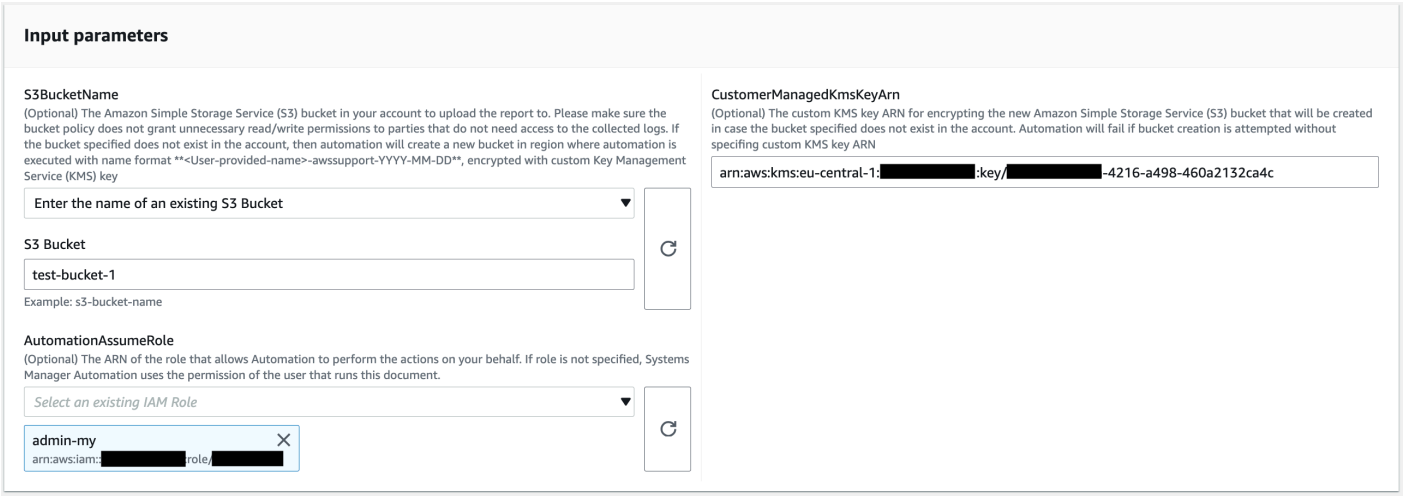
次の手順に従って自動化を設定します。

1. AWS Systems Manager コンソールで AWSSupport-AnalyzeEBSResourceUsage に移動します。
2. 次の入力パラメータを入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
   - S3BucketName (必須):

     レポートをアップロードするアカウントの Amazon S3 バケット。
   - CustomerManagedKmsKeyArn (オプション):

     指定されたバケットがアカウントに存在しない場合に が作成する新しい Amazon S3 バケットを暗号化するためのカスタム AWS KMS キー Amazon リソースネーム (ARN)。



3. [実行] を選択します。
4. 自動化が開始されます。
5. 自動化ランブックは以下のステップを実行します。
   - checkConcurrency:

     リージョンでこのランブックの開始が 1 つだけであることを確認します。ランブックが進行中の別の実行を検出すると、エラーが返され、終了します。

- verifyOrCreateS3bucket:

  Amazon S3 バケットが存在するかどうかを確認します。そうでない場合、カスタム AWS KMS キーで暗号化された名前形式 で自動化が開始されるリージョンに新しい Amazon S3 <User-provided-name>-awssupport-YYYY-MM-DDバケットが作成されます。

- gatherAmiDetails:

  Amazon EC2 インスタンスで使用されていない AMIs を検索し、名前形式 でレポートを生成し<region>-images.csv、Amazon S3 バケットにアップロードします。

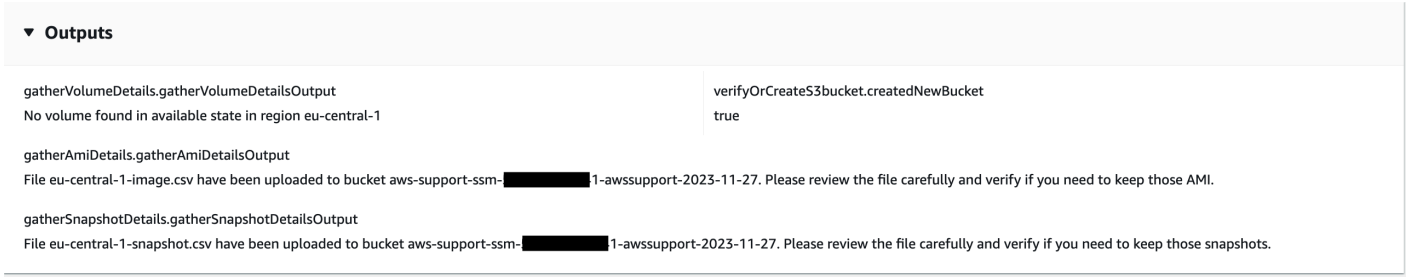
- gatherVolumeDetails:

  使用可能な状態の Amazon EBS ボリュームを検証し、名前形式 でレポートを生成し<region>-volume.csv、Amazon S3 バケットにアップロードします。

- gatherSnapshotDetails:

  既に削除されている Amazon EBS ボリュームの Amazon EBS スナップショットを検索し、名前形式 でレポートを生成して<region>-snapshot.csv、Amazon S3 バケットにアップロードします。

6. 完了したら、出力セクションで詳細な実行結果を確認します。



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS-ArchiveEBSSnapshots

説明

AWS-ArchiveEBSSnapshots ランブックでは、スナップショットに適用したタグを指定することで、Amazon Elastic Block Store (Amazon EBS) ボリュームのスナップショットをアーカイブできます。また、スナップショットにタグが付いていない場合は、ボリュームの ID を指定することもできます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- 説明

  タイプ: 文字列

  説明: (オプション) Amazon EBS スナップショットの説明
- DryRun

  タイプ: 文字列

  有効な値: はい | いいえ

説明: (必須) 実際にリクエストを実行することなく、アクションに必要なアクセス許可があるかどうかを確認し、エラーレスポンスを提供します。

- RetentionCount

  タイプ: 文字列

  説明: (オプション) アーカイブするスナップショットの数。RetentionDays の値を指定していない場合、このパラメータの値を指定しないでください。

- RetentionDays

  タイプ: 文字列

  説明: (オプション) アーカイブするスナップショットのそれ以前の日数。RetentionCount の値を指定していない場合、このパラメータの値を指定しないでください。

- SnapshotWithTag

  タイプ: 文字列

  有効な値: はい | いいえ

  説明: (必須) アーカイブするスナップショットにタグを付けるかどうかを指定します。

- TagKey

  タイプ: 文字列

  説明: (オプション) アーカイブするスナップショットに割り当てられたタグのキー。

- TagValue

  タイプ: 文字列

  説明: (オプション) アーカイブするスナップショットに割り当てられたタグの値。

- ボリューム

  タイプ: 文字列

  説明: (オプション) アーカイブするスナップショットのボリュームの ID。スナップショットにタグが付いていない場合は、このパラメータを使用してください。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ec2:ArchiveSnapshots
- ec2:DescribeSnapshots

ドキュメントステップ

aws:executeScript - TagKey および TagValue パラメータ、または VolumeId パラメータを使用して指定したタグを使用してスナップショットをアーカイブします。

AWS-AttachEBSVolume

説明

Amazon Elastic Block Store (Amazon EBS) ボリュームを Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- デバイス

  タイプ: 文字列

  説明: (必須) デバイス名 (たとえば、/dev/sdh または xvdh)。

- InstanceId

  タイプ: 文字列

  説明: (必須) ボリュームを接続するインスタンスの ID。

- ボリューム

  タイプ: 文字列

  説明: (必須) Amazon EBS ボリュームの ID。ボリュームとそのアタッチ先インスタンスは同じアベイラビリティーゾーンに存在している必要があります。

AWSSupport-CalculateEBSPerformanceMetrics

説明

AWSSupport-CalculateEBSPerformanceMetrics ランブックは、パフォーマンスメトリクスを計算して CloudWatch ダッシュボードに公開することで、Amazon EBS のパフォーマンス問題を診断するのに役立ちます。ダッシュボードには、ターゲット Amazon EBS ボリュームまたはターゲット Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされたすべてのボリュームの推定平均 IOPS とスループットが表示されます。Amazon EC2 インスタンスの場合、インスタンスの平均 IOPS とスループットも表示されます。ランブックは、関連する計算された CloudWatch メトリクスを表示する、新しく作成された CloudWatch ダッシュボードへのリンクを出力します。CloudWatch ダッシュボードは、 という名前でアカウントに作成されますAWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>。

動作の仕組み

ランブックは次のステップを実行します。

- 指定されたタイムスタンプが有効であることを確認します。
- リソース ID (Amazon EBS ボリュームまたは Amazon EC2 インスタンス) が有効かどうかを検証します。

- Amazon EC2 を ResourceID として指定すると、その Amazon EC2 インスタンスの実際の合計 IOPS/スループットと、Amazon EC2 インスタンスにアタッチされたすべての Amazon EBS ボリュームの推定平均 IOPS/スループットグラフを含む CloudWatch ダッシュボードが作成されます Amazon EC2。
- Amazon EBS ボリュームを ResourceID として指定すると、そのボリュームの推定平均 IOPS/スループットグラフを含む CloudWatch ダッシュボードが作成されます。
- CloudWatch ダッシュボードが生成された後、推定平均 IOPS または推定平均スループットがそれぞれ最大 IOPS または最大スループットより大きい場合、Amazon EC2 インスタンスにアタッチされたボリュームに対してマイクロバーストが発生する可能性があります。

> **Note**
>
> バースト可能なボリューム (gp2、sc2、st1) の場合、バーストバランスが得られるまで、最大 IOPS/スループットを考慮する必要があります。バーストバランスが完全に使用された後、つまりゼロになったら、ベースライン IOPS/スループットメトリクスを検討します。

> **Important**
>
> CloudWatch ダッシュボードを作成すると、アカウントに追加料金が発生する可能性があります。詳細については、Amazon CloudWatch 料金ガイドを参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

サンプルポリシー

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

指示

次の手順に従って自動化を設定します。

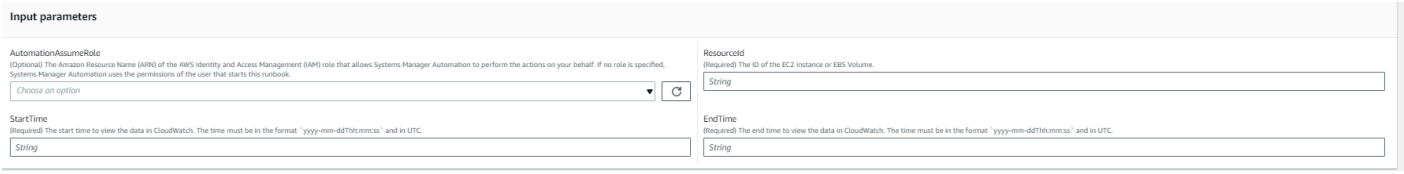
1. ドキュメントの下の Systems Manager AWSSupport-CalculateEBSPerformanceMetricsのに移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - ResourceID (必須):

     Amazon EC2 インスタンスまたは Amazon EBS ボリュームの ID。
   - 開始時刻 (必須):

     CloudWatch でデータを表示する開始時刻。時刻は 形式yyyy-mm-ddThh:mm:ssと UTC 形式である必要があります。
   - 終了時刻 (必須):

     CloudWatch でデータを表示する終了時刻。時刻は 形式yyyy-mm-ddThh:mm:ssと UTC 形式である必要があります。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - CheckResourceIdAndTimeStamps:

     終了時刻が開始時刻より少なくとも 1 分長く、提供されたリソースが存在するかどうかを確認します。
   - CreateCloudWatchDashboard:

     Amazon EBS のパフォーマンスを計算し、リソース ID に基づいてグラフを表示します。パラメータリソース ID に Amazon EBS ボリューム ID を指定すると、このランブックは Amazon

EBS ボリュームの推定平均 IOPS と推定平均スループットを持つ CloudWatch ダッシュボードを作成します。パラメータリソース ID に Amazon EC2 インスタンス ID を指定すると、このランブックはAmazon EC2 Amazon EC2インスタンスにアタッチされたすべての Amazon EBS ボリュームの推定平均 IOPS と推定平均スループットを持つ CloudWatch ダッシュボードを作成します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

Amazon EC2 インスタンスとしてのリソース ID の CloudWatch ダッシュボードの例

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

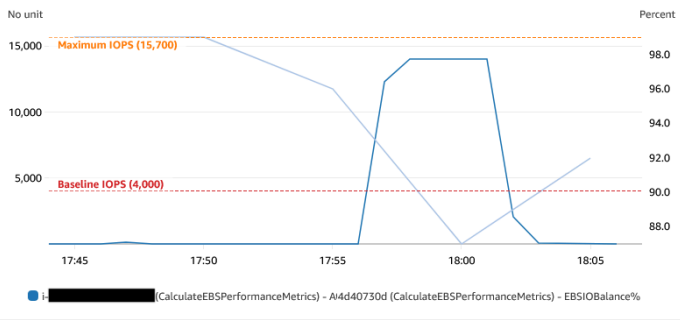
More details on EBS Optimized instances | More details on EBS Volume Types

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

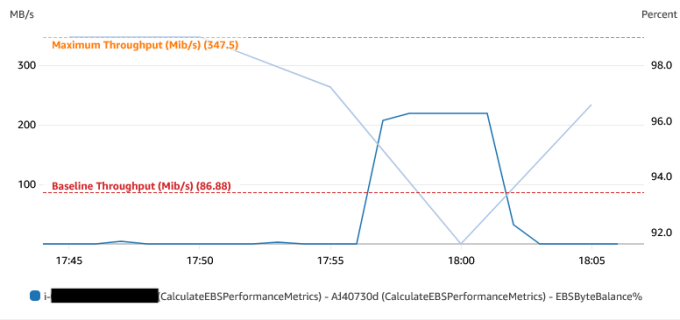
Calculated Metric	Mathematical Expression	Unit
Average Total IOPS	SUM(For All Volumes[(SUM(VolumeReadOps) + SUM(VolumeWriteOps))]) / Period	IOPS
Average Total Throughput	SUM(For All Volumes[(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes))]) / Period / 1024 / 1024	MiB/s

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

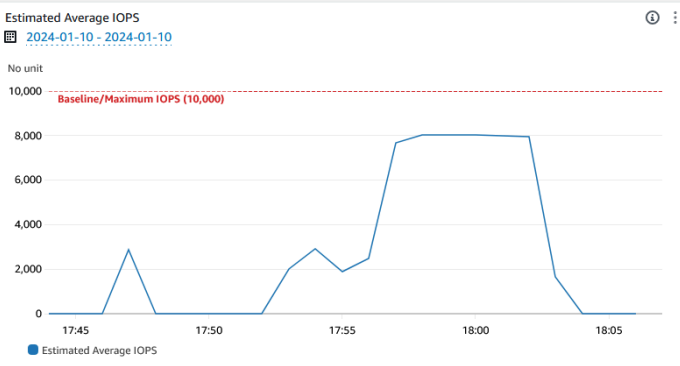
Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	(SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime))	IOPS
Estimated Average Throughput	(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024 / 1024	MiB/s

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.

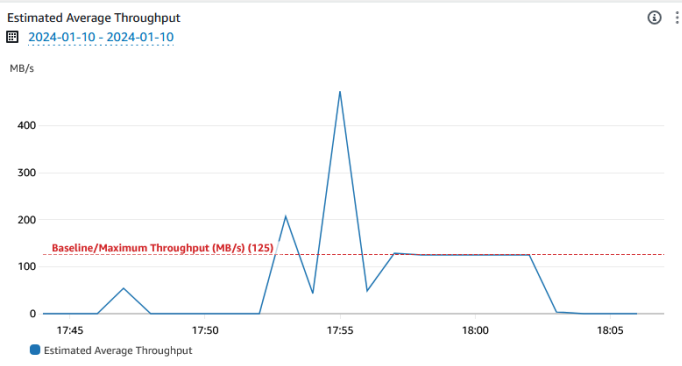
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

Volume: vol[redacted] Type: gp3

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

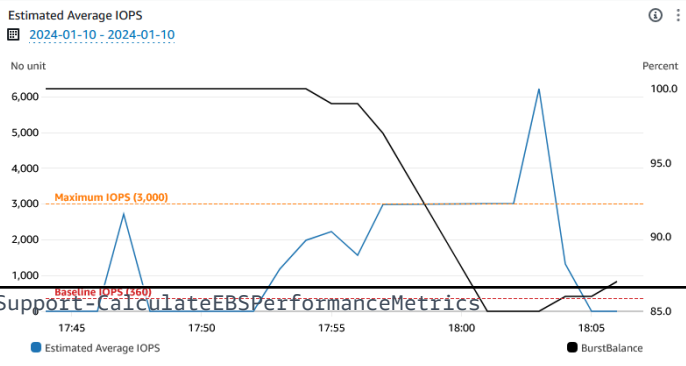


Estimated Average Throughput
2024-01-10 - 2024-01-10

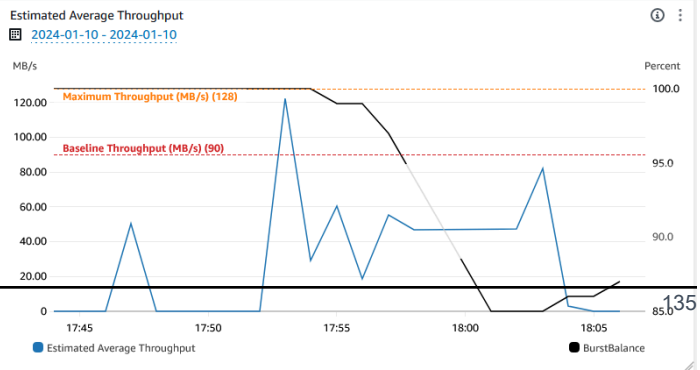


Volume: vol[redacted] | Type: gp2

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



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

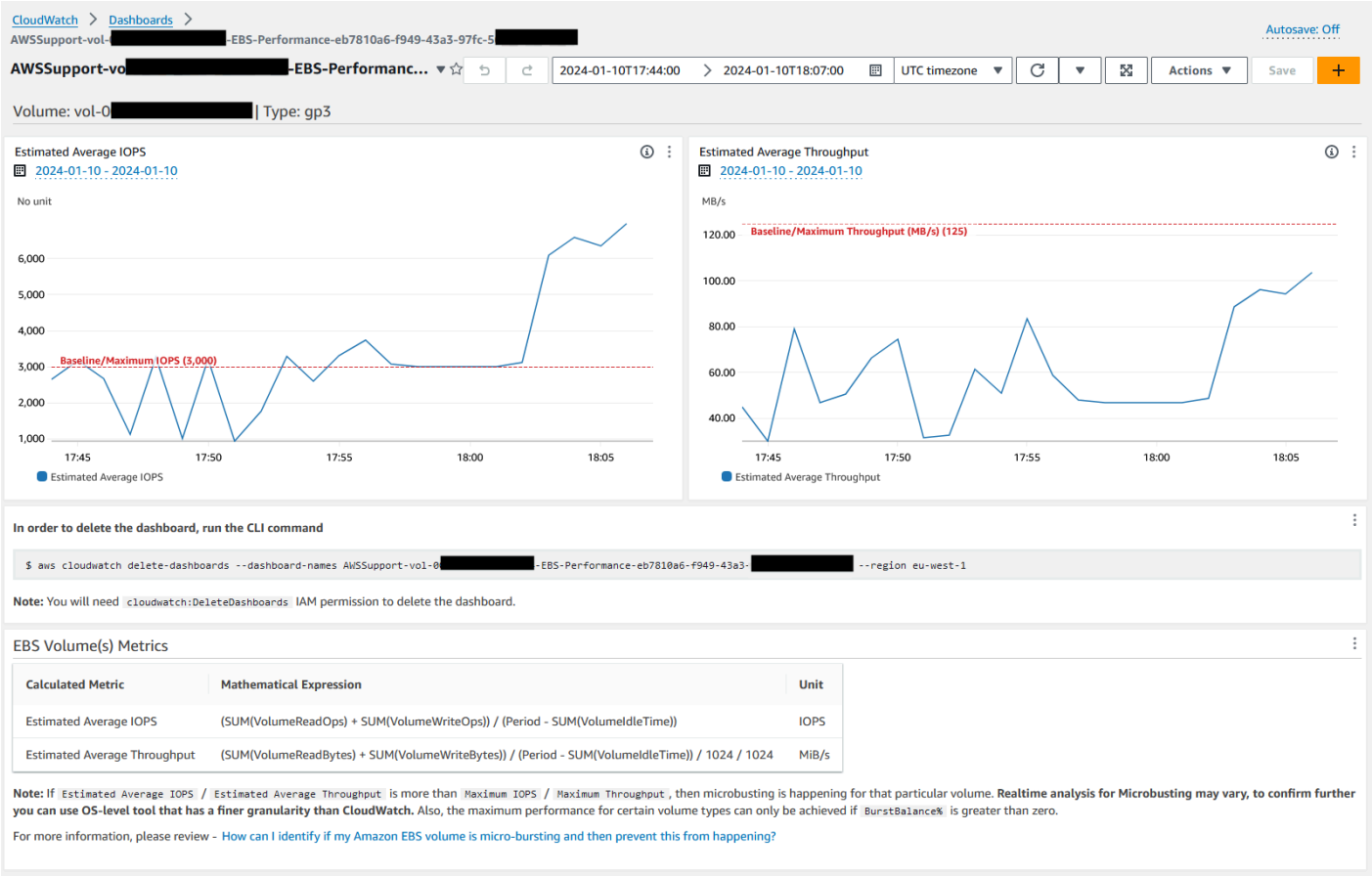


Volume: vol[redacted] | Type: gp3

Estimated Average IOPS

Estimated Average Throughput

Amazon EBS ボリューム ID としてのリソース ID の CloudWatch ダッシュボードの例



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスドキュメント

- Amazon EBS ボリュームがマイクロバーストしているかどうかを特定し、これを防ぐにはどうすればよいですか？
- CloudWatch を使用して EC2 インスタンスの Amazon EBS パフォーマンスメトリクスの集計を表示する方法

AWS-CopySnapshot

説明

Amazon Elastic Block Store (Amazon EBS) ボリュームのポイントインタイムスナップショットをコピーします。スナップショットは、同じリージョン内でコピー AWS リージョン することも、あるリージョンから別のリージョンにコピーすることもできます。暗号化された Amazon EBS スナップショットのコピーは暗号化されたままです。暗号化されていないスナップショットのコピーは暗号化されないままです。別のアカウントから共有された暗号化スナップショットをコピーするには、そのスナップショットの暗号化に使用された KMS キーのアクセス許可が必要です。別のスナップショットをコピーすることによって作成されたスナップショットの任意のボリューム ID は、いずれの目的にも使用しないでください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- 説明

  タイプ: 文字列

説明: (オプション) Amazon EBS スナップショットの説明

- SnapshotId

  タイプ: 文字列

  説明: (必須) コピーする Amazon EBS スナップショットの ID。

- SourceRegion

  タイプ: 文字列

  説明: (必須) ソースのスナップショットが現在存在するリージョン。

ドキュメントステップ

copySnapshot - Amazon EBS ボリュームのスナップショットをコピーします。

出力

copySnapshot.SnapshotId - 新しいスナップショットの ID。

AWS-CreateSnapshot

説明

Amazon EBS ボリュームのスナップショットを作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- 説明

  タイプ: 文字列

  説明: (オプション) スナップショットの説明

- ボリューム

  タイプ: 文字列

  説明: (必須) ボリュームの ID です。

AWS-DeleteSnapshot

説明

Amazon EBS ボリュームのスナップショットを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- SnapshotId

  タイプ: 文字列

  説明: (必須) EBS スナップショットの ID。

AWSConfigRemediation-DeleteUnusedEBSVolume

説明

AWSConfigRemediation-DeleteUnusedEBSVolume ランブックは、使用されていない Amazon Elastic Block Store (Amazon EBS) ボリュームを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- CreateSnapshot

  型: ブール値

  説明: (オプション) この値を `true` に設定すると、オートメーションは Amazon EBS ボリュームが削除される前に、そのボリュームのスナップショットを作成します。

- ボリューム

  タイプ: 文字列

  説明: (必須) 削除される Amazon EBS ボリュームの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeScript` - `VolumeId` パラメータで指定された Amazon EBS ボリュームが使用中でないことを確認し、`CreateSnapshot`パラメータで選択された値に応じてスナップショットを作成します。
- `aws:branch` - `CreateSnapshot` パラメータで選択された値に基づいて分岐させます。
- `aws:waitForAwsResourceProperty` - スナップショットが完了するまで待機します。
- `aws:executeAwsApi` - スナップショットの作成が失敗した場合に、そのスナップショットを削除します。

- aws:executeAwsApi - VolumeId パラメータで指定された Amazon EBS ボリュームを削除します。
- aws:executeScript - Amazon EBS ボリュームが削除されたことを確認します。

AWS-DeregisterAMIs

説明

AWS-DeregisterAMIs ランブックは、AMIs に適用したタグを指定することで Amazon Machine Images (AMIs) の登録を解除するのに役立ちます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- DryRun

  タイプ: 文字列

  有効な値: はい | いいえ

説明: (必須) 実際にリクエストを実行することなく、アクションに必要なアクセス許可があるかどうかを確認し、エラーレスポンスを提供します。

- RetainNumber

  タイプ: 文字列

  説明: (オプション) 保持する AMIs の番号。Age の値を指定していない場合、このパラメータの値を指定しないでください。

- 年齢

  タイプ: 文字列

  説明: (オプション) 保持する AMIs のそれ以前の日数。RetainNumber の値を指定していない場合、このパラメータの値を指定しないでください。

- TagKey

  タイプ: 文字列

  説明: (必須) 登録を解除する AMIs に割り当てられたタグのキー。

- TagValue

  タイプ: 文字列

  説明: (必須) 登録を解除する AMIs に割り当てられたタグの値。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ec2:DeregisterImage
- ec2:DescribeImages

ドキュメントステップ

- aws:executeAwsApi - ランブックの入力パラメータに指定した値を検証します。
- aws:executeAwsApi - TagKey および TagValue パラメータを使用して指定したタグを使用して AMIs の登録を解除します。

AWS-DetachEBSVolume

説明

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスから Amazon EBS ボリュームをデタッチします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- LambdaAssumeRole

  タイプ: 文字列

  説明: (オプション) Lambda によって引き受けられたロールの ARN
- ボリューム

  タイプ: 文字列

  説明: (必須) EBS ボリュームの ID。ボリュームとそのアタッチ先インスタンスは同じアベイラビリティーゾーンに存在している必要があります。

AWSConfigRemediation-EnableEbsEncryptionByDefault

説明

AWSConfigRemediation-EnableEbsEncryptionByDefault ランブックは、オートメーション AWS リージョン を実行する AWS アカウント および のすべての新しい Amazon Elastic Block Store (Amazon EBS) ボリュームで暗号化を有効にします。オートメーションを実行する前に作成されたボリュームは暗号化されません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeAwsApi - 現在のアカウントとリージョンで、デフォルトの Amazon EBS 暗号化設定を有効にします。
- aws:assertAwsResourceProperty - デフォルトの Amazon EBS 暗号化設定が有効化されているかを確認します。

AWS-ExtendEbsVolume

説明

AWS-ExtendEbsVolume ランブックは、Amazon EBS ボリュームのサイズを増やし、ファイルシステムを拡張します。この自動化は xfs および ext4 ファイルシステムをサポートします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- DriveLetter

  タイプ: 文字列

説明: (オプション) 拡張するファイルシステムのドライブの文字。このパラメータは Windows インスタンスに必須です。

- InstanceId

  タイプ: 文字列

  説明: (オプション) 拡張する Amazon EBS ボリュームがアタッチされた Amazon EC2 インスタンスの ID。

- KeepSnapshot

  型: ブール値

  デフォルト: true

  説明: (オプション) Amazon EBS ボリュームのサイズを増やす前に作成したスナップショットを保持するかどうかを決定します。

- MountPoint

  タイプ: 文字列

  説明: (オプション) 拡張するファイルシステムのドライブのマウントポイント。このパラメータは Linux インスタンスに必須です。

- SizeGib

  タイプ: 文字列

  説明: (必須) 変更する Amazon EBS ボリュームのサイズ (単位: GiB)。

- ボリューム

  タイプ: 文字列

  説明: (必須) 拡張される EBS ボリュームの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ec2:CreateSnapshot

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

ドキュメントステップ

- aws:executeScript - ボリュームのサイズを VolumeId パラメータで指定した値まで増やし、ファイルシステムを拡張します。

AWSSupport-ModifyEBSSnapshotPermission

説明

AWSSupport-ModifyEBSSnapshotPermission ランブックは、複数の Amazon Elastic Block Store (Amazon EBS) スナップショットに対するアクセス許可を変更するのに役立ちます。このランブックを使用すると、Public または Private スナップショットを作成したり、他の AWS アカウントと共有したりできます。デフォルトの KMS キーで暗号化されたスナップショットは、このランブックを使用する他のアカウントと共有することはできません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- AccountIds

  タイプ: StringList

  デフォルト: なし

  説明: (オプション) スナップショットを共有するアカウントの ID。このパラメータは、`Private` パラメータの値に `No` を入力する場合に必須です。

- AccountPermissionOperation

  タイプ: 文字列

  有効な値: 追加 | 削除

  デフォルト: なし

  説明: (オプション) 実行するオペレーションの種類。

- プライベート

  タイプ: 文字列

  有効な値: はい | いいえ

  説明: (必須) スナップショットを特定のアカウントと共有する場合、この値に `No` を入力します。

- SnapshotIds

  タイプ: StringList

  説明: (必須) アクセス許可を変更する Amazon EBS スナップショットの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

1. aws:executeScript - SnapshotIds パラメータで指定されたスナップショットの ID を検証します ID を確認した後、スクリプトは暗号化されたスナップショットを確認し、見つかった場合はリストを出力します。
2. aws:branch - Private パラメータで入力した値に基づいて自動化を分岐させます。
3. aws:executeScript - 指定したスナップショットの権限を変更して、指定したアカウントと共有します。
4. aws:executeScript - スナップショットの権限を Public から Private に変更します。

出力

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Result

MakePrivate.Result

MakePrivate.Commands

AWSConfigRemediation-ModifyEBSVolumeType

説明

AWSConfigRemediation-ModifyEBSVolumeType ランブックは、Amazon Elastic Block Store (Amazon EBS) ボリュームのボリュームタイプを変更します。ボリュームタイプが変更されると、ボリュームは optimizing 状態になります。ボリューム変更の進行状況のモニタリングについては、Amazon EC2 ユーザーガイド」の「ボリューム変更の進行状況のモニタリング」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- EbsVolumeId

  タイプ: 文字列

  説明: (必須) 変更する Amazon EBS ボリュームの ID。
- EbsVolumeType

  タイプ: 文字列

  有効な値: 標準 | io1 | io2 | gp2 | gp3 | sc1 | st1

  説明: Amazon EBS ボリュームを変更するボリュームタイプ。Amazon EBS ボリュームタイプの詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EBS ボリュームタイプ」を参照してください。 Amazon EC2

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:waitForAwsResourceProperty - ボリュームの状態が available または in-use であることを確認します。
- aws:executeAwsApi - EbsVolumeId パラメータで指定された Amazon EBS ボリュームを変更します。
- aws:waitForAwsResourceProperty - ボリュームタイプが EbsVolumeType パラメータで指定した値に変更されていることを確認します。

Amazon EC2

AWS Systems Manager Automation は、Amazon Elastic Compute Cloud 用に事前定義されたランブックを提供します。Amazon Elastic Block Storeのランブックは、ランブックリファレンスの Amazon EBS セクションにあります。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- 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

説明

Auto Scaling グループの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのスタンバイ状態を変更します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) Auto Scaling グループ内のスタンバイ状態を変更する Amazon EC2 インスタンスの ID。

- LambdaRoleArn

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Lambda がユーザーに代わってアクションを実行できるようにするロールの ARN。指定されていない場合、Lambda 関数を実行するために一時的なロールが作成されます。

AWS-ASGExitStandby

説明

Auto Scaling グループの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのスタンバイ状態を変更します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) Auto Scaling グループ内のスタンバイ状態を変更する EC2 インスタンスの ID。

- LambdaRoleArn

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Lambda がユーザーに代わってアクションを実行できるようにするロールの ARN。指定されていない場合、Lambda 関数を実行するために一時的なロールが作成されます。

AWS-CreateImage

説明

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスから新しい Amazon Machine Image (AMI) を作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: 文字列

  説明: (必須) EC2 インスタンスの ID。
- NoReboot

  型: ブール値

  説明: (オプション) イメージを作成する前にインスタンスを再起動しないでください。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

AWS-DeleteImage

説明

Amazon Machine Image (AMI) と、それに関連するすべてのスナップショットを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ImageId

  タイプ: 文字列

  説明: (必須) AMI の ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

```
{
```

```
    "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

説明

Auto Scaling グループの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスをパッチします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) パッチを適用するインスタンスの ID。メンテナンスウィンドウで実行するよう設定されているインスタンス ID は指定しないでください。

- LambdaRoleArn

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Lambda がユーザーに代わってアクションを実行できるようにするロールの ARN。指定されていない場合、Lambda 関数を実行するために一時的なロールが作成されます。

- WaitForInstance

  タイプ: 文字列

  デフォルト: PT2M

  説明: (オプション) インスタンスがサービスを再開するために自動化がスリープする時間。

- WaitForReboot

  タイプ: 文字列

  デフォルト: PT5M

  説明: (オプション) パッチ適用されたインスタンスを再起動するために自動化がスリープする時間。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

説明

EC2 インスタンスを適用可能なパッチベースラインに準拠させます。障害発生時にルートボリュームをロールバックします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: 文字列

  説明: (必須) パッチベースラインを適用する EC2 InstanceId。
- LambdaAssumeRole

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Lambda がユーザーに代わってアクションを実行できるようにするロールの ARN。指定されていない場合、Lambda 関数を実行するために一時的なロールが作成されます。
- ReportS3Bucket

  タイプ: 文字列

  説明: (オプション) 処理中に生成されたコンプライアンスレポートの Amazon S3 バケット送信先。

ドキュメントステップ

ステップ番号	ステップ名	自動化アクション
1	createDocumentStack	aws:createStack
2	IdentifyRootVolume	aws:invokeLambdaFunction
3	PrePatchSnapshot	aws:executeAutomation
4	installMissingUpdates	aws:runCommand
5	SleepThruInstallation	aws:invokeLambdaFunction
6	CheckCompliance	aws:invokeLambdaFunction
7	SaveComplianceReportToS3	aws:invokeLambdaFunction
8	ReportSuccessOrFailure	aws:invokeLambdaFunction
9	RestoreFromSnapshot	aws:invokeLambdaFunction
10	DeleteSnapshot	aws:invokeLambdaFunction
11	deleteCloudFormationTemplate	aws:deleteStack

出力

IdentifyRootVolume.Payload

PrePatchSnapshot.Output

SaveComplianceReportToS3.Payload

RestoreFromSnapshot.Payload

CheckCompliance.Payload

AWS-QuarantineEC2Instance

説明

AWS-QuarantineEC2Instance ランブックにより、インバウンドトラフィックまたはアウトバウンドトラフィックを一切許可しない Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにセキュリティグループを割り当てることができます。

> **Important**
>
> このランブックを実行する前に、RDP 設定に対し行った変更の内容を、慎重に確認しておく必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム

(ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) RDP 設定を管理するマネージドインスタンスの ID。

- IsolationSecurityGroup

  タイプ: 文字列

  説明: (必須) インバウンドトラフィックまたはアウトバウンドトラフィックを防ぐためにインスタンスに割り当てるセキュリティグループの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeAwsApi - インスタンスの詳細を収集します。
- aws:executeScript - インスタンスが Auto Scaling グループの一部ではないことを確認します。

- aws:executeAwsApi - インスタンスにアタッチされたルートボリュームのスナップショットを作成します。
- aws:waitForAwsResourceProperty - スナップショットの状態が completed になるまで待ちます。
- aws:executeAwsApi - IsolationSecurityGroup パラメータで指定されたセキュリティグループをインスタンスに割り当てます。

出力

GetEC2InstanceResources.RevokedSecurityGroupsIds

GetEC2InstanceResources.RevokedSecurityGroupsNames

createSnapshot.SnapId

AWS-ResizeInstance

説明

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのインスタンスタイプを変更します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) インスタンスの ID。

- InstanceType

  タイプ: 文字列

  説明: (必須) インスタンスタイプ。

AWS-RestartEC2Instance

説明

1 つ以上の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを再起動します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: StringList

  説明: (必須) 再起動するための Amazon EC2 インスタンスの ID。

AWS-SetupJupyter

説明

AWS-SetupJupyter ランブックは Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに Jupyter Notebook を設定するのに役立ちます。既存のインスタンスを指定することも、自動化に Amazon Machine Image (AMI) ID を指定して新しいインスタンスを起動してセットアップすることもできます。開始する前に、Jupyter Notebook のパスワードとして使用する SecureString パラメータを Parameter Store で作成する必要があります。Parameter Store は のツールです AWS Systems Manager。パラメータの作成に関する詳細については、「AWS Systems Manager ユーザーガイド」の「パラメータの作成」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- AmiId

  タイプ: 文字列

  説明: (オプション) 新しいインスタンスを起動して Jupyter Notebook を設定するのに使用する AMI の ID。

- InstanceId

  タイプ: 文字列

  説明: (必須) Jupyter Notebook をセットアップするインスタンスの ID。

- InstanceType

  タイプ: 文字列

  デフォルト: t3.medium

  説明: (オプション) Jupyter Notebook をセットアップするために新しいインスタンスを起動する場合は、使用するインスタンスタイプを指定します。

- JupyterPasswordSSMKey

  タイプ: 文字列

  説明: (必須) Jupyter Notebook のパスワードとして使用する Parameter Store 内の `SecureString` パラメータの名前。

- KeyPairName

  タイプ: 文字列

  説明: (オプション) 新しく起動されるインスタンスに関連付けるキーペア。

- RemoteAccessCidr

  タイプ: 文字列

  デフォルト: 0.0.0.0/0

説明: (オプション) SSH トラフィックを許可する CIDR 範囲。

- RoleName

  タイプ: 文字列

  デフォルト: SSMManagedInstanceProfileRole

  説明: (オプション) 新しく起動されるインスタンスのインスタンスプロファイルの名前。

- StackName

  タイプ: 文字列

  デフォルト: CreateManagedInstanceStack{{automation:EXECUTION_ID}}

  説明: (オプション) オートメーションで使用する AWS CloudFormation スタック名。

- SubnetId

  タイプ: 文字列

  デフォルト: Default

  説明: (オプション) 使用する新しいインスタンスを起動するサブネット。

- VpcId

  タイプ: 文字列

  デフォルト: Default

  説明: (オプション) 新しいインスタンスを起動する仮想プライベートクラウド (VPC) の ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `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

ドキュメントステップ

- aws:executeScript - ランブックの入力パラメータに指定した値を使用して、指定したインスタンスまたは新しく起動したインスタンスに Jupyter Notebook を設定します。

AWS-StartEC2Instance

説明

1 つ以上の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを起動します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: StringList

  説明: (必須) 起動する EC2 インスタンス。

AWS-StopEC2Instance

説明

1 つ以上の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを停止します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: StringList

  説明: (必須) 停止する EC2 インスタンス。

AWS-TerminateEC2Instance

説明

1 つ以上の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを終了します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: StringList

  説明: (必須) 終了する 1 つ以上の EC2 インスタンスの ID。

AWS-UpdateLinuxAmi

説明

Linux ディストリビューションパッケージと Amazon のソフトウェアを使用して、Amazon Machine Image (AMI) を更新します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ExcludePackages

  タイプ: 文字列

  デフォルト: なし

  説明: (オプション) すべての条件の下で、更新を保留するパッケージの名前。デフォルト ("none") では、パッケージは除外されません。

- IamInstanceProfileName

  タイプ: 文字列

  デフォルト: ManagedInstanceProfile

  説明: (必須) インスタンスを管理できるよう Systems Manager を有効にするインスタンスプロファイル。

- IncludePackages

  タイプ: 文字列

  デフォルト: all

  説明: (オプション) これらの名前付きパッケージのみを更新します。デフォルト ("all") では、すべての利用可能な更新が適用されます。

- InstanceType

  タイプ: 文字列

  デフォルト: t2.micro

  説明: (オプション) ワークスペースホストとして起動するインスタンスの種類。インスタンスタイプは、リージョンによって異なります。

- MetadataOptions

  型: StringMap

デフォルト: {"HttpEndpoint": "enabled", "HttpTokens": "optional"}

説明: (オプション) インスタンスのメタデータオプション。詳細については、「InstanceMetadataOptionsRequest」を参照してください。

- PostUpdateScript

  タイプ: 文字列

  デフォルト: なし

  説明: (オプション) パッケージの更新の適用後に実行するスクリプトの URL。デフォルト ("none") は、スクリプトを実行しません。

- PreUpdateScript

  タイプ: 文字列

  デフォルト: なし

  説明: (オプション) 更新の適用前に実行するスクリプトの URL。デフォルト ("none") は、スクリプトを実行しません。

- SecurityGroupIds

  タイプ: 文字列

  説明: (必須) に適用するセキュリティグループの IDs のカンマ区切りリストAMI。

- SourceAmiId

  タイプ: 文字列

  説明: (必須) Amazon マシンイメージ ID のソース。

- SubnetId

  タイプ: 文字列

  説明: (オプション) インスタンスを起動するサブネットの ID。デフォルトの VPC を削除した場合は、このパラメータは必須です。

- TargetAmiName

  タイプ: 文字列

デフォルト: UpdateLinuxAmi_from_{{SourceAmiId}}_on_{{global:DATE_TIME}}

説明: (オプション) 作成される新しい AMI の名前。デフォルトは、ソース AMI ID および作成日時を含む、システム生成文字列です。

AWS-UpdateWindowsAmi

説明

Microsoft Windows Amazon Machine Image (AMI) を更新します。デフォルトでは、このランブックはすべての Windows アップデート、Amazon ソフトウェア、および Amazon ドライバーをインストールします。次に、Sysprep を実行して新しい AMI を作成します。Windows Server 2008 R2 以降をサポートしています。

> **Important**
>
> インスタンスが VPC エンドポイント AWS Systems Manager を使用して に接続する場合、us-east-1 リージョンで使用しない限り、このランブックは失敗します。このランブックを使用するには、インスタンスで TLS 1.2 が有効になっている必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- カテゴリ

  タイプ: 文字列

  説明: (オプション) 1 つ以上の更新カテゴリを指定します。カンマ区切り値を使ってカテゴリをフィルターできます。オプション: Application、Connectors、CriticalUpdates、DefinitionUpdates、DeveloperKits、Drivers、FeaturePacks、有効な形式には、CriticalUpdates といった単一のエントリが含まれます。または、カンマ区切りリストを指定できます: CriticalUpdates、SecurityUpdates 注: カンマの周りにスペースは使用できません。

- ExcludeKbs

  タイプ: 文字列

  説明: (オプション) 除外する Microsoft Knowledge Base (KB) 記事 ID を 1 つ以上指定します。コンマ区切り値を使って複数の ID を除外できます。有効な形式: KB9876543 または 9876543。

- IamInstanceProfileName

  タイプ: 文字列

  デフォルト: ManagedInstanceProfile

  説明: (必須) インスタンスを管理できるよう Systems Manager を有効にするロールの名前。

- IncludeKbs

  タイプ: 文字列

  説明: (オプション) 含めたい Microsoft Knowledge Base (KB) 記事 ID を 1 つ以上指定します。コンマ区切り値を使って複数の ID をインストールできます。有効な形式: KB9876543 または 9876543。

- InstanceType

  タイプ: 文字列

デフォルト: t2.medium

説明: (オプション) ワークスペースホストとして起動するインスタンスの種類。インスタンスタイプは、リージョンによって異なります。デフォルトは t2.medium です。

- MetadataOptions

  型: StringMap

  デフォルト: {"HttpEndpoint": "enabled", "HttpTokens": "optional"}

  説明: (オプション) インスタンスのメタデータオプション。詳細については、「InstanceMetadataOptionsRequest」を参照してください。

- PostUpdateScript

  タイプ: 文字列

  説明: (オプション) 文字列として提供されるスクリプト。OS 更新をインストールした後に実行されます。

- PreUpdateScript

  タイプ: 文字列

  説明: (オプション) 文字列として提供されるスクリプト。OS 更新をインストールする前に実行されます。

- PublishedDateAfter

  タイプ: 文字列

  説明: (オプション) 後に公開する必要のある更新の日付を指定します。たとえば、2017/01/01 が指定されている場合、2017/01/01 以降に公開された更新が Windows Update の検索時に返されます。

- PublishedDateBefore

  タイプ: 文字列

  説明: (オプション) 以前に公開する必要のある更新の日付を指定します。たとえば、2017/01/01 が指定されている場合、2017/01/01 以前に公開された更新が Windows Update の検索時に返されます。

- PublishedDaysOld

タイプ: 文字列

説明: (オプション) 受け取る更新が公開日から何日経過しているかを指定できます。たとえば、10 が指定されている場合、10 日 以上前に発行された更新が Windows Update の検索時に返されます。

- SecurityGroupIds

  タイプ: 文字列

  説明: (必須) に適用するセキュリティグループの IDs のカンマ区切りリストAMI。

- SeverityLevels

  タイプ: 文字列

  説明: (オプション) 更新と関連付けられた MSRC 重要度レベルを 1 つ以上指定します。カンマ区切り値を使って重要度をフィルターできます。デフォルトでは、すべてのセキュリティレベルのパッチが選択されています。値が指定された場合、更新リストはこれらの値によってフィルタリングされます。オプション: 非常事態、重要、低、中、または指定しない。有効な形式には、「非常事態」といった単一のエントリが含まれます。または、カンマ区切りリストを指定できます: 非常事態,重要,低。

- SourceAmiId

  タイプ: 文字列

  説明: (必須) ソース AMI ID。

- SubnetId

  タイプ: 文字列

  説明: (オプション) インスタンスを起動するサブネットの ID。デフォルトの VPC を削除した場合は、このパラメータは必須です。

- TargetAmiName

  タイプ: 文字列

  デフォルト: UpdateWindowsAmi_from_{{SourceAmiId}}_on_{{global:DATE_TIME}}

  説明: (オプション) 作成される新しい AMI の名前。デフォルトは、ソース AMI ID および作成日時を含む、システム生成文字列です。

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

説明

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck ランブックでは、指定した Amazon EC2 Auto Scaling (Auto Scaling) グループのヘルスチェックを有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- AutoScalingGroupARN

  タイプ: 文字列

  説明: (必須) ヘルスチェックを有効にする Auto Scaling グループの Amazon リソースネーム (ARN)。
- HealthCheckGracePeriod

  タイプ: 整数

  デフォルト: 300

説明: (オプション) サービスの提供を開始した Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのヘルスステータスを確認するまでの Auto Scaling の待機時間 (秒)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- aws:executeScript - AutoScalingGroupARNパラメータで指定した Auto Scaling グループのヘルスチェックを有効にします。

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

説明

AWSConfigRemediation-EnforceEC2InstanceIMDSv2 ランブックで、インスタンスメタデータサービスのバージョン 2 (IMDSv2) を使用する際は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスが必要です。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- InstanceId

  タイプ: 文字列

  説明: (必須) IMDSv2 の使用が必要となる Amazon EC2 インスタンスの ID。
- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- HttpPutResponseHopLimit

  タイプ: 整数

  説明: (オプション) IMDS サービスからリクエスタに返されるホップレスポンスの制限。コンテナをホストする EC2 インスタンスの場合は、 を 2 以上に設定します。0 に設定すると、変更されません (デフォルト) 。

  許可されるパターン: `^([1-5]?\d|6[0-4])$`

  デフォルト: 0

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

- `aws:executeScript` - `InstanceId` パラメータで指定された Amazon EC2 インスタンスの、`HttpTokens` オプションを `required` に設定します。

- aws:assertAwsResourceProperty - Amazon EC2 インスタンスで IMDSv2 が必要であるかを確認します。

AWSEC2-CloneInstanceAndUpgradeSQLServer

説明

SQL Server 2008 (またはそれ以降) を実行している Windows Server の EC2 インスタンスから AMI を作成し、その AMI を SQL Server の後のバージョンにアップグレードします。SQL Server の英語バージョンのみがサポートされています。

サポートされているアップグレードパスは次のとおりです。

- SQL Server 2008 から SQL Server 2017、2016、または 2014 へ
- SQL Server 2008 R2 から SQL Server 2017、2016、または 2014 へ
- SQL Server 2012 から SQL Server 2019、2017、2016、または 2014 へ
- SQL Server 2014 から SQL Server 2019、2017、または 2016 へ
- SQL Server 2016 から SQL Server 2019 または 2017 へ

SQL Server 2019 と互換性のない以前のバージョンの Windows Server を使用している場合は、オートメーションドキュメントで Windows Server のバージョンを 2016 にアップグレードする必要があります。

アップグレードは、複数ステップのプロセスで、完了するまでに 2 時間かかる可能性があります。オートメーションは、インスタンスから AMI を作成し、指定された SubnetID 内で、この新しい AMI から一時インスタンスを起動します。元のインスタンスに関連付けられたセキュリティグループが一時インスタンスに適用されます。その後オートメーションは、一時インスタンス上で、TargetSQLVersion へのインプレースアップグレードを実行します。アップグレードが完了すると、オートメーションは一時インスタンスから新しい AMI を作成した上で、この一時インスタンスを終了します。

VPC で新しい AMI を起動することで、アプリケーション機能をテストできます。テストが終了したら、別のアップグレードを実行する前に、アップグレードされたインスタンスに完全に切り替える前にアプリケーションのダウンタイムをスケジュールします。

> **Note**
>
> 新しい AMI から起動された EC2 インスタンスのコンピュータ名を変更する場合は、「SQL Server のスタンドアロン インスタンスをホストするコンピューターの名前変更」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

前提条件

- TLS バージョン 1.2。
- SQL Server の英語バージョンのみがサポートされています。
- EC2 インスタンスでは、Windows Server 2008 R2 (またはそれ以降) および SQL Server 2008 (またはそれ以降) の Windows Server のバージョンを使用する必要があります。
- インスタンスに SSM Agent がインストールされていることを確認します。詳細については、「Windows Server の EC2 インスタンスで SSM Agent をインストールして設定する」を参照してください。
- AWS Identity and Access Management (IAM) インスタンスプロファイルロールを使用するようにインスタンスを設定します。詳細については「Systems Manager の IAM インスタンスプロファイルを作成する」を参照してください。
- インスタンスのブートディスクに 20 GB の空きディスク領域があるか、インスタンスを確認します。
- Bring Your Own License (BYOL) SQL Server バージョンを使用するインスタンスの場合、次の前提条件が追加で適用されます。

- ターゲットの SQL Server インストールメディアを含む EBS スナップショット ID を提供します。これを実行するには:

  1. EC2 インスタンスで Windows Server 2008 R2 以降が実行されていることを確認します。
  2. インスタンスが実行されているのと同じアベイラビリティーゾーンに 6 GB の EBS ボリュームを作成します。ボリュームをインスタンスにアタッチします。それをマウントします (例えばドライブ D として)。
  3. ISO を右クリックし、インスタンスにマウントします (例えばドライブ E として)。
  4. ISO の内容をドライブ E:\ からドライブ D:\ にコピーします。
  5. ステップ 2 で作成した 6 GB ボリュームの EBS スナップショットを作成します。

制約事項

- アップグレードはWindows 認証を使用して SQL Server 上でのみ実行できます。
- インスタンスに保留中のセキュリティパッチの更新がないことを確認します。[Control Panel (コントロール パネル)] を開き、[Check for updates (更新の確認)] を選択してください。
- HA およびミラーリングモードでの SQL Server のデプロイはサポートされていません。

パラメータ

- IamInstanceProfile

  タイプ: 文字列

  説明: (必須) IAM インスタンスプロファイル。

- InstanceId

  タイプ: 文字列

  説明: (必須) Windows Server 2008 R2 以降、および SQL Server 2008 以降を実行するインスタンス。

- KeepPreUpgradeImageBackUp

  タイプ: 文字列

説明: (オプション) `true` に設定すると、自動化はアップグレード前にインスタンスから作成された AMI を削除しません。`true` に設定されている場合は、AMI を削除する必要があります。デフォルトでは、AMI は削除されます。

- SubnetId

  タイプ: 文字列

  説明: (必須) アップグレードプロセスのサブネットを提供します。サブネットが AWS サービス、Amazon S3、Microsoft へのアウトバウンド接続があることを確認します (パッチをダウンロードするため) 。

- SQLServerSnapshotId

  タイプ: 文字列

  説明: (条件付き) ターゲット SQL Server インストールメディア用のスナップショット ID。このパラメータは、BYOL SQL Server バージョンを使用するインスタンスに必要です。このパラメータは、SQL Server ライセンス込みインスタンス (Microsoft SQL Server で Windows Server 用の AWS Amazon マシンイメージを使用して起動されるインスタンス) ではオプションです。

- RebootInstanceBeforeTakingImage

  タイプ: 文字列

  説明: (オプション) `true` に設定すると、自動化はアップグレード前の AMI を作成する前にインスタンスを再起動します。デフォルトでは、自動化はアップグレードの前に再起動しません。

- TargetSQLVersion

  タイプ: 文字列

  説明: (オプション) ターゲット SQL Server のバージョンを選択します。

  可能なターゲット:

  - SQL Server 2019
  - SQL Server 2017
  - SQL Server 2016
  - SQL Server 2014

  デフォルトのターゲット: SQL Server 2016

出力

AMIId: 後のバージョンの SQL Server にアップグレードされたインスタンスから作成された AMI の ID。

AWSEC2-CloneInstanceAndUpgradeWindows

説明

2008 R2、2012 R2、2016、または Windows Server 2019 インスタンスから Amazon Machine Image (AMI) を作成し、 AMIを Windows Server 2016、2019、または 2022 にアップグレードします。サポートされているアップグレードパスは次のとおりです。

- Windows Server 2008 R2 から Windows Server 2016。
- Windows Server 2012 R2 から Windows Server 2016。
- Windows Server 2012 R2 から Windows Server 2019。
- Windows Server 2012 R2 から Windows Server 2022。
- Windows Server 2016 から Windows Server 2019。
- Windows Server 2016 から Windows Server 2022。
- Windows Server 2019 から Windows Server 2022。

アップグレード操作は、複数ステップのプロセスで、完了するまでに 2 時間かかる可能性があります。少なくとも 2 つの vCPU と 4GB の RAM を持つインスタンスでオペレーティングシステムのアップグレードを実行することをお勧めします。オートメーションは、インスタンスから AMI を作成し、ユーザーにより指定された `SubnetId` 内で、この新しく作成した AMI から一時インスタンスを起動します。元のインスタンスに関連付けられたセキュリティグループが一時インスタンスに適用されます。その後オートメーションは、一時インスタンス上で、`TargetWindowsVersion` へのインプレースアップグレードを実行します。Windows Server 2008 R2 インスタンスから Windows Server 2016、2019 または 2022 へのアップグレードでは、Windows Server 2008 R2 から Windows Server 2016、2019 または 2022 への直接アップグレードはサポートされていないため、インプレースアップグレードが 2 回実行されます。また、オートメーションは、一時インスタンスに必要な AWS ドライバーの、更新もしくはインストールも行います。アップグレードが完了すると、オートメーションは一時インスタンスから新しい AMI を作成した上で、この一時インスタンスを終了します。

Amazon Virtual Private Cloud (Amazon VPC) のアップグレードされた AMI からテストインスタンスを起動することで、アプリケーションの機能をテストできます。テストが終了したら、別のアップグ

レードを実行する前に、アップグレードされた AMI に完全に切り替える前にアプリケーションのダウンタイムをスケジュールします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows Server 2008 R2、2012 R2、2016 または 2019 の Standard Edition と Datacenter Edition

前提条件

- TLS バージョン 1.2。
- インスタンスに SSM Agent がインストールされていることを確認します。詳細については、「Windows Server の EC2 インスタンスで SSM Agent をインストールして設定する」を参照してください。
- Windows PowerShell 3.0 以降をインスタンスにインストールする必要があります。
- Microsoft Active Directory ドメインに参加しているインスタンスの場合はホスト名の競合を避けるために、ドメインコントローラーに接続できない SubnetId を指定することをお勧めします。
- インスタンスサブネットにはインターネットへのアウトバウンド接続が必要です。これにより、Amazon S3 AWS のサービス などの へのアクセスと、Microsoft からパッチをダウンロードするためのアクセスが提供されます。この要件はサブネットがパブリックサブネットでインスタンスにパブリック IP アドレスがある場合、またはサブネットがインターネットトラフィックをパブリック NAT デバイスに送信するルートを持つプライベートサブネットの場合に満たされます。
- この Automation は、Windows Server 2008 R2、2012 R2、2016、および 2019 インスタンスでのみ動作します。
- Systems Manager に必要なアクセス許可を提供する AWS Identity and Access Management (IAM) インスタンスプロファイルWindows Serverを使用してインスタンスを設定します。詳細については「Systems Manager の IAM インスタンスプロファイルを作成する」を参照してください。
- インスタンスでブートディスクに 20 GB の空きディスク領域があることを確認します。

- インスタンスが AWSが提供する Windows ライセンスを使用しない場合は、2012 R2 インストールメディアを含む Amazon EBS Windows Server スナップショット ID を指定します。これを実行するには:
  - EC2 インスタンスで Windows Server 2012 以降が実行されていることを確認します。
  - インスタンスが実行されているのと同じアベイラビリティーゾーンに 6 GB の EBS ボリュームを作成します。ボリュームをインスタンスにアタッチします。それをマウントします (例えばドライブ D として)。
  - ISO を右クリックし、インスタンスにマウントします (例えばドライブ E として)。
  - ISO の内容をドライブ E:\ からドライブ D:\ にコピーします。
  - 上記の手順 2 で作成した 6 GB ボリュームの EBS スナップショットを作成します。

制約事項

この Automation では、Windows のドメインコントローラー、クラスター、または Windows デスクトップオペレーティングシステムのアップグレードはサポートされていません。このオートメーションでは、以下のロールがインストールされた Windows Server の EC2 インスタンスもサポートされていません。

- リモートデスクトップセッションホスト (RDSH)
- リモートデスクトップ接続ブローカー (RDCB)
- リモートデスクトップ仮想化ホスト (RDVH)
- リモートデスクトップウェブアクセス (RDWA)

パラメータ

- AlternativeKeyPairName

  タイプ: 文字列

  説明: (オプション) アップグレードプロセス中に使用する代替キーペアの名前。このキーペアは、元のインスタンスに割り当てられたキーペアが使用できない場合に便利に利用できます。元のインスタンスにキーペアが割り当てられていない場合は、このパラメータの値を指定する必要があります。
- BYOLWindowsMediaSnapshotId

  タイプ: 文字列

説明: (オプション) Windows Server 2012 R2 のインストールメディアを含む、コピーする Amazon EBS スナップショットの ID。BYOL インスタンスをアップグレードする場合にのみ必要です。

- IamInstanceProfile

  タイプ: 文字列

  説明: (必須) Systems Manager でのインスタンスの管理を可能にする IAM インスタンスプロファイルの名前。

- InstanceId

  タイプ: 文字列

  説明: (必須) Windows Server 2008 R2、2012 R2、2016、または 2019 を実行している EC2 インスタンス。

- KeepPreUpgradeImageBackUp

  タイプ: 文字列

  説明: (オプション) True に設定すると、オートメーションはアップグレード前に EC2 インスタンスから作成された AMI を削除しません。True に設定されている場合は、AMI を削除する必要があります。デフォルトでは、AMI は削除されます。

- SubnetId

  タイプ: 文字列

  説明: (必須) このサブネットはアップグレードプロセス用であり、ソース EC2 インスタンスの場所を指します。サブネットが AWS サービス、Amazon S3、Microsoft へのアウトバウンド接続があることを確認します (パッチをダウンロードするため) 。

- TargetWindowsVersion

  タイプ: 文字列

  説明: (必須) 対象の Windows バージョンを選択します。

  デフォルト: 2022

- RebootInstanceBeforeTakingImage

  タイプ: 文字列

説明: (オプション) True に設定すると、自動化はアップグレード前の AMI を作成する前にインスタンスを再起動します。デフォルトでは、自動化はアップグレードの前に再起動しません。

AWSEC2-ConfigureSTIG

セキュリティ技術実装ガイド (STIG) は、防衛情報システム局 (DISA) が情報システムとソフトウェアを保護するために作成した設定強化標準です。システムを STIG 標準に準拠させるには、さまざまなセキュリティ設定をインストール、設定、およびテストする必要があります。

Amazon EC2 には Systems Manager コマンドドキュメント が用意されています。これを使用して AWSEC2-ConfigureSTIGインスタンスに STIG 設定を適用できます。このドキュメントは、STIG 標準に準拠したイメージを迅速に構築するのに役立ちます。STIG Systems Manager ドキュメントは、設定ミスがないかをスキャンし、修復スクリプトを実行します。STIG Systems Manager ドキュメントにより、国防総省 (DoD) からの InstallRoot が Windows AMI にインストールされます。これにより、DoD 証明書のインストールや更新が行われ、STIG コンプライアンスを維持する上では不必要な証明書は削除されます。STIG Systems Manager ドキュメントの使用には、追加料金はかかりません。

> **Note**
>
> AWSEC2-ConfigureSTIG はコマンドドキュメントです。 AWS Systems Manager コンソールAWSEC2-ConfigureSTIGで を検索するには、 コマンドドキュメントカテゴリを選択します。

このページには、Amazon EC2 がサポートし、STIG 強化コンポーネントが EC2 インスタンスに適用されているすべての STIG がリストされています。

適用する STIG コンプライアンスカテゴリを選択できます。

コンプライアンスレベル

- 高 (カテゴリ I)

  最も深刻なリスクです。機密性、可用性、または整合性の損失につながる可能性のある脆弱性が含まれます。
- ミディアム (カテゴリ II)

機密性、可用性、整合性の損失につながる可能性があるものの、そのリスクが緩和される可能性がある脆弱性が含まれます。

- 低 (カテゴリー III)

  機密性、可用性、または整合性の喪失から保護するための対策を低下させる脆弱性が含まれます。

トピック

- STIG 強化コンポーネントのダウンロード
- Windows の STIG 設定
- Windows STIG バージョン履歴
- Linux の STIG 設定
- Linux STIG のバージョン履歴

STIG 強化コンポーネントのダウンロード

Amazon は STIG 強化コンポーネントをリリースごとにオペレーティングシステム関連のバンドルにまとめます。バンドルは、ダウンロードして実行するターゲットオペレーティングシステムに適したアーカイブファイルです。Linux コンポーネントバンドルは TAR ファイル (.tgz ファイル拡張子) として保存されます。Windows コンポーネントバンドルは ZIP ファイル (.zip ファイル拡張子) として保存されます。

Amazon はコンポーネントバンドルをそれぞれの AWS リージョンの Image Builder S3 `STIG` バケットに保存します。SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。

> **Important**
>
> この Systems Manager ドキュメントがダウンロードする STIG 強化コンポーネントは、いくつかの例外を除いて、サードパーティのパッケージをインストールしません。サードパーティのパッケージがインスタンスにすでにインストールされていて、Amazon EC2 がそのパッケージでサポートしている関連 STIG がある場合は、それらの STIG が適用されます。

コンポーネントストレージパスとバンドルファイル名のパターンと例は次のとおりです。

コンポーネントストレージパス

`s3://aws-windows-downloads-<region>/STIG/<bundle file name>`

コンポーネントパス変数

region

AWS リージョン（各リージョンには独自のコンポーネントバケットがあります）。

bundle file name

形式は *<os bundle name>*_*<YYYY>*_Q*<quarter>*[_*<release>*].*<file extension>* です。名前のノード間にはピリオドではなくアンダースコアが付いていることに注意してください。

os bundle name

オペレーティングシステムバンドルの標準名プレフィックスは `LinuxAWSConfigureSTIG` または `AWSConfigureSTIG` です。下位互換性を維持するために、Windows 用の ダウンロードにはプラットフォームプレフィックスは含まれていません。

YYYY

4 桁のリリースの年。

quarter

1、2、3、4 のいずれかの四半期を識別します。

release

1 から始まり、新しいリリースごとに 1 ずつ増える増分番号。このリリースは、四半期内の最初のリリースには含まれず、以降のリリースにのみ追加されます。

file extension

圧縮ファイルフォーマット `tgz` (Linux) または `zip` (Windows)。

バンドルファイル名の例

- `LinuxAWSConfigureSTIG_2023_Q1_2.tgz`
- `AWSConfigureSTIG_2022_Q4.zip`

Windows の STIG 設定

Amazon EC2 Windows の STIG AMI および強化コンポーネントは、スタンドアロンサーバー用に設計され、ローカルグループポリシーを適用します。STIG 準拠のコンポーネントは、国防総省 (DoD) から Windows AMI に InstallRoot をインストールし、DoD 証明書をダウンロード、イン

ストール、更新します。また、STIG への準拠を維持するために不要な証明書も削除します。現在、Amazon EC2 は Windows Server の次のバージョンの STIG ベースラインをサポートしています: 2012 R2、2016、2019、2022。

このセクションでは、Amazon EC2 が Windows インフラストラクチャでサポートしている現在の STIG 設定をリストし、その後にバージョン履歴ログを示します。

低、中、高の STIG 設定を適用できます。

Windows STIG Low (Category III)

次のリストには、Amazon EC2 がインフラストラクチャに対してサポートしている STIG 設定が含まれています。サポートされている設定がお客様のインフラストラクチャに適用できない場合、Amazon EC2 はその設定をスキップして次に進みます。例えば、一部の STIG 強化設定は、スタンドアロンサーバーには適用されない場合があります。組織固有のポリシーも、適用される設定に影響を与える可能性があります (例: 管理者がドキュメントの設定を確認する必要がある)。

Windows 向け STIG の完全なリストについては、「STIG ドキュメントライブラリ」を参照してください。完全なリストを表示する方法の詳細については、「STIG 表示ツール」を参照してください。

- Windows Server 2022 STIG バージョン 2 リリース 2

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363, および V-254481
- Windows Server 2019 STIG バージョン 3 リリース 2

  V-205691、V-205819、V-205858、V-205859、V-205860、V-205870、V-205871、および V-205923
- Windows Server 2016 STIG バージョン 2 リリース 9

  V-224916、V-224917、V-224918、V-224919、V-224931、V-224942、および V-225060
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 5

  V-225537、V-225536、V-225526、V-225525、V-225514、V-225511、V-225490、V-225489、V-225488 および V-225250
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 2

  Microsoft .NET フレームワークには、カテゴリ III の脆弱性に対応する STIG 設定は適用されません。
- Windows Firewall STIG バージョン 2 リリース 2

V-241994、V-241995、V-241996、V-241999、V-242000、V-242001、V-242006、V-242007、V-242008

- Internet Explorer 11 STIG バージョン 2 リリース 5

  V-223016, V-223056、および V-223078

- Microsoft Edge STIG バージョン 2 リリース 2 (Windows Server 2022 のみ)

  V-235727、V-235731、V-235751、V-235752 および V-235765

Windows STIG Medium (Category II)

次のリストには、Amazon EC2 がインフラストラクチャに対してサポートしている STIG 設定が含まれています。サポートされている設定がお客様のインフラストラクチャに適用できない場合、Amazon EC2 はその設定をスキップして次に進みます。例えば、一部の STIG 強化設定は、スタンドアロンサーバーには適用されない場合があります。組織固有のポリシーも、適用される設定に影響を与える可能性があります (例: 管理者がドキュメントの設定を確認する必要がある)。

Windows 向け STIG の完全なリストについては、「STIG ドキュメントライブラリ」を参照してください。完全なリストを表示する方法の詳細については、「STIG 表示ツール」を参照してください。

> **Note**
>
> Windows STIG Medium カテゴリには、Amazon EC2 が Category II の脆弱性をサポートする STIG 強化設定に加えて、Windows STIG Low (Category III) に適用されるリスト済みのすべての STIG 強化設定が含まれます。

- Windows Server 2022 STIG バージョン 2 リリース 2

  Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  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-254365、 V-254366、 V-254367、 V-254368、
V-254369、 V-254370、 V-254371、 V-254372、 V-254373、 V-254375、 V-254376、
V-254377、 V-254379、 V-254380、 V-254382、 V-254383、 V-254384、 V-254431、
V-254432、 V-254433、 V-254434、 V-254435、 V-254436、 V-254438、 V-254439、
V-254442、 V-254443、 V-254444 V-254445、 V-254449、 V-254450、 V-254451、 V-254452、
V-254453、 V-254454、 V-254455、 V-254456、 V-254459、 V-254460、 V-254461、
V-254462、 V-254463、 V-254464、 V-254468、 V-254470、 V-254471、 V-254472、
V-254473、 V-254476、 V-254477、 V-254478、 V-254479、 V-254480、 V-254482、
V-254483、 V-254484、 V-254485、 V-254486、 V-254487、 V-254488、 V-254489、
V-254490、 V-254493、 V-254494、 V-254495、 V-254497、 V-254499、 V-254501、
V-254502、 V-254503、 V-254504、 V-254505、 V-254507、 V-254508、 V-254509、
V-254510、 V-254511、 および V-254512

- Windows Server 2019 STIG バージョン 3 リリース 2

  Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  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-205652、 V-205655、 V-205656、
  V-205659、 V-205660、 V-205662、 V-205671、 V-205672、 V-205673、 V-205675、
  V-205676、 V-205678、 V-205679、 V-205680、 V-205681、 V-205682、 V-205683、
  V-205684、 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-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-205825、 V-205826、
  V-205827、 V-205828、 V-205830、 V-205832、 V-205833、 V-205834、 V-205835、

V-205836、 V-205837、 V-205838、 V-205839、 V-205840、 V-205841、 V-205842、 V-205861、 V-205863、 V-205865、 V-205866、 V-205867、 V-205868、 V-205869、 V-205872、 V-205873、 V-205874、 V-205911、 V-205912、 V-205915、 V-205916、 V-205917、 V-205918、 V-205920、 V-205921、 V-205922、 V-205924、 V-205925、 V-236001、 および V-257503

- Windows Server 2016 STIG バージョン 2 リリース 9

  Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  V-224850、 V-224852、 V-224853、 V-224854、 V-224855、 V-224856、 V-224857、 V-224858、 V-224859、 V-224866、 V-224867、 V-224868、 V-224869、 V-224870、 V-224871、 V-224872、 V-224873、 V-224881、 V-224882、 V-224883、 V-224884、 V-224885、 V-224886、 V-224887、 V-224888、 V-224889、 V-224890、 V-224891、 V-224892、 V-224893、 V-224894、 V-224895、 V-224896、 V-224897、 V-224898、 V-224899、 V-224900、 V-224901、 V-224902、 V-224903、 V-224904、 V-224905、 V-224906、 V-224907、 V-224908、 V-224909、 V-224910、 V-224911、 V-224912、 V-224913、 V-224914、 V-224915、 V-224920、 V-224922、 V-224924、 V-224925、 V-224926、 V-224927、 V-224928、 V-224929、 V-224930、 V-224935、 V-224936、 V-224937、 V-224938、 V-224939、 V-224940、 V-224941、 V-224943、 V-224944、 V-224945、 V-224946、 V-224947、 V-224948、 V-224949、 V-224951、 V-224952、 V-224953、 V-224955、 V-224956、 V-224957、 V-224959、 V-224960、 V-224962、 V-224963、 V-225010、 V-225013、 V-225014、 V-225015、 V-225016、 V-225017、 V-225018、 V-225019、 V-225021、 V-225022、 V-225023、 V-225024、 V-225028、 V-225029、 V-225030、 V-225031、 V-225032、 V-225033、 V-225034、 V-225035、 V-225038、 V-225039、 V-225040、 V-225041、 V-225042、 V-225043、 V-225047、 V-225049、 V-225050、 V-225051、 V-225052、 V-225055、 V-225056、 V-225057、 V-225058、 V-225059、 V-225061、 V-225062、 V-225063、 V-225064、 V-225065、 V-225066、 V-225067、 V-225068、 V-225069、 V-225072、 V-225073、 V-225074、 V-225076、 V-225078、 V-225080、 V-225081、 V-225082、 V-225083、 V-225084、 V-225086、 V-225087、 V-225088、 V-225089、 V-225092、 V-225093、 V-236000、 および V-257502

- Windows Server 2012 R2 MS STIG バージョン 3 リリース 5

  Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

V-225574、V-225573、V-225572、V-225571、V-225570、V-225569、V-225568、V-225567、V-225566 および V-225239

- Microsoft .NET Framework STIG 4.0 バージョン 2 リリース 2

  Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  V-225238

- Windows Firewall STIG バージョン 2 リリース 2

  Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  V-241989, V-241990, V-241991, V-241993, V-241993, V-241998, V-241998, V-242003、および V-242003

- Internet Explorer 11 STIG バージョン 2 リリース 5

  Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  V-223015、 V-223017、 V-223018、 V-223019、 V-223020、 V-223021、 V-223022、
  V-223023、 V-223024、 V-223025、 V-223026、 V-223027、 V-223028、 V-223029、
  V-223030、 V-223031、 V-223032、 V-223033、 V-223034、 V-223035、 V-223036、
  V-223037、 V-223038、 V-223039、 V-223040、 V-223041、 V-223042、 V-223043、
  V-223044、 V-223045、 V-223046、 V-223048、 V-223049、 V-223050、 V-223051、
  V-223052、 V-223053、 V-223054、 V-223055、 V-223057、 V-223058、 V-223059、
  V-223060、 V-223061、 V-223062、 V-223063、 V-223064、 V-223065、 V-223066、
  V-223067、 V-223068、 V-223069、 V-223070、 V-223071、 V-223072、 V-223073、
  V-223074、 V-223075、 V-223076、 V-223077、 V-223079、 V-223080、 V-223081、
  V-223082、 V-223083、 V-223084、 V-223085、 V-223086、 V-223087、 V-223088、
  V-223089、 V-223090、 V-223091、 V-223092、 V-223093、 V-223094、 V-223095、
  V-223096、 V-223097、 V-223098、 V-223099、 V-223100、 V-223101、 V-223102、
  V-223103、 V-223104、 V-223105、 V-223106、 V-223107、 V-223108、 V-223109、
  V-223110、 V-223111、 V-223112、 V-223113、 V-223114、 V-223115、 V-223116、
  V-223117、 V-223118、 V-223119、 V-223120、 V-223121、 V-223122、 V-223123、
  V-223124、 V-223125、 V-223126、 V-223127、 V-223128、 V-223129、 V-223130、
  V-223131、 V-223132、 V-223133、 V-223134、 V-223135、 V-223136、 V-223137、

V-223138、 V-223139、 V-223140、 V-223141、 V-223142、 V-223143、 V-223144、 V-223145、 V-223146、 V-223147、 V-223148、 V-223149、 V-250540、 および V-250541

- Microsoft Edge STIG バージョン 2 リリース 2 (Windows Server 2022 のみ)

  V-235720、V-235721、V-235723、V-235724、V-235725、V-235726、V-235728、V-235729、V-235730 および V-246736

- Microsoft Defender STIG バージョン 2 リリース 4

  V-213427、V-213429、V-213430、V-213431、V-213432、V-213433、V-213434、V-213435、V-213436 および V-213466

Windows STIG High (Category I)

次のリストには、Amazon EC2 がインフラストラクチャに対してサポートしている STIG 設定が含まれています。サポートされている設定がお客様のインフラストラクチャに適用できない場合、Amazon EC2 はその設定をスキップして次に進みます。例えば、一部の STIG 強化設定は、スタンドアロンサーバーには適用されない場合があります。組織固有のポリシーも、適用される設定に影響を与える可能性があります (例: 管理者がドキュメントの設定を確認する必要がある)。

Windows 向け STIG の完全なリストについては、「STIG ドキュメントライブラリ」を参照してください。完全なリストを表示する方法の詳細については、「STIG 表示ツール」を参照してください。

> **Note**
>
> Windows STIG High カテゴリには、Amazon EC2 が Category I の脆弱性をサポートする STIG 強化設定に加えて、Windows STIG Medium および Low カテゴリに適用されるリスト済みのすべての STIG 強化設定が含まれます。

- Windows Server 2022 STIG バージョン 2 リリース 2

  V-254293、V-254352、V-254353、V-254354、V-254374、V-254378、V-254381、V-254446、V-254465 および V-254500

- Windows Server 2019 STIG バージョン 3 リリース 2

  Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

V-205653、V-205654、V-205711、V-205713、V-205724、V-205725、V-205757、V-205802、V-205804 および V-205919

- Windows Server 2016 STIG バージョン 2 リリース 9

  Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  V-224874、V-224932、V-224933、V-224934、V-224954、V-224958、V-224961、V-225025、V-225044 および V-225079

- Windows Server 2012 R2 MS STIG バージョン 3 リリース 5

  Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  V-225556、V-225552、V-225547、V-225507、V-225505、V-225498、V-225497、V-225496、V-225493 および V-225274

- Microsoft .NET Framework STIG 4.0 バージョン 2 リリース 2

  Microsoft .NET Framework のカテゴリ II および III (Medium および Low) の脆弱性に対して Amazon EC2 がサポートするすべての STIG 強化設定が含まれます。カテゴリ I の脆弱性に対して、追加的な STIG 設定は適用されません。

- Windows Firewall STIG バージョン 2 リリース 2

  Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  V-241992、V-241997、および V-242002

- Internet Explorer 11 STIG バージョン 2 リリース 5

  Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  V-252910

- Microsoft Edge STIG バージョン 2 リリース 2 (Windows Server 2022 のみ)

  Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

V-235758 および V-235759

- Microsoft Defender STIG バージョン 2 リリース 4

  Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

  V-213426, V-213426, V-213452, V-213452, V-213452, V-213453, V-213453、および V-213453

Windows STIG バージョン履歴

このセクションには、四半期ごとの STIG アップデートに関する Windows コンポーネントのバージョン履歴が記録されます。四半期ごとの変更点と公開されたバージョンを確認するには、タイトルを選択して情報を展開します。

2025 年Q1 四半期の変更 - 05/04/2025:

2025 年第 1 四半期リリースのすべての STIG コンポーネントの Internet Explorer 11 STIG バージョン 2 リリース 5 の STIGS を更新しました。

- STIG-Build-Windows-Low バージョン 2025.1.x
- STIG-Build-Windows-Medium バージョン 2025.1.x
- STIG-Build-Windows-High バージョン 2025.1.x

2024 年Q4 四半期の変更 - 12/10/2024:

STIG バージョンを更新し、2024 年Q4 四半期リリースの STIGS を次のように適用しました。

STIG-Build-Windows-Low バージョン 2024.4.0

- Windows Server 2022 STIG バージョン 2 リリース 2
- Windows Server 2019 STIG バージョン 3 リリース 2
- Windows Server 2016 STIG バージョン 2 リリース 9
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 5
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 2
- Windows Firewall STIG バージョン 2 リリース 2
- Internet Explorer 11 STIG バージョン 2 リリース 5

- Microsoft Edge STIG バージョン 2 リリース 2 (Windows Server 2022 のみ)

STIG-Build-Windows-Medium バージョン 2024.4.0

- Windows Server 2022 STIG バージョン 2 リリース 2
- Windows Server 2019 STIG バージョン 3 リリース 2
- Windows Server 2016 STIG バージョン 2 リリース 9
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 5
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 2
- Windows Firewall STIG バージョン 2 リリース 2
- Internet Explorer 11 STIG バージョン 2 リリース 5
- Microsoft Edge STIG バージョン 2 リリース 2 (Windows Server 2022 のみ)
- Defender STIG バージョン 2 リリース 4

STIG-Build-Windows-High バージョン 2024.4.0

- Windows Server 2022 STIG バージョン 2 リリース 2
- Windows Server 2019 STIG バージョン 3 リリース 2
- Windows Server 2016 STIG バージョン 2 リリース 9
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 5
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 2
- Windows Firewall STIG バージョン 2 リリース 2
- Internet Explorer 11 STIG バージョン 2 リリース 5
- Microsoft Edge STIG バージョン 2 リリース 2 (Windows Server 2022 のみ)
- Defender STIG バージョン 2 リリース 4

2024 年Q3 四半期の変更 - 10/04/2024 (変更なし):

2024 年第 3 四半期リリースでは、Windows コンポーネント STIGS に変更はありませんでした。

2024 年第 2 四半期の変更 - 2024 年 5 月 10 日 (変更なし):

2024 年第 2 四半期リリースの Windows コンポーネント STIG には変更はありませんでした。

2024 年Q1 四半期の変更 - 02/23/2024 (変更なし):

2024 年第 1 四半期リリースの Windows コンポーネント STIG には変更はありませんでした。

2023 年Q4 四半期の変更 - 12/07/2023 (変更なし):

2023 年第 4 四半期リリースの Windows コンポーネント STIG には変更はありませんでした。

2023 年第 3 四半期の変更-2023 年 4 月 10 日 (変更なし):

2023 年第 3 四半期リリースの Windows コンポーネント STIGS には変更はありませんでした。

2023 年第 2 四半期の変更-2023 年 5 月 3 日 (変更なし):

2023 年第 2 四半期リリースの Windows コンポーネント STIGS には変更はありませんでした。

2023 年第 1 四半期の変更-2023 年 3 月 27 日 (変更なし):

2023 年第 1 四半期リリースの Windows コンポーネント STIGS には変更はありませんでした。

2022 年第 4 四半期の変更-2023 年 2 月 1 日:

STIG のバージョンを更新し、2022 年第 4 四半期のリリースに向けて以下のように STIGS を適用しました。

STIG-Build-Windows-Low バージョン 2022.4.0

- Windows Server 2022 STIG バージョン 1 リリース 1
- Windows Server 2019 STIG バージョン 2 リリース 5
- Windows Server 2016 STIG バージョン 2 リリース 5
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 5
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 2
- Windows Firewall STIG バージョン 2 リリース 1
- Internet Explorer 11 STIG バージョン 2 リリース 3
- Microsoft Edge STIG バージョン 1 リリース 6 (Windows Server 2022 のみ)

STIG-Build-Windows-Medium バージョン 2022.4.0

- Windows Server 2022 STIG バージョン 1 リリース 1

- Windows Server 2019 STIG バージョン 2 リリース 5
- Windows Server 2016 STIG バージョン 2 リリース 5
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 5
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 2
- Windows Firewall STIG バージョン 2 リリース 1
- Internet Explorer 11 STIG バージョン 2 リリース 3
- Microsoft Edge STIG バージョン 1 リリース 6 (Windows Server 2022 のみ)
- Defender STIG バージョン 2 リリース 4 (Windows Server 2022 のみ)

STIG-Build-Windows-High バージョン 2022.4.0

- Windows Server 2022 STIG バージョン 1 リリース 1
- Windows Server 2019 STIG バージョン 2 リリース 5
- Windows Server 2016 STIG バージョン 2 リリース 5
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 5
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 2
- Windows Firewall STIG バージョン 2 リリース 1
- Internet Explorer 11 STIG バージョン 2 リリース 3
- Microsoft Edge STIG バージョン 1 リリース 6 (Windows Server 2022 のみ)
- Defender STIG バージョン 2 リリース 4 (Windows Server 2022 のみ)

2022 年第 3 四半期の変更-2022 年 9 月 30 日 (変更なし):

2022 年第 3 四半期リリースの Windows コンポーネント STIGS には変更はありませんでした。

2022 年第 2 四半期の変更-2022 年 8 月 2 日:

STIG のバージョンを更新し、2022 年第 2 四半期のリリースに向けて STIGS を適用しました。

STIG-Build-Windows-Low バージョン 1.5.0

- Windows Server 2019 STIG バージョン 2 リリース 4
- Windows Server 2016 STIG バージョン 2 リリース 4
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 3

- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 1
- Windows Firewall STIG バージョン 2 リリース 1
- Internet Explorer 11 STIG バージョン 1 リリース 19

STIG-Build-Windows-Medium バージョン 1.5.0

- Windows Server 2019 STIG バージョン 2 リリース 4
- Windows Server 2016 STIG バージョン 2 リリース 4
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 3
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 1
- Windows Firewall STIG バージョン 2 リリース 1
- Internet Explorer 11 STIG バージョン 1 リリース 19

STIG-Build-Windows-High バージョン 1.5.0

- Windows Server 2019 STIG バージョン 2 リリース 4
- Windows Server 2016 STIG バージョン 2 リリース 4
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 3
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 1
- Windows Firewall STIG バージョン 2 リリース 1
- Internet Explorer 11 STIG バージョン 1 リリース 19

2022 年第 1 四半期の変更-2022 年 8 月 2 日 (変更なし):

2022 年第 1 四半期リリースの Windows コンポーネント STIGS には変更はありませんでした。

2021 年第 4 四半期の変更-2021 年 12 月 20 日:

STIG のバージョンを更新し、2021 年第 4 四半期のリリースに向けて STIGS を適用しました。

STIG-Build-Windows-Low バージョン 1.5.0

- Windows Server 2019 STIG バージョン 2 リリース 3
- Windows Server 2016 STIG バージョン 2 リリース 3
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 3

- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 1
- Windows Firewall STIG バージョン 2 リリース 1
- Internet Explorer 11 STIG バージョン 1 リリース 19

STIG-Build-Windows-Medium バージョン 1.5.0

- Windows Server 2019 STIG バージョン 2 リリース 3
- Windows Server 2016 STIG バージョン 2 リリース 3
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 3
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 1
- Windows Firewall STIG バージョン 2 リリース 1
- Internet Explorer 11 STIG バージョン 1 リリース 19

STIG-Build-Windows-High バージョン 1.5.0

- Windows Server 2019 STIG バージョン 2 リリース 3
- Windows Server 2016 STIG バージョン 2 リリース 3
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 3
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 1
- Windows Firewall STIG バージョン 2 リリース 1
- Internet Explorer 11 STIG バージョン 1 リリース 19

2021 年第 3 四半期の変更-2021 年 9 月 30 日:

STIG のバージョンを更新し、2021 年第 3 四半期のリリースに向けて STIGS を適用しました。

STIG-Build-Windows-Low バージョン 1.4.0

- Windows Server 2019 STIG バージョン 2 リリース 2
- Windows Server 2016 STIG バージョン 2 リリース 2
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 2
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 1
- Windows ファイアウォール STIG バージョン 1 リリース 7
- Internet Explorer 11 STIG バージョン 1 リリース 19

STIG-Build-Windows-Medium バージョン 1.4.0

- Windows Server 2019 STIG バージョン 2 リリース 2
- Windows Server 2016 STIG バージョン 2 リリース 2
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 2
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 1
- Windows ファイアウォール STIG バージョン 1 リリース 7
- Internet Explorer 11 STIG バージョン 1 リリース 19

STIG-Build-Windows-High バージョン 1.4.0

- Windows Server 2019 STIG バージョン 2 リリース 2
- Windows Server 2016 STIG バージョン 2 リリース 2
- Windows Server 2012 R2 MS STIG バージョン 3 リリース 2
- Microsoft .NET Framework 4.0 STIG バージョン 2 リリース 1
- Windows ファイアウォール STIG バージョン 1 リリース 7
- Internet Explorer 11 STIG バージョン 1 リリース 19

Linux の STIG 設定

このセクションには、Amazon EC2 がサポートする Linux STIG 強化設定に関する情報と、その後にバージョン履歴ログが含まれています。Linux ディストリビューションに独自の STIG 強化設定がない場合、Amazon EC2 は RHEL 設定を使用します。サポート済みの STIG 強化設定は、Linux ディストリビューションに基づき、Amazon EC2 Linux AMI およびコンポーネントに以下のように適用されます。

- Red Hat Enterprise Linux (RHEL) 7 STIG 設定
  - RHEL 7
  - CentOS 7
  - Amazon Linux 2 (AL2)
- RHEL 8 STIG 設定
  - RHEL 8
  - CentOS 8

  - Amazon Linux 2023 (AL 2023)
- RHEL 9 STIG 設定
  - RHEL 9
  - CentOS Stream 9

Linux STIG Low (Category III)

次のリストには、Amazon EC2 がインフラストラクチャに対してサポートしている STIG 設定が含まれています。サポートされている設定がお客様のインフラストラクチャに適用できない場合、Amazon EC2 はその設定をスキップして次に進みます。例えば、一部の STIG 強化設定は、スタンドアロンサーバーには適用されない場合があります。組織固有のポリシーも、適用される設定に影響を与える可能性があります (例: 管理者がドキュメントの設定を確認する必要がある)。

詳細なリストについては、「STIGs Document Library」を参照してください。完全なリストを表示する方法の詳細については、「STIG 表示ツール」を参照してください。

RHEL 7 STIG バージョン 3 リリース 14

- RHEL 7/CentOS 7/AL2

  V-204452、V-204576、および V-204605

RHEL 8 STIG バージョン 2 リリース 2

- RHEL 8/CentOS 8/AL 2023

  V-230241, V-230281, V-244527, V-230269, V-230270, V-230285, V-230346, V-230381, V-230395, V-230491, V-230468, V-230469, V-230485, V-230486, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499、V-230253

RHEL 9 STIG バージョン 2 リリース 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、および V-257947

Ubuntu 18.04 STIG バージョン 2 リリース 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, および V-219333

Ubuntu 20.04 STIG バージョン 2 リリース 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、および V-238308

Ubuntu 22.04 STIG バージョン 2 リリース 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、および V-260596

Ubuntu 24.04 STIG バージョン 1 リリース 1

V-270645, V-270646, V-270664, V-270820, V-270677, V-270690, V-270706, V-270710, V-270695, V-270749, V-270752、および V-270818

Linux STIG Medium (Category II)

次のリストには、Amazon EC2 がインフラストラクチャに対してサポートしている STIG 設定が含まれています。サポートされている設定がお客様のインフラストラクチャに適用できない場合、Amazon EC2 はその設定をスキップして次に進みます。例えば、一部の STIG 強化設定は、スタンドアロンサーバーには適用されない場合があります。組織固有のポリシーも、適用される設定に影響を与える可能性があります (例: 管理者がドキュメントの設定を確認する必要がある)。

詳細なリストについては、「STIGs Document Library」を参照してください。完全なリストを表示する方法の詳細については、「STIG 表示ツール」を参照してください。

> **Note**
>
> Linux STIG Medium カテゴリには、Amazon EC2 が Category II の脆弱性をサポートする STIG 強化設定に加えて、Linux STIG Low (Category III) に適用されるリスト済みのすべての STIG 強化設定が含まれます。

RHEL 7 STIG バージョン 3 リリース 15

Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

- RHEL 7/CentOS 7/AL2

  V-204405、 V-204406、 V-204407、 V-204408、 V-204409、 V-204410、 V-204411、
  V-204412、 V-204413、 V-204414、 V-204415、 V-204416、 V-204417、 V-204418、
  V-204422、 V-204423、 V-204426、 V-204427、 V-204431、 V-204434、 V-204435、
  V-204437、 V-204449、 V-204450、 V-204451、 V-204457、 V-204466、 V-204490、
  V-204491、 V-204503、 V-204507、 V-204508、 V-204510、 V-204511、 V-204512、
  V-204514、 V-204515、 V-204516、 V-204517、 V-204521、 V-204524、 V-204531、
  V-204536、 V-204537、 V-204538、 V-204539、 V-204540、 V-204541、 V-204542、
  V-204543、 V-204544、 V-204545、 V-204546、 V-204547、 V-204548、 V-204549、
  V-204550、 V-204551、 V-204552、 V-204553、 V-204554、 V-204555、 V-204556、
  V-204557、 V-204558、 V-204559、 V-204560、 V-204562、 V-204563、 V-204564、
  V-204565、 V-204566、 V-204567、 V-204568、 V-204572、 V-204578、 V-204579、
  V-204584、 V-204585、 V-204587、 V-204588、 V-204589、 V-204590、 V-204591、
  V-204592、 V-204593、 V-204595、 V-204596、 V-204597、 V-204598、 V-204599、
  V-204600、 V-204601、 V-204602、 V-204609、 V-204610、 V-204611、 V-204612、
  V-204613、 V-204614、 V-204615、 V-204616、 V-204617、 V-204619、 V-204622、
  V-204625、 V-204630、 V-204631、 V-204633、 V-233307、 V-237634、 V-237635、
  V-251703、 V-255925、 V-255927、 V-255928、 および V-256970

RHEL 8 STIG バージョン 2 リリース 2

Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

- 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、 V-230561、 V-237640、
  V-244547、 V-256974、 V-230525、 V-244544、 V-230248、 V-230249、 V-230250、
  V-230245、 V-230246、 V-230247、 V-230397、 V-230399、 V-230400、 V-230401、
  V-244543、 V-230228、 V-230298、 V-230387、 V-230482、 V-230231、 V-230233、
  V-230324、 V-230365、 V-230370、 V-230373、 V-230378、 V-230383、 V-230236、
  V-230314、 V-230315、 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-230368、 V-230369、 V-230375、 V-230376、 V-230377、 V-244524、 V-244533、 V-251713、 V-251717、 V-251714、 V-251715、 V-251716、 V-230332、 V-230333、 V-230335、 V-230337、 V-230339、 V-230341、 V-230343、 V-230345、 V-230240、 V-230282、 V-250315、 V-250316、 V-230255、 V-230277、 V-230278、 V-230348、 V-230353、 V-230386、 V-230390、 V-230392、 V-230394、 V-230396、 V-230393、 V-230398、 V-230402、 V-230403、 V-230404、 V-230405、 V-230406、 V-230407、 V-230408、 V-230409、 V-230410、 V-230411、 V-230412、 V-230413、 V-230418、 V-230419、 V-230421、 V-230422、 V-230423、 V-230424、 V-230425、 V-230426、 V-230427、 V-230428、 V-230429、 V-230430、 V-230431、 V-230432、 V-230433、 V-230434、 V-230435、 V-230436、 V-230437、 V-230438、 V-230439、 V-230444、 V-230446、 V-230447、 V-230448、 V-230449、 V-230455、 V-230456、 V-230462、 V-230463、 V-230464、 V-230465、 V-230466、 V-230467、 V-230471、 V-230472、 V-230473、 V-230474、 V-230480、 V-230483、 V-244542、 V-230503、 V-230507、 V-244525、 V-230244、 V-230286、 V-230287、 V-230288、 V-230290、 V-230291、 V-230296、 V-230330、 V-230382、 V-230526、 V-230527、 V-230555、 V-230556、 V-244526、 V-244528、 V-237642、 V-237643、 および V-251711

RHEL 9 STIG バージョン 2 リリース 3

Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

- RHEL 9/CentOS Stream 9

V-257981、 V-257780、 V-257825、 V-257827、 V-257828、 V-257829、 V-257830、 V-257831、 V-257832、 V-257833、 V-257834、 V-257836、 V-257838、 V-257839、 V-257840、 V-257841、 V-257842、 V-257882、 V-257883、 V-257884、 V-257885、 V-257889、 V-257890、 V-257891、 V-257892、 V-257893、 V-257894、 V-257895、 V-257896、 V-257897、 V-257898、 V-257899、 V-257900、 V-257901、 V-257902、 V-257903、 V-257904、 V-257905、 V-257906、 V-257907、 V-257908、 V-257909、 V-257910、 V-257911、 V-257912、 V-257913、 V-257914、 V-257915、 V-257918、 V-257919、 V-257920、 V-257921、 V-257922、 V-257923、 V-257928、 V-257929、 V-257930、 V-257934、 V-257935、 V-257943、 V-257948、 V-257954、 V-257978、 V-257980、 V-258035、 V-258041、 V-258046、 V-258052、 V-258063、 V-258068、

V-258081、V-258082、V-258083、V-258089、V-258120、V-258124、V-258126、
V-258140、V-258141、V-258151、V-258234、V-257886、V-257916、V-257917、
V-257952、V-257936、V-257939、V-257940、V-258036、V-258038、V-257887、
V-257924、V-257925、V-258145、V-258152、V-258153、V-258154、V-258156、
V-258157、V-258158、V-258159、V-258160、V-258161、V-258162、V-258163、
V-258164、V-258165、V-258166、V-258167、V-258168、V-258169、V-258170、
V-258171、V-258172、V-258176、V-258177、V-258178、V-258179、V-258180、
V-258181、V-258182、V-258183、V-258184、V-258185、V-258186、V-258187、
V-258188、V-258189、V-258190、V-258191、V-258192、V-258193、V-258194、
V-258195、V-258196、V-258197、V-258198、V-258199、V-258200、V-258201、
V-258202、V-258203、V-258204、V-258205、V-258206、V-258207、V-258208、
V-258209、V-258210、V-258211、V-258212、V-258213、V-258214、V-258215、
V-258216、V-258217、V-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-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-258119、V-257979、V-257982、V-257983、V-257985、V-257987、
V-257988、V-257992、V-257993、V-257994、V-257995、V-257996、V-257997、
V-257998、V-257999、V-258000、V-258001、V-258002、V-258003、V-258004、
V-258005、V-258006、V-258007、V-258008、V-258009、V-258010、V-258011、
V-258130、V-257814、V-258054、V-258055、V-258056、V-258057、V-258060、
V-258070、V-258080、V-258088、V-258091、V-258092、V-258093、V-258095、
V-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-258142、V-258144、V-258146、V-258147、V-258148、
V-258150、V-258064、V-258065、V-258066、V-258232、V-258237、V-258239、
V-258240、V-257788、V-257790、V-257791、V-257792、V-257793、V-257794、
V-257817、V-258175、V-257804、V-257805、V-257806、V-257807、V-257808、
V-258034、V-258039、V-257888、V-257926、V-257927、V-257933、V-258084、

V-258085、 V-257949、 V-258040、 V-257818、 V-257849、 V-258122、 V-258123、 V-258133、 V-257944、 V-258028、 V-258079、 V-258125、 および V-258137

Ubuntu 18.04 STIG バージョン 2 リリース 15

Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

V-219149、 V-219155、 V-219156、 V-219160、 V-219166、 V-219168、 V-219176、 V-219181、 V-219184、 V-219186、 V-219188、 V-219189、 V-219190、 V-219191、 V-219192、 V-219193、 V-219194、 V-219195、 V-219196、 V-219197、 V-219198、 V-219199、 V-219200、 V-219201、 V-219202、 V-219203、 V-219204、 V-219205、 V-219206、 V-219207、 V-219208、 V-219209、 V-219213、 V-219214、 V-219215、 V-219216、 V-219217、 V-219218、 V-219219、 V-219220、 V-219221、 V-219222、 V-219223、 V-219224、 V-219225、 V-219226、 V-219227、 V-219228、 V-219229、 V-219230、 V-219231、 V-219232、 V-219233、 V-219234、 V-219235、 V-219236、 V-219238、 V-219239、 V-219240、 V-219241、 V-219242、 V-219243、 V-219244、 V-219250、 V-219254、 V-219257、 V-219263、 V-219264、 V-219265、 V-219266、 V-219267、 V-219268、 V-219269、 V-219270、 V-219271、 V-219272、 V-219273、 V-219274、 V-219275、 V-219276、 V-219277、 V-219279、 V-219281、 V-219287、 V-219291、 V-219297、 V-219298、 V-219299、 V-219300、 V-219303、 V-219304、 V-219306、 V-219309、 V-219310、 V-219311、 V-219312、 V-219315、 V-219318、 V-219319、 V-219323、 V-219326、 V-219328、 V-219330、 V-219331、 V-219335、 V-219336、 V-219337、 V-219338、 V-219339、 V-219342、 V-219344、 V-233779、 V-233780、 および V-255906

Ubuntu 20.04 STIG バージョン 2 リリース 2

Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

V-238200、 V-238205、 V-238207、 V-238231、 V-238329、 V-238337、 V-238339、 V-238340、 V-238344、 V-238345、 V-238346、 V-238347、 V-238348、 V-238349、 V-238350、 V-238351、 V-238352、 V-238371、 V-238376、 V-238377、 V-238378、 V-238209、 V-238325、 V-238330、 V-238333、 V-238369、 V-238230、 V-238338、 V-238341、 V-238342、 V-238343、 V-238324、 V-238353、 V-238228、 V-238225、 V-238227、 V-238299、 V-238238、 V-238239、 V-238240、 V-238241、 V-238242、 V-238244、 V-238245、 V-238246、 V-238247、 V-238248、 V-238249、 V-238250、 V-238251、 V-238252、 V-238253、 V-238254、 V-238255、 V-238256、 V-238257、 V-238258、 V-238264、 V-238268、 V-238271、 V-238277、 V-238278、 V-238279、 V-238280、 V-238281、 V-238282、 V-238283、 V-238284、 V-238285、 V-238286、 V-238287、 V-238288、

V-238289、 V-238290、 V-238291、 V-238292、 V-238293、 V-238294、 V-238295、 V-238297、 V-238300、 V-238301、 V-238302、 V-238304、 V-238309、 V-238310、 V-238315、 V-238316、 V-238317、 V-238318、 V-238319、 V-238320、 V-251505、 V-238360、 V-238210、 V-238211、 V-238212、 V-238213、 V-238220、 V-255912、 V-238355、 V-238236、 V-238303、 V-238356、 V-238359、 V-238370、 V-238334、 および V-238232

Ubuntu 22.04 STIG バージョン 2 リリース 3

Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

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-260649、 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-260527、 V-260528、 V-260530、 V-260533、 V-260534、 V-260575、 V-260505、 V-260506、 V-260512、 V-260582、 V-260584、 V-260585、 V-260586、 V-260477、 V-260545、 V-260555、 V-260556、 V-260557、 V-260509、 V-260588、 V-260589、 V-260537、 V-260538、 および V-260535

Ubuntu 24.04 STIG バージョン 1 リリース 1

Amazon EC2 が Category III (Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

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-270709、 V-270715、 V-270716、 V-270718、 V-270720、 V-270721、 V-270722、 V-270723、 V-270724、 V-270725、 V-270726、 V-270727、 V-270728、 V-270729、 V-270730、 V-270731、 V-270732、 V-270733、 V-270737、 V-270739、 V-270740、 V-270741、 V-270742、 V-270743、 V-270746、 V-270750、 V-270753、 V-270755、 V-270756、 V-270757、 V-270758、 V-270759、 V-270760、 V-270765、 V-270766、 V-270767、 V-270768、 V-270769、 V-270770、 V-270771、 V-270772、 V-270773、 V-270775、 V-270776、 V-270777、 V-270778、 V-270779、 V-270780、 V-270781、 V-270782、 V-270783、 V-270784、 V-270785、 V-270786、 V-270787、 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-270802、 V-270803、 V-270804、 V-270805、 V-270806、 V-270807、 V-270808、 V-270809、 V-270810、 V-270811、 V-270812、 V-270813、 V-270814、 V-270815、 V-270821、 V-270822、 V-270823、 V-270824、 V-270825、 V-270826、 V-270827、 V-270828、 V-270829、 V-270830、 V-270831、 および V-270832

Linux STIG High (Category I)

次のリストには、Amazon EC2 がインフラストラクチャに対してサポートしている STIG 設定が含まれています。サポートされている設定がお客様のインフラストラクチャに適用できない場合、Amazon EC2 はその設定をスキップして次に進みます。例えば、一部の STIG 強化設定は、スタンドアロンサーバーには適用されない場合があります。組織固有のポリシーも、適用される設定に影響を与える可能性があります (例: 管理者がドキュメントの設定を確認する必要がある)。

詳細なリストについては、「STIGs Document Library」を参照してください。完全なリストを表示する方法の詳細については、「STIG 表示ツール」を参照してください。

> **Note**
>
> Linux STIG High カテゴリには、Amazon EC2 が Category I の脆弱性をサポートする STIG 強化設定に加えて、Linux STIG Medium および Low カテゴリに適用されるリスト済みのすべての STIG 強化設定が含まれます。

RHEL 7 STIG バージョン 3 リリース 15

Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

- 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、および V-204621

RHEL 8 STIG バージョン 2 リリース 2

Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

- RHEL 8/CentOS 8/AL 2023

  V-230223, V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533, V-230558、および V-244540

RHEL 9 STIG バージョン 2 リリース 3

Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

- 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、および V-258235

Ubuntu 18.04 STIG バージョン 2 リリース 15

Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

V-219157, V-219158, V-219177, V-219212, V-219308, V-219314, V-219316, V-251507、および V-264388

Ubuntu 20.04 STIG バージョン 2 リリース 2

Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

V-238218, V-238219, V-238201, V-251504, V-238326, V-238327、および V-238380

Ubuntu 22.04 STIG バージョン 2 リリース 3

Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

V-260482, V-260483, V-260523, V-260524, V-260469, V-260526, V-260529, V-260570, V-260571, V-260579、および V-260539

Ubuntu 24.04 STIG バージョン 1 リリース 1

Amazon EC2 が Category II および III (Medium および Low) の脆弱性をサポートするすべての STIG 強化設定に加えて、以下が含まれます。

V-270647, V-270648, V-270665, V-270666, V-270708, V-270717, V-270711, V-270712, V-270713、および V-270714

Linux STIG のバージョン履歴

このセクションには、四半期ごとの STIG アップデートに関する Linux コンポーネントのバージョン履歴が記録されます。四半期ごとの変更点と公開されたバージョンを確認するには、タイトルを選択して情報を展開します。

2025 年Q1 四半期の変更 - 04/11/2025:

次の STIG バージョンを更新し、2025 年第 1 四半期リリースに STIGS を適用し、Ubuntu 24.04 のサポートを追加しました。

STIG-Build-Linux-Low バージョン 2025.1.x

- RHEL 7 STIG バージョン 3 リリース 15
- RHEL 8 STIG バージョン 2 リリース 2
- RHEL 9 STIG バージョン 2 リリース 3
- Ubuntu 18.04 STIG バージョン 2 リリース 15
- Ubuntu 20.04 STIG バージョン 2 リリース 2
- Ubuntu 22.04 STIG バージョン 2 リリース 3
- Ubuntu 24.04 STIG バージョン 1 リリース 1

STIG-Build-Linux-Medium バージョン 2025.1.x

- RHEL 7 STIG バージョン 3 リリース 15
- RHEL 8 STIG バージョン 2 リリース 2
- RHEL 9 STIG バージョン 2 リリース 3
- Ubuntu 18.04 STIG バージョン 2 リリース 15
- Ubuntu 20.04 STIG バージョン 2 リリース 2

- Ubuntu 22.04 STIG バージョン 2 リリース 3
- Ubuntu 24.04 STIG バージョン 1 リリース 1

STIG-Build-Linux-High バージョン 2025.1.x

- RHEL 7 STIG バージョン 3 リリース 15
- RHEL 8 STIG バージョン 2 リリース 2
- RHEL 9 STIG バージョン 2 リリース 3
- Ubuntu 18.04 STIG バージョン 2 リリース 15
- Ubuntu 20.04 STIG バージョン 2 リリース 2
- Ubuntu 22.04 STIG バージョン 2 リリース 3
- Ubuntu 24.04 STIG バージョン 1 リリース 1

2024 年Q4 四半期の変更 - 12/10/2024:

次の STIG バージョンを更新し、2024 年第 4 四半期リリースに STIGS を適用し、Linux コンポーネントの 2 つの新しい入力パラメータに関する情報を追加しました。

STIG-Build-Linux-Low バージョン 2024.4.x

- RHEL 7 STIG バージョン 3 リリース 15
- RHEL 8 STIG バージョン 2 リリース 1
- RHEL 9 STIG バージョン 2 リリース 2
- Ubuntu 18.04 STIG バージョン 2 リリース 15
- Ubuntu 20.04 STIG バージョン 2 リリース 1
- Ubuntu 22.04 STIG バージョン 2 リリース 2

STIG-Build-Linux-Medium バージョン 2024.4.x

- RHEL 7 STIG バージョン 3 リリース 15
- RHEL 8 STIG バージョン 2 リリース 1
- RHEL 9 STIG バージョン 2 リリース 2
- Ubuntu 18.04 STIG バージョン 2 リリース 15
- Ubuntu 20.04 STIG バージョン 2 リリース 1

- Ubuntu 22.04 STIG バージョン 2 リリース 2

STIG-Build-Linux-High バージョン 2024.4.x

- RHEL 7 STIG バージョン 3 リリース 15
- RHEL 8 STIG バージョン 2 リリース 1
- RHEL 9 STIG バージョン 2 リリース 2
- Ubuntu 18.04 STIG バージョン 2 リリース 15
- Ubuntu 20.04 STIG バージョン 2 リリース 1
- Ubuntu 22.04 STIG バージョン 2 リリース 2

2024 年Q3 四半期の変更 - 10/04/2024 (変更なし):

2024 年第 3 四半期リリースでは、Linux コンポーネント STIGS に変更はありませんでした。

2024 年第 2 四半期の変更 - 2024 年 5 月 10 日:

STIG バージョンを更新し、2024 年第 2 四半期リリースの STIG を適用しました。また、RHEL 9、CentOS Stream 9、Ubuntu 22.04 のサポートを以下のように追加しました。

STIG-Build-Linux-Low バージョン 2024.2.x

- RHEL 7 STIG バージョン 3 リリース 14
- RHEL 8 STIG バージョン 1 リリース 14
- RHEL 9 STIG バージョン 1 リリース 3
- Ubuntu 18.04 STIG バージョン 2 リリース 14
- Ubuntu 20.04 STIG バージョン 1 リリース 12
- Ubuntu 22.04 STIG バージョン 1 リリース 1

STIG-Build-Linux-Medium バージョン 2024.2.x

- RHEL 7 STIG バージョン 3 リリース 14
- RHEL 8 STIG バージョン 1 リリース 14
- RHEL 9 STIG バージョン 1 リリース 3
- Ubuntu 18.04 STIG バージョン 2 リリース 14

- Ubuntu 20.04 STIG バージョン 1 リリース 12
- Ubuntu 22.04 STIG バージョン 1 リリース 1

STIG-Build-Linux-High バージョン 2024.2.x

- RHEL 7 STIG バージョン 3 リリース 14
- RHEL 8 STIG バージョン 1 リリース 14
- RHEL 9 STIG バージョン 1 リリース 3
- Ubuntu 18.04 STIG バージョン 2 リリース 14
- Ubuntu 20.04 STIG バージョン 1 リリース 12
- Ubuntu 22.04 STIG バージョン 1 リリース 1

2024 年第 1 四半期の変更 - 2024 年 2 月 6 日:

STIG バージョンを更新し、次のように 2024 年第 1 四半期リリースの STIG を適用しました。

STIG-Build-Linux-Low バージョン 2024.1.x

- RHEL 7 STIG バージョン 3 リリース 14
- RHEL 8 STIG バージョン 1 リリース 13
- Ubuntu 18.04 STIG バージョン 2 リリース 13
- Ubuntu 20.04 STIG バージョン 1 リリース 11

STIG-Build-Linux-Medium バージョン 2024.1.x

- RHEL 7 STIG バージョン 3 リリース 14
- RHEL 8 STIG バージョン 1 リリース 13
- Ubuntu 18.04 STIG バージョン 2 リリース 13
- Ubuntu 20.04 STIG バージョン 1 リリース 11

STIG-Build-Linux-High バージョン 2024.1.x

- RHEL 7 STIG バージョン 3 リリース 14
- RHEL 8 STIG バージョン 1 リリース 13

- Ubuntu 18.04 STIG バージョン 2 リリース 13
- Ubuntu 20.04 STIG バージョン 1 リリース 11

2023 年第 4 四半期の変更 - 2023 年 12 月 7 日:

STIG バージョンを更新し、次のように 2023 年第 4 四半期リリースの STIG を適用しました。

STIG-Build-Linux-Low バージョン 2023.4.x

- RHEL 7 STIG バージョン 3 リリース 13
- RHEL 8 STIG バージョン 1 リリース 12
- Ubuntu 18.04 STIG バージョン 2 リリース 12
- Ubuntu 20.04 STIG バージョン 1 リリース 10

STIG-Build-Linux-Medium バージョン 2023.4.x

- RHEL 7 STIG バージョン 3 リリース 13
- RHEL 8 STIG バージョン 1 リリース 12
- Ubuntu 18.04 STIG バージョン 2 リリース 12
- Ubuntu 20.04 STIG バージョン 1 リリース 10

STIG-Build-Linux-High バージョン 2023.4.x

- RHEL 7 STIG バージョン 3 リリース 13
- RHEL 8 STIG バージョン 1 リリース 12
- Ubuntu 18.04 STIG バージョン 2 リリース 12
- Ubuntu 20.04 STIG バージョン 1 リリース 10

2023 年第 3 四半期の変更-2023 年 4 月 10 日:

STIG のバージョンを更新し、2023 年第 3 四半期のリリースに向けて以下のように STIGS を適用しました。

Linux STIG Low (Category III)

- RHEL 7 STIG バージョン 3 リリース 12

- RHEL 8 STIG バージョン 1 リリース 11
- Ubuntu 18.04 STIG バージョン 2 リリース 11
- Ubuntu 20.04 STIG バージョン 1 リリース 9

Linux STIG Medium (Category II)

- RHEL 7 STIG バージョン 3 リリース 12
- RHEL 8 STIG バージョン 1 リリース 11
- Ubuntu 18.04 STIG バージョン 2 リリース 11
- Ubuntu 20.04 STIG バージョン 1 リリース 9

Linux STIG High (Category I)

- RHEL 7 STIG バージョン 3 リリース 12
- RHEL 8 STIG バージョン 1 リリース 11
- Ubuntu 18.04 STIG バージョン 2 リリース 11
- Ubuntu 20.04 STIG バージョン 1 リリース 9

2023 第 2 四半期の変更-2023 年 5 月 3 日:

STIG のバージョンを更新し、2023 年第 2 四半期のリリースに向けて以下のように STIGS を適用しました。

Linux STIG Low (Category III)

- RHEL 7 STIG バージョン 3 リリース 11
- RHEL 8 STIG バージョン 1 リリース 10
- Ubuntu 18.04 STIG バージョン 2 リリース 11
- Ubuntu 20.04 STIG バージョン 1 リリース 8

Linux STIG Medium (Category II)

- RHEL 7 STIG バージョン 3 リリース 11
- RHEL 8 STIG バージョン 1 リリース 10

- Ubuntu 18.04 STIG バージョン 2 リリース 11
- Ubuntu 20.04 STIG バージョン 1 リリース 8

Linux STIG High (Category I)

- RHEL 7 STIG バージョン 3 リリース 11
- RHEL 8 STIG バージョン 1 リリース 10
- Ubuntu 18.04 STIG バージョン 2 リリース 11
- Ubuntu 20.04 STIG バージョン 1 リリース 8

2023 年第 1 四半期の変更-2023 年 3 月 27 日:

STIG のバージョンを更新し、2023 年第 1 四半期のリリースに向けて以下のように STIGS を適用しました。

Linux STIG Low (Category III)

- RHEL 7 STIG バージョン 3 リリース 10
- RHEL 8 STIG バージョン 1 リリース 9
- Ubuntu 18.04 STIG バージョン 2 リリース 10
- Ubuntu 20.04 STIG バージョン 1 リリース 7

Linux STIG Medium (Category II)

- RHEL 7 STIG バージョン 3 リリース 10
- RHEL 8 STIG バージョン 1 リリース 9
- Ubuntu 18.04 STIG バージョン 2 リリース 10
- Ubuntu 20.04 STIG バージョン 1 リリース 7

Linux STIG High (Category I)

- RHEL 7 STIG バージョン 3 リリース 10
- RHEL 8 STIG バージョン 1 リリース 9
- Ubuntu 18.04 STIG バージョン 2 リリース 10

- Ubuntu 20.04 STIG バージョン 1 リリース 7

2022 年第 4 四半期の変更-2023 年 2 月 1 日:

STIG のバージョンを更新し、2022 年第 4 四半期のリリースに向けて以下のように STIGS を適用しました。

Linux STIG Low (Category III)

- RHEL 7 STIG バージョン 3 リリース 9
- RHEL 8 STIG バージョン 1 リリース 8
- Ubuntu 18.04 STIG バージョン 2 リリース 9
- Ubuntu 20.04 STIG バージョン 1 リリース 6

Linux STIG Medium (Category II)

- RHEL 7 STIG バージョン 3 リリース 9
- RHEL 8 STIG バージョン 1 リリース 8
- Ubuntu 18.04 STIG バージョン 2 リリース 9
- Ubuntu 20.04 STIG バージョン 1 リリース 6

Linux STIG High (Category I)

- RHEL 7 STIG バージョン 3 リリース 9
- RHEL 8 STIG バージョン 1 リリース 8
- Ubuntu 18.04 STIG バージョン 2 リリース 9
- Ubuntu 20.04 STIG バージョン 1 リリース 6

2022 年第 3 四半期の変更-2022 年 9 月 30 日 (変更なし):

2022 年第 3 四半期リリースの Linux コンポーネント STIGS には変更はありませんでした。

2022 年第 2 四半期の変更-2022 年 8 月 2 日:

Ubuntu サポートの導入、STIG バージョンの更新、および 2022 年第 2 四半期リリース向けの STIGS の適用を以下のとおり実施しました。

Linux STIG Low (Category III)

- RHEL 7 STIG バージョン 3 リリース 7
- RHEL 8 STIG バージョン 1 リリース 6
- Ubuntu 18.04 STIG バージョン 2 リリース 6 (新規)
- Ubuntu 20.04 STIG バージョン 1 リリース 4 (新規)

Linux STIG Medium (Category II)

- RHEL 7 STIG バージョン 3 リリース 7
- RHEL 8 STIG バージョン 1 リリース 6
- Ubuntu 18.04 STIG バージョン 2 リリース 6 (新規)
- Ubuntu 20.04 STIG バージョン 1 リリース 4 (新規)

Linux STIG High (Category I)

- RHEL 7 STIG バージョン 3 リリース 7
- RHEL 8 STIG バージョン 1 リリース 6
- Ubuntu 18.04 STIG バージョン 2 リリース 6 (新規)
- Ubuntu 20.04 STIG バージョン 1 リリース 4 (新規)

2022 年第 1 四半期の変更-2022 年 4 月 26 日:

コンテナのサポートを強化するようにリファクタリングされました。以前の AL2 スクリプトと RHEL 7 を組み合わせました。STIG のバージョンを更新し、2022 年第 1 四半期のリリースに向けて以下のように STIGS を適用しました。

Linux STIG Low (Category III)

- RHEL 7 STIG バージョン 3 リリース 6
- RHEL 8 STIG バージョン 1 リリース 5

Linux STIG Medium (Category II)

- RHEL 7 STIG バージョン 3 リリース 6
- RHEL 8 STIG バージョン 1 リリース 5

Linux STIG High (Category I)

- RHEL 7 STIG バージョン 3 リリース 6
- RHEL 8 STIG バージョン 1 リリース 5

2021 年第 4 四半期の変更-2021 年 12 月 20 日:

STIG のバージョンを更新し、2021 年第 4 四半期のリリースに向けて以下のように STIGS を適用しました。

Linux STIG Low (Category III)

- RHEL 7 STIG バージョン 3 リリース 5
- RHEL 8 STIG バージョン 1 リリース 4

Linux STIG Medium (Category II)

- RHEL 7 STIG バージョン 3 リリース 5
- RHEL 8 STIG バージョン 1 リリース 4

Linux STIG High (Category I)

- RHEL 7 STIG バージョン 3 リリース 5
- RHEL 8 STIG バージョン 1 リリース 4

2021 年第 3 四半期の変更-2021 年 9 月 30 日:

STIG のバージョンを更新し、2021 年第 3 四半期のリリースに向けて以下のように STIGS を適用しました。

Linux STIG Low (Category III)

- RHEL 7 STIG バージョン 3 リリース 4
- RHEL 8 STIG バージョン 1 リリース 3

Linux STIG Medium (Category II)

- RHEL 7 STIG バージョン 3 リリース 4

- RHEL 8 STIG バージョン 1 リリース 3

Linux STIG High (Category I)

- RHEL 7 STIG バージョン 3 リリース 4
- RHEL 8 STIG バージョン 1 リリース 3

AWSEC2-PatchLoadBalancerInstance

説明

任意のロードバランサー (クラシック、ALB、または NLB) に接続されている Amazon EC2 インスタンス (Windows または Linux) のマイナーバージョンをアップグレードしてパッチを適用します。デフォルトの Connection Draining 時間は、インスタンスにパッチが適用される前に適用されます。ConnectionDrainTime パラメータにカスタムのドレイン時間を分 (1-59) 単位で入力することで、待機時間をオーバーライドできます。

自動化ワークフローは次のとおりです。

1. インスタンスがアタッチされているロードバランサーまたはターゲットグループが決定され、インスタンスが正常であることが確認されます。
2. インスタンスはロードバランサーまたはターゲットグループから削除されます。
3. オートメーションは、Connection Draining 時間として指定された時間だけ待機します。
4. AWS-RunPatchBaseline オートメーションが呼び出され、インスタンスにパッチが適用されます。
5. インスタンスはロードバランサーまたはターゲットグループに再アタッチされます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

前提条件

- インスタンスに SSM Agent がインストールされていることを確認します。詳細については、「Windows Server の EC2 インスタンスで SSM Agent を使用する」を参照してください。

パラメータ

- InstanceId

  タイプ: 文字列

  説明: (必須) ロードバランサー (クラシック、ALB、または NLB) に関連付けられているパッチに対するインスタンスの ID。
- ConnectionDrainTime

  タイプ: 文字列

  説明: (オプション) ロードバランサーの Connection Draining 時間 (分) (1-59)。
- S3BucketLog

  タイプ: 文字列

  説明: (オプション) コマンド出力レスポンスの保存に使用する Amazon S3 バケットの名前。所有しているバケットまたは共有されているバケットを指定できます。このパラメータを指定する場合は、runCommandAssumeRole も指定する必要があります。
- runCommandAssumeRole

  タイプ: 文字列

  説明: (オプション) インスタンスでコマンドを実行するために使用する IAM ロールの ARN。ロールにはサービス`ssm.amazonaws.com`プリンシパルとの信頼関係が必要です。また、AmazonSSMManagedInstanceCore ポリシーがアタッチされている必要があります。また、S3BucketLog に指定された Amazon S3 バケットに対する書き込みアクセス許可が必要です。

AWSEC2-SQLServerDBRestore

説明

この `AWSEC2-SQLServerDBRestore` ランブックは、Amazon S3 に保存されている Microsoft SQL Server データベースのバックアップを、Amazon Elastic Compute Cloud (EC2) Linux インスタンスで実行されている SQL Server 2017 に復元します。SQL Server 2017 Linux を実行している独自の

EC2 インスタンスを提供することができます。EC2 インスタンスが提供されていない場合、この自動化では、SQL Server 2017 を使用する新しい Ubuntu 16.04 EC2 インスタンスを起動して設定します。自動化は、フル、差分、およびトランザクションログのバックアップの復元をサポートします。この自動化は、複数のデータベースバックアップファイルを受け入れて、提供されたファイル内の各データベースの最新の有効なバックアップを自動的に復元します。

SQL Server 2017 Linux を実行している EC2 インスタンスへのオンプレミス SQL Server データベースのバックアップと復元の両方を自動化するには、署名 AWS付き PowerShell スクリプト を使用できますMigrateSQLServerToEC2Linux。

> **Important**
>
> このランブックは、自動化が実行されるたびに SQL Server のサーバー管理者 (SA) ユーザーパスワードをリセットします。ユーザーは、自動化が完了した後、SQL Server インスタンスに接続する前に、独自の SA ユーザーパスワードを再設定する必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

前提条件

このオートメーションを実行するには、以下の前提条件を満たす必要があります。

- このオートメーションを実行する IAM ユーザーまたはロールには、必要な IAM 許可 で説明されている権限を含むインラインポリシーがアタッチされている必要があります。
- 独自の EC2 インスタンスを提供している場合:
  - 提供する EC2 インスタンスは、Microsoft SQL Server 2017 を実行している Linux インスタンスである必要があります。

- 指定する EC2 インスタンスは、AmazonSSMManagedInstanceCore 管理ポリシーがアタッチされた AWS Identity and Access Management (IAM) インスタンスプロファイルを使用して設定する必要があります。詳細については「Systems Manager の IAM インスタンスプロファイルを作成する」を参照してください。
- EC2 インスタンスに SSM エージェントがインストールされている必要があります。詳細については、「Linux の EC2 インスタンスでの SSM エージェントのインストールと設定」を参照してください。
- EC2 インスタンスは、SQL Server バックアップをダウンロードして復元するのに十分な空きディスク容量がある必要があります。

制限

このオートメーションは、Windows Server の EC2 インスタンスで実行されている SQL Server への復元をサポートしません。この自動化は、SQL Server Linux 2017 と互換性のあるデータベースバックアップのみを復元します。詳細については、「Linux 上の SQL Server 2017 のエディションとサポートされる機能に関する記事」を参照してください。

パラメータ

この自動化には以下のパラメータがあります。

- DatabaseNames

  タイプ: 文字列

  説明: (オプション)復元するデータベースの名前のカンマ区切りリスト。
- DataDirectorySize

  タイプ: 文字列

  説明: (オプション) 新しい EC2 インスタンスの SQL Server Data ディレクトリの必要なボリュームサイズ (GiB)。

  デフォルト値: 100
- KeyPair

  タイプ: 文字列

  説明: (オプション) 新しい EC2 インスタンスを作成するときに使用するキーペア。

- IamInstanceProfileName

  タイプ: 文字列

  説明: (オプション) 新しい EC2 インスタンスにアタッチする IAM インスタンスプロファイル。IAM インスタンスプロファイルには、AmazonSSMManagedInstanceCore 管理ポリシーがアタッチされている必要があります。

- InstanceId

  タイプ: 文字列

  説明: (オプション) Linux で SQL Server 2017 を実行しているインスタンス。InstanceId が指定されていない場合、オートメーションは提供されている InstanceType と SQLServerEdition を使用して新しい EC2 インスタンスを起動します。

- InstanceType

  タイプ: 文字列

  説明: (オプション) インスタンスを起動する EC2 インスタンスのインスタンスタイプ。

- IsS3PresignedUrl

  タイプ: 文字列

  説明: (オプション) S3Input が署名付き S3 URL の場合は「yes」を指定。

  デフォルト値: no

  有効な値: はい | いいえ

- LogDirectorySize

  タイプ: 文字列

  説明: (オプション) 新しい EC2 インスタンスの SQL Server Log ディレクトリの必要なボリュームサイズ (GiB)。

  デフォルト値: 100

- S3Input

  タイプ: 文字列

説明: (必須) S3 バケット名、S3 オブジェクトキーのカンマ区切りリスト、または復元対象の SQL バックアップファイルを含む署名付き S3 URL のカンマ区切りリスト。

- SQLServerEdition

  タイプ: 文字列

  説明: (オプション) 新しく作成された EC2 インスタンスにインストールされる SQL Server 2017 のエディション。

  有効な値: Standard | Enterprise | Web | Express

- SubnetId

  タイプ: 文字列

  説明: (オプション) 新しい EC2 インスタンスを起動するサブネット。サブネットには、 AWS サービスへのアウトバウンド接続が必要です。SubnetId の値が指定されていない場合、自動化はデフォルトのサブネットを選択します。

- TempDbDirectorySize

  タイプ: 文字列

  説明: (オプション) 新しい EC2 インスタンスの SQL Server TempDB ディレクトリの必要なボリュームサイズ (GiB)。

  デフォルト値: 100

必要な IAM 許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

この自動化を使用するには、ご使用のインスタンスタイプに適用される手順に従ってください。

新しい EC2 インスタンスの場合:

1. `aws:executeAwsApi` - Ubuntu 16.04 で SQL Server 2017 の AMI ID を取得します。
2. `aws:runInstances` - Linux 用の新しい EC2 インスタンスを起動します。
3. `aws:waitForAwsResourceProperty` - 新しく作成された EC2 インスタンスの準備が完了するまで待ちます。
4. `aws:executeAwsApi` - インスタンスの準備ができていない場合はインスタンスを再起動します。
5. `aws:assertAwsResourceProperty` - SSM エージェントがインストールされていることを確認します。
6. `aws:runCommand` - SQL Server の復元スクリプトを PowerShell で実行します。

既存の EC2 インスタンスの場合:

1. aws:waitForAwsResourceProperty - EC2 インスタンスの準備ができていることを確認します。
2. aws:executeAwsApi - インスタンスの準備ができていない場合はインスタンスを再起動します。
3. aws:assertAwsResourceProperty - SSM エージェントがインストールされていることを確認します。
4. aws:runCommand - SQL Server の復元スクリプトを PowerShell で実行します。

出力

getInstance.InstanceId

restoreToNewInstance.Output

restoreToExistingInstance.Output

AWSSupport-ActivateWindowsWithAmazonLicense

説明

AWSSupport-ActivateWindowsWithAmazonLicense ランブックでは、Amazon が提供するライセンスを使用して、Windows Server の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスをアクティブ化します。このオートメーションでは、必要なキー管理サービスのオペレーティングシステム設定を検証して設定し、アクティベーションを試行します。これには、Amazon のキー管理サーバーへのオペレーティングシステムのルーティング、およびキー管理サービスのオペレーティングシステムの設定などの処理が含まれます。AllowOffline パラメータを に設定すると、オートメーションは によって管理されていないインスタンスを正常にターゲットにtrueできますが AWS Systems Manager、インスタンスの停止と起動が必要です。

> **Note**
>
> このランブックは、ユーザーが独自のライセンスを導入する (BYOL) モデルの Windows Server インスタンスでは使用できません。お客様自身のライセンスの使用方法については、「AWSでの Microsoft ライセンス」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

- AllowOffline

  タイプ: 文字列

  有効な値: true | false

  デフォルト: false

  説明: (オプション) オンラインのトラブルシューティングが失敗した場合や、提供されたインスタンスがマネージドインスタンスでない場合に、オフラインの Windows がアクティベーションを修復することを許可する場合は、`true` に設定します。

  > **Important**
  >
  > オフライン方式では、指定された EC2 インスタンスを停止してから起動する必要があります。インスタンスストアボリュームに保存されているデータは失われます。Elastic IP を使用していない場合、パブリック IP アドレスが変わります。

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ForceActivation

  タイプ: 文字列

有効な値: true | false

デフォルト: false

説明: (オプション) Windows が既にアクティブになっていても処理を続行させたい場合は、`true` に設定します。

- InstanceId

  タイプ: 文字列

  説明: (必須) Windows Server のマネージド EC2 インスタンスの ID。

- SubnetId

  タイプ: 文字列

  デフォルト: CreateNewVPC

  説明: (オプション) オフラインのみ - オフラインのトラブルシューティングを実行するために使用される EC2Rescue インスタンスのサブネット ID。インスタンスと同じサブネットを使用する場合は `SelectedInstanceSubnet` を設定し、新しい VPC を作成する場合は `CreateNewVPC` を設定します。重要: サブネットは InstanceId と同じアベイラビリティーゾーンである必要があり、SSM エンドポイントへのアクセスを許可する必要があります。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

このコマンドを受信する EC2 インスタンスには、[AmazonSSMManagedInstanceCore] Amazon 管理ポリシーがアタッチされた IAM ロールがあることが推奨されます。
オートメーションを実行し、インスタンスにコマンドを送信するには、少なくとも [ssm:StartAutomationExecution] と [ssm:SendCommand] が必要です。また、自動化出力を読み取るためには、[ssm:GetAutomationExecution] も必要です。オフラインの修復の場合は、`AWSSupport-StartEC2RescueWorkflow` に必要なアクセス許可を参照してください。

ドキュメントステップ

1. `aws:assertAwsResourceProperty` - 指定されたインスタンスのプラットフォームが Windows であることを確認します。

2. aws:assertAwsResourceProperty - 提供されたインスタンスがマネージドインスタンスであることを確認します。
   a. (オンラインのアクティベーションの修正) 入力インスタンスがマネージドインスタンスの場合は、aws:runCommand を実行して PowerShell スクリプトを実行し、Windows アクティベーションの修正を試みることができます。
   b. (オフラインアクティベーション修正) 入力インスタンスがマネージドインスタンスでない場合。
      i. aws:assertAwsResourceProperty - AllowOffline フラグが true に設定されていることを確認します。これが設定されている場合、オフラインでの修復が開始されます。そうでない場合、オートメーションが終了します。
      ii. aws:executeAutomation - Windows のアクティベーションオフライン修復スクリプトで AWSSupport-StartEC2RescueWorkflow を呼び出します。このスクリプトは、OS のバージョンに応じて、EC2Config または EC2Launch のどちらかを使用します。
      iii. aws:executeAwsApi - AWSSupport-StartEC2RescueWorkflow から結果を読み込みます。

出力

activateWindows.Output

getActivateWindowsOfflineResult.Output

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

説明

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 ランブックでは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたはエラスティックネットワークインターフェイスから AWS のサービス エンドポイントへの接続が分析されます。IPv6 はサポートされていません。ランブックは、ServiceEndpoint パラメータに指定した値を使用してエンドポイントへの接続を分析します。VPC に AWS PrivateLink エンドポイントが見つからない場合、ランブックは現在の AWS リージョンのサービスのパブリック IP アドレスを使用します。この自動化では、Amazon Virtual Private Cloud の Reachability Analyzer を使用します。詳細については、Reachability Analyzerの「Reachability Analyzer とは」を参照してください。

この自動化では、次の項目がチェックされます。

- 仮想プライベートクラウド (VPC) が Amazon が提供する DNS サーバーを使用するように設定されているかどうかを確認します。
- 指定した の VPC AWS のサービス に AWS PrivateLink エンドポイントが存在するかどうかを確認します。エンドポイントが見つかると、`privateDns` 属性がオンになっていることが自動化によって検証されます。
- AWS PrivateLink エンドポイントがデフォルトのエンドポイントポリシーを使用しているかどうかを確認します。

考慮事項

- ソースとターゲットの間で分析が実行されるたびに課金されます。詳細については、「Amazon VPC の料金」を参照してください。
- 自動化中に、ネットワークインサイトパスとネットワークインサイト分析が作成されます。自動化が正常に完了すると、ランブックはこれらのリソースを削除します。クリーンアップステップが失敗した場合、ネットワークインサイトパスはランブックによって削除されないため、手動で削除する必要があります。ネットワークインサイトパスを手動で削除しないと、引き続き AWS アカウントの割り当てにカウントされます。Reachability Analyzer のクォータの詳細については、Reachability Analyzer のReachability Analyzer のクォータを参照してください。
- プロキシ、ローカル DNS リゾルバー、ホストファイルの使用などのオペレーティングシステムレベルの構成は、Reachability Analyzer が `PASS` を返しても接続に影響する可能性があります。
- Reachability Analyzer によって実行されたすべてのチェックの評価を確認します。いずれかのチェックが `FAIL` ステータスで返されると、全体の到達可能性チェックで `PASS` ステータスが返されたとしても、接続に影響する可能性があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ソース

  タイプ: 文字列

  説明: (必須) 到達可能性を分析する Amazon EC2 インスタンスまたはネットワークインターフェイスの ID。

- ServiceEndpoint

  タイプ: 文字列

  説明: (必須) 到達可能性を分析されるサービスエンドポイントのホスト名。

- RetainVpcReachabilityAnalysis

  タイプ: 文字列

  デフォルト: false

  説明: (オプション) 作成されたネットワークインサイトパスと関連する分析を保持するかどうかを決定します。デフォルトでは、到達可能性の分析に使用されたリソースは、分析が成功すると削除されます。分析を保存することを選択した場合、ランブックは分析を削除しないため、Amazon VPC コンソールで分析を視覚化できます。自動化出力にはコンソールリンクがあります。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `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

ドキュメントステップ

1. aws:executeScript: ホスト名の解決を試みてサービスエンドポイントを検証します。
2. aws:executeScript: VPC とサブネットの詳細を収集します。
3. aws:executeScript: VPC の DNS 設定を評価します。
4. aws:executeScript: VPC エンドポイントチェックを評価します。
5. aws:executeScript: パブリックサービスエンドポイントに接続するインターネットゲートウェイを検索します。
6. aws:executeScript: 到達可能性分析に使用する宛先を決定します。
7. aws:executeScript: Reachability Analyzer を使用してソースからエンドポイントへの到達可能性を分析し、分析が成功したらリソースをクリーンアップします。
8. aws:executeScript: 到達可能性評価レポートを生成します。
9. aws:executeScript: JSON 形式での出力を生成します。

出力

- generateReport.EvalReport - 自動化が実行したチェックの結果 (テキスト形式)。

- generateJsonOutput.Output - 結果の最小バージョン (JSON 形式)。

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

説明

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD ランブックでは、Intel 搭載の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスから同等の AMD 搭載インスタンスタイプへの移行を自動化します。このランブックは、Nitro システムで構築された汎用 (M)、バースタブル汎用 (T)、コンピューティング最適化 (C)、およびメモリ最適化 (R) インスタンスをサポートします。このランブックは、Systems Manager によって管理されていないインスタンスでも使用できます。

データ損失やダウンタイムの潜在的なリスクを軽減するために、ランブックはインスタンスの停止動作、インスタンスが Amazon EC2 Auto Scaling グループに属しているかどうか、インスタンスの状態、および同等の AMD 搭載インスタンスタイプが同じアベイラビリティーゾーンで利用可能かどうかをチェックします。デフォルトでは、インスタンスストアボリュームがアタッチされている場合、またはインスタンスが AWS CloudFormation スタックの一部である場合、このランブックはインスタンスタイプを変更しません。この動作を変更する場合は、AllowInstanceStoreInstances および AllowCloudFormationInstances パラメータのいずれかに yes を指定してください。

> **Important**
>
> AWSPremiumSupport-* ランブックにアクセスするには、エンタープライズサポートまたはビジネスサポートサブスクリプションが必要です。詳細については、「Compare サポート Plans」を参照してください。

考慮事項

- このランブックを使用する前にインスタンスをバックアップすることをおすすめします。
- インスタンスタイプを変更すると、ランブックでインスタンスを停止する必要があります。インスタンスが停止すると、RAM またはインスタンスストアボリュームに保存されているデータはすべて失われ、自動パブリック IPv4 アドレスは解放されます。詳細については、「インスタンスの停止と起動」を参照してください。
- TargetInstanceType パラメータに値を指定しない場合、ランブックは同じインスタンスファミリー内の仮想 CPU とメモリの観点から同等の AMD インスタンスを識別しようとします。同等の AMD インスタンスタイプを特定できない場合、ランブックは終了します。

- DryRun オプションを使用すると、インスタンスタイプを実際に変更しなくても、同等の AMD インスタンスタイプを取得して要件を検証できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- 了解

  タイプ: 文字列

  説明: (必須) 現在実行中のターゲットインスタンスが停止することを確認するには yes を入力してください。
- InstanceId

  タイプ: 文字列

  説明: (必須) タイプを変更する Amazon EC2 インスタンスの ID。
- TargetInstanceType

  タイプ: 文字列

デフォルト: 自動

説明: (オプション) 変更したい AMD インスタンスのタイプ。デフォルトの automatic 値では、仮想 CPU とメモリに関しては同等のインスタンスタイプを使用します。たとえば、m5.large は m5a.large に変更されます。

- AllowInstanceStoreInstances

  タイプ: 文字列

  有効な値: no | yes

  デフォルト: いいえ

  説明: (オプション) yes を指定すると、インスタンスストアボリュームがアタッチされているインスタンスでランブックを実行できるようになります。

- AllowCloudFormationInstances

  タイプ: 文字列

  有効な値: no | yes

  デフォルト: いいえ

  説明: (オプション) に設定するとyes、ランブックは AWS CloudFormation スタックの一部であるインスタンスで実行されます。

- AllowCrossGeneration

  タイプ: 文字列

  有効な値: no | yes

  デフォルト: いいえ

  説明: (オプション) yes に設定すると、ランブックは同じインスタンスファミリー内の最新かつ同等の AMD インスタンスタイプを検索しようとします。

- DryRun

  タイプ: 文字列

  有効な値: no | yes

デフォルト: いいえ

説明: (オプション) yes に設定すると、ランブックは同等の AMD インスタンスタイプを返し、インスタンスタイプを変更せずに移行要件を検証します。

- SleepWait

  タイプ: 文字列

  デフォルト: PT3S

  説明: (オプション) 新しい自動化を開始する前にランブックが待機する必要がある時間です。このパラメータに指定する値は、ISO 8601 標準と一致する必要があります。ISO 8601 文字列の作成の詳細については、「Systems Manager の日付と時刻の文字列のフォーマット」を参照してください。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

1. aws:assertAwsResourceProperty: ターゲット Amazon EC2 インスタンスのステータスがrunning、pending、stopped または stopping であることを確認します。それ以外の場合、自動化は終了します。
2. aws:executeAwsApi: ターゲット Amazon EC2 インスタンスからプロパティを収集します。
3. aws:branch: Amazon EC2 インスタンスの状態に基づいて自動化を分岐します。
   a. stopped または stopping の場合、Amazon EC2 インスタンスが完全に停止するまで自動化が aws:waitForAwsResourceProperty を実行します。
   b. running または pending の場合、Amazon EC2 インスタンスがステータスチェックに合格するまで自動化が aws:waitForAwsResourceProperty を実行します。
4. aws:assertAwsResourceProperty: aws:autoscaling:groupName タグが適用されているかどうかを確認することで、Amazon EC2 インスタンスが Auto Scaling グループに含まれていないことを確認します。
5. aws:executeAwsApi: 現在のインスタンスタイププロパティを収集して、同等の AMD インスタンスタイプを見つけます。
6. aws:assertAwsResourceProperty: AWS Marketplace 製品コードが Amazon EC2 インスタンスに関連付けられていないことを確認します。一部の製品は、すべてのインスタンスタイプで使用できるわけではありません。
7. aws:branch: Amazon EC2 インスタンスが AWS CloudFormation スタックの一部であるかどうかをオートメーションで確認するかどうかに応じて、オートメーションを分岐させます
   a. aws:cloudformation:stack-name タグがインスタンスに適用されると、オートメーションが実行されaws:assertAwsResourceProperty、インスタンスが AWS CloudFormation スタックの一部ではないことが確認されます。
8. aws:branch: インスタンスのルートボリュームタイプが Amazon Elastic Block Store (Amazon EBS) であるかどうかに基づいて自動化を分岐させます。
9. aws:assertAwsResourceProperty: インスタンスのシャットダウン動作が stop であり、terminateではないことを確認します。
10. aws:executeScript: 現在のインスタンスをターゲットとするこのランブックの自動化が 1 つしかないことを確認します。同じインスタンスをターゲットとする別の自動化がすでに進行中の場合は、エラーを返して終了します。
11. aws:executeAwsApi: 同じ量のメモリと vCPU を搭載した AMD インスタンスタイプのリストを返します。
12. aws:executeScript: 現在のインスタンスタイプがサポートされているかどうかを確認し、同等の AMD インスタンスタイプを返します。対応するものがない場合は、自動化は終了します。

13. aws:executeScript: AMD インスタンスタイプが同じアベイラビリティーゾーンで利用可能であることを確認し、提供された IAM 権限を検証します。
14. aws:branch: DryRun パラメータ値が yes であるかどうかに基づいて自動化を分岐させます。
15. aws:branch: 元のインスタンスタイプとターゲットインスタンスタイプが同じかどうかを確認します。一致する場合、自動化は終了します。
16. aws:executeAwsApi: 現在のインスタンスの状態を取得します。
17. aws:changeInstanceState: Amazon EC2 インスタンスを停止します。
18. aws:changeInstanceState: インスタンスが停止の状態で動かなくなった場合、インスタンスを強制的に停止します。
19. aws:executeAwsApi: インスタンスタイプをターゲットの AMD インスタンスタイプに変更します。
20. aws:sleep: インスタンスタイプを変更した後、最終的に一貫性が保たれるまで 3 秒間待ちます。
21. aws:branch: 前のインスタンスの状態に基づいて自動化を分岐します。running であった場合、インスタンスが起動されます。
    a. aws:changeInstanceState: インスタンスタイプを変更する前に Amazon EC2 インスタンスが起動していた場合、Amazon EC2 インスタンスを起動します。
    b. aws:waitForAwsResourceProperty: Amazon EC2 インスタンスがステータスチェックに合格するのを待ちます。インスタンスがステータスチェックに合格しない場合、インスタンスは元のインスタンスタイプに戻されます。
        i. aws:changeInstanceState: Amazon EC2 インスタンスを停止してから、元のインスタンスタイプに変更します。
        ii. aws:changeInstanceState: Amazon EC2 インスタンスが停止状態で停止した場合に、元のインスタンスタイプに変更する前に強制的に Amazon EC2 インスタンスを停止します。
        iii. aws:executeAwsApi: Amazon EC2 インスタンスを元のタイプに変更します。
        iv. aws:sleep: インスタンスタイプを変更した後、最終的に一貫性が保たれるまで 3 秒間待ちます。
        v. aws:changeInstanceState: インスタンスタイプを変更する前に Amazon EC2 インスタンスが起動していた場合、Amazon EC2 インスタンスを起動します。
        vi. aws:waitForAwsResourceProperty: Amazon EC2 インスタンスがステータスチェックに合格するのを待ちます。
22. aws:sleep: ランブックを終了するまで待ちます。

AWSSupport-CheckXenToNitroMigrationRequirements

説明

AWSSupport-CheckXenToNitroMigrationRequirements ランブックは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスが、インスタンスタイプを Xen タイプのインスタンスから Nitro ベースのインスタンスタイプに正常に変更するための前提条件を満たしていることを確認します。この自動化では、次の項目がチェックされます。

- ルートデバイスは、Amazon Elastic Block Store (Amazon EBS) ボリュームです。
- enaSupport 属性は有効になっています。
- ENA モジュールがインスタンスにインストールされます。
- NVMe モジュールがインスタンスにインストールされます。「はい」の場合、モジュールがインストールされ、スクリプトによってモジュールが initramfs イメージに読み込まれているかどうか確認されます。
- /etc/fstab を分析して、デバイス名を使用してマウントされているブロックデバイスを探します。
- オペレーティングシステム (OS) がデフォルトで予測可能なネットワークインターフェイス名を使用するかどうかを確認します。

このランブックでは、以下のオペレーティングシステムがサポートされています。

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux
- Debian サーバー
- Ubuntu Server
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: 文字列

  デフォルト: false

  説明: (必須) Nitro ベースのインスタンスタイプに移行する前に前提条件を確認する Amazon EC2 インスタンスの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `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

ドキュメントステップ

- aws:executeAwsApi - インスタンスの詳細を収集します。
- aws:executeAwsApi - インスタンスのハイパーバイザーに関する情報を収集します。
- aws:branch - ターゲットインスタンスがすでに Nitro ベースのインスタンスタイプを実行しているかどうかに基づいて分岐します。
- aws:branch - インスタンスの OS が Nitro ベースのインスタンスでサポートされているかどうかを確認します。
- aws:assertAwsResourceProperty - 指定したインスタンスが Systems Manager によって管理されており、ステータスが Online であることを確認します。
- aws:branch - インスタンスのルートデバイスが Amazon EBS ボリュームかどうかに基づいて分岐します。
- aws:branch - インスタンスの ENA 属性が有効になっているかどうかに基づいて分岐します。
- aws:runCommand - インスタンスの ENA ドライバーをチェックします。
- aws:runCommand - インスタンスの NVMe ドライバーをチェックします。
- aws:runCommand - fstab ファイルに認識できないフォーマットがないかチェックします。
- aws:runCommand - インスタンス上の予測可能なインターフェイス名設定をチェックします。
- aws:executeScript - 前のステップに基づいて出力を生成します。

出力

finalOutput.output - 自動化によって実行されたチェックの結果。

AWSSupport-ConfigureEC2Metadata

説明

このランブックは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのインスタンスメタデータサービス (IMDS) オプションの設定に役立ちます。このランブックを使用して以下を設定できます。

- インスタンスメタデータに IMDSv2 の使用を強制します。
- `HttpPutResponseHopLimit` 値を設定します。
- インスタンスメタデータへのアクセスを許可または拒否します。

インスタンスメタデータの詳細については、Amazon EC2 ユーザーガイド」の「インスタンスメタデータサービスの設定」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- EnforceIMDSv2

  タイプ: 文字列

  有効な値: 必須 | オプション

  デフォルト: オプション

  説明: (オプション) IMDSv2 を強制します。`required` を選択した場合、Amazon EC2 インスタンスは IMDSv2 のみを使用します。`optional` を選択した場合、メタデータへのアクセスに IMDSv1 と IMDSv2 のどちらかを選択できます。

  > **Important**
  >
  > IMDSv2 を強制すると、IMDSv1 を使用するアプリケーションが正しく機能しなくなる可能性があります。IMDSv2 を強制する前に、IMDS を使用するアプリケーションが IMDSv2 をサポートするバージョンにアップグレードされていることを確認してください。インスタンスメタデータサービスバージョン 2 (IMDSv2) の詳細については、Amazon EC2 ユーザーガイド」の「インスタンスメタデータサービスの設定」を参照してください。

- HttpPutResponseHopLimit

  タイプ: 整数

  有効な値: 0 ~ 64

  デフォルト: 0

  説明: (オプション) インスタンスメタデータリクエストで必要な HTTP PUT レスポンスのホップ制限値 (1 ~ 64)。この値は PUT レスポンスが通過できるホップ数を制御します。レスポンスがインスタンスの外部に伝わらないようにするには、パラメータ値を 1 に指定します。

- InstanceId

  タイプ: 文字列

  説明: (必須) メタデータの設定を変更する Amazon EC2 インスタンスの ID。

- MetadataAccess

  タイプ: 文字列

  有効な値: 有効 | 無効

デフォルト: 有効

説明: (オプション) Amazon EC2 インスタンスでのインスタンスメタデータアクセスを許可または拒否します。disabled を指定すると、他のすべてのパラメータは無視され、インスタンスのメタデータアクセスは拒否されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

ドキュメントステップ

1. branchOnMetadataAccess - MetadataAccess パラメータの値に基づいて自動化を分岐します。
2. disableMetadataAccess - ModifyInstanceMetadataOptions API アクションを呼び出して、メタデータエンドポイントへのアクセスを無効にします。
3. branchOnHttpPutResponseHopLimit - HttpPutResponseHopLimit パラメータの値に基づいて自動化を分岐します。
4. maintainHopLimitAndConfigureImdsVersion - HttpPutResponseHopLimit が 0 の場合、現在のホップ制限を維持し、その他のメタデータオプションを変更します。
5. waitBeforeAssertingIMDSv2State - IMDSv2 のステータスをアサートする前に 30 秒待ちます。
6. setHopLimitAndConfigureImdsVersion - HttpPutResponseHopLimit が 0 より大きい場合、指定された入力パラメータを使用してメタデータオプションを設定します。
7. waitBeforeAssertingHopLimit - メタデータオプションをアサートする前に 30 秒待ちます。
8. assertHopLimit - HttpPutResponseHopLimit プロパティが指定した値に設定されていることをアサートします。
9. branchVerificationOnIMDSv2Option - EnforceIMDSv2 パラメータの値に基づいて検証を分岐させます。

10assertIMDSv2IsOptional - HttpTokens 値が optional に設定されていることをアサートします。

11assertIMDSv2IsEnforced - HttpTokens 値が required に設定されていることをアサートします。

12waitBeforeAssertingMetadataState - メタデータの状態が無効になったことをアサートするまで 30 秒待ちます。

13assertMetadataIsDisabled - メタデータが disabled であることをアサートします。

14describeMetadataOptions - 指定した変更が適用された後にメタデータオプションを取得します。

出力

describeMetadataOptions.State

describeMetadataOptions.MetadataAccess

describeMetadataOptions.IMDSv2

describeMetadataOptions.HttpPutResponseHopLimit

AWSSupport-ContainEC2Instance

説明

AWSSupport-ContainEC2Instance ランブックは、「How do I isolate the Amazon EC2 Instance when faced with a potential compromised or suspicious?」という記事で説明されている手順の自動ソリューションを提供します。オートメーションは、指定した値に応じて分岐します。

動作の仕組み

この自動化ランブックは、一連の調整されたステップを通じて Amazon EC2 インスタンスのネットワーク封じ込めAWSSupport-ContainEC2Instanceを実行します。Contain モードで実行すると、まず入力パラメータを検証し、インスタンスが終了していないかどうかを確認します。次に、現在のセキュリティグループ設定を Amazon S3 バケットにバックアップし、後で復元します。ランブックは、一時的な「すべてのアクセス」セキュリティグループと最終的な「封じ込め」セキュリティグループの 2 つのセキュリティグループを作成します。インスタンスのネットワークインターフェイスを元のセキュリティグループからオールアクセスセキュリティグループに徐々に移行し、最後に封じ込めセキュリティグループに移行します。指定した場合、インスタンスの暗号化されていないバックアップと暗号化されたAMIバックアップの両方が作成されます。Auto Scaling グループのイ

ンスタンスの場合、必要な Auto Scaling グループの変更を処理し、インスタンスをスタンバイ状態にします。Release モードで実行すると、Amazon S3 のバックアップ設定を使用してインスタンスを元のネットワーク設定に復元します。ランブックは、実際の変更を行うことなくアクションをプレビューするためのDryRunパラメータをサポートし、封じ込めおよびリリースワークフロー全体で包括的なエラー処理とレポートメカニズムが含まれています。

Important

- このランブックは、セキュリティグループの変更、 AMIの作成、Auto Scaling グループとのやり取りなど、昇格された権限を必要とするさまざまなオペレーションを実行します。これらのアクションは、特権のエスカレーションや、アカウントの他のワークロードに影響を与える可能性があります。AutomationAssumeRole パラメータで指定されたロールに付与されたアクセス許可を確認し、それらが意図したユースケースに適していることを確認する必要があります。IAM アクセス許可の詳細については、次の AWS ドキュメントを参照してください: AWS Identity and Access Management (IAM) Permissions AWS Systems Manager Automation Permissions。
- このランブックは、ワークロードの可用性の低下や中断を引き起こす可能性のある変更アクションを実行します。具体的には、ターゲット Amazon EC2 インスタンスに関連付けられたセキュリティグループを変更し、ネットワーク接続に影響を与える可能性があります。さらに、インスタンスが Auto Scaling グループの一部である場合、ランブックはグループの設定を変更し、スケーリング動作に影響を与える可能性があります。
- 封じ込めプロセス中に、このランブックはセキュリティグループや などの追加のリソースを作成しますAMI。これらのリソースには識別用のタグが付けられていますが、リソースの作成に注意し、封じ込めプロセスの完了後に適切なクリーンアップまたは管理を行う必要があります。
- Action パラメータが に設定されている場合Release、このランブックは Amazon EC2 インスタンスの設定を元の状態に復元しようとします。ただし、復元プロセスが失敗し、インスタンスが整合性のない状態になるリスクがあります。ランブックには、このような障害が発生した場合の手動復元の手順が記載されていますが、復元プロセス中に発生する可能性のある問題に対処する準備を整えておく必要があります。

本番環境で実行する前に、ランブックを徹底的に確認し、その潜在的な影響を理解し、非本番環境でテストすることをお勧めします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

/

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- autoscaling:CreateOrUpdateTags
- 自動スケーリング:DeleteTags
- autoscaling:DescribeAutoScalingGroups
- autoscaling:DescribeAutoScalingInstances
- 自動スケーリング:DescribeTags
- 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: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

ポリシーの例：

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

指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager AWSSupport-ContainEC2Instanceで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):
     - 説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
     - 型: `AWS::IAM::Role::Arn`
   - アクション (必須):

  - 説明: (必須) Amazon EC2 インスタンスをContain分離するかRestore、以前のバックアップから Amazon EC2 インスタンス設定の元の設定を復元しようとします。
  - タイプ: 文字列
  - 許可されたパターン: Contain|Restore
- DryRun (オプション):
  - 説明: (オプション) に設定するとtrue、オートメーションはコマンドを実行せず、試行した内容を報告し、各ステップの詳細を表示します。デフォルト値: true。
  - 型: ブール値
  - 許可される値: true|false
- CreateAMIBackup (オプション):
  - 説明: (オプション) に設定するとtrue、封じ込めアクションを実行する前に Amazon EC2 インスタンスAMIの が作成されます。
  - 型: ブール値
  - 許可される値: true|false
- KmsKey (オプション):
  - 説明: (オプション) ターゲット Amazon EC2 インスタンスの暗号化された を作成するために使用される AWS KMS キーAMIの ID。デフォルトでは alias/aws/ebs に設定されています。
  - タイプ: 文字列
  - 許可されたパターン: ^(((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,})$
- BackupS3BucketName (条件付き):
  - 説明: (条件付き) が の場合は設定をアップロードし、 Action が の場合は設定を復元Containする Amazon Amazon S3 Action バケットRelease。注: 指定されたバケットがアカウントに存在しない場合、自動化はユーザーに代わって Amazon S3 バケットを作成します。
  - 型: AWS::S3::Bucket::Name
- TagIdentifier (オプション):

  - 説明: (オプション) 封じ込めワークフロー中にこのランブックによって作成または変更Key=BatchId,Value=78925される AWS リソースに追加される形式のタグ。このタグは、封じ込めプロセス中に関連付けられたリソースを識別および管理するために使用できます。復元ワークフロー中、このパラメータで指定されたタグはリソースから削除されます。注： タグキーと値は大文字と小文字が区別されます。
  - タイプ: 文字列
  - 許可されたパターン: ^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\._\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\._\\:\\/@a-zA-Z0-9]{0,128}$
- BackupS3BucketAccess (条件付き):
  - 説明: (条件付き) 封じ込めアクションを実行した後にバックアップ Amazon S3 バケットへのアクセスを許可する IAM ユーザーまたはロールの ARN。このパラメータは、 Actionが の場合に必要ですContain。AutomationAssumeRole、または存在しない場合は、自動化が実行されているコンテキストのユーザーが自動的にリストに追加されます。
  - タイプ: 文字列
  - 許可されたパターン: ^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$
- IngressTrafficRules (オプション):
  - 説明: (オプション) Amazon EC2 インスタンス[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort":"22", "ToPort":"22"}]に適用する形式の Cidr、IpProtocol、FromPort、ToPort を使用したセキュリティグループの進入ルールのカンマ区切りマップ。ルールが指定されていない場合、進入ルールのないセキュリティグループが Amazon EC2 インスタンスにアタッチされ、受信トラフィックから効果的に分離されます。
  - タイプ: MapList
  - 許可されたパターン: ^\\{\\}$|^\\{\"Cidr\":\"[\\x00-\\x7F+]{1,128}\", \"IpProtocol\":\"[\\x00-\\x7F+]{1,128}\",\"FromPort\":\"[\\x00-\\x7F+]{1,128}\",\"ToPort\":\"[\\x00-\\x7F+]{0,255}\"\\}
- EgressTrafficRules (オプション):
  - 説明: (オプション) Amazon EC2 インスタンス[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort":"22", "ToPort":"22"}]に適用する形式の Cidr、IpProtocol、FromPort、ToPort を使用したセキュリティグループ出力ルールのカンマ区切りマップ。ルールが指定されていない場合、出力ルールのないセキュリティグループが Amazon EC2 インスタンスにアタッチされるため、すべての送信トラフィックを効果的に防止できます。

    - タイプ: MapList
    - 許可されたパターン: ^\\{\\}$|^\\{\"Cidr\":\"[\\x00-\\x7F+]{1,128}\",\"IpProtocol\":\"[\\x00-\\x7F+]{1,128}\",\"FromPort\":\"[\\x00-\\x7F+]{1,128}\",\"ToPort\":\"[\\x00-\\x7F+]{0,255}\"\\}
  - BackupS3KeyName (オプション):
    - 説明: (オプション) Actionが に設定されている場合Restore、オートメーションがターゲット Amazon EC2 インスタンス設定の復元を試みるために使用する Amazon Amazon S3 キーを指定します。Amazon S3 キーは通常、 の形式に従います{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json。キーは、前の封じ込め自動化実行の出力から取得できます。
    - タイプ: 文字列
    - 許可されたパターン: ^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$
4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
  - ValidateRequiredInputs

    必要な入力がすべて提供されていることを検証します。
  - AssertInstanceIsNotTerminated

    ターゲット Amazon EC2 インスタンスが終了 (削除) していないかどうかを確認します。
  - GetAutoScalingInstanceInfo

    ターゲット Amazon EC2 インスタンスが Auto Scaling グループの一部である場合、Amazon EC2 インスタンスのライフサイクルとグループ名を取得します。
  - CheckBackupS3BucketName

    ターゲット Amazon S3 バケットがオブジェクトへのwriteパブリックアクセスを許可readしている可能性があるかどうかを確認します。バケットが存在しない場合、新しい Amazon S3 BackupS3BucketNameバケットが作成されます。
  - BranchOnActionAndMode

    入力パラメータ Actionと に基づいてオートメーションを分岐しますDryRun。
  - BranchOnAutoScalingGroupMembership

ターゲット Amazon EC2 インスタンスが Auto Scaling グループの一部であるかどうかとそのライフサイクル状態に基づいてオートメーションを分岐します。

- DescribeAutoScalingGroups

  関連付けられた Amazon EC2 Auto Scaling グループ設定を取得して保存します。

- ModifyAutoScalingGroup

  封じ込めアクションの関連する Amazon EC2 Auto Scaling グループ設定を変更し、Amazon EC2 インスタンスを `Standby`状態に設定し、Auto Scaling グループの`MinSize`容量を調整します。

- BackupInstanceSecurityGroups

  ターゲット Amazon EC2 インスタンスセキュリティグループの設定を取得して保存します。

- CreateAllAccessSecurityGroup

  ターゲット Amazon EC2 インスタンスのセキュリティグループを置き換えるすべての進入トラフィックを許可する一時的なセキュリティグループを作成します。

- CreateContainmentSecurityGroup

  指定されたイングレスルールとエグレスルールを使用して制限的な封じ込めセキュリティグループを作成し、一時的なオールアクセスグループをそのグループに置き換えます。

- BranchOnCreateAMIBackup

  `CreateAMIBackup` 入力パラメータに基づいてオートメーションを分岐します。

- AssertSourceInstanceRootVolumeIsEbs

  ターゲット Amazon EC2 インスタンスのルートボリュームが Amazon EBS かどうかを確認します。

- CreateImage

  ターゲット Amazon EC2 インスタンスAMIの を作成します。

- RestoreInstanceConfiguration

  バックアップからターゲット Amazon EC2 インスタンス設定を復元します。

- ReportContain

  封じ込めアクションのドライランの詳細を出力します。

- ReportRestore

  復元アクションのドライランの詳細を出力します。

- ReportRestoreFailure

  復元ワークフローの失敗シナリオ中に、ターゲット Amazon EC2 インスタンスの元の設定を復元する手順を示します。

- ReportContainmentFailure

  封じ込めワークフローの失敗シナリオ中に、ターゲット Amazon EC2 インスタンスの元の設定を復元する手順について説明します。

- FinalOutput

  封じ込めアクションの詳細を出力します。

7. 実行が完了したら、出力セクションで実行の詳細な結果を確認します。

- FinalOutput.Output

  が False にDryRun設定されている場合、このランブックによって実行される封じ込めアクションの詳細を出力します。

- RestoreInstanceConfiguration.Output

  が False に設定されている場合DryRun、このランブックによって実行される復元アクションを出力します。

- ReportContain.Output

  が True にDryRun設定されている場合、このランブックによって実行される封じ込めアクションの詳細を出力します。

- ReportRestore.Output

  が True にDryRun設定されている場合、このランブックによって実行される復元アクションの詳細を出力します。

- ReportContainmentFailure.Output

  封じ込めワークフローの失敗シナリオ中に、ターゲット Amazon EC2 インスタンスの元の設定を復元する手順について説明します。

- ReportRestoreFailure.Output

復元ワークフローの失敗シナリオ中に、ターゲット Amazon EC2 インスタンスの元の設定を復元する手順を示します。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- シンプルなオートメーションワークフローを実行する
- 自動化のセットアップ
- 自動化ワークフローのサポート

AWSSupport-CopyEC2Instance

説明

AWSSupport-CopyEC2Instance ランブックは、ナレッジセンター記事「EC2 インスタンスを別のサブネット、アベイラビリティーゾーン、または VPC に移動する方法」で説明されている手順についての、自動化されたソリューションを提供します。自動化は、Region および SubnetId パラメータに指定した値に基づいて分岐します。

SubnetId パラメータに値を指定し、Region パラメータに値を指定しない場合、自動化はターゲットインスタンスの Amazon Machine Image (AMI) を作成し、指定したサブネットの AMI から新しいインスタンスを起動します。

SubnetId パラメータと Regionパラメータの値を指定すると、オートメーションはターゲットインスタンスAMIの を作成し、 AWS リージョン 指定した AMI に をコピーし、指定したサブネットAMIの から新しいインスタンスを起動します。

Region パラメータに値を指定し、SubnetId パラメータに値を指定しない場合、自動化はターゲットインスタンスの AMI を作成し、指定したリージョンに AMI をコピーし、送信先リージョンの仮想プライベートクラウド (VPC) のデフォルトサブネットの AMI から新しいインスタンスを起動します。

Region または SubnetId パラメータのいずれにも値が指定されていない場合、自動化はターゲットインスタンスの AMI を作成し、VPC のデフォルトサブネットの AMI から新しいインスタンスを起動します。

AMI を別のリージョンにコピーするには、AutomationAssumeRole パラメータに値を指定する必要があります。waitForAvailableDestinationAmi ステップ中に自動化がタイムアウトしても、AMI はまだコピー中である可能性があります。その場合は、コピーが完了するのを待ってから、インスタンスを手動で起動できます。

このオートメーションを実行する前に、次の点に注意してください。

- AMI は Amazon Elastic Block Store (Amazon EBS) スナップショットに基づいています。スナップショットが事前にない大規模なファイルシステムの場合、AMI 作成には数時間かかることがあります。AMI 作成時間を短縮するには、AMI を作成する前に Amazon EBS スナップショットを作成してください。
- AMI を作成しても、そのインスタンス上のインスタンスストアボリュームのスナップショットは作成されません。Amazon EBS にインスタンスストアボリュームをバックアップする方法については、「Amazon EC2 インスタンスのインスタンスストアボリュームを Amazon EBS にバックアップする方法」を参照してください。
- 新しい Amazon EC2 インスタンスには、別のプライベート IPv4 またはパブリック IPv6 IP アドレスが割り当てられています。古い IP アドレス (DNS エントリにあるものなど) へのリファレンスはすべて、新しいインスタンスに割り当てられた新しい IP アドレスで更新する必要があります。ソースインスタンスで Elastic IP アドレスを使用している場合、新しいインスタンスにそのアドレスをアタッチしてください。
- コピーが起動してドメインにアクセスしようとすると、ドメインセキュリティ識別子 (SID) の競合の問題が発生する可能性があります。AMI をキャプチャする前に、Sysprep を使用するか、ドメインに参加しているインスタンスをドメインから削除して競合の問題を防止してください。詳細については、「Sysprep を使用して再利用可能なカスタム Windows AMI を作成およびインストールする方法を教えてください」を参照してください。

このオートメーションを実行する (コンソール)

> **Important**
>
> このランブックを使用して Microsoft Active Directory ドメインコントローラーのインスタンスをコピーすることはお勧めしません。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: 文字列

  説明: (必須) コピーするインスタンスの ID。
- KeyPair

  タイプ: 文字列

  説明: (オプション) 新しくコピーされるインスタンスに関連付けるキーペア。インスタンスを別のリージョンにコピーする場合は、キーペアが指定したリージョンに存在することを確認してください。
- リージョン

  タイプ: 文字列

  説明: (オプション) インスタンスをコピーするリージョン。このパラメータに値を指定し、SubnetId および SecurityGroupIds パラメータに値を指定しなかった場合、自動化はデフォルトのセキュリティグループを使用してデフォルト VPC でインスタンスを起動しようとします。送信先リージョンで EC2-Classic が有効になっている場合、起動は失敗します。
- SubnetId

  タイプ: 文字列

説明: (オプション) インスタンスを起動するサブネットの ID。EC2-Classic が送信先リージョンで有効になっている場合は、このパラメータに値を指定する必要があります。

- InstanceType

  タイプ: 文字列

  説明: (オプション) コピーされたインスタンスを起動する時のインスタンスタイプ。このパラメータに値を指定しない場合、ソースインスタンスタイプが使用されます。ソースインスタンスタイプがインスタンスのコピー先のリージョンでサポートされていない場合、自動化は失敗します。

- SecurityGroupIds

  タイプ: 文字列

  説明: (オプション) コピーされたインスタンスに関連付けるセキュリティグループ ID のカンマ区切りリスト。このパラメータに値を指定せず、インスタンスを別のリージョンにコピーしない場合、ソースインスタンスに関連付けられているセキュリティグループが使用されます。インスタンスを別のリージョンにコピーする場合、コピー先のリージョンのデフォルトの VPC のデフォルトのセキュリティグループが使用されます。

- KeepImageSourceRegion

  型: ブール値

  有効な値: true | false

  デフォルト: true

  説明: (オプション) このパラメータに `true` を指定した場合、自動化はソースインスタンスの AMI を削除しません。このパラメータに `false` を指定すると、自動化は AMI の登録を解除し、関連するスナップショットを削除します。

- KeepImageDestinationRegion

  型: ブール値

  有効な値: true | false

  デフォルト: true

説明: (オプション) このパラメータに `true` を指定した場合、自動化は、指定したリージョンにコピーされた AMI を削除しません。このパラメータに `false` を指定すると、自動化は AMI の登録を解除し、関連するスナップショットを削除します。

- NoRebootInstanceBeforeTakingImage

  型: ブール値

  有効な値: true | false

  デフォルト: false

  説明: (オプション) このパラメータに `true` を指定した場合、ソースインスタンスは AMI を作成する前に再起動されません。このオプションを使用すると、作成したイメージのファイルシステムの完全性は保証できません。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

インスタンスを別のリージョンにコピーする場合、以下の権限も必要になります。

- `ec2:CopyImage`

ドキュメントステップ

- describeOriginalInstanceDetails - コピーするインスタンスから詳細情報を収集します。
- assertRootVolumeIsEbs - ルートボリュームのデバイスタイプが `ebs` であるかどうかを確認し、そうでない場合は自動化を終了します。

- evalInputParameters - 入力パラメータに指定された値を評価します。
- createLocalAmi - ソースインスタンスの AMI を作成します。
- tagLocalAmi - 前のステップで作成した AMI にタグを付けます。
- branchAssertRegionIsSame - インスタンスを同じリージョン内でコピーするか、別のリージョンにコピーするかに基づいて分岐します。
- branchAssertSameRegionWithKeyPair - 同じリージョン内でコピーされているインスタンスの `KeyPair` パラメータに値が指定されているかどうかに基づいて分岐します。
- sameRegionLaunchInstanceWithKeyPair - 同じサブネットまたは指定したサブネットのソースインスタンスの AMI から、指定したキーペアを使用して Amazon EC2 インスタンスを起動します。
- sameRegionLaunchInstanceWithoutKeyPair - 同じサブネットまたは、キーペアなしで指定したサブネットのソースインスタンスの AMI から Amazon EC2 インスタンスを起動します。
- copyAmiToRegion - AMI をコピー先リージョンにコピーします。
- waitForAvailableDestinationAmi - コピーされた AMI の状態が `available` になるのを待ちます。
- destinationRegionLaunchInstance - コピーされた AMI を使用して Amazon EC2 インスタンスを起動します。
- branchAssertDestinationAmiToDelete - `KeepImageDestinationRegion` パラメータで指定された値に基づく分岐。
- deregisterDestinationAmiAndDeleteSnapshots - コピーされた AMI を登録解除し、関連するスナップショットを削除します。
- branchAssertSourceAmiTodelete - `KeepImageSourceRegion` パラメータで指定された値に基づく分岐。
- deregisterSourceAmiAndDeleteSnapshots - 作成された AMI をソースインスタンスから登録解除し、関連するスナップショットを削除します。
- sleep - 自動化を 2 秒間スリープ状態にします。これは終了ステップです。

出力

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchInstance.DestinationInstanceId

AWSSupport-EnableWindowsEC2SerialConsole

説明

ランブックAWSSupport-EnableWindowsEC2SerialConsoleは、Amazon EC2 Windows インスタンスで Amazon EC2 シリアルコンソール、特殊管理コンソール (SAC)、およびブートメニューを有効にするのに役立ちます。Amazon Elastic Compute Cloud (Amazon EC2) シリアルコンソール機能を使用すると、Amazon EC2 インスタンスのシリアルポートにアクセスして、起動、ネットワーク設定、その他の問題のトラブルシューティングを行うことができます。ランブックは、実行中の状態で によって管理されているインスタンスと AWS Systems Manager、停止状態または によって管理されていないインスタンスでこの機能を有効にするために必要なステップを自動化します AWS Systems Manager。

動作の仕組み

AWSSupport-EnableWindowsEC2SerialConsole オートメーションランブックは、Microsoft Windows Server を実行している Amazon EC2 インスタンスで SAC とブートメニューを有効にするのに役立ちます。実行中の状態で によって管理されているインスタンスの場合 AWS Systems Manager、ランブックは AWS Systems Manager Run Command PowerShell スクリプトを実行して SAC とブートメニューを有効にします。停止状態または によって管理されていないインスタンスの場合 AWS Systems Manager、ランブックは AWSSupport-StartEC2RescueWorkflow を使用して一時的な Amazon EC2 インスタンスを作成し、必要な変更をオフラインで実行します。

詳細については、「Windows インスタンス用の Amazon EC2 シリアルコンソール」を参照してください。

Important

- インスタンスで SAC を有効にすると、パスワードの取得に依存する Amazon EC2 サービスは Amazon EC2 コンソールから動作しません。詳細については、「SAC を使用して Windows インスタンスをトラブルシューティングする」を参照してください。
- シリアルコンソールへのアクセスを設定するには、アカウントレベルでシリアルコンソールアクセスを許可し、ユーザーにアクセス権を付与するように AWS Identity and Access Management (IAM) ポリシーを設定する必要があります。また、ユーザーがトラブルシューティングのためにシリアルコンソールを使用できるように、すべてのインスタンスでパスワードベースのユーザーを設定する必要があります。詳細については、Amazon EC2 シリアルコンソールへのアクセスを設定する」を参照してください。

- アカウントでシリアルコンソールが有効になっているかどうかを確認するには、「シリアルコンソールへのアカウントアクセスステータスの表示」を参照してください。
- シリアルコンソールアクセスは、Nitro System 上に構築された仮想化インスタンスでのみサポートされます。

詳細については、Amazon EC2 シリアルコンソールの前提条件」を参照してください。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

指示

次の手順に従って自動化を設定します。

1. AWS Systems Manager コンソールAWSSupport-EnableWindowsEC2SerialConsoleで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - InstanceId: (必須)

     Amazon EC2 シリアルコンソール、 (SAC)、およびブートメニューを有効にする Amazon EC2 インスタンスの ID。
   - AutomationAssumeRole: (オプション)

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする IAM ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - HelperInstanceType: (条件付き)

オフラインインスタンスの Amazon EC2 シリアルコンソールを設定するためにランブックがプロビジョニングする Amazon EC2 インスタンスのタイプ。

- HelperInstanceProfileName: (条件付き)

  ヘルパーインスタンスの既存の IAM インスタンスプロファイルの名前。停止状態または によって管理されていないインスタンスで SAC とブートメニューを有効にする場合は AWS Systems Manager、これが必要です。IAM インスタンスプロファイルが指定されていない場合、自動化はユーザーに代わってインスタンスプロファイルを作成します。

- SubnetId: (条件付き)

  ヘルパーインスタンスのサブネット ID。デフォルトでは、指定されたインスタンスが存在するのと同じサブネットを使用します。

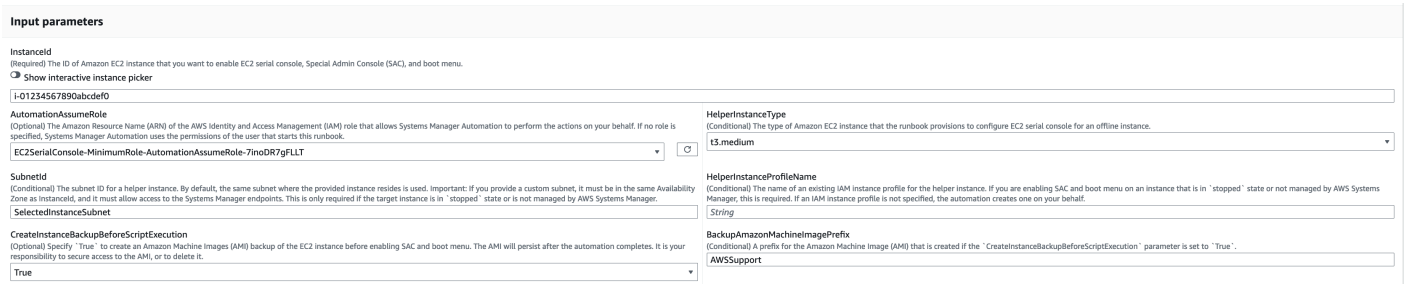
  > **Important**
  >
  > カスタムサブネットを指定する場合は、InstanceId と同じアベイラビリティーゾーンに存在し、Systems Manager エンドポイントへのアクセスを許可する必要があります。これは、ターゲットインスタンスが停止状態であるか、 によって管理されていない場合にのみ必要です AWS Systems Manager。

- CreateInstanceBackupBeforeScriptExecution: (オプション)

  SAC とブートメニューを有効にする前に、True を指定して Amazon EC2 インスタンスの Amazon マシンイメージ (AMI) バックアップを作成します。AMI は、自動化が完了した後も維持されます。AMI へのアクセスを保護するか、削除するのはお客様の責任です。

- BackupAmazonMachineImagePrefix: (条件付き)

  `CreateInstanceBackupBeforeScriptExecution` パラメータが に設定されている場合に作成される Amazon マシンイメージ (AMI) のプレフィックス`True`。



4. [実行] を選択します。

5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - CheckIfEc2SerialConsoleAccessEnabled:

     Amazon EC2 シリアルコンソールアクセスがアカウントレベルで有効になっているかどうかを確認します。注: シリアルコンソールへのアクセスは、デフォルトでは利用できません。詳細については、Amazon EC2 シリアルコンソールへのアクセスを設定する」を参照してください。
   - CheckIfEc2InstanceIsWindows:

     ターゲットインスタンスプラットフォームが Windows であるかどうかをアサートします。
   - GetInstanceType:

     ターゲットインスタンスのインスタンスタイプを取得します。
   - CheckIfInstanceTypeIsNitro:

     インスタンスタイプのハイパーバイザーが Nitro ベースかどうかを確認します。シリアルコンソールアクセスは、Nitro System 上に構築された仮想化インスタンスでのみサポートされます。
   - CheckIfInstanceIsInAutoScalingGroup:

     `DescribeAutoScalingInstances` API を呼び出して、Amazon EC2 インスタンスが Amazon EC2 Auto Scaling グループの一部かどうかを確認します。インスタンスが Amazon EC2 Auto Scaling グループの一部である場合、Porting Assistant for .NET インスタンスがスタンバイライフサイクル状態になります。
   - WaitForEc2InstanceStateStablized:

     インスタンスが実行中または停止状態になるまで待機します。
   - GetEc2InstanceState:

     インスタンスの現在の状態を取得します。
   - BranchOnEc2InstanceState:

     前のステップで取得したインスタンスの状態に基づいて分岐します。そのインスタンスの状態が実行中の場合は ステップに、そう`CheckIfEc2InstanceIsManagedBySSM`でない場合は `CheckIfHelperInstanceProfileIsProvided` ステップに進みます。
   - CheckIfEc2InstanceIsManagedBySSM:

インスタンスが によって管理されているかどうかを確認します AWS Systems Manager。管理されている場合、ランブックは PowerShell Run Command を使用して SAC とブートメニューを有効にします。

- BranchOnPreEC2RescueBackup:

  `CreateInstanceBackupBeforeScriptExecution` 入力パラメータに基づいて分岐します。

- CreateAmazonMachineImageBackup:

  インスタンスの AMI バックアップを作成します。

- EnableSACAndBootMenu:

  PowerShell Run Command スクリプトを実行して SAC とブートメニューを有効にします。

- RebootInstance:

  Amazon EC2 インスタンスを再起動して設定を適用します。これは、インスタンスがオンラインであり、 によって管理されている場合の最後のステップです AWS Systems Manager。

- CheckIfHelperInstanceProfileIsProvided:

  一時的な Amazon EC2 インスタンスを使用して SAC とブートメニューをオフラインで有効にする前に、`HelperInstanceProfileName`指定された が存在するかどうかを確認します。

- RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu:

  インスタンスが停止状態であるか、 によって管理されていないときに、 を実行して SAC とブートメニュー`AWSSupport-StartEC2RescueWorkflow`を有効にします AWS Systems Manager。

- GetExecutionDetails:

  バックアップスクリプト出力とオフラインスクリプト出力のイメージ ID を取得します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

   - EnableSACAndBootMenu.Output:

     `EnableSACAndBootMenu` ステップでのコマンド実行の出力。

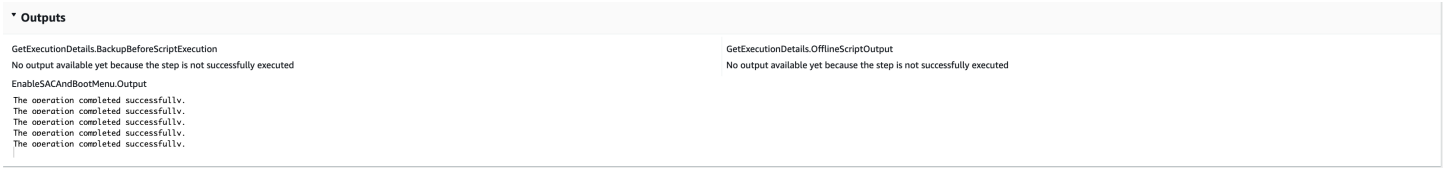
   - GetExecutionDetails.OfflineScriptOutput:

     `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` ステップで実行されたオフラインスクリプトの出力。

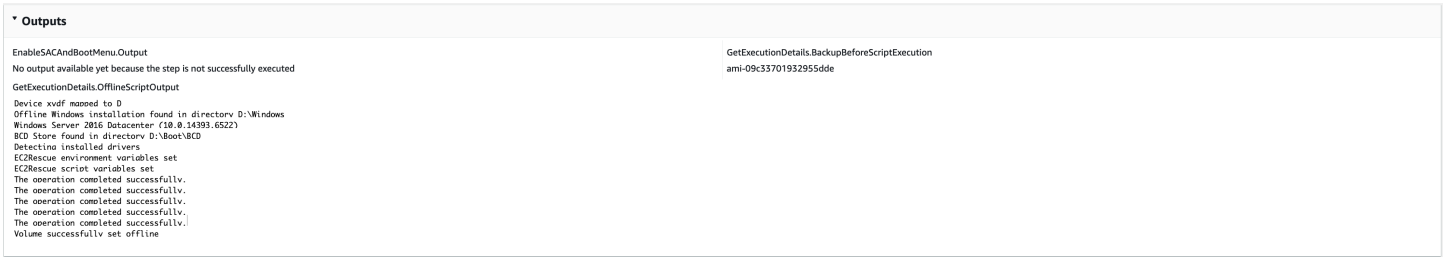
- GetExecutionDetails.BackupBeforeScriptExecution:

  `CreateInstanceBackupBeforeScriptExecution` 入力パラメータが True の場合に取得される AMI バックアップのイメージ ID。

によって実行および管理されているインスタンスでの実行の出力 AWS Systems Manager



によって停止または管理されていないインスタンスの実行の出力 AWS Systems Manager



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWSSupport-ExecuteEC2Rescue

説明

このランブックでは、EC2Rescue ツールを使用してトラブルシューティングを行い、可能な場合は、指定された Linux または Windows Server 向け Amazon Elastic Compute Cloud (Amazon EC2) で発生する、一般的な接続の問題を修復します。暗号化されたルートボリュームを持つインスタンスはサポートされていません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- EC2RescueInstanceType

  タイプ: 文字列

  有効な値: t2.small | t2.medium | t2.large

  デフォルト: t2.small

  説明: (必須) EC2Rescue インスタンスの EC2 インスタンスタイプ。推奨サイズ: `t2.small`
- LogDestination

  タイプ: 文字列

  説明: (オプション) トラブルシューティングのログをアップロードするアカウントの Amazon S3 バケット名。収集されたログにアクセスする必要がないユーザーへの不必要な読み取り/書き込みアクセス権限をバケットポリシーに付与しないようにします。
- SubnetId

  タイプ: 文字列

デフォルト: CreateNewVPC

説明: (オプション) EC2Rescue インスタンスのサブネット ID。デフォルトでは、 AWS Systems Manager Automation は新しい VPC を作成します。または、SelectedInstanceSubnet を使用してインスタンスと同じサブネットを使用するか、カスタムサブネット ID を指定します。

> **Important**
>
> サブネットは UnreachableInstanceId と同じアベイラビリティーゾーンである必要があり、SSM エンドポイントへのアクセスを許可する必要があります。

- UnreachableInstanceId

  タイプ: 文字列

  説明: (必須) 接続できない EC2 インスタンスの ID。

> **Important**
>
> Systems Manager Automation はこのインスタンスを停止し、操作を試みる前に AMI を作成します。インスタンスストアボリュームに保存されているデータは失われます。Elastic IP アドレスを使用していない場合、パブリック IP アドレスが変わります。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

自動化の出力を読み取るには、少なくとも ssm:StartAutomationExecution と ssm:GetAutomationExecution が必要です。必要な許可の詳細については、「AWSSupport-StartEC2RescueWorkflow」を参照してください。

ドキュメントステップ

1. aws:assertAwsResourceProperty - 提供されたインスタンスが Windows Server かどうかをアサートします。
   a. (Windows Server 用の EC2Rescue) 提供されたインスタンスが Windows Server インスタンスの場合:

i. `aws:executeAutomation` - Windows Server オフラインスクリプトの EC2Rescue を使用して `AWSSupport-StartEC2RescueWorkflow` を呼び出します。
ii. `aws:executeAwsApi` - ネスト化された自動化からバックアップ AMI ID を取得します。
iii. `aws:executeAwsApi` - ネスト化された自動化から EC2Rescue の要約を取得します。

b. (Linux 用の EC2Rescue) 提供されたインスタンスが Linux インスタンスの場合:
i. `aws:executeAutomation` - Linux オフラインスクリプトの EC2Rescue を使用して `AWSSupport-StartEC2RescueWorkflow` を呼び出します。
ii. `aws:executeAwsApi` - ネスト化された自動化からバックアップ AMI ID を取得します。
iii. `aws:executeAwsApi` - ネスト化された自動化から EC2Rescue の要約を取得します。

出力

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

説明

`AWSSupport-ListEC2Resources` ランブックは、 AWS リージョン 指定した からAmazon EC2 インスタンス、および Amazon Elastic Block Store (Amazon EBS) ボリューム、Elastic IP アドレス、Amazon EC2 Auto Scaling グループなどの関連リソースに関する情報を返します。デフォルトでは、情報はすべてのリージョンから収集され、オートメーションの出力に表示されます。オプションで、情報のアップロード先の Amazon Simple Storage Service (Amazon S3) バケットをカンマ区切り値 (.csv) ファイルで指定できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- BucketName

  タイプ: 文字列

  説明: (オプション) 収集された情報がアップロードされる S3 バケットの名前。
- DisplayResourceDeletionDocumentation

  タイプ: 文字列

  デフォルト: true

  説明: (オプション) `true` に設定すると、オートメーションはリソースの削除に関連するドキュメントへの出力でリンクを作成します。
- RegionsToQuery

  タイプ: 文字列

  デフォルト: All

  説明: (オプション) Amazon EC2 に関連する情報を収集するリージョン。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `autoscaling:DescribeAutoScalingGroups`

- ec2:DescribeAddresses
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRegions
- ec2:DescribeVolumes
- ec2:DescribeSnapshots
- elasticloadbalancing:DescribeLoadBalancers

さらに、指定した S3 バケットに収集された情報を正常にアップロードするには、AutomationAssumeRole で次のアクションが必要です。

- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:PutObject

ドキュメントステップ

- aws:executeAwsApi - アカウントに対して有効になっているリージョンを収集します。
- aws:executeScript - アカウントに対して有効になっているリージョンが、RegionsToQuery パラメータで指定されたリージョンをサポートしていることを確認します。
- aws:branch - アカウントに対して有効になっているリージョンがない場合、自動化は終了します。
- aws:executeScript - 指定したアカウントおよびリージョンのすべての EC2 インスタンスを一覧表示します。
- aws:executeScript - 指定したアカウントおよびリージョンのすべての Amazon マシンイメージ (AMI) を一覧表示します。
- aws:executeScript - 指定したアカウントおよびリージョンのすべての EBS ボリュームを一覧表示します。
- aws:executeScript - 指定したアカウントおよびリージョンのすべての Elastic IP アドレスを一覧表示します。
- aws:executeScript - 指定したアカウントおよびリージョンのすべてのエラスティックネットワークインターフェイスを一覧表示します。

- aws:executeScript - 指定したアカウントおよびリージョンのすべての Auto Scaling グループを一覧表示します。
- aws:executeScript - 指定したアカウントおよびリージョンのすべてのロードバランサーを一覧表示します。
- aws:executeScript - Bucket パラメータに値を指定した場合、指定された S3 バケットに収集された情報をアップロードします。

AWSSupport-ManageRDPSettings

説明

AWSSupport-ManageRDPSettings ランブックを使用することで、一般的なリモートデスクトッププロトコル (RDP) 設定 (RDP ポートやネットワークレイヤー認証 (NLA) など) を管理できます。デフォルトでは、このランブックは読み取った設定の値を出力します。

> **Important**
>
> このランブックを実行する前に、RDP 設定に対し行った変更の内容を、慎重に確認しておく必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) RDP 設定を管理するマネージドインスタンスの ID。

- NLASettingAction

  タイプ: 文字列

  有効な値: Check | Enable | Disable

  デフォルト: Check

  説明: (必須) NLA 設定で実行するアクションは次のとおりです。Check、Enable、Disable。

- RDPPort

  タイプ: 文字列

  デフォルト: 3389

  説明: (オプション) 新しい RDP ポートを指定します。アクションが Modify に設定されている場合にのみ使用されます。ポート番号は 1025 ~ 65535 の間である必要があります。注意: ポートが変更されると RDP サービスが再開されます。

- RDPPortAction

  タイプ: 文字列

  有効な値: Check | Modify

  デフォルト: Check

  説明: (必須) RDP ポートに適用するアクション。

- RemoteConnections

  タイプ: 文字列

有効な値: Check | Enable | Disable

デフォルト: Check

説明: (必須) fDenyTSConnections 設定で実行するアクション。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

このコマンドを受信する EC2 インスタンスには、[AmazonSSMManagedInstanceCore] Amazon 管理ポリシーがアタッチされた IAM ロールが必要です。オートメーションを実行し、インスタンスにコマンドを送信するには、少なくとも [ssm:SendCommand] が必要です。また、コマンド出力を読み取ることができる [ssm:GetCommandInvocation] も必要です。

ドキュメントステップ

aws:runCommand - PowerShell スクリプトを実行して、ターゲットインスタンスの RDP 設定を変更または確認します。

出力

manageRDPSettings.Output

AWSSupport-ManageWindowsService

説明

AWSSupport-ManageWindowsService ランブックを使用すると、ターゲットインスタンス上の Windows サービスを停止、開始、再起動、一時停止、または無効にすることができます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) サービスを管理するマネージドインスタンスの ID。

- ServiceAction

  タイプ: 文字列

  有効な値: Check | Restart | Force-Restart | Start | Stop | Force-Stop | Pause

  デフォルト: Check

  説明: (必須) Windows サービスに適用するアクション。`Force-Restart` および `Force-Stop` を使用して、依存サービスがあるサービスを再起動および停止することができます。

- StartupType

  タイプ: 文字列

  有効な値: Check | Auto | Demand | Disabled | DelayedAutoStart

  デフォルト: Check

  説明: (必須) Windows サービスに適用するスタートアップタイプ。

- WindowsServiceName

  タイプ: 文字列

  説明: (必須) 有効な Windows サービス名。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

このコマンドを受信する EC2 インスタンスには、[AmazonSSMManagedInstanceCore] Amazon 管理ポリシーがアタッチされた IAM ロールがあることが推奨されます。このオートメーションを実行してコマンドをインスタンスに送信するには、少なくとも ssm:StartAutomationExecution と ssm:SendCommand が必要です。さらに、オートメーションから出力を読み取るには、ssm:GetAutomationExecution が必要です。

ドキュメントステップ

aws:runCommand - PowerShell スクリプトを実行して、対象となるインスタンスの Windows サービスに必要な設定を適用します。

出力

manageWindowsService.Output

AWSSupport-MigrateEC2ClassicToVPC

説明

AWSSupport-MigrateEC2ClassicToVPC ランブックでは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを EC2-Classic から仮想プライベートクラウド (VPC) に移行します。このランブックでは、ハードウェア仮想マシン (HVM) 仮想化タイプの Amazon EC2 インスタンスを Amazon Elastic Block Store (Amazon EBS) ルートボリュームで移行できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- ApproverIAM

  タイプ: StringList

  説明: (オプション) アクションを承認または拒否できる IAM ユーザーの Amazon リソースネーム (ARN)。このパラメータは、`MigrationType` パラメータの `CutOver` 値を指定した場合にのみ適用されます。

- DestinationSecurityGroupId

  タイプ: StringList

  説明: (オプション) VPC で起動される Amazon EC2 インスタンスに関連付けるセキュリティグループの ID。このパラメータに値を指定しない場合、自動化は VPC 内にセキュリティグループを作成し、EC2-Classic のセキュリティグループからルールをコピーします。ルールが新しいセキュリティグループにコピーできない場合、VPC のデフォルトセキュリティグループが Amazon EC2 インスタンスに関連付けられます。

- DestinationSubnetId

  タイプ: 文字列

  説明: (オプション) Amazon EC2 インスタンスを移行するサブネットの ID。このパラメータに値を指定しない場合、自動化は VPC からサブネットをランダムに選択します。

- InstanceId

  タイプ: 文字列

  説明: (必須) 移行する Amazon EC2 インスタンスの ID。

- MigrationType

  タイプ: 文字列

  有効な値: カットオーバー | テスト

  説明: (必須) 実行する移行のタイプ。

EC2-Classic で実行されている Amazon EC2 インスタンスを停止するには、CutOver オプションの承認が必要です。このアクションが承認されると、Amazon EC2 インスタンスは停止し、自動化によって Amazon Machine Image (AMI) が作成されます。AMI ステータスが available の場合、VPC で指定した DestinationSubnetId のこの AMI から新しい Amazon EC2 インスタンスが起動されます。EC2-Classic で実行されている Amazon EC2 インスタンスに Elastic IP アドレスがアタッチされている場合、インスタンスは VPC 内で新しく作成された Amazon EC2 インスタンスに移動されます。VPC で起動する Amazon EC2 インスタンスの作成が何らかの理由で失敗した場合、インスタンスは終了され、EC2-Classic で Amazon EC2 インスタンスを開始する承認が要求されます。

Test オプションは、再起動せずに EC2-Classic で実行されている Amazon EC2 インスタンスの AMI を作成します。Amazon EC2 インスタンスは再起動しないため、作成されたイメージのファイルシステムの整合性は保証できません。AMI ステータスが available の場合、VPC で指定した DestinationSubnetId のこの AMI から新しい Amazon EC2 インスタンスが起動されます。EC2-Classic で実行されている Amazon EC2 インスタンスに Elastic IP アドレスがアタッチされている場合、自動化は指定した DestinationSubnetId がパブリックであることを確認します。VPC で起動する Amazon EC2 インスタンスの作成が何らかの理由で失敗した場合、インスタンスは終了し、自動化は終了します。

- SNSNotificationARNforApproval

  タイプ: 文字列

  説明: (オプション) 承認要求を送信する Amazon Simple Notification Service (Amazon SNS) トピックの ARN。このパラメータは、MigrationType パラメータの CutOver 値を指定した場合にのみ適用されます。

- TargetInstanceType

  タイプ: 文字列

  デフォルト: t2.2xlarge

  説明: (オプション) VPC で起動する Amazon EC2 インスタンスのタイプ。T2、M4、C4 など、Xen ベースのインスタンスタイプのみがサポートされます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeAwsApi - InstanceId パラメータで指定された Amazon EC2 インスタンスの詳細を収集します。
- aws:assertAwsResourceProperty - TargetInstanceType パラメータで指定したインスタンスタイプが Xen ベースであることを確認します。
- aws:assertAwsResourceProperty - InstanceId パラメータで指定した Amazon EC2 インスタンスが HVM 仮想化タイプであることを確認します。
- aws:assertAwsResourceProperty - InstanceId パラメータで指定した Amazon EC2 インスタンスに Amazon EBS ルートボリュームがあることを確認します。
- aws:executeScript - DestinationSecurityGroupId パラメータに指定した値に応じて、必要なときにセキュリティグループを作成します。
- aws:branch - DestinationSubnetId パラメータで指定された値に基づくブランチ。
- aws:executeAwsApi - このオートメーションを実行する AWS リージョン のデフォルトの VPC を識別します。
- aws:executeAwsApi - デフォルト VPC にあるサブネットの ID をランダムに選択します。
- aws:createImage - Amazon EC2 インスタンスを再起動せずに AMI を作成します。
- aws:branch - MigrationType パラメータで指定された値に基づくブランチ。
- aws:branch - DestinationSubnetId パラメータで指定された値に基づくブランチ。
- aws:runInstances - EC2-Classic で Amazon EC2 インスタンスを再起動せずに、作成された AMI から新しいインスタンスを起動します。
- aws:changeInstanceState - 前のステップが何らかの理由で失敗した場合、新しく起動した Amazon EC2 インスタンスを終了します。
- aws:runInstances - DestinationSubnetId の EC2-Classic で Amazon EC2 インスタンスが指定されている場合、それを再起動せずに、作成された AMI から新しいインスタンスを起動します。
- aws:changeInstanceState - 前のステップが何らかの理由で失敗した場合、新しく起動した Amazon EC2 インスタンスを終了します。
- aws:assertAwsResourceProperty - EC2-Classic で実行されている Amazon EC2 インスタンスの停止動作を確認します。

- aws:approve - Amazon EC2 インスタンスの停止承認を待機します。
- aws:changeInstanceState - EC2-Classic で実行されている Amazon EC2 インスタンスを停止します。
- aws:changeInstanceState - 必要な場合、EC2-Classic で実行されている Amazon EC2 インスタンスを強制停止します。
- aws:createImage - Amazon EC2 インスタンスが停止した後に、そのインスタンスの AMI を作成します。
- aws:branch - DestinationSubnetId パラメータで指定した値に基づいて分岐させます。
- aws:runInstances - EC2-Classic で停止済みの Amazon EC2 インスタンスについて、作成された AMI から新しいインスタンスを起動します。
- aws:approve - 何らかの理由で前のステップが失敗した場合、新しく起動したインスタンスを終了し、EC2-Classic で Amazon EC2 インスタンスを起動するまで承認を待ちます。
- aws:changeInstanceState - 新しく起動した Amazon EC2 インスタンスを終了します。
- aws:runInstances - DestinationSubnetId パラメータから EC2-Classic で停止した Amazon EC2 インスタンスについて、作成された AMI から新しいインスタンスを起動します。
- aws:approve - 何らかの理由で前のステップが失敗した場合、新しく起動したインスタンスを終了し、EC2-Classic で Amazon EC2 インスタンスを起動するまで承認を待ちます。
- aws:changeInstanceState - 新しく起動した Amazon EC2 インスタンスを終了します。
- aws:changeInstanceState - EC2-Classic で停止した Amazon EC2 インスタンスを起動します。
- aws:branch - Amazon EC2 インスタンスにパブリック IP アドレスがあるかどうかに基づいてブランチします。
- aws:executeAwsApi - パブリック IP アドレスが Elastic IP アドレスであるかどうかを確認します。
- aws:branch - MigrationType パラメータで指定された値に基づくブランチ。
- aws:executeAwsApi - Elastic IP アドレスをお客様の VPC に移動します。
- aws:executeAwsApi - VPC に移動された Elastic IP アドレスの割り当て ID を収集します。
- aws:branch - VPC で実行されている Amazon EC2 インスタンスが起動されたサブネットに基づくブランチ。
- aws:executeAwsApi - VPC で新しく起動したインスタンスに Elastic IP アドレスをアタッチします。

- aws:executeScript - VPC で実行されている新しく起動した Amazon EC2 インスタンスがパブリックであるサブネットを確認します。

出力

getInstanceProperties.virtualizationType - EC2-Classic で実行されている Amazon EC2 インスタンスの仮想化タイプ。

getInstanceProperties.rootDeviceType - EC2-Classic で実行されている Amazon EC2 インスタンスのルートデバイスタイプ。

createAMIWithoutReboot.ImageId - EC2-Classic で実行されている Amazon EC2 インスタンスを再起動せずに作成された AMI の ID。

getDefaultVPC.VpcId - DestinationSubnetId パラメータの値が指定されていない場合、新しい Amazon EC2 インスタンスが起動されるデフォルトの VPC の ID。

getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc - DestinationSubnetId パラメータの値が指定されていない場合、新しい Amazon EC2 インスタンスが起動されるデフォルトの VPC のサブネットの ID。

launchTestInstanceDefaultVPC.InstanceIds - Test 移行タイプ中にデフォルト VPC で新しく起動された Amazon EC2 インスタンスの ID。

launchTestInstanceProvidedSubnet.InstanceIds - Test 移行タイプ中に指定した DestinationSubnetId で新しく起動された Amazon EC2 インスタンスの ID。

createAMIAfterStoppingInstance.ImageId - EC2-Classic で実行されている Amazon EC2 インスタンスを停止した後に作成された AMI の ID。

launchCutOverInstanceProvidedSubnet.InstanceIds - CutOver 移行タイプ中に指定した DestinationSubnetId で新しく起動された Amazon EC2 インスタンスの ID。

launchCutOverInstanceDefaultVPC.InstanceIds - CutOver 移行タイプ中にデフォルト VPC で新しく起動された Amazon EC2 インスタンスの ID。

verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic - デフォルト VPC の自動化によって選択されたサブネットがパブリックであるかどうか。

verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic - DestinationSubnetId で指定したサブネットがパブリックかどうか。

AWSSupport-MigrateXenToNitroLinux

説明

AWSSupport-MigrateXenToNitroLinux ランブックでは、Amazon Elastic Compute Cloud (Amazon EC2) Linux Xen インスタンスをNitro インスタンスタイプにクローンし、準備し、移行します。このランブックには、オペレーションタイプに 2 つのオプションがあります。

- Clone&Migrate — このオプションのワークフローは、事前チェック、テスト、Clone&Migrateフェーズで構成されています。ワークフローは AWSSupport-CloneXenEC2InstanceAndMigrateToNitro ランブックを使用して実行されます。
- FullMigration — このオプションは Clone&Migrate ワークフローを実行してから、「ルート Amazon EBS ボリュームを置き換える」という追加ステップを実行します。

> **Important**
>
> このランブックを使用すると、Amazon EC2 インスタンスの実行時間、Amazon Elastic Block Store (Amazon EBS) ボリュームの作成および AMIs など、アカウントにコストが発生します。詳細については、「Amazon EC2 料金表」および「Amazon EBS 料金表」を参照してください。

事前チェック

自動化は、移行を続行する前に、以下の事前チェックを実行します。いずれかのチェックが失敗すると、自動化は終了します。このフェーズは Clone&Migrate ワークフローの一部にすぎません。

- ターゲットインスタンスが既に Nitro インスタンスタイプであるかどうかを確認します。
- ターゲットインスタンスにスポットインスタンス購入オプションが使用されたかどうかを確認します。
- インスタンスストアボリュームがターゲットインスタンスにアタッチされているかどうかを確認します。
- ターゲットインスタンスのオペレーティングシステム (OS) が Linux であることを確認します。
- ターゲットインスタンスが Amazon EC2 Auto Scaling グループの一部であるかどうかを確認します。Auto Scaling グループの一部である場合、自動化はインスタンスが standby 状態にあることを確認します。
- インスタンスが によって管理されていることを確認します AWS Systems Manager。

テスト

自動化はターゲットインスタンスから Amazon Machine Image (AMI) を作成し、新しく作成された AMI からテストインスタンスを起動します。このフェーズは Clone&Migrate ワークフローの一部にすぎません。

テストインスタンスがすべてのステータスチェックに合格すると、自動化は一時停止し、Amazon Simple Notification Service (Amazon SNS) 通知を通じて指定されたプリンシパルからの承認が要求されます。承認が得られた場合、自動化はテストインスタンスを終了し、ターゲットインスタンスを停止して移行を続行します。その間、新しく作成された AMI は Clone&Migrate ワークフローの最後で登録解除されます。

> **Note**
>
> 承認を行う前に、ターゲットインスタンスで実行中のすべてのアプリケーションが正常に閉じられていることを確認することをお勧めします。

クローニングと移行

自動化により、ターゲットインスタンスから別の AMI が作成され、新しいインスタンスが起動して Nitro インスタンスタイプに変更されます。自動化は、移行を続行する前に、以下の事前チェックを実行します。いずれかのチェックが失敗すると、自動化は終了します。このフェーズも Clone&Migrate ワークフローの一部にすぎません。

- 拡張ネットワーク (ENA) 属性を有効にします。
- ENA ドライバーがまだインストールされていない場合は最新バージョンをインストールし、ENA ドライバーのバージョンを最新バージョンに更新します。ネットワークパフォーマンスを最大化するには、Nitro インスタンスタイプが第 6 世代の場合は、最新の ENA ドライバーバージョンに更新する必要があります。
- NVMe モジュールがインストールされていることを確認します。モジュールがインストールされている場合、自動化はモジュールが initramfs にロードされたことを確認します。
- /etc/fstab を分析し、ブロックデバイス名 (/dev/sd* または /dev/xvd*) のエントリをそれぞれの UUID に置き換えます。設定を変更する前に、自動化はパス /etc/fstab* にあるファイルのバックアップを作成します。
- /etc/default/grub ファイル内に GRUB_CMDLINE_LINUX 行が存在する場合、その行に、または /boot/grub/menu.lst 内のカーネルに net.ifnames=0 オプションを追加することで、予測可能なインターフェイス命名を無効にします。

- /etc/udev/rules.d/70-persistent-net.rules ファイルが存在する場合、それを削除します。ファイルを削除する前に、自動化はパス /etc/udev/rules.d/ にあるファイルのバックアップを作成します。

すべての要件を確認した後、インスタンスタイプは、指定した Nitro インスタンスタイプに変更されます。自動化は、新しく作成されたインスタンスが Nitro インスタンスタイプとして起動した後、すべてのステータスチェックに合格するのを待ちます。その後、自動化は指定されたプリンシパルからの承認を待って、Nitro インスタンスが正常に起動された AMI を作成します。承認が拒否されると、自動化は終了し、新しく作成されたインスタンスは実行されたままになり、ターゲットインスタンスは停止したままになります。

Amazon EBS ボリュームの置き換え

OperationType として FullMigration を選択した場合、自動化はターゲット Amazon EC2 インスタンスを指定した Nitro インスタンスタイプに移行します。自動化は、ターゲット Amazon EC2 インスタンスのルート Amazon EBS ボリュームを、クローンされた Amazon EC2 インスタンスのルートボリュームに置き換える承認を、指定されたプリンシパルにリクエストします。移行が成功すると、クローンされた Amazon EC2 インスタンスは終了します。自動化が失敗した場合、元の Amazon EBS ルートボリュームがターゲット Amazon EC2 インスタンスにアタッチされます。ターゲット Amazon EC2 インスタンスにアタッチされたルート Amazon EBS ボリュームに、aws: プレフィックスが適用されたタグがある場合、FullMigration オペレーションはサポートされません。

[開始する前に]

ターゲットインスタンスには、アウトバウンドのインターネットアクセスが必要です。これは、ドライバーのリポジトリや kernel-devel、gcc、patch、rpm-build、wget、dracut、make、linux-headers、unzip などの依存関係にアクセスするためです。必要に応じて Package マネージャーを使用します。

承認と更新の通知を送信するには、Amazon SNS トピックが必要です。Amazon SNS トピックの作成の詳細については、Amazon Simple Notification Service デベロッパーガイドの「Amazon SNS トピックの作成」を参照してください。

このランブックでは、以下のオペレーティングシステムがサポートされています。

- RHEL 7.x ~ 8.5
- Amazon Linux (2018.03)、Amazon Linux 2
- Debian サーバー

- Ubuntu Server 18.04 LTS、20.04 LTS、20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5、SUSE15SP2)

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- 確認

  タイプ: 文字列

  説明: (必須) この自動化ランブックで実行されるアクションの完全な詳細を読み、「**Yes, I understand and acknowledge**」と入力してランブックの使用を続行してください。
- ApproverIAM

  タイプ: 文字列

  説明: (必須) 自動化を承認できる IAM ロール、ユーザー、またはユーザー名の ARN。最大 10 の承認者を指定できます。
- DeleteResourcesOnFailure

型: ブール値

説明: (オプション) 自動化が失敗した場合に、新しく作成されたインスタンスと移行用の AMI を削除するかどうかを決定します。

有効な値: True | False

デフォルト: True

- MinimumRequiredApprovals

  タイプ: 文字列

  説明: (オプション) 承認がリクエストされたときに、自動化を継続して実行するために必要な最小承認数。

  有効な値: 1 ~ 10

  デフォルト: 1

- NitroInstanceType

  タイプ: 文字列

  説明: (必須) インスタンスを変更したい Nitro インスタンスタイプ。サポートされているインスタンスタイプには、M5、M6、C5、C6、R5、R6、T3 があります。

  デフォルト: m5.xlarge

- OperationType

  タイプ: 文字列

  説明: (必須) 実行する操作。FullMigration オプションは Clone&Migrate と同じタスクを実行し、さらにターゲットインスタンスのルートボリュームを置き換えます。ターゲットインスタンスのルートボリュームは、移行プロセスの後に新しく作成されたインスタンスのルートボリュームに置き換えられます。FullMigration 操作は、ロジカルボリュームマネージャー (LVM) によって定義されたルートボリュームをサポートしていません。

  有効な値: Clone&Migrate | FullMigration

- SNSTopicArn

  タイプ: 文字列

説明: (必須) 承認通知の Amazon SNS トピックの ARN。Amazon SNS トピックは、自動化中に必要な承認通知を送信するために使用されます。

- TargetInstanceId

  タイプ: 文字列

  説明: (必須) 移行する Amazon EC2 インスタンスの ID。

Clone&Migrate のワークフロー

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- startOfPreliminaryChecksBranch - 予備チェックワークフローに分岐します。
- getTargetInstanceProperties - ターゲットインスタンスから詳細を収集します。
- checkIfNitroInstanceTypeIsSupportedInAZ - ターゲットの Amazon EC2 インスタンスタイプが、ターゲットインスタンスと同じアベイラビリティーゾーンでサポートされているかどうかを判断します。
- getXenInstanceTypeDetails - ソースインスタンスタイプの詳細を収集します。
- checkIfInstanceHypervisorIsNitroAlready - ターゲットインスタンスが既に Nitro インスタンスタイプとして実行されているかを確認します。
- checkIfTargetInstanceLifecycleIsSpot - ターゲットインスタンスの購入オプションがスポットかどうかをチェックします。
- checkIfOperatingSystemIsLinux - ターゲットインスタンス OS が Linux かどうかを確認します。
- verifySSMConnectivityForTargetInstance - ターゲットインスタンスが Systems Manager によって管理されていることを確認します。
- checkIfEphemeralVolumeAreSupported - ターゲットインスタンスの現在のインスタンスタイプがインスタンスストアボリュームをサポートしているかどうかを確認します。
- verifyIfTargetInstanceHasEphemeralVolumesAttached - ターゲットインスタンスがインスタンスストアボリュームにアタッチされているかどうかを確認します。
- checkIfRootVolumeIsEBS - ターゲットインスタンスのルートボリュームタイプが EBS かどうかを確認します。

- checkIfTargetInstanceIsInASG - ターゲットインスタンスが Auto Scaling グループの一部であるかどうかを確認します。
- endOfPreliminaryChecksBranch - 予備チェック分岐の終了。
- startOfTestBranch - テストワークフローへの分岐。
- createTestImage - ターゲットインスタンスのテスト AMI を作成します。
- launchTestInstanceInSameSubnet - ターゲットインスタンスと同じ設定を使用して、テスト AMI からテストインスタンスを起動します。
- cleanupTestInstance - テストインスタンスを終了します。
- endOfTestBranch - テスト分岐の終了。
- checkIfTestingBranchSucceeded - テスト分岐のステータスをチェックします。
- approvalToStopTargetInstance - 指定されたプリンシパルからの承認を待って、ターゲットインスタンスを停止します。
- stopTargetEC2Instance - ターゲットインスタンスを停止します。
- forceStopTargetEC2Instance - 前のステップでインスタンスを停止できなかった場合にのみ、ターゲットインスタンスを強制停止します。
- startOfCloneAndMigrateBranch - Clone&Migrate ワークフローへの分岐。
- createBackupImage - バックアップとして機能するターゲットインスタンスの AMI を作成します。
- launchInstanceInSameSubnet - ソースインスタンスと同じ設定を使用して、バックアップ AMI から新しいインスタンスを起動します。
- waitForClonedInstanceToPassStatusChecks - 新しく作成されたインスタンスがすべてのステータスチェックに合格するのを待ちます。
- verifySSMConnectivityForClonedInstance - 新しく作成されたインスタンスが Systems Manager によって管理されていることを確認します。
- checkAndInstallENADrivers - 新しく作成されたインスタンスに ENA ドライバーがインストールされているかどうかを確認し、必要に応じてドライバーをインストールします。
- checkAndAddNVMEDrivers - 新しく作成されたインスタンスに NVMe ドライバーがインストールされているかどうかを確認し、必要に応じてドライバーをインストールします。
- checkAndModifyFSTABEntries - /etc/fstab でデバイス名が使用されているかどうかを確認し、必要に応じて UUID に置き換えます。
- stopClonedInstance - 新しく作成されたインスタンスを停止します。

- forceStopClonedInstance - 前のステップでインスタンスを停止できなかった場合にのみ、新しく作成されたインスタンスを強制停止します。
- checkENAAttributeForClonedInstance - 新しく作成されたインスタンスの拡張ネットワーキング属性がオンになっているかどうかを確認します。
- setNitroInstanceTypeForClonedInstance - 新しく作成されたインスタンスのインスタンスタイプを、指定した Nitro インスタンスタイプに変更します。
- startClonedInstance - インスタンスタイプを変更した、新しく作成されたインスタンスを起動します。
- approvalForCreatingImageAfterDriversInstallation - インスタンスが Nitro インスタンスタイプとして正常に起動すると、自動化は必要なプリンシパルからの承認を待ちます。承認が与えられると、ゴールデン AMI として使用するための AMI が作成されます。
- createImageAfterDriversInstallation - ゴールデン AMI として使用される AMI を作成します。
- endOfCloneAndMigrateBranch - Clone&Migrate 分岐の終了。
- cleanupTestImage - テスト用に作成された AMI の登録を解除します。
- failureHandling - 障害発生時にリソースを終了するように選択したかどうかをチェックします。
- onFailureTerminateClonedInstance - 自動化に失敗した場合、新しく作成されたインスタンスを終了します。
- onFailurecleanupTestImage - テスト用に作成された AMI の登録を解除します。
- onFailureApprovalToStartTargetInstance - 自動化に失敗した場合、指定されたプリンシパルからの承認を待ってターゲットインスタンスを起動します。
- onFailureStartTargetInstance - 自動化が失敗した場合、ターゲットインスタンスを起動します。

FullMigration のワークフロー

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

FullMigration ワークフローは Clone&Migrate ワークフローと同じステップを実行し、さらに以下のステップを実行します。

- checkConcurrency - 指定した Amazon EC2 インスタンスをターゲットとするこのランブックの自動化が 1 つしかないことを確認します。同じインスタンスをターゲットとする別の自動化が進行中であることをランブックが検知した場合、その自動化は終了します。
- getTargetInstanceProperties - ターゲットインスタンスから詳細を収集します。
- checkRootVolumeTags - ターゲット Amazon EC2 インスタンスのルートボリュームに AWS 予約済みタグが含まれているかどうかを決定します。
- cloneTargetInstanceAndMigrateToNitro - AWS-CloneXenInstanceToNitro ランブックを使用して子自動化を開始します。
- branchOnTheOperationType - OperationType パラメータで指定した値に基づいて分岐させます。
- getClonedInstanceId - 新しく起動したインスタンスの ID を子自動化から取得します。
- checkIfRootVolumeIsBasedOnLVM - ルートパーティションが LVM によって管理されているかどうかを判断します。
- branchOnTheRootVolumeLVMStatus - プリンシパルから必要最小限の承認が得られると、自動化はルートボリュームの置き換えに進みます。
- manualInstructionsInCaseOfLVM - ルートボリュームが LVM によって管理されている場合、自動化はルートボリュームを手動で置き換える方法に関する指示を含む出力を送信します。
- startOfReplaceRootEBSVolumeBranch - ルート EBS ボリュームを置き換える分岐ワークフローを開始します。
- checkIfTargetInstanceIsManagedByCFN - ターゲットインスタンスが AWS CloudFormation スタックによって管理されているかどうかを決定します。
- branchOnCFNStackStatus - CloudFormation スタックのステータスに基づいて分岐させます。
- approvalForRootVolumesReplacement(WithCFN) - ターゲットインスタンスが CloudFormation によって起動された場合、自動化は、新しく起動されたインスタンスが Nitro インスタンスタイプとして正常に起動した後、承認を待ちます。承認が行われると、ターゲットインスタンスの Amazon EBS ボリュームは、新しく起動されたインスタンスのルートボリュームに置き換えられます。
- approvalForRootVolumesReplacement - 新しく起動したインスタンスが Nitro インスタンスタイプとして正常に起動した後、承認を待ちます。承認が行われると、ターゲットインスタンスの

Amazon EBS ボリュームは、新しく起動されたインスタンスのルートボリュームに置き換えられます。

- assertIfTargetEC2InstanceIsStillStopped - ルートボリュームを置き換える前に、ターゲットインスタンスが stopped の状態にあることを確認します。
- stopTargetInstanceForRootVolumeReplacement - ターゲットインスタンスが実行中の場合、自動化はルートボリュームを置き換える前にインスタンスを停止します。
- forceStopTargetInstanceForRootVolumeReplacement - 前のステップで失敗した場合、ターゲットインスタンスは強制停止されます。
- stopClonedInstanceForRootVolumeReplacement - Amazon EBS ボリュームを置き換える前に、新しく作成されたインスタンスを停止します。
- forceStopClonedInstanceForRootVolumeReplacement - 前のステップが失敗した場合、新しく作成されたインスタンスを強制停止します。
- getBlockDeviceMappings - ターゲットインスタンスと新しく作成されたインスタンスの両方のブロックデバイスマッピングを取得します。
- replaceRootEbsVolumes - ターゲットインスタンスのルートボリュームを、新しく作成されたインスタンスのルートボリュームに置き換えます。
- EndOfReplaceRootEBSVolumeBranch - ルート EBS ボリュームを置き換える分岐ワークフローの終了。
- checkENAAttributeForTargetInstance - ターゲット Amazon EC2 インスタンスの拡張ネットワーキング (ENA) 属性が有効になっているかどうかを確認します。
- enableENAAttributeForTargetInstance - 必要に応じて、ターゲット Amazon EC2 インスタンスの ENA 属性を有効にします。
- setNitroInstanceTypeForTargetInstance - ターゲットインスタンスを指定した Nitro インスタンスタイプに変更します。
- replicateRootVolumeTags - ターゲット Amazon EC2 インスタンスから、ルート Amazon EBS ボリュームのタグを複製します。
- startTargetInstance - インスタンスタイプを変更した後、ターゲット Amazon EC2 インスタンスを開始します。
- onFailureStopTargetEC2Instance - ターゲット Amazon EC2 インスタンスが Nitro インスタンスタイプとして起動できない場合、そのインスタンスを停止します。
- onFailureForceStopTargetEC2Instance - 前のステップで失敗した場合、Amazon EC2 インスタンスは強制停止されます。

- OnFailureRevertOriginalInstanceType - ターゲットインスタンスが Nitro インスタンスタイプとして起動できない場合、ターゲット Amazon EC2 インスタンスを元のインスタンスタイプに戻します。
- onFailureRollbackRootVolumeReplacement - 必要に応じて、replaceRootEbsVolumes ステップで行った変更をすべて元に戻します。
- onFailureApprovalToStartTargetInstance - 指定されたプリンシパルの承認を待って、以前の変更をロールバックした後、ターゲット Amazon EC2 インスタンスを起動します。
- onFailureStartTargetInstance - ターゲットの Amazon EC2 インスタンスを開始します。
- terminateClonedEC2Instance - ルート Amazon EBS ボリュームを置き換えた後、クローンされた Amazon EC2 インスタンスを終了します。

AWSSupport-ResetAccess

説明

このランブックは、指定された EC2 インスタンスの EC2Rescue ツールを使用しながら、EC2 コンソール (Windows) を通じたパスワードの復号を再度有効にするか、新しい SSH キーペア (Linux) を生成して追加します。キーペアを紛失した場合、この自動化により、ユーザーが所有するキーペア (Windows) で新しい EC2 インスタンスを起動するために使用できるパスワード対応の AMI が作成されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- EC2RescueInstanceType

  タイプ: 文字列

  有効な値: t2.small | t2.medium | t2.large

  デフォルト: t2.small

  説明: (必須) EC2Rescue インスタンスの EC2 インスタンスタイプ。推奨サイズ: t2.small。

- InstanceId

  タイプ: 文字列

  説明: (必須) アクセスをリセットする EC2 インスタンスの ID。

  > **Important**
  >
  > Systems Manager Automation はこのインスタンスを停止し、操作を試みる前に AMI を作成します。インスタンスストアボリュームに保存されているデータは失われます。Elastic IP を使用していない場合、パブリック IP アドレスが変わります。

- SubnetId

  タイプ: 文字列

  デフォルト: CreateNewVPC

  説明: (オプション) EC2Rescue インスタンスのサブネット ID。デフォルトでは、Systems Manager Automation が新しい VPC を作成します。または、SelectedInstanceSubnet を使用してインスタンスと同じサブネットを使用するか、カスタムサブネット ID を指定します。

  > **Important**
  >
  > サブネットは InstanceId と同じアベイラビリティーゾーンである必要があり、SSM エンドポイントへのアクセスを許可する必要があります。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

このオートメーションの出力を読み取るには少なくとも、[ssm:StartAutomationExecution]、[ssm:GetParameter] (SSH キーパラメータ名を取得するため) と、[ssm:GetAutomationExecution] が必要です。必要な許可の詳細については、「AWSSupport-StartEC2RescueWorkflow」を参照してください。

ドキュメントステップ

1. aws:assertAwsResourceProperty - 指定されたインスタンスが Windows の場合にアサートします。
   a. (Windows 用の EC2Rescue) 提供されたインスタンスが Windows の場合:
      i. aws:executeAutomation - Windows 用の EC2Rescue オフラインパスワードリセットスクリプトを使用して AWSSupport-StartEC2RescueWorkflow を呼び出します。
      ii. aws:executeAwsApi - ネスト化された自動化からバックアップ AMI ID を取得します
      iii. aws:executeAwsApi - ネスト化された自動化からパスワード対応 AMI ID を取得します
      iv. aws:executeAwsApi - ネスト化された自動化から EC2Rescue の要約を取得します
   b. (Linux 用の EC2Rescue) 提供されたインスタンスが Linux の場合:
      i. aws:executeAutomation - Linux 用の EC2Rescue オフライン SSH キーインジェクションスクリプトを使用して AWSSupport-StartEC2RescueWorkflow を呼び出します
      ii. aws:executeAwsApi - ネスト化された自動化からバックアップ AMI ID を取得します
      iii. aws:executeAwsApi - 挿入された SSH キーの SSM パラメータ名を取得します
      iv. aws:executeAwsApi - ネスト化された自動化から EC2Rescue の要約を取得します

出力

getEC2RescueForWindowsResult.Output

getWindowsBackupAmi.ImageId

getWindowsPasswordEnabledAmi.ImageId

getEC2RescueForLinuxResult.Output

getLinuxBackupAmi.ImageId

getLinuxSSHKeyParameter.Name

AWSSupport-ResetLinuxUserPassword

説明

AWSSupport-ResetLinuxUserPassword ランブックは、ローカルオペレーティングシステム (OS) ユーザーのパスワードをリセットするのに役立ちます。このランブックは、シリアルコンソールを使用して Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアクセスする必要があるユーザーに特に役立ちます。ランブックは、 に一時的な Amazon EC2 インスタンス AWS アカウント を作成し、パスワードを含む AWS Secrets Manager シークレット値を取得するアクセス許可を持つ AWS Identity and Access Management (IAM) ロールを作成します。

ランブックは、ターゲットの Amazon EC2 インスタンスを停止し、ルート Amazon Elastic Block Store (Amazon EBS) ボリュームをデタッチし、一時の Amazon EC2 インスタンスにアタッチします。Run Command を使用すると、一時インスタンス上でスクリプトが実行され、指定した OS ユーザーのパスワードが設定されます。次に、ルート Amazon EBS ボリュームがターゲットインスタンスに再アタッチされます。ランブックには、自動化の開始時にルートボリュームのスナップショットを作成するオプションも用意されています。

[開始する前に]

OS ユーザーに割り当てるパスワードの値を使用して Secrets Manager シークレットを作成します。値はプレーンテキストである必要があります。詳細については、AWS Secrets Manager ユーザーガイドの「Create an AWS Secrets Manager secret」を参照してください。

考慮事項

- このランブックを使用する前にインスタンスをバックアップすることをおすすめします。CreateSnapshot パラメータの値を **Yes** として設定することを検討してください。
- ローカルユーザーパスワードを変更すると、ランブックでインスタンスを停止する必要があります。インスタンスが停止すると、メモリまたはインスタンスストアボリュームに保存されているすべてのデータは失われます。また、自動的に割り当てられたパブリック IPv4 アドレスはすべて解放されます。インスタンスを停止するとどうなるかの詳細については、Amazon EC2 ユーザーガイド」の「インスタンスの停止と起動」を参照してください。
- ターゲットの Amazon EC2 インスタンスにアタッチされた Amazon EBS ボリュームがカスタマーマネージド AWS Key Management Service （ AWS KMS) キーで暗号化されている場合は、 AWS KMS キーが deletedまたは でないか、インスタンスの起動に失敗disabledします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: 文字列

  説明: (必須) リセットする OS ユーザーパスワードを含む Amazon EC2 Linux インスタンスの ID。
- LinuxUserName

  タイプ: 文字列

  デフォルト: ec2-ユーザー

  説明: (オプション) パスワードをリセットする OS ユーザーアカウント。
- SecretArn

  タイプ: 文字列

  説明: (必須) 新しいパスワードを含む Secrets Manager シークレットのARN。

- SecurityGroupId

  タイプ: 文字列

  説明: (オプション) Amazon EC2 一時インスタンスにアタッチするセキュリティグループの ID。このパラメータに値を指定しない場合は、デフォルトの Amazon Virtual Private Cloud (Amazon VPC) セキュリティグループが使用されます。

- SubnetId

  タイプ: 文字列

  説明: (オプション) Amazon EC2 一時インスタンスを起動するサブネットの ID。デフォルトでは、自動化はターゲットインスタンスと同じサブネットを選択します。別のサブネットを指定する場合は、そのサブネットはターゲットインスタンスと同じアベイラビリティーゾーンに存在し、Systems Manager エンドポイントにアクセスできる必要があります。

- CreateSnapshot

  タイプ: 文字列

  有効な値: はい | いいえ

  デフォルト: Yes

  説明: (オプション) オートメーションを実行する前に、ターゲット Amazon EC2 インスタンスのルートボリュームのスナップショットを作成するかどうかを決定します。

- StopConsent

  タイプ: 文字列

  有効な値: はい | いいえ

  デフォルト: いいえ

  説明: **Yes** を入力して、この自動化の間にターゲット Amazon EC2 インスタンスが停止することを確認します。Amazon EC2 インスタンスが停止すると、メモリまたはインスタンスストアボリュームに保存されているデータはすべて失われ、自動パブリック IPv4 アドレスは解放されます。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの停止と起動」を参照してください。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

1. aws:branch — ターゲットの Amazon EC2 インスタンスの停止に同意したかどうかに基づいて分岐します。
2. aws:assertAwsResourceProperty – Amazon EC2 インスタンスのステータスが runningまたは stopped状態であることを確認します。それ以外の場合、自動化は終了します。
3. aws:executeAwsApi – Amazon EC2 インスタンスのプロパティを取得します。
4. aws:executeAwsApi – ルートボリュームのプロパティを取得します。
5. aws:branch – 一時的な Amazon EC2 インスタンスのサブネット ID が提供されたかどうかに応じて、オートメーションを分岐させます。
6. aws:assertAwsResourceProperty – SubnetIdパラメータで指定したサブネットが、ターゲット Amazon EC2 インスタンスと同じアベイラビリティーゾーンにあることを確認します。
7. aws:assertAwsResourceProperty– ターゲット Amazon EC2 インスタンスのルートボリュームが Amazon EBS ボリュームであることを確認します。
8. aws:assertAwsResourceProperty – Amazon EC2 インスタンスアーキテクチャが arm64または であることを確認しますx86_64。
9. aws:assertAwsResourceProperty – Amazon EC2 インスタンスのシャットダウン動作がstopであり、 ではないことを確認しますterminate。
10. aws:branch – Amazon EC2 インスタンスがスポットインスタンスではないことを確認します。それ以外の場合、自動化は終了します。
11. aws:executeScript – Amazon EC2 インスタンスが Auto Scaling グループの一部ではないことを確認します。インスタンスが Auto Scaling グループの一部である場合、自動化は Amazon EC2 インスタンスが Standby ライフサイクル状態にあることを確認します。
12. aws:createStack – 指定した OS ユーザーのパスワードをリセットするために使用される一時的な Amazon EC2 インスタンスを作成します。

13. aws:waitForAwsResourceProperty – 新しく起動された一時的な Amazon EC2 インスタンスが実行されるまで待ちます。
14. aws:executeAwsApi – 一時的な Amazon EC2 インスタンスの ID を取得します。
15. aws:waitForAwsResourceProperty – 一時的な Amazon EC2 インスタンスが Systems Manager によって管理されているとレポートするのを待ちます。
16. aws:changeInstanceState– ターゲット Amazon EC2 インスタンスを停止します。
17. aws:changeInstanceState – ターゲット Amazon EC2 インスタンスが停止状態でスタックした場合に備えて、インスタンスを強制的に停止します。
18. aws:branch – ターゲット Amazon EC2 インスタンスのルートボリュームのスナップショットがリクエストされたかどうかに応じて、オートメーションを分岐させます。
19. aws:executeAwsApi – ターゲット Amazon EC2 インスタンスのルート Amazon EBS ボリュームのスナップショットを作成します。
20. aws:waitForAwsResourceProperty – スナップショットが completed状態になるまで待機します。
21. aws:executeAwsApi – ターゲット Amazon EC2 インスタンスから Amazon EBS ルートボリュームをデタッチします。
22. aws:waitForAwsResourceProperty – Amazon EBS ルートボリュームがターゲット Amazon EC2 インスタンスからデタッチされるのを待ちます。
23. aws:executeAwsApi – ルート Amazon EBS ボリュームを一時的な Amazon EC2 インスタンスにアタッチします。
24. aws:waitForAwsResourceProperty – Amazon EBS ルートボリュームが一時的な Amazon EC2 インスタンスにアタッチされるのを待ちます。
25. aws:runCommand – 一時的な Amazon EC2 インスタンスで Run Command を使用してシェルスクリプトを実行して、ターゲットユーザーのパスワードをリセットします。
26. aws:executeAwsApi – 一時的な Amazon EC2 インスタンスから Amazon EBS ルートボリュームをデタッチします。
27. aws:waitForAwsResourceProperty – Amazon EBS ルートボリュームが一時的な Amazon EC2 インスタンスからデタッチされるのを待ちます。
28. aws:executeAwsApi – エラー後に、一時的な Amazon EC2 インスタンスから Amazon EBS ルートボリュームをデタッチします。
29. aws:waitForAwsResourceProperty – エラー後に Amazon EBS ルートボリュームが一時的な Amazon EC2 インスタンスからデタッチされるのを待ちます。

30aws:branch – エラーが発生した場合に復旧パスを決定するためにルートボリュームのスナップショットがリクエストされたかどうかに応じて、自動化を分岐させます。

31aws:executeAwsApi – ルート Amazon EBS ボリュームをターゲット Amazon EC2 インスタンスに再アタッチします。

32aws:waitForAwsResourceProperty – Amazon EBS ルートボリュームが Amazon EC2 インスタンスにアタッチされるのを待ちます。

33aws:executeAwsApi – ターゲット Amazon EC2 インスタンスのルートボリュームスナップショットから新しい Amazon EBS ボリュームを作成します。

34aws:waitForAwsResourceProperty – 新しい Amazon EBS ボリュームが available状態になるまで待ちます。

35aws:executeAwsApi – 新しい Amazon EBS ボリュームをルートボリュームとしてターゲットインスタンスにアタッチします。

36aws:waitForAwsResourceProperty – Amazon EBS ボリュームが attached状態になるまで待ちます。

37aws:executeAwsApi – ランブックが AWS CloudFormation スタックの作成または更新に失敗した場合の AWS CloudFormation スタックイベントについて説明します。

38aws:branch – 以前の Amazon EC2 インスタンスの状態に応じてオートメーションを分岐させます。状態が running の場合、インスタンスは起動されます。stopped 状態であった場合、自動化は続行されます。

39aws:changeInstanceState – 必要に応じて Amazon EC2 インスタンスを起動します。

40aws:waitForAwsResourceProperty – AWS CloudFormation スタックがターミナルステータスになるまで待ってから削除します。

41aws:executeAwsApi – 一時的な Amazon EC2 インスタンスを含む AWS CloudFormation スタックを削除します。

AWSPremiumSupport-ResizeNitroInstance

説明

AWSPremiumSupport-ResizeNitroInstance ランブックは、Nitro System 上に構築された Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのサイズを変更するための自動化ソリューションを提供します。

データ損失やダウンタイムの潜在的なリスクを軽減するために、ランブックでは以下を検証しています。

- インスタンス停止動作。
- インスタンスが Amazon EC2 Auto Scaling グループの一部であり、かつ standby モードに入っている場合。
- インスタンスの状態とテナンシー。
- 変更したいインスタンスタイプは、インスタンスに現在アタッチされているネットワークインターフェースの数をサポートします。
- 現在のインスタンスタイプとターゲットインスタンスタイプのプロセッサアーキテクチャと仮想化タイプは同じです。
- インスタンスが実行中であれば、すべてのステータスチェックに合格しているということです。
- 変更するインスタンスタイプは、同一のアベイラビリティーゾーンで使用できます。

インスタンスタイプを変更した後に Amazon EC2 がステータスチェックに合格しなかった場合、ランブックは自動的に前のインスタンスタイプにロールバックします。

デフォルトでは、このランブックが実行中でインスタンスストアボリュームがアタッチされている場合、インスタンスタイプは変更されません。インスタンスが AWS CloudFormation スタックの一部である場合、ランブックはインスタンスタイプを変更しません。これらの動作のいずれかを変更する場合は、AllowInstanceStoreInstances および AllowCloudFormationInstances パラメータに yes を指定してください。

ランブックには、変更先のインスタンスタイプを指定する方法が 2 つ用意されています。

- 1 つのインスタンスを対象とする単純な自動化では、TargetInstanceTypeFromParameter パラメータを使用して変更するインスタンスタイプを指定します。
- 自動化を大規模に実行して複数のインスタンスのインスタンスタイプを変更する場合は、TargetInstanceTypeFromTagValue パラメータを使用してインスタンスタイプを指定します。自動化の実行については、「自動化を大規模に実行」を参照してください。

どちらのパラメータにも値を指定しないと、自動化は失敗します。

> **Important**
>
> AWSPremiumSupport-* ランブックにアクセスするには、エンタープライズサポートまたはビジネスサポートサブスクリプションが必要です。詳細については、「Compare サポート Plans」を参照してください。

考慮事項

- このランブックを使用する前にインスタンスをバックアップすることをおすすめします。
- インスタンスタイプを変更する際の互換性については、「インスタンスタイプ変更の互換性」を参照してください。
- 自動化が失敗して元のインスタンスタイプにロールバックする場合は、「インスタンスタイプを変更する場合のトラブルシューティング」を参照してください。
- インスタンスタイプを変更すると、ランブックでインスタンスを停止する必要があります。インスタンスが停止すると、メモリまたはインスタンスストアボリュームに保存されているすべてのデータは失われます。また、自動的に割り当てられたパブリック IPv4 アドレスはすべて解放されます。インスタンスを停止するとどうなるかについては、「インスタンスの停止と開始」を参照してください。
- `SkipInstancesWithTagKey` パラメータを使用すると、特定の Amazon EC2 タグキーが適用されているインスタンスをスキップできます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- 了解

  タイプ: 文字列

  説明: (必須) 現在実行中のインスタンスが停止することを確認するには **yes** を入力してください。

- AllowInstanceStoreInstances

  タイプ: 文字列

  有効な値: no | yes

  デフォルト: いいえ

  説明: (オプション) yes を指定すると、インスタンスストアボリュームがアタッチされているインスタンスでランブックを実行できるようになります。

- AllowCloudFormationInstances

  タイプ: 文字列

  有効な値: no | yes

  デフォルト: いいえ

  説明: (オプション) を指定した場合yes、ランブックは AWS CloudFormation スタックの一部であるインスタンスで実行されます。

- DryRun

  タイプ: 文字列

  有効な値: no | yes

  デフォルト: いいえ

  説明: (オプション) yes を指定すると、ランブックはインスタンスタイプを変更せずにサイズ変更要件を検証します。

- InstanceId

  タイプ: 文字列

  説明: (必須) タイプを変更する Amazon EC2 インスタンスの ID。

- SkipInstancesWithTagKey

タイプ: 文字列

説明: (オプション) 指定したタグキーがインスタンスに適用されている場合、自動化はターゲットインスタンスをスキップします。

- SleepTime

  タイプ: 文字列

  デフォルト: 3

  説明: (オプション) 完了後、このランブックがスリープ状態になる秒数。

- TagInstance

  タイプ: 文字列

  説明: (オプション)*#Key=ChangingType,Value=True#*の形式を使用して、インスタンスに任意のキーと値をタグ付けします。このオプションにより、このランブックのターゲットとなったインスタンスを追跡できます。タグのキーと値では、大文字と小文字が区別されます。

- TargetInstanceTypeFromParameter

  タイプ: 文字列

  説明: (オプション) 変更したいインスタンスのタイプ。`TargetInstanceTypeFromTagValue` パラメータに指定されたタグキーの値を使用する場合は、このパラメータを空のままにしてください。

- TargetInstanceTypeFromTagValue

  タイプ: 文字列

  説明: (オプション) 変更したいインスタンスタイプが値に含まれているターゲットインスタンスに適用されるタグキー。この `TargetInstanceTypeFromParameter` パラメータ値を指定すると、このパラメータに指定した任意の値はオーバーライドされます。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `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

ドキュメントステップ

1. aws:assertAwsResourceProperty: Amazon EC2 インスタンスが、SkipInstancesWithTagKeyパラメータで指定されたリソースタグキーでタグ付けされていないことを確認します。タグキーがインスタンスに適用されていることが判明した場合、ステップは失敗し、自動化は終了します。
2. aws:assertAwsResourceProperty: ターゲット Amazon EC2 インスタンスのステータスがrunning、pending、stopped または stopping であることを確認します。それ以外の場合、自動化は終了します。
3. aws:executeAwsApi: Amazon EC2 インスタンスからプロパティを収集します。
4. aws:executeAwsApi: 現在の Amazon EC2 インスタンスタイプに関する詳細を収集します。
5. aws:branch: 現在のインスタンスタイプと TargetInstanceTypeFromParameter パラメータで指定されたインスタンスタイプが同じかどうかを確認します。一致する場合、自動化は終了します。
6. aws:assertAwsResourceProperty: インスタンスが Nitro System で実行されていることを確認します。
7. aws:branch: Amazon EC2 インスタンスのルートボリュームタイプが、Amazon Elastic Block Store (Amazon EBS) ボリュームであることを確認します。
8. aws:assertAwsResourceProperty: インスタンスのシャットダウン動作が stop であり、terminateではないことを確認します。

9. aws:branch: Amazon EC2 インスタンスがスポットインスタンスではないことを確認します。
10. aws:branch: Amazon EC2 インスタンスのテナンシーがデフォルトであり、専有ホストや専有インスタンスではないことを確認します。
11. aws:executeScript: 現在のインスタンス ID をターゲットとするこのランブックの自動化が 1 つしかないことを確認します。同じインスタンスをターゲットとする別の自動化がすでに進行中の場合、その自動化はエラーを返して終了します。
12. aws:branch: Amazon EC2 インスタンスの状態に基づいて自動化を分岐します。
    a. stopped または stopping の場合、Amazon EC2 インスタンスが完全に停止するまで自動化が aws:waitForAwsResourceProperty を実行します。
    b. running または pending の場合、Amazon EC2 インスタンスがステータスチェックに合格するまで自動化が aws:waitForAwsResourceProperty を実行します。
13. aws:assertAwsResourceProperty: DescribeAutoScalingInstances API オペレーションを呼び出して、Amazon EC2 インスタンスが Auto Scaling グループの一部ではないことを確認します。インスタンスが Auto Scaling グループの一部である場合、Amazon EC2 インスタンスは standby モードに入っています。
14. aws:branch: Amazon EC2 インスタンスが AWS CloudFormation スタックの一部であるかどうかをオートメーションで確認するかどうかに応じて、オートメーションを分岐させます。
    a. aws:executeScript DescribeStackResources API オペレーションを呼び出して、Amazon EC2 インスタンスが AWS CloudFormation スタックの一部ではないことを確認します。
15. aws:executeAwsApi: プロセッサアーキテクチャタイプ、仮想化タイプが同じで、ターゲットインスタンスに現在アタッチされているネットワークインターフェイスの数をサポートするインスタンスタイプのリストを返します。
16. aws:executeAwsApi: TargetInstanceTypeFromTagValue パラメータで指定されたタグキーからターゲットインスタンスタイプ値を取得します。
17. aws:executeScript: 現在のインスタンスタイプとターゲットインスタンスタイプに互換性があることを確認します。ターゲットインスタンスタイプが同じサブネットで利用可能であることを確認します。ランブックを起動したプリンシパルに、インスタンスタイプを変更する権限があり、実行中の場合はインスタンスを停止して起動する権限があることを確認します。
18. aws:branch: DryRun パラメータ値が yes に設定されているかどうかに基づいて自動化を分岐させます。yes の場合、自動化は終了します。
19. aws:branch: 元のインスタンスタイプとターゲットインスタンスタイプが同じかどうかを確認します。一致する場合、自動化は終了します。
20. aws:executeAwsApi: 現在のインスタンスの状態を取得します。

21. aws:changeInstanceState: Amazon EC2 インスタンスを停止します。
22. aws:changeInstanceState: インスタンスが stopping の状態で動かなくなった場合、強制的に停止します。
23. aws:executeAwsApi: インスタンスタイプをターゲットインスタンスタイプに変更します。
24. aws:sleep: インスタンスタイプを変更した後、最終的に一貫性が保たれるまで 3 秒間待ちます。
25. aws:branch: 前のインスタンスの状態に基づいて自動化を分岐します。running であった場合、インスタンスが起動されます。
    a. aws:changeInstanceState: インスタンスタイプを変更する前に Amazon EC2 インスタンスが起動していた場合、Amazon EC2 インスタンスを起動します。
    b. aws:waitForAwsResourceProperty: Amazon EC2 インスタンスがステータスチェックに合格するのを待ちます。インスタンスがステータスチェックに合格しない場合、インスタンスは元のインスタンスタイプに戻されます。
        i. aws:changeInstanceState: Amazon EC2 インスタンスを停止してから、元のインスタンスタイプに変更します。
        ii. aws:changeInstanceState: Amazon EC2 インスタンスが停止状態で停止した場合に、元のインスタンスタイプに変更する前に強制的に Amazon EC2 インスタンスを停止します。
        iii. aws:executeAwsApi: Amazon EC2 インスタンスを元のタイプに変更します。
        iv. aws:sleep: インスタンスタイプを変更した後、最終的に一貫性が保たれるまで 3 秒間待ちます。
        v. aws:changeInstanceState: インスタンスタイプを変更する前に Amazon EC2 インスタンスが起動していた場合、Amazon EC2 インスタンスを起動します。
        vi. aws:waitForAwsResourceProperty: Amazon EC2 インスタンスがステータスチェックに合格するのを待ちます。
26. aws:sleep: ランブックを終了するまで待ちます。

AWSSupport-RestoreEC2InstanceFromSnapshot

説明

AWSSupport-RestoreEC2InstanceFromSnapshot ランブックは、ルートボリュームの動作中の Amazon Elastic Block Store (Amazon EBS) のスナップショットから Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを識別して復元するのに役立ちます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- EndDate

  タイプ: 文字列

  説明: (オプション) 自動化にスナップショットを検索する最後の日付。
- InplaceSwap

  型: ブール値

  有効な値: true | false

  説明: (オプション) このパラメータの値が `true` に設定されている場合、スナップショットから新しく作成されたボリュームが、インスタンスにアタッチされている既存のルートボリュームと置き換わります。
- InstanceId

  タイプ: 文字列

説明: (必須) スナップショットから復元するインスタンスの ID。

- LookForInstanceStatusCheck

  型: ブール値

  有効な値: true | false

  デフォルト: true

  説明: (オプション) このパラメータの値が `true` に設定されている場合、自動化はスナップショットから起動されたテストインスタンスでインスタンスステータスチェックが失敗するかどうかをチェックします。

- SkipSnapshotsBy

  タイプ: 文字列

  説明: (オプション) インスタンスを復元するためにスナップショットを検索する時にスナップショットがスキップされる間隔。たとえば、使用可能なスナップショットが 100 個あり、このパラメータに 2 を指定すると、3 つおきのスナップショットがレビューされます。

  デフォルト: 0

- SnapshotId

  タイプ: 文字列

  説明: (オプション) インスタンスを復元するスナップショットの ID。

- StartDate

  タイプ: 文字列

  説明: (オプション) 自動化にスナップショットを検索する最初の日付。

- TotalSnapshotsToLook

  タイプ: 文字列

  説明: (オプション) 自動化でレビューするスナップショットの数。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

1. aws:executeAwsApi - ターゲットインスタンスの詳細を収集します。
2. aws:assertAwsResourceProperty - ターゲットインスタンスが存在することを確認します。
3. aws:assertAwsResourceProperty - ルートボリュームが Amazon EBS ボリュームであることを確認します。
4. aws:assertAwsResourceProperty - このインスタンスをターゲットとする別の自動化がまだ実行されていないことを確認します。

5. aws:executeAwsApi - ターゲットインスタンスにタグを付けます。
6. aws:executeAwsApi - インスタンスの AMI を作成します。
7. aws:executeAwsApi - 前のステップで作成した AMI に関する詳細を収集します。
8. aws:waitForAwsResourceProperty - AMI の状態が available になるのを待ってから処理を進めます。
9. aws:executeScript - 新しく作成された AMI から新しいインスタンスを起動します。
10. aws:assertAwsResourceProperty - インスタンスの状態が available であることを確認します。
11. aws:executeAwsApi - 新しく起動したインスタンスの詳細を収集します。
12. aws:branch - SnapshotId パラメータに値を指定したかどうかに応じて分岐します。
13. aws:executeScript - 指定した期間内のスナップショットのリストを返します。
14. aws:executeAwsApi - インスタンスを停止します。
15. aws:waitForAwsResourceProperty - ボリュームの状態が available になるまで待機します。
16. aws:waitForAwsResourceProperty - インスタンスの状態が stopped になるまで待機します。
17. aws:executeAwsApi - ルートボリュームをデタッチします。
18. aws:waitForAwsResourceProperty - ルートボリュームがデタッチされるまで待機します。
19. aws:executeAwsApi - 新しいルートボリュームをアタッチします。
20. aws:waitForAwsResourceProperty - 新しいボリュームがアタッチされるまで待機します。
21. aws:executeAwsApi - インスタンスを起動します。
22. aws:waitForAwsResourceProperty - インスタンスの状態が available になるまで待機します。
23. aws:waitForAwsResourceProperty - システムおよびインスタンスのステータスチェックがインスタンスに合格するまで待機します。
24. aws:executeScript - スクリプトを実行して、ボリュームを正常に作成するために使用できるスナップショットを検出します。
25. aws:executeScript - 自動化によって識別されたスナップショットから新しく作成されたボリューム、または SnapshotId パラメータで指定したスナップショットから作成されたボリュームを使用して、インスタンスを復元するスクリプトを実行します。
26. aws:executeScript - この自動化によって作成されたリソースを削除します。

出力

launchCloneInstance.InstanceIds

ListSnapshotByDate.finalSnapshots

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.workingSnapshot

InstanceRecovery.result

AWSSupport-SendLogBundleToS3Bucket

説明

AWSSupport-SendLogBundleToS3Bucket ランブックは、EC2Rescue ツールによって生成されたログバンドルを、ターゲットインスタンスから指定された S3 バケットにアップロードします。このランブックは、EC2Rescue のプラットフォーム固有のバージョンを、ターゲットインスタンスのプラットフォームに対応してインストールします。EC2Rescue を使用して、使用可能なすべてのオペレーティングシステム (OS) ログを収集します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) ログを収集する Windows または Linux のマネージドインスタンスの ID。

- S3BucketName

  タイプ: 文字列

  説明: (必須) ログをアップロードする S3 バケット。

- S3Path

  タイプ: 文字列

  デフォルト: `AWSSupport-SendLogBundleToS3Bucket/`

  説明: (オプション) 収集されたログの S3 パス。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

このコマンドを受信する EC2 インスタンスには、[AmazonSSMManagedInstanceCore] Amazon 管理ポリシーがアタッチされた IAM ロールがあることが推奨されます。このオートメーションを実行してコマンドをインスタンスに送信するには、少なくとも ssm:StartAutomationExecution と ssm:SendCommand が必要です。さらに、オートメーションから出力を読み取るには、ssm:GetAutomationExecution が必要です。

ドキュメントステップ

1. `aws:runCommand` - `AWS-ConfigureAWSPackage` 経由で EC2Rescue をインストールします。
2. `aws:runCommand` - PowerShell スクリプトを実行し、EC2Rescue で Windows トラブルシューティングログを収集します。

3. aws:runCommand - bash スクリプトを実行し、EC2Rescue で Linux トラブルシューティングログを収集します。

出力

collectAndUploadWindowsLogBundle.Output

collectAndUploadLinuxLogBundle.Output

AWSSupport-StartEC2RescueWorkflow

説明

AWSSupport-StartEC2RescueWorkflow ランブックは、指定された base64 エンコードのスクリプト (Bash または Powershell) を、インスタンスをレスキューするために作成されたヘルパーインスタンス上で実行します。インスタンスのルートボリュームは、EC2Rescue インスタンスとも呼ばれるヘルパーインスタンスにアタッチおよびマウントされます。インスタンスが Windows の場合、Powershell スクリプトを指定します。それ以外の場合は、Bash を使用します。このランブックでは、スクリプトで使用するための、いくつかの環境変数が設定されます。環境変数には、入力した入力情報とオフラインルートボリュームに関する情報が含まれています。オフラインボリュームはすでにマウントされており、すぐに使用できます。たとえば、Desired State Configuration ファイルをオフラインの Windows ルートボリュームに保存するか、または chroot をオフラインの Linux ルートボリュームに保存して、オフライン修復を実行することができます。

このオートメーションを実行する (コンソール)

> **Important**
>
> Marketplace Amazon マシンイメージ (AMI) から作成された Amazon EC2 インスタンスは、このオートメーションではサポートされていません。

追加情報

Powershell または Bash を使用し、スクリプトを Base64 にエンコードにすることができます。Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

Bash:

```
base64 PATH_TO_FILE
```

以下に示しているのは、ターゲットの OS に応じて、オフラインスクリプトで使用できる環境変数のリストです

Windows:

可変	説明	値の例
$env:EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
$env:EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
$env:EC2RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
$env:EC2RESCUE_EC2RW_DIR	Windows インストールパスの EC2Rescue	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EC2RW_DIR	Windows インストールパスの EC2Rescue	C:\Program Files\Amazon\EC2Rescue
$env:EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
$env:EC2RESCUE_OFFLINE_CURRENT_CONTROL_SET	オフラインの Windows Current Control Set のパス	`HKLM:\AWSTempSystem\ControlSet001`
$env:EC2RESCUE_OFFLINE_DRIVE	オフラインの Windows ドライブ文字	D:\
$env:EC2RESCUE_OFFLINE_EBS_DEVICE	オフラインのルートボリューム EBS デバイス	xvdf
$env:EC2RESCUE_OFFLINE_KERNEL_VER	オフラインの Windows カーネルバージョン	6.1.7601.24214

可変	説明	値の例
$env:EC2RESCUE_OFFLINE_OS_ARCHITECTURE	オフラインの Windows アーキテクチャ	AMD64
$env:EC2RESCUE_OFFLINE_OS_CAPTION	オフラインの Windows キャプション	Windows Server 2008 R2 Datacenter
$env:EC2RESCUE_OFFLINE_OS_TYPE	オフラインの Windows OS タイプ	[Server] (サーバー)
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR	オフラインの Windows Program files のディレクトリパス	D:\Program Files
$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	オフラインの Windows Program files (x86) のディレクトリパス	D:\Program Files (x86)
$env:EC2RESCUE_OFFLINE_REGISTRY_DIR	オフラインの Windows レジストリのディレクトリパス	D:\Windows\System32\config
$env:EC2RESCUE_OFFLINE_SYSTEM_ROOT	オフラインの Windows システムのルートディレクトリパス	D:\Windows
$env:EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
$env:EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	amzn-s3-demo-bucket
$env:EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
$env:EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
$script:EC2RESCUE_OFFLINE_WINDOWS_INSTALL	オフラインの Windows インストールメタデータ	Customer Powershell Object

Linux:

可変	説明	値の例
EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
EC2RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_EC2RL_DIR	Linux インストールパスの EC2Rescue	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTIO N_ID	{{ automation:EXECUTI ON_ID }}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_ DEVICE	オフラインのデバイス名	/dev/xvdf1
EC2RESCUE_OFFLINE_ EBS_DEVICE	オフラインのルートボリューム EBS デバイス	/dev/sdf
EC2RESCUE_OFFLINE_ SYSTEM_ROOT	オフラインのルートボリュームのマウントポイント	/mnt/mount
EC2RESCUE_PYTHON	Python バージョン	python2.7
EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	amzn-s3-demo-bucket
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_I NSTANCE	{{ InstanceId }}	i-abcdefgh123456789

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AMIPrefix

  タイプ: 文字列

  デフォルト: `AWSSupport-EC2Rescue`

  説明: (オプション) バックアップ AMI 名のプレフィックス。

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- CreatePostEC2RescueBackup

  タイプ: 文字列

  有効な値: true | false

  デフォルト: false

  説明: (オプション) スクリプトを開始する前に、`true` に設定して、InstanceId の AMI を作成します。AMI は、自動化が完了した後も維持されます。AMI へのアクセスを保護したり、削除したりするのはサービス利用者の責任となります。

- CreatePreEC2RescueBackup

  タイプ: 文字列

  有効な値: true | false

  デフォルト: false

説明: (オプション) スクリプトを実行する前に、`true` に設定して InstanceId の AMI を作成します。AMI は、自動化が完了した後も維持されます。AMI へのアクセスを保護したり、削除したりするのはサービス利用者の責任となります。

- EC2RescueInstanceType

  タイプ: 文字列

  有効な値: t2.small | t2.medium | t2.large | t3.small | t3.medium | t3.large | i3.large

  デフォルト: t3.medium

  説明: (オプション) EC2Rescue インスタンスの EC2 インスタンスタイプ。

- InstanceId

  タイプ: 文字列

  説明: (必須) EC2 インスタンスの ID。重要： AWS Systems Manager Automation はこのインスタンスを停止します。インスタンスストアボリュームに保存されているデータは失われます。Elastic IP を使用していない場合、パブリック IP アドレスが変わります。

- OfflineScript

  タイプ: 文字列

  説明: (必須) ヘルパーインスタンスに対して実行する Base64 エンコードのスクリプト。ソースインスタンスが Linux の場合は Bash を使用し、Linux の場合は PowerShell を使用します。

- S3BucketName

  タイプ: 文字列

  説明: (オプション) トラブルシューティングのログをアップロードするアカウントの S3 バケット名。収集されたログにアクセスする必要がないユーザーへの不必要な読み取り/書き込みアクセス権限をバケットポリシーに付与しないようにします。

- S3Prefix

  タイプ: 文字列

  デフォルト: `AWSSupport-EC2Rescue`

  説明: (オプション) S3 ログのプレフィックス。

- SubnetId

  タイプ: 文字列

  デフォルト: SelectedInstanceSubnet

  説明: (オプション) EC2Rescue インスタンスのサブネット ID。デフォルトでは、指定されたインスタンスが存在しているのと同じサブネットが使用されます。重要: カスタムサブネットを指定する場合は、InstanceId と同じアベイラビリティーゾーンに存在し、SSM エンドポイントへのアクセスを許可する必要があります。

- UniqueId

  タイプ: 文字列

  デフォルト: {{ automation:EXECUTION_ID }}

  説明: (オプション) オートメーションの一意の識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

オートメーションを実行するユーザーには [AmazonSSMAutomationRole] IAM 管理ポリシーがアタッチされていることが推奨されます。そのポリシー以外にも、ユーザーには次のものが必要です。

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

ドキュメントステップ

1. aws:executeAwsApi - 提供されたインスタンスを記述します
2. aws:executeAwsApi - 提供されたインスタンスのルートボリュームを記述します
3. aws:assertAwsResourceProperty - ルートボリュームのデバイスタイプが EBS であることを確認します
4. aws:assertAwsResourceProperty - ルートボリュームが暗号化されていないことを確認します
5. aws:assertAwsResourceProperty - 指定するサブネット ID を確認します
   a. (現在のインスタンスサブネットを使用) - *SubnetId = SelectedInstanceSubnet * の場合、aws:createStack を実行して EC2Rescue CloudFormation スタックをデプロイします
   b. (新しい VPC を作成する) - *SubnetId = CreateNewVPC* の場合、aws:createStack を実行して EC2Rescue CloudFormation スタックをデプロイします
   c. (カスタムサブネットの使用) - それ以外の場合:

      aws:assertAwsResourceProperty - 指定されたサブネットが、指定されたインスタンスと同じアベイラビリティーゾーンにあることを確認します

      aws:createStack - EC2Rescue CloudFormation スタックをデプロイします
6. aws:invokeLambdaFunction - 追加入力の検証を実行します
7. aws:executeAwsApi - EC2Rescue CloudFormation スタックを更新し EC2Rescue ヘルパーインスタンスを作成します

8. aws:waitForAwsResourceProperty - EC2Rescue CloudFormation スタックの更新が完了するまで待ちます
9. aws:executeAwsApi - EC2Rescue ヘルパーインスタンス ID を取得するための EC2Rescue CloudFormation スタック出力を表示します
10. aws:waitForAwsResourceProperty - EC2Rescue ヘルパーインスタンスがマネージドインスタンスになるのを待ちます
11. aws:changeInstanceState - 指定されたインスタンスを停止します
12. aws:changeInstanceState - 指定されたインスタンスを停止します
13. aws:changeInstanceState - 指定されたインスタンスを強制停止します
14. aws:assertAwsResourceProperty - CreatePreEC2RescueBackup の入力値を確認します
    a. (pre-EC2Rescue バックアップの作成) - *CreatePreEC2RescueBackup = true* の場合
    b. aws:executeAwsApi - 指定されたインスタンスの AMI バックアップを作成します
    c. aws:createTags - AMI バックアップにタグを付けます
15. aws:runCommand - EC2Rescue ヘルパーインスタンスに EC2Rescue をインストールします
16. aws:executeAwsApi - 指定されたインスタンスからルートボリュームをデタッチします
17. aws:assertAwsResourceProperty - 指定されたインスタンスのプラットフォームを確認します
    a. (インスタンスが Windows の場合):

       aws:executeAwsApi - EC2Rescue ヘルパーインスタンスにルートボリュームを *xvdf* としてアタッチします

       aws:sleep - 10 秒間スリープします

       aws:runCommand - Powershell で提供されるオフラインスクリプトを実行します
    b. (インスタンスが Linux の場合):

       aws:executeAwsApi - EC2Rescue ヘルパーインスタンスにルートボリュームを */dev/sdf* としてアタッチします

       aws:sleep - 10 秒間スリープします

       aws:runCommand - Bash で提供されるオフラインスクリプトを実行します
18. aws:changeInstanceState - EC2Rescue ヘルパーインスタンスを停止します
19. aws:changeInstanceState - EC2Rescue ヘルパーインスタンスを強制停止します

20. aws:executeAwsApi - EC2Rescue ヘルパーインスタンスからルートボリュームをデタッチします
21. aws:executeAwsApi - 指定されたインスタンスへ戻りルートボリュームをアタッチします
22. aws:assertAwsResourceProperty - CreatePostEC2RescueBackup の入力値を確認します
    a. (post-EC2Rescue バックアップの作成) - *CreatePostEC2RescueBackup = true* の場合
    b. aws:executeAwsApi - 指定されたインスタンスの AMI バックアップを作成します
    c. aws:createTags - AMI バックアップにタグを付けます
23. aws:executeAwsApi - 提供されたインスタンスのルートボリュームの終了状態での最初の削除を復元します
24. aws:changeInstanceState - 指定されたインスタンスの初期状態を復元します (実行中/停止中)
25. aws:deleteStack - EC2Rescue CloudFormation スタックを削除します

出力

runScriptForLinux.Output

runScriptForWindows.Output

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSPremiumSupport-TroubleshootEC2DiskUsage

説明

AWSPremiumSupport-TroubleshootEC2DiskUsage ランブックは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのルートディスクおよび非ルートディスクの使用状況に関する問題を調査し、潜在的に修正するのに役立ちます。可能であれば、ランブックはボリュームとそのファイルシステムを拡張して問題の修復を試みます。これらのタスクを実行するために、このランブックは、影響を受けるインスタンスのオペレーティングシステムに基づいて、複数のランブックの実行をオーケストレーションします。

最初のランブックである AWSPremiumSupport-DiagnoseDiskUsageOnWindows または AWSPremiumSupport-DiagnoseDiskUsageOnLinux は、ボリュームを拡張することでディスクの問題を軽減できるかどうかを決定します。

2 番目のランブック、AWSPremiumSupport-ExtendVolumesOnWindows または AWSPremiumSupport-ExtendVolumesOnLinux は、最初のランブックの出力を使用して、ボリュームを変更する Python コードを実行します。ボリュームが変更されると、ランブックは影響を受けるボリュームのパーティションとファイルシステムを拡張します。

> **Important**
>
> AWSPremiumSupport-* ランブックにアクセスするには、エンタープライズサポートまたはビジネスサポートサブスクリプションが必要です。詳細については、「AWS サポート プランの比較」を参照してください。

このドキュメントは AWS Managed Services 、 (AMS) と共同で構築されました。AMS は、 AWS インフラストラクチャをより効率的かつ安全に管理するのに役立ちます。また、運用上の柔軟性、セキュリティとコンプライアンスの強化、容量の最適化、コストを削減できる分野の特定も行います。詳細については、「AWS Managed Services」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、Windows

パラメータ

- InstanceId

  タイプ: 文字列

  許可される値: ^i-[a-z0-9]{8,17}$

  説明: (必須) Amazon EC2 インスタンスの ID。

- VolumeExpansionEnabled

  型: ブール値

  説明:(オプション) 影響を受けるボリュームとパーティションを拡張するかどうかを制御するフラグ。

  デフォルト: true

- VolumeExpansionUsageTrigger

  タイプ: 文字列

  説明: (オプション) 拡張をトリガーするために必要なパーティション領域の最小使用量 (パーセント)。

  許可される値: ^[0-9]{1,2}$

  デフォルト: 85

- VolumeExpansionCapSize

  タイプ: 文字列

  説明: (オプション) Amazon Elastic Block Store (Amazon EBS) ボリュームが増加する最大サイズ (GiB 単位)。

  許可される値: ^[0-9]{1,4}$

  デフォルト: 2048

- VolumeExpansionGibIncrease

  タイプ: 文字列

  説明: (オプション) ボリュームの増加量 (GiB 単位)。VolumeExpansionGibIncrease と VolumeExpansionPercentageIncrease の間の最大の純増加量が使用されます。

  許可される値: ^[0-9]{1,4}$

  デフォルト: 20

- VolumeExpansionPercentageIncrease

  タイプ: 文字列

説明: (オプション) ボリュームの増加量 (%)。VolumeExpansionGibIncrease と VolumeExpansionPercentageIncrease の間の最大の純増加量が使用されます。

許可される値: ^[0-9]{1,2}$

デフォルト: 20

- AutomationAssumeRole

タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

1. aws:assertAwsResourceProperty - インスタンスが Systems Manager によって管理されているかを確認します
2. aws:executeAwsApi - プラットフォームを取得するためのインスタンスを説明します。
3. aws:branch - インスタンスのプラットフォームに基づいて自動化を分岐させます。
   a. インスタンスが Windows の場合:
      i. aws:executeAutomation - AWSPremiumSupport-DiagnoseDiskUsageOnWindows ランブックを実行して、インスタンスでのディスク使用量の問題を診断します。
      ii. aws:executeAwsApi - 前の自動化の出力を取得します。
      iii. aws:branch - 診断の出力に基づいて分岐し、アラートを軽減するために拡張できるボリュームがあるかどうかを確認します。
         A. 拡張する必要のあるボリュームがありません: 自動化を終了します
         B. 拡張する必要がある以下のボリュームがあります。
            I. aws:executeAwsApi - インスタンスの Amazon Machine Image (AMI) を作成します。
            II. aws:waitForAwsResourceProperty - AMI の状態が available になるのを待ちます。
            III. aws:executeAutomation - AWSPremiumSupport-ExtendVolumesOnWindows ランブックを実行して、ボリュームの変更と、新しい領域を使用できるようにするために OS で必要な手順を実行します。
   b. (プラットフォームは Windows ではない) 入力インスタンスが Windows でない場合:
      i. aws:executeAutomation - AWSPremiumSupport-DiagnoseDiskUsageOnLinux ランブックを実行して、インスタンスでのディスク使用量の問題を診断します。
      ii. aws:executeAwsApi - 前の自動化の出力を取得します。
      iii. aws:branch - 診断の出力に基づいて分岐し、アラートを軽減するために拡張できるボリュームがあるかどうかを確認します。
         A. 拡張する必要のあるボリュームがありません: 自動化を終了します
         B. 拡張する必要がある以下のボリュームがあります。

I. `aws:executeAwsApi` - インスタンスの AMI を作成します。

II. `aws:waitForAwsResourceProperty` - AMI の状態が `available` になるのを待ちます。

III. `aws:executeAutomation` - `AWSPremiumSupport-ExtendVolumesOnLinux` ランブックを実行して、ボリュームの変更と、新しい領域を使用できるようにするために OS で必要な手順を実行します。

出力

diagnoseDiskUsageAlertOnWindows.Output

extendVolumesOnWindows.Output

diagnoseDiskUsageAlertOnLinux.Output

extendVolumesOnLinux.Output

BackupAMILinux.ImageId

BackupAMIWindows.ImageId

AWSSupport-TroubleshootEC2InstanceConnect

説明

`AWSSupport-TroubleshootEC2InstanceConnect` オートメーションは、Amazon EC2 Instance Connect を使用して Amazon Elastic Compute Cloud (Amazon EC2) インスタンスへの接続を妨げるエラーを分析および検出するのに役立ちます。サポートされていない Amazon マシンイメージ (AMI)、OS レベルのパッケージのインストールまたは設定の欠落、 (IAM) アクセス許可の欠落 AWS Identity and Access Management 、またはネットワーク設定の問題によって引き起こされる問題を特定します。

動作の仕組み

ランブックは、Amazon EC2 Instance Connect で問題が発生している IAM ロールまたはユーザーの Amazon EC2 インスタンス ID、ユーザー名、接続モード、ソース IP CIDR、SSH ポート、および Amazon リソースネーム (ARN) を取得します。次に、Amazon EC2 Instance Connect を使用して Amazon EC2 インスタンスに接続するための前提条件を確認します。

- インスタンスは実行中で、正常な状態です。

- インスタンスは、Amazon EC2 Instance Connect でサポートされている AWS リージョンにあります。
- インスタンスの AMI は Amazon EC2 Instance Connect でサポートされています。
- インスタンスは、インスタンスメタデータサービス (IMDSv2) に到達できます。
- Amazon EC2 Instance Connect パッケージは、OS レベルで適切にインストールおよび設定されています。
- ネットワーク設定 (セキュリティグループ、ネットワーク ACL、ルートテーブルルール) により、Amazon EC2 Instance Connect 経由でインスタンスに接続できます。
- Amazon EC2 Instance Connect の活用に使用される IAM ロールまたはユーザーは、Amazon EC2 インスタンスにキーをプッシュするアクセス権を持ちます。

Important

- インスタンス AMI、IMDSv2 到達可能性、および Amazon EC2 Instance Connect パッケージのインストールを確認するには、インスタンスが SSM マネージドである必要があります。それ以外の場合、これらのステップはスキップされます。詳細については、Amazon EC2 インスタンスがマネージドノードとして表示されない理由」を参照してください。
- ネットワークチェックでは、SourceIpCIDR が入力パラメータとして指定されている場合に、セキュリティグループとネットワーク ACL ルールがトラフィックをブロックする場合にのみ検出されます。それ以外の場合は、SSH 関連のルールのみが表示されます。
- Amazon EC2 Instance Connect Endpoint を使用した接続は、このランブックでは検証されません。
- プライベート接続の場合、オートメーションは SSH クライアントがソースマシンにインストールされているかどうか、およびインスタンスのプライベート IP アドレスに到達できるかどうかをチェックしません。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ec2:DescribeInstances
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeInternetGateways
- iam:SimulatePrincipalPolicy
- ssm:DescribeInstanceInformation
- ssm:ListCommands
- ssm:ListCommandInvocations
- ssm:SendCommand

指示

次の手順に従って自動化を設定します。

1. AWS Systems Manager コンソールAWSSupport-TroubleshootEC2InstanceConnectで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - InstanceId (必須):

     Amazon EC2 Instance Connect を使用して接続できなかったターゲット Amazon EC2 インスタンスの ID。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする IAM ロールの ARN。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。

- ユーザー名 (必須):

  Amazon EC2 Instance Connect を使用して Amazon EC2 インスタンスに接続するために使用されるユーザー名。この特定のユーザーに IAM アクセスが付与されているかどうかを評価するために使用されます。

- EC2InstanceConnectRoleOrUser (必須):

  Amazon EC2 Instance Connect を活用してキーをインスタンスにプッシュする IAM ロールまたはユーザーの ARN。

- SSHPort (オプション):

  Amazon EC2 インスタンスに設定されている SSH ポート。デフォルト値は 22 です。ポート番号は の間にする必要があります1-65535。

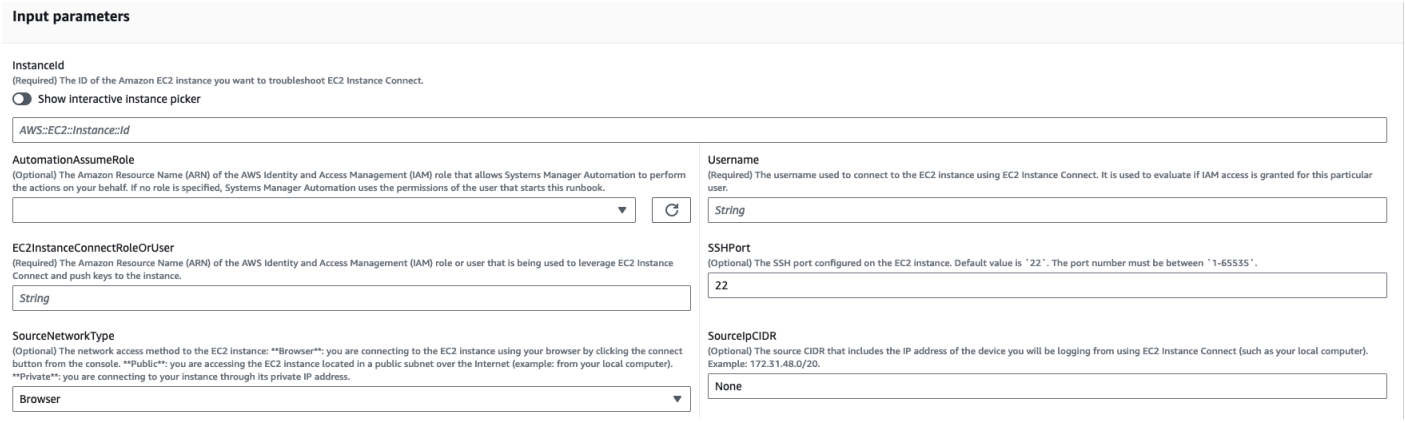
- SourceNetworkType (オプション):

  Amazon EC2 インスタンスへのネットワークアクセス方法：

  - ブラウザ： AWS マネジメントコンソールから接続します。
  - パブリック： インターネット経由でパブリックサブネットにあるインスタンスに接続します (ローカルコンピュータなど)。
  - プライベート： インスタンスのプライベート IP アドレスを介して接続します。

- SourceIpCIDR (オプション):

  Amazon EC2 Instance Connect を使用してログに記録するデバイス (ローカルコンピュータなど) の IP アドレスを含むソース CIDR。例: 172.31.48.6/32。パブリックアクセスモードまたはプライベートアクセスモードで値が指定されていない場合、ランブックは Amazon EC2 インスタンスセキュリティグループとネットワーク ACL ルールが SSH トラフィックを許可しているかどうかを評価しません。代わりに SSH 関連のルールが表示されます。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。

- AssertInitialState:

  Amazon EC2 インスタンスのステータスが実行されていることを確認します。それ以外の場合、自動化は終了します。

- GetInstanceProperties:

  現在の Amazon EC2 インスタンスプロパティ (PlatformDetails、PublicIpAddress、VpcId、SubnetId、MetadataHttpEndpoint) を取得します。

- GatherInstanceInformationFromSSM:

  インスタンスが SSM 管理の場合は、Systems Manager インスタンスの ping ステータスとオペレーティングシステムの詳細を取得します。

- CheckIfAWSRegionSupported

  Amazon EC2 インスタンスが Amazon EC2 Instance Connect でサポートされている AWS リージョンにあるかどうかを確認します。

- BranchOnIfAWSRegionSupported:

  AWS リージョンが Amazon EC2 Instance Connect でサポートされている場合は、実行を続行します。それ以外の場合は、出力が作成され、オートメーションを終了します。

- CheckIfInstanceAMIIsSupported

  インスタンスに関連付けられた AMI が Amazon EC2 Instance Connect でサポートされているかどうかを確認します。

- BranchOnIfInstanceAMIIsSupported

  インスタンス AMI がサポートされている場合、メタデータの到達可能性や Amazon EC2 Instance Connect パッケージのインストールや設定など、OS レベルのチェックが実行されます。それ以外の場合は、API を使用して AWS HTTP メタデータが有効になっているかどうかを確認し、ネットワークチェックステップに進みます。

- CheckIMDSReachabilityFromOs:

  ターゲット Amazon EC2 Linux インスタンスで Bash スクリプトを実行して、IMDSv2 に到達できるかどうかを確認します。

- CheckEICPackageInstallation:

  ターゲット Amazon EC2 Linux インスタンスで Bash スクリプトを実行して、Amazon EC2 Instance Connect パッケージが正しくインストールおよび設定されているかどうかを確認します。

- CheckSSHConfigFromOs:

  ターゲット Amazon EC2 Linux インスタンスで Bash スクリプトを実行して、設定された SSH ポートが入力パラメータSSHPort.`

- CheckMetadataHTTPEndpointIsEnabled:

  インスタンスメタデータサービスの HTTP エンドポイントが有効になっているかどうかを確認します。

- CheckEICNetworkAccess:

  ネットワーク設定 (セキュリティグループ、ネットワーク ACL、ルートテーブルルール) で Amazon EC2 Instance Connect を介したインスタンスへの接続が許可されているかどうかを確認します。

- CheckIAMRoleOrUserPermissions:

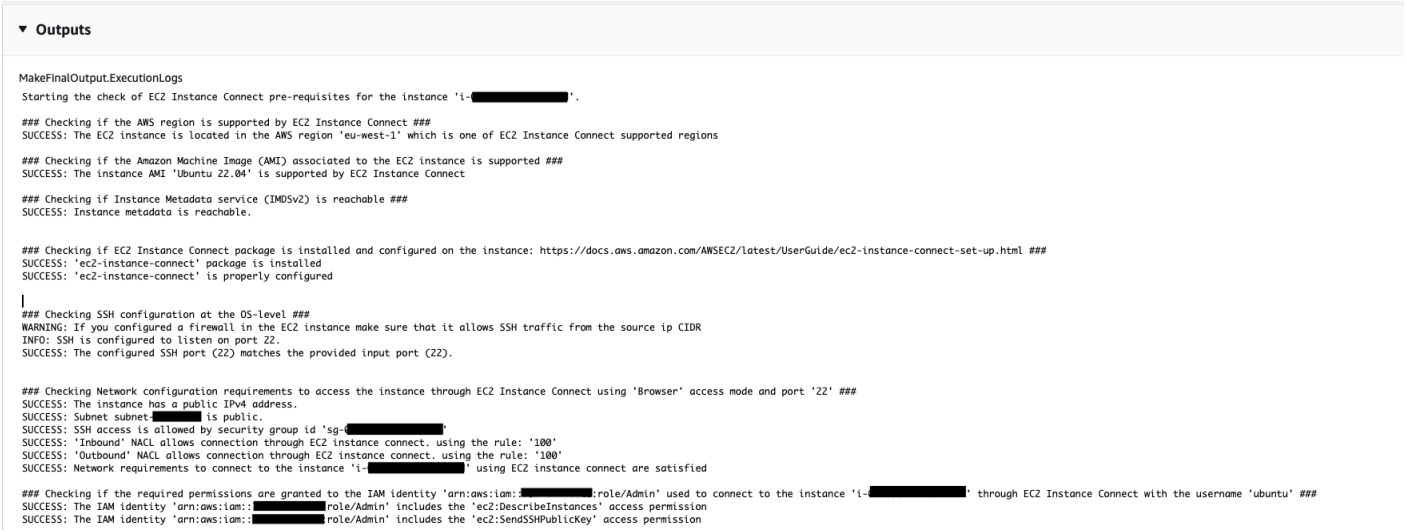
  Amazon EC2 Instance Connect の活用に使用した IAM ロールまたはユーザーが、指定されたユーザー名を使用して Amazon EC2 インスタンスにキーをプッシュするアクセス権を持っているかどうかを確認します。

- MakeFinalOutput:

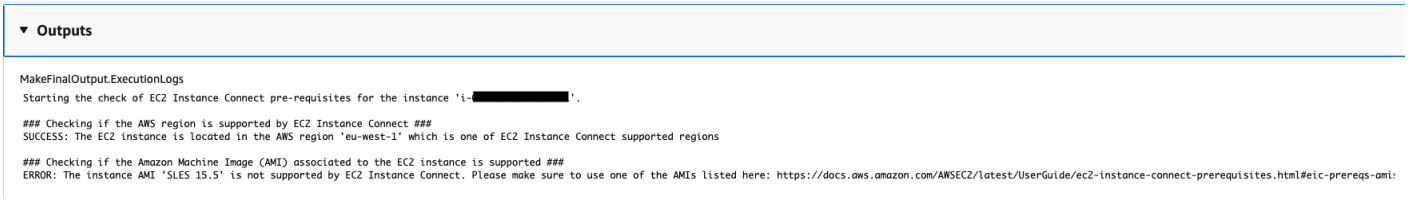
  前のすべてのステップの出力を統合します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

   ターゲットインスタンスに必要なすべての前提条件がある実行：



ターゲットインスタンスの AMI がサポートされていない実行：



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスドキュメント

- Amazon EC2 Instance Connect を使用した Amazon EC2 インスタンスへの接続に関する問題のトラブルシューティング方法を教えてください。

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

説明

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs オートメーションランブックは、Linux サーバーに AWS Application Migration Service（AWS MGN) および AWS Elastic Disaster Recovery（AWS DRS) レプリケーションエージェントをインストールしてソースサーバーを AWS クラウドに移行するときに一般的なエラーを検出するために使用されます。

動作の仕組み

ランブックAWSSupport-TroubleshootLinuxMGNDRSAgentLogsは、MGN または AWS DRS インストールログaws_replication_agent_installer.logがパラメータとしてアップロードされる Amazon Simple Storage Service (Amazon S3) AWS パスを取得します。次に、次のタスクを実行します。

- 検証： 提供されたログファイルが有効で、少なくとも 1 つのエージェントインストールが含まれているかどうかを確認します。
- 解析： ログファイルにインストールされた最新のエージェントを、既知の MGN AWS または AWS DRS エラーがないか完全に解析します。
- エラーの検出と解決： 解析に基づいて、エージェントのインストールプロセス中にエラーや問題を検出して一覧表示します。ランブックには、検出されたエラーごとに、問題の解決または軽減に役立つ詳細な手順が記載されています。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- s3:GetObject
- s3:ListBucket

指示

次の手順に従って自動化を設定します。

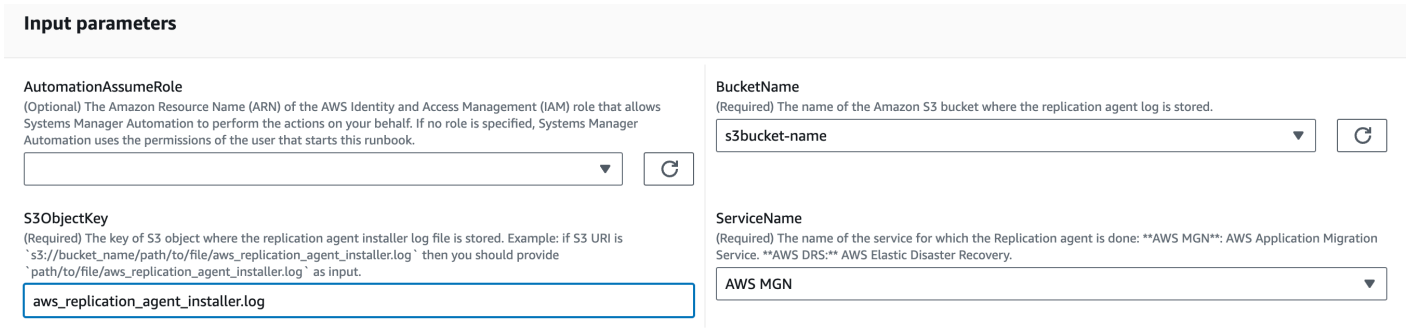
1. ドキュメントの Systems Manager AWSSupport-TroubleshootLinuxMGNDRSAgentLogsで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - BucketName (必須):

     レプリケーションエージェントログが保存されている Amazon S3 バケットの名前。
   - S3ObjectKey (必須):

     レプリケーションエージェントのインストーラログファイルが保存されている Amazon S3 オブジェクトのキー。例: Amazon S3 URI が の場合はs3://bucket_name/path/to/file/aws_replication_agent_installer.log、 と入力する必要がありますpath/to/file/aws_replication_agent_installer.log。
   - ServiceName (必須):

     レプリケーションエージェントがインストールされているサービスの名前。使用できる値: AWS MGN または AWS DRS

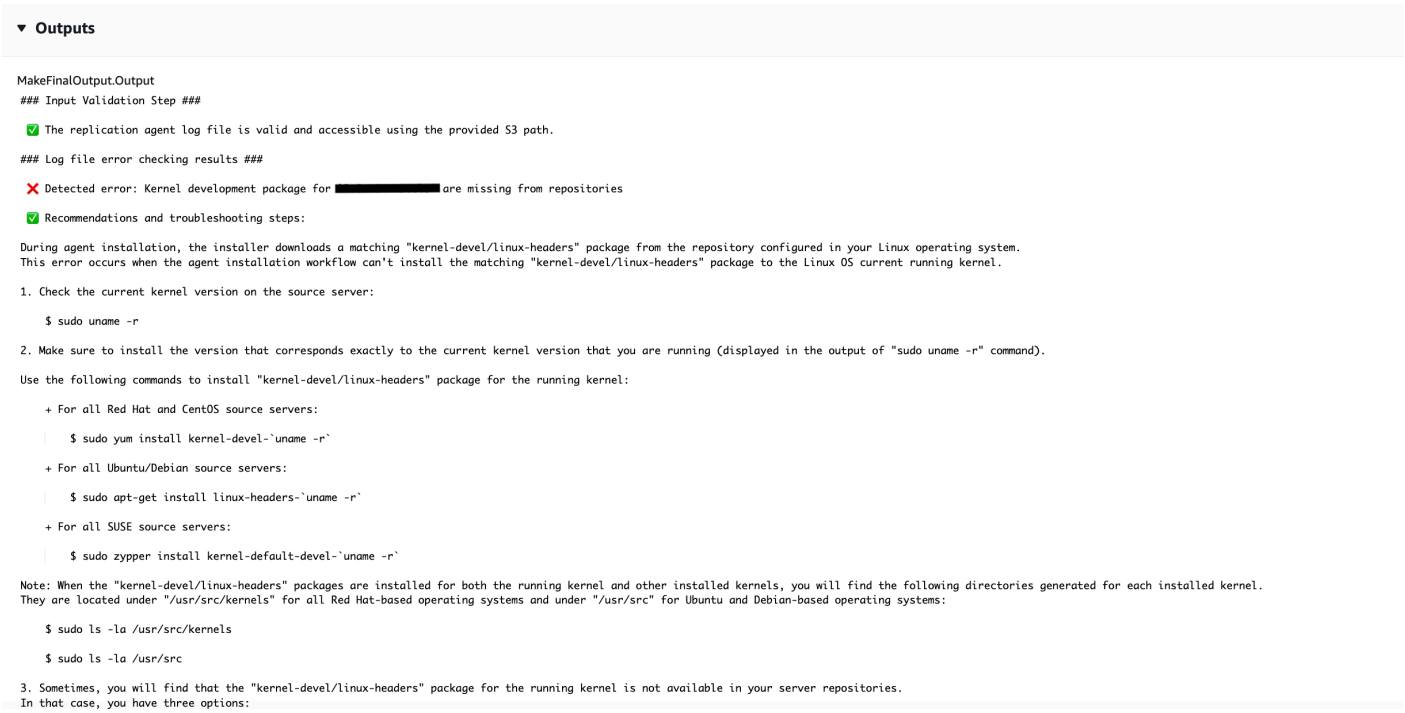


4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - **`ValidateInput`**

     指定された Amazon S3 バケット名とオブジェクトへのパスを使用して、レプリケーションエージェントのログファイルが有効でアクセス可能であることを確認し、最新のエージェントインストールのバイト番号を返します。
   - **`CheckReplicationAgentLogErrors`**

     最新のインストールバイトからレプリケーションエージェントのログファイルを読み取り、既知の AWS MGN または AWS DRS エラーを検索します。
   - **`MakeFinalOutput`**

     見つかったエラーに関する情報やトラブルシューティングの推奨事項など、前のチェックからの出力を作成します。
7. 完了したら、出力セクションで実行の詳細な結果を確認します。



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWSSupport-TroubleshootRDP

説明

AWSSupport-TroubleshootRDP ランブックを使用すると、ターゲットインスタンスの一般設定の中でリモートデスクトッププロトコル (RDP) 接続に影響する可能性があるもの (RDP ポート、ネットワークレイヤー認証 (NLA)、Windows ファイアウォールプロファイルなど) を、確認または変更できるようになります。オプションで、ユーザーがオフラインの修復を明示的に許可している場合は、インスタンスを停止して起動することで、オフラインで変更を適用できます。デフォルトでは、このランブックは読み取った設定の値を出力します。

> **Important**
>
> RDP 設定、RDP サービス、および Windows ファイアウォールのプロファイルへの変更内容は、このランブックを実行する前に慎重に確認しておく必要があります。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

- アクション

  タイプ: 文字列

  有効な値: CheckAll | FixAll | Custom

  デフォルト: Custom

  説明: (オプション) [カスタム] ファイアウォール、RDPServiceStartupType、RDPServiceAction、RDPPortAction、NLASettingAction、および RemoteConnections の値を使用して設定を管理します。[CheckAll] 設定の値を変更せずに読み取ります。[FixAll] RDP のデフォルト設定を復元し、Windows ファイアウォールを無効にします。

- AllowOffline

  タイプ: 文字列

  有効な値: true | false

  デフォルト: false

説明: (オプション) 修正のみ - オンラインのトラブルシューティングが失敗した場合、または提供されたインスタンスがマネージドインスタンスではない場合に、オフラインで RDP の修復を許可する場合は true に設定します。注: オフライン修復の場合、SSM Automation はインスタンスを停止し、操作を試みる前に AMI を作成します。

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ファイアウォール

  タイプ: 文字列

  有効な値: Check | Disable

  デフォルト: Check

  説明: (オプション) Windows のファイアウォール (すべてのプロファイル) を確認または無効にします。

- InstanceId

  タイプ: 文字列

  説明: (必須) RDP 設定のトラブルシューティングを行うインスタンスの ID。

- NLASettingAction

  タイプ: 文字列

  有効な値: Check | Disable

  デフォルト: Check

  説明: (オプション) ネットワークレイヤー認証 (NLA) を確認または無効にします。

- RDPPortAction

  タイプ: 文字列

有効な値: Check | Modify

デフォルト: Check

説明: (オプション) RDP 接続に使用されている現在のポートを確認するか、または RDP ポートを 3389 に変更してサービスを再起動します。

- RDPServiceAction

  タイプ: 文字列

  有効な値: Check | Start | Restart | Force-Restart

  デフォルト: Check

  説明: (オプション) RDP サービス (TermService) を確認、開始、再起動、または強制的に再起動します。

- RDPServiceStartupType

  タイプ: 文字列

  有効な値: Check | Auto

  デフォルト: Check

  説明: (オプション) RDP サービスを Windows の起動時に自動的に起動するように確認または設定します。

- RemoteConnections

  タイプ: 文字列

  有効な値: Check | Enable

  デフォルト: Check

  説明: (オプション) fDenyTSConnections 設定で実行するアクション: Check、Enable。

- S3BucketName

  タイプ: 文字列

説明: (オプション) オフラインのみ - トラブルシューティングのログをアップロードするアカウントの S3 バケット名です。収集されたログにアクセスする必要がないユーザーへの不必要な読み取り/書き込みアクセス権限をバケットポリシーに付与しないようにします。

- SubnetId

  タイプ: 文字列

  デフォルト: SelectedInstanceSubnet

  説明: (オプション) オフラインのみ - オフラインのトラブルシューティングを実行するために使用される EC2Rescue インスタンスのサブネット ID。サブネット ID が指定されていない場合、AWS Systems Manager Automation は新しい VPC を作成します。重要: サブネットは InstanceId と同じアベイラビリティーゾーンである必要があり、SSM エンドポイントへのアクセスを許可する必要があります。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

このコマンドを受信する EC2 インスタンスには、[AmazonSSMManagedInstanceCore] Amazon 管理ポリシーがアタッチされた IAM ロールがあることが推奨されます。オンライン修復の場合、オートメーションを実行し、インスタンスにコマンドを送信するには少なくとも [ssm:DescribeInstanceInformation]、[ssm:StartAutomationExecution] および [ssm:SendCommand] が必要です。また、オートメーションの出力を読み取るためには、[ssm:GetAutomationExecution] も必要です。オフライン修復の場合、自動化の出力を読み取るためには、少なくとも [ssm:DescribeInstanceInformation]、[ssm:StartAutomationExecution]、[ec2:DescribeInstances]、および [ssm:GetAutomationExecution] が必要です。`AWSSupport-TroubleshootRDP` は `AWSSupport-ExecuteEC2Rescue`を呼び出してオフライン修復を実行します。自動化を正常に実行できるように、`AWSSupport-ExecuteEC2Rescue` のアクセス許可を確認してください。

ドキュメントステップ

1. `aws:assertAwsResourceProperty` - インスタンスが Windows Server インスタンスかを確認します
2. `aws:assertAwsResourceProperty` - インスタンスがマネージドインスタンスかを確認します
3. (オンラインのトラブルシューティング) インスタンスがマネージドインスタンスの場合は、次のようになります。

a. aws:assertAwsResourceProperty - 指定されたアクション値を確認します

b. (オンラインチェック) [Action = CheckAll] の場合、次のようになります。

aws:runPowerShellScript - PowerShell スクリプトを実行して、Windows ファイアウォールのプロファイルのステータスを取得します。

aws:executeAutomation - RDP サービスのステータスを取得するために AWSSupport-ManageWindowsService を呼び出します。

aws:executeAutomation - RDP 設定を取得するために AWSSupport-ManageRDPSettings を呼び出します。

c. (オンライン修正) [Action = FixAll] の場合、次のようになります。

aws:runPowerShellScript - PowerShell スクリプトを実行して、すべての Windows ファイアウォールのプロファイルを無効にします。

aws:executeAutomation - RDP サービスを開始するために AWSSupport-ManageWindowsService を呼び出します。

aws:executeAutomation - リモート接続を有効にし、NLA を無効にするために AWSSupport-ManageRDPSettings を呼び出します。

d. (オンライン管理) [Action = Custom] の場合、次のようになります。

aws:runPowerShellScript - PowerShell スクリプトを実行して、Windows ファイアウォールのプロファイルを管理します。

aws:executeAutomation - RDP サービスを管理するために AWSSupport-ManageWindowsService を呼び出します。

aws:executeAutomation - RDP 設定を管理するために AWSSupport-ManageRDPSettings を呼び出します。

4. (オフラインの修復) インスタンスがマネージドインスタンスでない場合は以下のようになります。

a. aws:assertAwsResourceProperty - AllowOffline = true をアサートします

b. aws:assertAwsResourceProperty - Action = FixAll をアサートします

c. aws:assertAwsResourceProperty - SubnetId の値をアサートします

(提供されたインスタンスのサブネットを使用) SubnetId が SELECTED_INSTANCE_SUBNET の場合

`aws:executeAwsApi` - 現在のインスタンスのサブネットを取得します。

`aws:executeAutomation` - 指定したインスタンスのサブネットで `AWSSupport-ExecuteEC2Rescue` を実行します。

d. (提供されたカスタムサブネットを使用) SubnetId が SELECTED_INSTANCE_SUBNET でない場合

`aws:executeAutomation` - 指定された SubnetId 値を使用して `AWSSupport-ExecuteEC2Rescue` を実行します。

出力

manageFirewallProfiles.Output

manageRDPServiceSettings.Output

manageRDPSettings.Output

checkFirewallProfiles.Output

checkRDPServiceSettings.Output

checkRDPSettings.Output

disableFirewallProfiles.Output

restoreDefaultRDPServiceSettings.Output

restoreDefaultRDPSettings.Output

troubleshootRDPOffline.Output

troubleshootRDPOfflineWithSubnetId.Output

AWSSupport-TroubleshootSSH

説明

AWSSupport-TroubleshootSSH ランブックは、Linux 用の Amazon EC2Rescue ツールをインストールし、その EC2Rescue ツールを使用して、Linux マシンへの SSH 経由でのリモートからの接続を妨げる、一般的な問題を確認しその修正を試みます。オプションで、ユーザーがオフラインの修復を明示的に許可している場合は、インスタンスを停止して起動することで、オフラインで変更を適用できます。デフォルトでは、このランブックは読み込み専用モードで動作します。

このオートメーションを実行する (コンソール)

AWSSupport-TroubleshootSSH ランブックの使用の詳細については、 AWS プレミアムサポートの「AWSSupport-TroubleshootSSHトラブルシューティングトピック」を参照してください。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- アクション

  タイプ: 文字列

  有効な値: CheckAll | FixAll

  デフォルト: CheckAll

  説明: (必須) 検出された問題を修正せずにチェックのみを行うか、チェックし自動的に修正するかを指定します。

- AllowOffline

  タイプ: 文字列

  有効な値: true | false

  デフォルト: false

説明: (オプション) 修正のみ - オンラインのトラブルシューティングが失敗した場合、または提供されたインスタンスがマネージドインスタンスではない場合に、オフラインで SSH の修復を許可する場合は true に設定します。注: オフライン修復の場合、SSM Automation はインスタンスを停止し、操作を試みる前に AMI を作成します。

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) Linux 用 EC2 インスタンスの ID。

- S3BucketName

  タイプ: 文字列

  説明: (オプション) オフラインのみ - トラブルシューティングのログをアップロードするアカウントの S3 バケット名です。収集されたログにアクセスする必要がないユーザーへの不必要な読み取り/書き込みアクセス権限をバケットポリシーに付与しないようにします。

- SubnetId

  タイプ: 文字列

  デフォルト: SelectedInstanceSubnet

  説明: (オプション) オフラインのみ - オフラインのトラブルシューティングを実行するために使用される EC2Rescue インスタンスのサブネット ID。サブネット ID が指定されていない場合、AWS Systems Manager Automation は新しい VPC を作成します。

  > **Important**
  >
  > サブネットは InstanceId と同じアベイラビリティーゾーンである必要があり、SSM エンドポイントへのアクセスを許可する必要があります。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

このコマンドを受信する EC2 インスタンスには、[AmazonSSMManagedInstanceCore] Amazon 管理ポリシーがアタッチされた IAM ロールがあることが推奨されます。オンライン修復の場合、オートメーションを実行し、インスタンスにコマンドを送信するには少なくとも [ssm:DescribeInstanceInformation]、[ssm:StartAutomationExecution] および [ssm:SendCommand] が必要です。また、オートメーションの出力を読み取るためには、[ssm:GetAutomationExecution] も必要です。オフライン修復の場合、自動化の出力を読み取るためには、少なくとも [ssm:DescribeInstanceInformation]、[ssm:StartAutomationExecution]、[ec2:DescribeInstances]、および [ssm:GetAutomationExecution] が必要です。AWSSupport-TroubleshootSSH は AWSSupport-ExecuteEC2Rescueを呼び出してオフライン修復を実行します。自動化を正常に実行できるように、AWSSupport-ExecuteEC2Rescue のアクセス許可を確認してください。

ドキュメントステップ

1. aws:assertAwsResourceProperty - インスタンスがマネージドインスタンスかを確認します
   a. (オンラインの修復) インスタンスがマネージドインスタンスの場合は以下のようになります。
      i. aws:configurePackage - AWS-ConfigureAWSPackage 経由で Linux 用 EC2Rescue をインストールします。
      ii. aws:runCommand - bash スクリプトを実行し、Linux 用の EC2Rescue を実行します。
   b. (オフラインの修復) インスタンスがマネージドインスタンスでない場合は以下のようになります。
      i. aws:assertAwsResourceProperty - AllowOffline = true をアサートします
      ii. aws:assertAwsResourceProperty - Action = FixAll をアサートします
      iii. aws:assertAwsResourceProperty - SubnetId の値をアサートします
      iv. (指定されたインスタンスのサブネットを使用) SubnetId が SelectedInstanceSubnet の場合は、aws:executeAutomation を使用し、提供されたインスタンスのサブネットで AWSSupport-ExecuteEC2Rescue を実行します。
      v. (指定されたカスタムサブネットを使用) SubnetId が SelectedInstanceSubnet ではない場合、aws:executeAutomation を使用し、提供された SubnetId の値で AWSSupport-ExecuteEC2Rescue を実行します。

出力

troubleshootSSH.Output

troubleshootSSHOffline.Output

troubleshootSSHOfflineWithSubnetId.Output

AWSSupport-TroubleshootSUSERegistration

説明

AWSSupport-TroubleshootSUSERegistration ランブックでは、SUSE 更新インフラストラクチャへの Amazon Elastic Compute Cloud (Amazon EC2) SUSE Linux Enterprise Server インスタンスの登録が失敗した理由を特定できます。自動化出力には、問題を解決する手順やトラブルシューティングに役立つ情報が記載されています。自動化中にインスタンスがすべてのチェックに合格すると、そのインスタンスは SUSE 更新インフラストラクチャに登録されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: 文字列

説明: (必須) トラブルシューティングを行う Amazon EC2 インスタンスの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:DescribeInstanceProperties
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:SendCommand
- ssm:ListCommands

ドキュメントステップ

- aws:assertAwsResourceProperty - Amazon EC2 インスタンスが によって管理されているかどうかを確認します AWS Systems Manager。
- aws:runCommand - Amazon EC2 インスタンスプラットフォームが SLES であるかどうかを確認します。
- aws:runCommand - パッケージ cloud-regionsrv-client バージョンが、必要なバージョン 9.0.10 以上かどうかをチェックします。
- aws:runCommand - ベース製品のシンボリックリンクが壊れていないかをチェックし、壊れている場合はリンクを修正します。
- aws:runCommand - ホストファイル (/etc/hosts) に smt-ec2-suscloud.net のレコードが含まれているかどうかを確認します。自動化は重複するエントリをすべて削除します。
- aws:runCommand - curl コマンドがインストールされているかどうかを確認します。
- aws:runCommand - Amazon EC2 インスタンスがインスタンスメタデータサービス (IMDS) のアドレス 169.254.169.254 にアクセスできるかどうかを確認します。
- aws:runCommand - Amazon EC2 インスタンスに請求コードまたは AWS Marketplace 製品コードがあるかどうかを確認します。
- aws:runCommand - Amazon EC2 インスタンスが HTTPS 経由で少なくとも 1 つのリージョン別サーバーに到達できるかどうかを確認します。

- aws:runCommand - Amazon EC2 インスタンスが HTTP 経由でサブスクリプション管理ツール (SMT) サーバーに到達できるかどうかを確認します。
- aws:runCommand - Amazon EC2 インスタンスが HTTPS 経由でサブスクリプション管理ツール (SMT) サーバーに到達できるかどうかを確認します。
- aws:runCommand - Amazon EC2 インスタンスが HTTPS 経由で smt-ec2.susecloud.net アドレスに到達できるかどうかを確認します。
- aws:runCommand - Amazon EC2 インスタンスを SUSE 更新インフラストラクチャに登録します。
- aws:executeScript - これまでのすべてのステップの出力を収集して出力します。

AWSSupport-TroubleshootWindowsPerformance

説明

ランブックは、Amazon Elastic Compute Cloud (Amazon EC2) Windows インスタンスで進行中のパフォーマンス問題のトラブルシューティングAWSSupport-TroubleshootWindowsPerformanceに役立ちます。ランブックは、ターゲットインスタンスからログをキャプチャし、CPU、メモリ、ディスク、ネットワークパフォーマンスメトリクスを分析します。オプションで、オートメーションはプロセスダンプをキャプチャして、パフォーマンス低下の潜在的な原因を特定するのに役立ちます。このランブックにインストールを許可すると、オートメーションは最新のEC2Rescueツールを使用してイベントログとシステムログもキャプチャします。

動作の仕組み

ランブックは次のステップを実行します。

- Amazon EC2 インスタンスの前提条件を確認します。
- Amazon EC2 Windows インスタンスのルートディスクにパフォーマンスログを生成します
- キャプチャされたログを フォルダに保存します。 C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance
- Amazon Simple Storage Service (Amazon S3) バケットが提供されていて、オートメーションの継承ロールに必要なアクセス許可がある場合、キャプチャされたログは Amazon S3 バケットにアップロードされます。
- Amazon EC2 Windows インスタンスに最新のEC2Rescueツールをインストールして、インストールを選択した場合はイベントとシステムログをキャプチャしますが、 によってキャプチャされたプロセスダンプとログは分析されませんEC2Rescue。

Important

- このランブックを実行するには、Amazon EC2 Windows インスタンスを で管理する必要があります AWS Systems Manager。詳細については、Amazon EC2 インスタンスがマネージドノードとして表示されない理由」を参照してください。
- このランブックを実行するには、Amazon EC2 Windows インスタンスが、PowerShell 4.0 以降の Windows 8.1/Windows Server 2012 R2 (6.3) 以降で実行されている必要があります。詳細については、「Windows オペレーティングシステムのバージョン」を参照してください。
- パフォーマンスログを生成するには、ルートデバイスに少なくとも 10 GB の空き容量が必要です。ルートディスクが 100 GB を超える場合、空き容量はディスクサイズの 10% を超える必要があります。実行中にプロセスをダンプする場合、空き容量は 10 GB に、プロセスが 10 GB を超えるメモリを消費するときにプロセスが消費する合計メモリサイズを加えた値である必要があります。
- ルートデバイスで生成されたログは自動的に削除されません。
- ランブックはEC2Rescueツールをアンインストールしません。詳細については、「Windows Server で を使用するEC2Rescue」を参照してください。
- パフォーマンスに影響する場合は、このオートメーションを実行することをお勧めします。 AWS Systems Manager ステートマネージャーの関連付けを使用するか、 AWS Systems Manager メンテナンスウィンドウをスケジュールして定期的に実行することもできます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

(オプション) インスタンスプロファイルにアタッチされた IAM ロール、またはインスタンスに設定された IAM ユーザーは、パラメータ に指定された Amazon S3 バケットにログをアップロードするために以下のアクションが必要です*LogUploadBucketName*。

- s3:PutObject
- s3:GetObject
- s3:ListBucket

指示

次の手順に従って自動化を設定します。

1. ドキュメントの下の Systems Manager AWSSupport-TroubleshootWindowsPerformanceのに移動します。

2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - InstanceId (必須):

     オートメーションを実行するターゲット Amazon EC2 Windows インスタンスの ID。インスタンスは、オートメーションを実行するために Systems Manager によって管理される必要があります。
   - CaptureProcessDump (オプション):

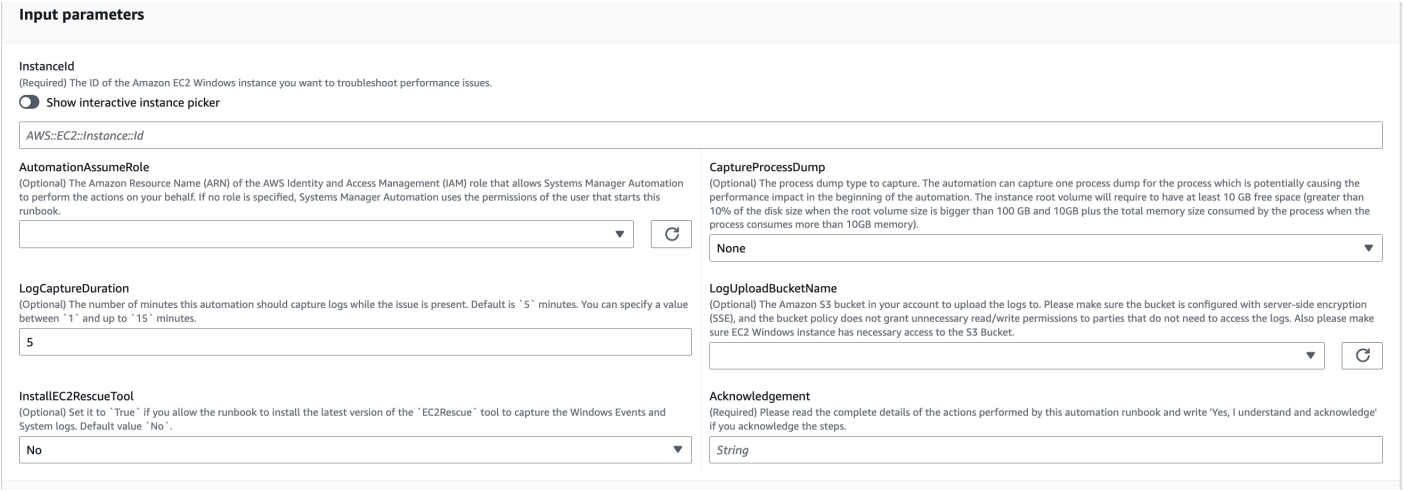
     キャプチャするプロセスダンプタイプ。自動化は、自動化の開始時にパフォーマンスへの影響を引き起こす可能性のあるプロセスの 1 つのプロセスダンプをキャプチャできます。インスタンスのルートボリュームには、少なくとも 10 GB の空き容量が必要です (ルートボリュームサイズが 100 GB より大きい場合はディスクサイズの 10% を超え、プロセスが 10 GB を超えるメモリを消費すると、プロセスが消費する合計メモリサイズが 10 GB を超える) 。
   - LogCaptureDuration (オプション):

     問題が存在する間、この自動化がログをキャプチャ15する 1 から までの分数。デフォルトは 5 です。
   - LogUploadBucketName (オプション):

     ログをアップロードするアカウントの Amazon S3 バケット。バケットはサーバー側の暗号化 (SSE) で設定する必要があります。また、バケットポリシーは、キャプチャされたログへのアクセスを必要としない当事者に不要な読み取り/書き込みアクセス許可を付与してはいけません。Amazon EC2 Windows インスタンスは、Amazon S3 バケットにアクセスできる必要があります。
   - InstallEC2RescueTool (オプション):

     Yes に設定すると、ランブックは最新バージョンのEC2Rescueツールをインストールして Windows イベントとシステムログをキャプチャできます。デフォルトは No です。
   - 確認 (必須):

このオートメーションランブックによって実行されるアクションの詳細をすべて読み、同意する場合は「」と入力しますYes, I understand and acknowledge。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。

   - **CheckConcurrency:**

     インスタンスをターゲットとするこのランブックの実行が 1 つだけであることを確認します。ランブックが同じインスタンスをターゲットとする別の実行を検出すると、エラーが返され、終了します。

   - **AssertInstanceIsWindows:**

     Amazon EC2 インスタンスが Windows オペレーティングシステムで実行されていることをアサートします。それ以外の場合、自動化は終了します。

   - **AssertInstanceIsManagedInstance:**

     Amazon EC2 インスタンスが管理されていることをアサートします AWS Systems Manager。それ以外の場合、オートメーションは終了します。

   - **VerifyPrerequisites:**

     インスタンス OS の PowerShell バージョンを検証し、インスタンスが Systems Manager を介して接続され、PowerShell コマンドを実行できることを確認します。このオートメーションは、Windows 8.1 / Server 2012 R2 (6.3) 以降で実行されている PowerShell 4.0 以降をサポートしています。バージョンが古い場合、自動化は失敗します。Amazon S3 バケットにログをアッ

プロードすることを選択すると、この自動化により AWS Tools for PowerShell モジュールが利用可能であることを確認します。そうでない場合、オートメーションは終了します。

- **BranchOnProcessDump:**

  パフォーマンスに影響を与えたプロセスのダンプをキャプチャするように設定した場合、 に基づいて分岐します。

- **CaptureProcessDump:**

  インスタンスに、このオートメーションを実行するのに十分なスペースがあるかどうかを確認します (CPU/メモリが最大 を選択した場合) 。

- **CapturePerformanceLogs:**

  ディスク容量を再度チェックし、インスタンスで PowerShell スクリプトを実行して perfmon カウンターを作成し、Performance Monitor と Windows Performance Recorder のログ記録を開始します。定義された が満たされると、スクリプトLogCaptureDurationは停止します。

- **SummarizePerformanceLogs:**

  前のステップ で生成された XML レポートを要約してCapturePerformanceLogs、オートメーションの出力として表示される WorkingSet64 (メモリ) と % プロセッサ時間 (CPU) を最も多く消費する責任のあるプロセスを見つけます。LogicalDisk、Network Interface、Memory、TCPv4, IPv4UDPv4 の使用に関する同様の情報を生成し、出力フォルダanalysis_output.logに保存します。

- **BranchOnInstallEC2Rescue:**

  Amazon EC2 インスタンスに最新のEC2Rescueツールをインストールするように設定した場合、 は分岐します。

- **InstallEC2RescueTool:**

  を使用してEC2Rescueログをキャプチャするためにec2rescue、 ツールをインスタンス OS にインストールしますAWS-ConfigureAWSPackage。

- **RunEC2RescueTool:**

  インスタンス OS でEC2Rescueツールを実行して、必要なすべてのログをキャプチャします。は、スペースを節約するために必要なログのみをEC2Rescueキャプチャします。

- **BranchOnIfS3BucketProvided:**

のユーザー入力に基づいて分岐LogUploadBucketNameし、ログをアップロードできるバケット名があるかどうかを確認します。

- **GetS3BucketPublicStatus:**

  Amazon S3 バケットが提供されているかどうかを判断し、提供されている場合は、Amazon S3 バケットがパブリックではなく、SSE で設定されていることを確認します。

- **UploadLogResult:**

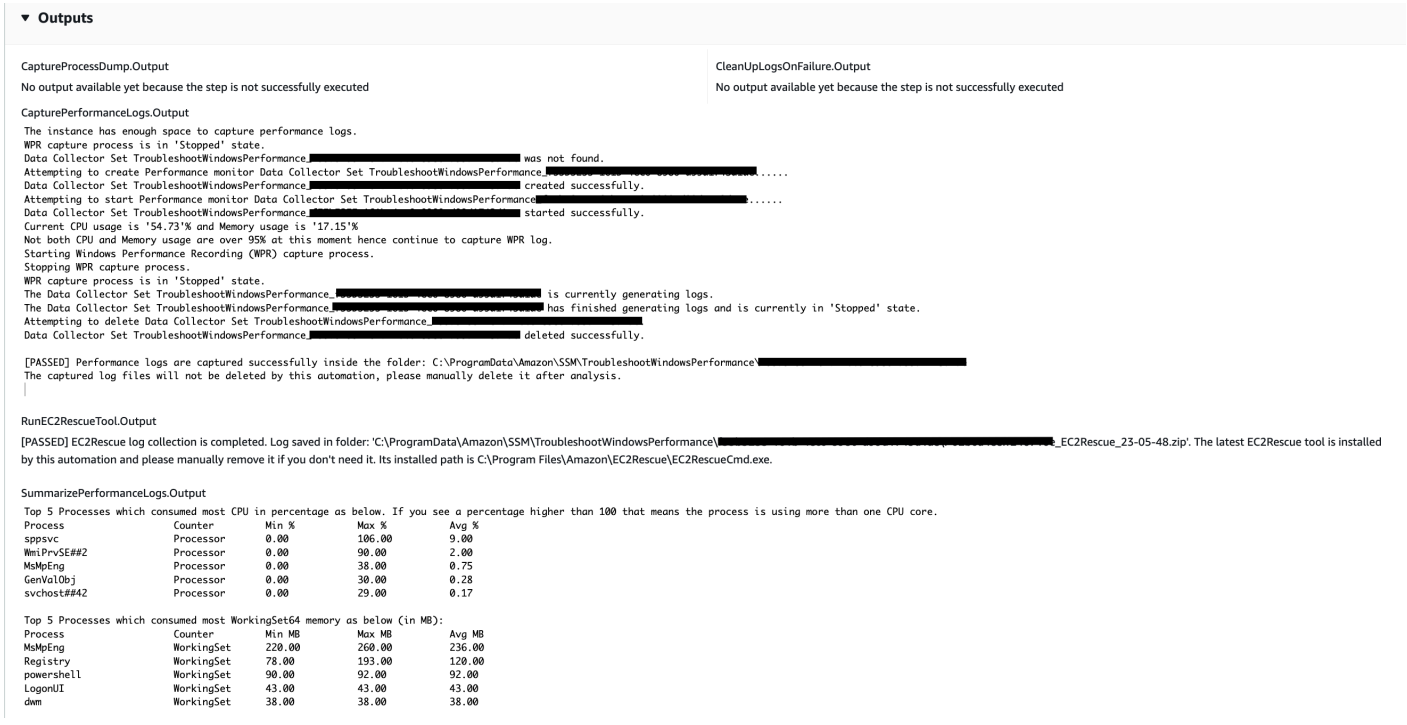
  指定された Amazon S3 バケットにログをアップロードします。PowerShell バージョンが 5.0 以降の場合、ログは ZIP アーカイブに圧縮され、アップロードされます。アップロードが完了すると、ZIP ファイルを削除します。PowerShell バージョンが 5.0 未満の場合、ファイルはフォルダに直接アップロードされます。

- **CleanUpLogsOnFailure:**

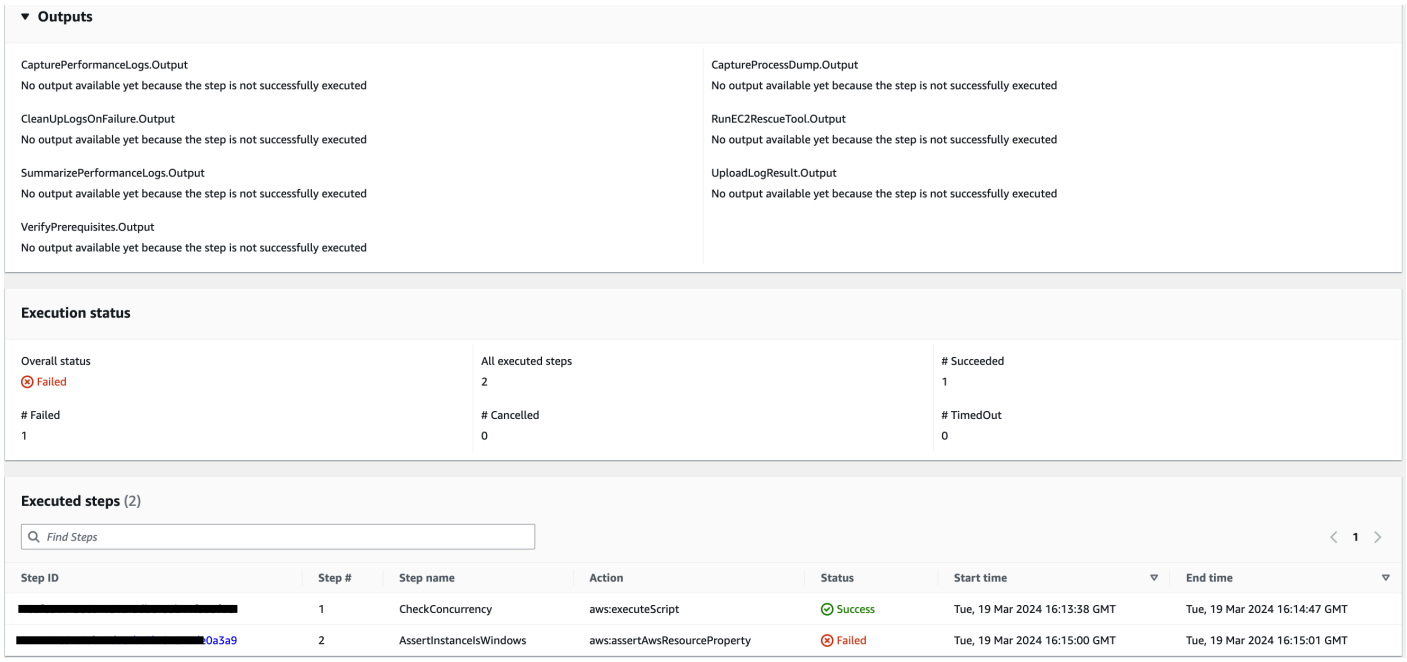
  CapturePerformanceLogs ステップが失敗したときに生成されたすべてのログをクリーンアップします。SSM Agent が正しく動作しない場合、または Windows システムが応答しない場合、CleanUpLogsOnFailureステップが失敗またはタイムアウトすることがあります。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

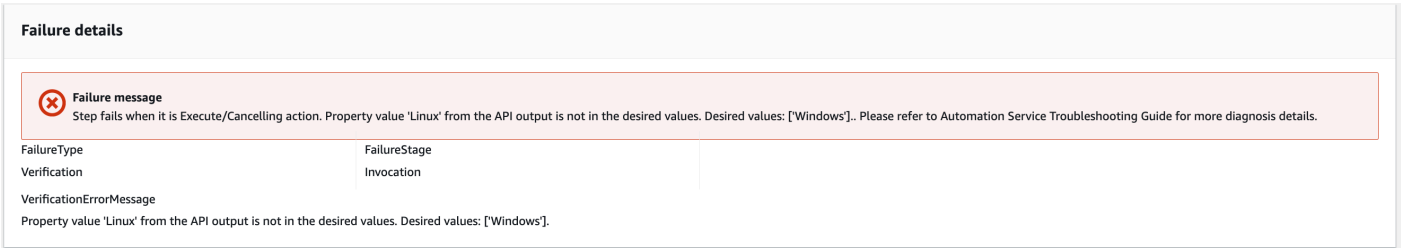
   ターゲットインスタンスに必要なすべての前提条件がある実行。



ターゲットインスタンスが Linux プラットフォームにあり、実行が失敗した実行。ステップ ID を選択すると、失敗の詳細が表示されます。



ステップ の失敗の詳細`AssertInstanceIsWindows`。



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWSSupport-TroubleshootWindowsUpdate

説明

AWSSupport-TroubleshootWindowsUpdate ランブックは、Amazon Elastic Compute Cloud (Amazon EC2) Windows インスタンスの Windows 更新に失敗する可能性のある問題を特定するために使用されます。

動作の仕組み

ランブックは次のステップを実行します。

- ターゲット Amazon EC2 インスタンスが によって管理されているかどうかを確認します AWS Systems Manager。
- AWS Systems Manager エージェント (SSM Agent) と Windows Server のバージョンが Systems Manager のパッチ適用オペレーションでサポートされているかどうかを確認します。
- Windows 更新に推奨される使用可能なディスク容量と、再起動が保留中かどうかを確認します。通常、保留中の再起動は更新が保留中であることを示します。追加の更新を実行する前に再起動が必要です。
- プロキシ設定をオペレーティングシステムレベルで設定します。これにより、接続の問題のトラブルシューティングに役立ちます。
- Amazon Simple Storage Service (Amazon S3) エンドポイント接続テストを実行し、GetDeployablePatchSnapshotForInstance API オペレーションを呼び出して、マネージドノードが使用するパッチベースラインの現在のスナップショットを取得します。
- 接続が失敗した場合、 はAWSSupport-AnalyzeAWSEndpointReachabilityFromEC2ランブックを実行してインスタンスの Amazon S3 エンドポイントへの接続を分析するオプションを提供します。
- Windows 更新の設定を検証し、Windows Server Update Services (WSUS) (該当する場合) をテストします。

> **Important**
>
> - Active Directory ドメインコントローラーはサポートされていません。
> - Windows Server バージョン 2008 R2 以前のバージョンはサポートされていません。
> - SSM Agent 1.2.371 以前のバージョンはサポートされていません。
> - AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 ランブックは を使用してVPC Reachability Analyzer、ソースとサービスエンドポイント間のネットワーク接続を分析します。ソースとターゲットの間で分析が実行されるたびに課金されます。詳細については、「Amazon VPC の料金」を参照してください。

- AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 ランブックは、Systems Manager がサポートされているすべてのリージョンで利用できるわけではありません。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:DescribeInstanceInformation
- ssm:SendCommand
- ssm:ListCommandInvocations
- ssm:ListCommands

> **Note**
>
> 子ランブック を実行するにはAWSSupport-AnalyzeAWSEndpointReachabilityFromEC2、このドキュメントに記載されているアクセス許可を追加します。

指示

次の手順に従って自動化を設定します。

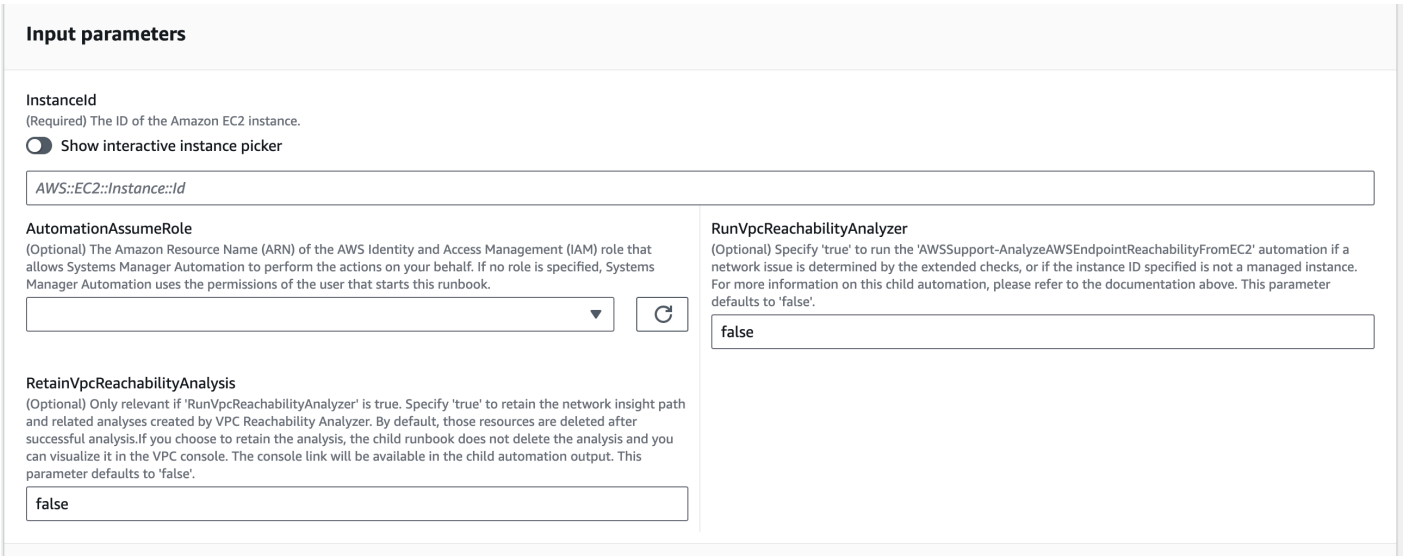
1. ドキュメントの Systems Manager AWSSupport-TroubleshootWindowsUpdateで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - InstanceId (必須):

     Windows 更新が失敗した Amazon EC2 インスタンスの ID を入力します。
   - RunVpcReachabilityAnalyzer (オプション):

     ネットワークの問題が拡張チェックによって決定された場合、または指定されたインスタンス ID がマネージドインスタンスでない場合は、AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2オートメーションtrueを実行するように を指定します。この子オートメーションの詳細については、 ドキュメントを参照してください。デフォルト値は false です。
   - RetainVpcReachabilityAnalysis (オプション):

     RunVpcReachabilityAnalyzer が の場合にのみ関連しますtrue。を指定trueして、 によって作成されたネットワークインサイトパスと関連する分析を保持しますReachability Analyzer。デフォルトでは、これらのリソースは分析が成功すると削除されます。分析を保持することを選択した場合、子ランブックは分析を削除せず、Amazon VPC コンソールで視覚化できます。コンソールリンクは、子オートメーション出力で使用できます。デフォルト値は ですfalse。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - **`getWindowsServerAndSSMAgentVersion:`**

     ターゲットインスタンスが によって管理されていることを確認し AWS Systems Manager 、SSM エージェントのバージョンと Windows のバージョンに関する詳細を取得します。
   - **`assertifInstanceIsSsmManaged:`**

     Amazon EC2 インスタンスが AWS Systems Manager (SSM) によって管理されていることを確認します。管理されていない場合、オートメーションは終了します。
   - **`CheckProxy:`**

     Windows インスタンスのすべてのプロキシタイプをチェックします。
   - **`CheckPrerequisites:`**

     SSM エージェントのバージョンと Windows のバージョンを取得し、それが Active Directory ドメインコントローラー (DC) であるかどうかを判断します。インスタンスが DC であるか、SSM エージェントまたは Windows バージョンがサポートされていない場合、ランブックは停止します。
   - **`CheckDiskSpace:`**

Windows 更新を実行するのに十分であれば、Windows インスタンスで使用可能なディスク容量を取得して検証します。

- **CheckPendingReboot:**

  Windows インスタンスでの保留中の再起動をチェックします。

- **CheckS3Connectivity:**

  インスタンスが の Amazon S3 エンドポイントに到達できるかどうかを確認しますPatchbaseline。

- **branchOnRunVpcReachabilityAnalyzer:**

  RunVpcReachabilityAnalyzer が true の場合、自動化を分岐させて、デバッグ中の Amazon S3 接続のより詳細な分析を実行します。

- **GenerateEndpoints:**

  Amazon S3 エンドポイントの拡張接続チェックを行うエンドポイントを生成します。

- **analyzeAwsEndpointReachabilityFromEC2:**

  オートメーションランブック AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2を呼び出して、必要なエンドポイントへの選択したインスタンスの到達可能性を確認します。

- **CheckWindowsUpdateServices:**

  Windows Update サービスのステータスと開始タイプを確認します。

- **CheckWindowsUpdateSettings:**

  Windows インスタンスで設定された Windows Update ポリシーをチェックします。

- **CheckWSUSSettings:**

  Windows 更新プログラムが WSUS または Microsoft Update Catalog で設定されているかどうかを確認し、接続を検証します。

- **CheckWUGlobalSettings:**

  Windows インスタンスで設定された Windows Update グローバル設定を確認します。

- **GenerateLogs:**

Windows Update ログと CBS ログをインスタンスデスクトップにダウンロードし、Windows イベントログに障害がないかどうかを確認します。

- **FinalReport:**

  すべてのステップの完全なレポートを生成します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

```
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
"
```

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスに関連するドキュメント

- 詳細については、記事TroubleShoot Windows Update」を参照してください。

AWSSupport-UpgradeWindowsAWSDrivers

説明

AWSSupport-UpgradeWindowsAWSDrivers ランブックは、指定された EC2 インスタンスのストレージドライバーとネットワーク AWS ドライバーをアップグレードまたは修復します。ランブックは、SSM エージェントを呼び出して、最新バージョンの AWS ドライバーをオンラインでインストールしようとします。SSM Agent が連絡可能でない場合、明示的にリクエストされた場合、ランブックは AWS ドライバーのオフラインインストールを実行できます。

このランブックでは、以下のオペレーティングシステムがサポートされています。

- Windows Server 2016
- [Windows Server 2019]
- Windows Server 2022
- Windows Server 2025

> **Note**
>
> オンラインおよびオフラインのどちらでアップグレードした場合も、いずれかのオペレーションが試行される前に AMI が作成されます。この AMI はオートメーションが完了した後も維持されます。AMI へのアクセスを保護したり、削除したりするのはサービス利用者の責任となります。オンライン方法はアップグレードプロセスの一部としてインスタンスを再起

動しますが、オフライン方法では、提供された EC2 インスタンスを停止してから起動する必要があります。

Important

インスタンスが VPC エンドポイント AWS Systems Manager を使用して に接続すると、us-east-1 リージョンで使用されない限り、このランブックは失敗します。このランブックはドメインコントローラーでも失敗します。ドメインコントローラーの PV AWS ドライバーを更新するには、「ドメインコントローラーのアップグレード (AWS PV アップグレード)」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

- AllowOffline

  タイプ: 文字列

  有効な値: true | false

  デフォルト: false

  説明: (オプション) オンラインインストールが実行できない場合にオフラインでドライバーのアップグレードを許可する場合は、この値を true に設定します。注意: オフライン方式では、指定された EC2 インスタンスを停止してから起動する必要があります。インスタンスストアボリュームに保存されているデータは失われます。Elastic IP を使用していない場合、パブリック IP アドレスが変わります。

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ForceUpgrade

  タイプ: 文字列

  有効な値: true | false

  デフォルト: false

  説明: (オプション) オフラインのみ - インスタンスに既に最新のドライバーがインストールされている場合でも、オフラインでドライバーのアップグレードを続行できるようにする場合は、これを true に設定します。

- InstanceId

  タイプ: 文字列

  説明: (必須) Windows Server の EC2 インスタンスの ID。

- SubnetId

  タイプ: 文字列

  デフォルト: SelectedInstanceSubnet

  説明: (オプション) オフラインのみ - オフラインでドライバアップグレードを実行するために使用される EC2Rescue インスタンスのサブネット ID。サブネット ID が指定されていない場合、Systems Manager Automation は新しい VPC を作成します。

  > **Important**
  >
  > サブネットは InstanceId と同じアベイラビリティーゾーンである必要があり、SSM エンドポイントへのアクセスを許可する必要があります。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

コマンドを受け取る EC2 インスタンスには、少なくとも、[ssm:StartAutomationExecution] および [ssm:SendCommand] のアクセス許可を含む IAM ロールが必要です。このロールは、オートメーションを実行し、コマンドをインスタンスに送信します。さらに、[ssm:GetAutomationExecution] でオートメーション出力を読み取ることができます。AmazonSSMManagedInstanceCore Amazon マネージドポリシーを IAM ロールにアタッチして、これらのアクセス許可を提供できます。ただし、この目的には、オートメーション IAM ロール AmazonSSMAutomationRole を使用することをお勧めします。詳細については、「IAM を使用して自動化のロールを設定する」を参照してください。

オフラインアップグレードを実行する場合、必要なアクセス権限は「AWSSupport-StartEC2RescueWorkflow」を参照してください。

ドキュメントステップ

1. aws:assertAwsResourceProperty - 入力インスタンスが Windows であることを確認します。
2. aws:assertAwsResourceProperty - 入力インスタンスがマネージドインスタンスであることを確認します。その場合、オンラインアップグレードが開始され、その他の場合はオフラインアップグレードが評価されます。
   a. (オンラインアップグレード) インプットインスタンスがマネージドインスタンスの場合は以下のようになります。
      i. aws:createImage - AMI バックアップを作成します。
      ii. aws:createTags - AMI バックアップにタグを付けます。
      iii. aws:runCommand - ENA ネットワークドライバーをインストールします。
      iv. aws:runCommand - NVMe ドライバーをインストールします。
      v. aws:runCommand - PV AWS ドライバーをインストールします。
   b. (オフラインアップグレード) インプットインスタンスがマネージドインスタンスでない場合は以下のようになります。
      i. aws:assertAwsResourceProperty - AllowOffline フラグが true に設定されていることを確認します。設定されている場合は、オフラインアップグレードが開始されます。そうでない場合、このオートメーションは終了します。
      ii. aws:changeInstanceState - ソースインスタンスを停止します。

iii. `aws:changeInstanceState` - ソースインスタンスを強制停止します。

iv. `aws:createImage` - ソースインスタンスの AMI バックアップを作成します。

v. `aws:createTags` - ソースインスタンスの AMI バックアップにタグを付けます。

vi. `aws:executeAwsApi` - インスタンスの ENA を有効にします

vii.`aws:assertAwsResourceProperty` - ForceUpgrade フラグをアサートします。

viii強制オフラインアップグレード) ForceUpgrade = true の場合は、ドライバーの強制アップグレードスクリプトで `aws:executeAutomation` を実行して `AWSSupport-StartEC2RescueWorkflow` を呼び出します。これにより、インストールされている現在のバージョンに関係なくドライバーがインストールされます

ix. (オフラインアップグレード) ForceUpgrade = false の場合は、ドライバーのアップグレードスクリプトで `aws:executeAutomation` を実行して `AWSSupport-StartEC2RescueWorkflow` を呼び出します。

出力

preUpgradeBackup.ImageId

preOfflineUpgradeBackup.ImageId

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

upgradeDriversOffline.Output

forceUpgradeDriversOffline.Output

Amazon ECS

AWS Systems Manager Automation は、Amazon Elastic Container Service 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-CollectECSInstanceLogs

- AWS-InstallAmazonECSAgent
- AWS-ECSRunTask
- AWSSupport-TroubleshootECSContainerInstance
- AWSSupport-TroubleshootECSTaskFailedToStart
- AWS-UpdateAmazonECSAgent

AWSSupport-CollectECSInstanceLogs

説明

AWSSupport-CollectECSInstanceLogs ランブックは、一般的な Amazon ECS の問題のトラブルシューティングに役立つように、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスからオペレーティングシステムと Amazon Elastic Container Service (Amazon ECS) に関連するログファイルを収集します。自動化が関連するログファイルを収集している間に、ファイルシステムに変更が加えられます。これらの変更には、一時ディレクトリとログディレクトリの作成、これらのディレクトリへのログファイルのコピー、ログファイルのアーカイブへの圧縮が含まれます。

LogDestination パラメータの値を指定する場合、ターゲットインスタンスには Linux インスタンス用の コマンドラインインターフェイス (AWS CLI) AWS または Windows インスタンス用の AWS Tools for Windows PowerShell がインストールされている必要があります。オートメーションは、指定した Amazon Simple Storage Service (Amazon S3) バケットのポリシーステータスを評価します。Amazon EC2 インスタンスから収集されたログのセキュリティを支援するために、ポリシーステータス isPublic が true に設定されている場合、またはアクセスコントロールリスト (ACL) が All Users Amazon S3 事前定義済みグループに READ|WRITE アクセス許可を付与している場合、ログはアップロードされません。また、指定したバケットがアカウントで利用できない場合、ログはアップロードされません。Amazon S3 事前定義された g ループの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon Amazon S3 事前定義されたグループ」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ECSInstanceId

  タイプ: 文字列

  説明: (必須) ログを収集する元のインスタンスの ID。指定するインスタンスは Systems Manager によって管理される必要があります。
- LogDestination

  タイプ: 文字列

  説明: (オプション) アーカイブされたログをアップロード AWS アカウント する の Amazon S3 バケット。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`

`ECSInstanceId` パラメータに指定する Amazon EC2 インスタンスには、`AmazonSSMManagedInstanceCore` Amazon 管理ポリシーがアタッチされた IAM ロールがあ

ることが推奨されます。LogDestination パラメータで指定した Amazon S3 バケットにログアーカイブをアップロードするには、以下のアクセス許可を追加する必要があります。

- s3:PutObject
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl

ドキュメントステップ

- assertInstanceIsManaged - ECSInstanceId パラメータで指定されたインスタンスが Systems Manager によって管理されているかどうかを確認します。
- getInstancePlatform - ECSInstanceId パラメータで指定されたインスタンスのオペレーティングシステム (OS) プラットフォームに関する情報を取得します。
- verifyInstancePlatform - OS プラットフォームに基づいて自動化を分岐させます。
- runLogCollectionScriptOnLinux - Linux インスタンスでオペレーティングシステムと Amazon ECS に関連するログファイルを収集し、/var/log/collectECSlogs ディレクトリにアーカイブファイルを作成します。
- runLogCollectionScriptOnWindows - Windows インスタンスでオペレーティングシステムと Amazon ECS に関連するログファイルを収集し、C:\ProgramData\collectECSlogs ディレクトリにアーカイブファイルを作成します。
- verifyIfS3BucketProvided - LogDestination パラメータに値が指定されているかどうかを確認します。
- runUploadScript - OS のプラットフォームに基づいて自動化ステップを分岐させます。
- runUploadScriptOnLinux - LogDestination パラメータで指定された Amazon S3 バケットにログアーカイブをアップロードし、アーカイブされたログファイルを OS から削除します。
- runUploadScriptOnWindows - LogDestination パラメータで指定された Amazon S3 バケットにログアーカイブをアップロードし、アーカイブされたログファイルを OS から削除します。

AWS-InstallAmazonECSAgent

説明

AWS-InstallAmazonECSAgent ランブックでは、指定した Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上の Amazon Elastic Container Service (Amazon ECS) エージェントを

インストールします。このランブックは、Amazon Linux および Amazon Linux 2 インスタンスのみをサポートします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceIds

  タイプ: StringList

  説明: (必須) Amazon ECS エージェントをインストールする Amazon EC2 インスタンスの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances

ドキュメントステップ

aws:executeScript - InstanceIds パラメータで指定した Amazon EC2 インスタンスに Amazon ECS エージェントをインストールします。

出力

InstallAmazonECSAgent.SuccessfulInstances - Amazon ECS エージェントのインストールが成功したインスタンスの ID。

InstallAmazonECSAgent.FailedInstances - Amazon ECS エージェントのインストールが失敗したインスタンスの ID。

InstallAmazonECSAgent.InProgressInstances - Amazon ECS エージェントのインストールが進行中のインスタンスの ID。

AWS-ECSRunTask

説明

AWS-ECSRunTask ランブックは、指定した Amazon Elastic Container Service (Amazon ECS) タスクを実行します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- capacityProviderStrategy

  タイプ: 文字列

  説明: (オプション) タスクに使用するキャパシティープロバイダー戦略。

- クラスター

  タイプ: 文字列

  説明: (オプション) タスクを実行するクラスターの短縮名または ARN。クラスターを指定しない場合、デフォルトのクラスターが使用されます。

- count

  タイプ: 文字列

  説明: (オプション) クラスターに配置する指定されたタスクのインスタンス化の数。リクエストごとに最大 10 個のタスクを指定できます。

- enableECSManagedTags

  型: ブール値

  説明: (オプション) タスクに Amazon ECS マネージドタグを使用するかどうかを指定します。詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS リソースにタグを付ける」を参照してください。

- enableExecuteCommand

  型: ブール値

  説明: (オプション) このタスクのコンテナの実行コマンド機能をアクティブ化するかどうかを決定します。true の場合、タスク内のすべてのコンテナでコマンド実行機能が有効になります。

- グループ

タイプ: 文字列

説明: (オプション) タスクに関連付けるタスクグループの名前。デフォルト値は、タスク定義のファミリー名です。例えば、`family:my-family-name`。

- launchType

  タイプ: 文字列

  有効な値: EC2 | FARGATE | EXTERNAL

  説明: (オプション) スタンドアロンタスクを実行するインフラストラクチャ。

- networkConfiguration

  タイプ: 文字列

  説明: (オプション) タスクのネットワーク設定。このパラメータは、 `awsvpc`ネットワークモードを使用して独自の Elastic Network Interface を受信するタスク定義に必要です。他のネットワークモードではサポートされていません。

- オーバーライド

  タイプ: 文字列

  説明: (オプション) 指定されたタスク定義でコンテナの名前を指定する JSON 形式のコンテナオーバーライドのリストと、コンテナが受け取るオーバーライド。タスク定義または Docker イメージで指定されたコンテナのデフォルトコマンドをコマンドオーバーライドで上書きできます。タスク定義またはコンテナの Docker イメージで指定された既存の環境変数を上書きすることもできます。さらに、環境オーバーライドを使用して新しい環境変数を追加できます。

- placementConstraints

  タイプ: 文字列

  説明: (オプション) タスクに使用する配置制約オブジェクトの配列。タスク定義の制約と実行時に指定された制約を含め、タスクごとに最大 10 個の制約を指定できます。

- placementStrategy

  タイプ: 文字列

  説明: (オプション) タスクに使用する配置戦略オブジェクト。タスクごとに最大 5 つの戦略ルールを指定できます。

- platformVersion

  タイプ: 文字列

  説明: (オプション) タスクが使用するプラットフォームバージョン。プラットフォームバージョンは、Fargate でホストされているタスクに対してのみ指定されます。プラットフォームバージョンが指定されない場合、LATEST プラットフォームバージョンが使用されます。

- propagateTags

  タイプ: 文字列

  説明: (オプション) タグがタスク定義からタスクに伝達されるかどうかを決定します。値を指定しない場合、タグは伝播されません。タグは、タスクの作成時にのみタスクに伝播できます。

- referenceId

  タイプ: 文字列

  説明: (オプション) タスクに使用するリファレンス ID。リファレンス ID の最大長は 1024 文字です。

- startedBy

  タイプ: 文字列

  説明: (オプション) タスクの開始時に指定されたオプションのタグ。これにより、ListTasksAPI オペレーションの結果をフィルタリングして、特定のジョブに属するタスクを特定できます。最大 36 文字 (大文字と小文字) 、数字、ハイフン (-)、アンダースコア (_) を使用できます。

- tags

  タイプ: 文字列

  説明: (オプション) タスクの分類と整理に役立つようにタスクに適用するメタデータ。各タグはユーザー定義のキーと値で構成されます。

- taskDefinition

  タイプ: 文字列

  説明: (オプション) 実行するタスク定義の familyおよび revision (family : revision) または完全な ARN。リビジョンが指定されていない場合は、最新のACTIVEリビジョンが使用されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ecs:RunTask

ドキュメントステップ

aws:executeScript - ランブック入力パラメータに指定した値に基づいて Amazon ECS タスクを実行します。

AWSSupport-TroubleshootECSContainerInstance

説明

AWSSupport-TroubleshootECSContainerInstance ランブックは、Amazon EC2 クラスターへの登録に失敗した Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのトラブルシューティングに役立ちます。この自動化では、インスタンスのユーザーデータに正しいクラスター情報が含まれているかどうか、インスタンスプロファイルに必要なアクセス権限が含まれているかどうか、およびネットワーク設定の問題が確認されます。

> **Important**
>
> この自動化を正常に実行するには、Amazon EC2 インスタンスの状態は running で、Amazon ECS クラスターの状態は ACTIVE でなければなりません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ClusterName

  タイプ: 文字列

  説明: (必須) インスタンスが登録に失敗した Amazon ECS クラスターの名前。

- InstanceId

  タイプ: 文字列

  説明: (必須) トラブルシューティングを行う Amazon EC2 インスタンスの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

aws:executeScript: Amazon EC2 インスタンスが Amazon ECS クラスターへの登録に必要な前提条件を満たしているかどうかを確認します。

AWSSupport-TroubleshootECSTaskFailedToStart

説明

AWSSupport-TroubleshootECSTaskFailedToStart ランブックは、Amazon ECS クラスター内の Amazon Elastic Container Service (Amazon ECS) タスクが起動に失敗した理由をトラブルシューティングするのに役立ちます。このランブックは、起動に失敗したタスク AWS リージョンと同じ で実行する必要があります。ランブックは、タスクの開始を妨げる可能性がある次のような一般的な問題を分析します。

- 設定済みのコンテナレジストリーへのネットワーク接続
- タスク実行ロールに必要な IAM 権限の欠落
- VPC エンドポイント接続
- セキュリティグループのルール設定
- AWS Secrets Manager シークレットリファレンス
- ログ作成設定

> **Note**
>
> 分析の結果、ネットワーク接続をテストする必要があると判断された場合は、Lambda 関数と必要な IAM ロールがアカウントに作成されます。これらのリソースは、失敗したタスクのネットワーク接続をシミュレートするために使用されます。自動化は、不要になったらリソースを削除します。ただし、自動化がリソースの削除に失敗した場合は、手動で削除する必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ClusterName

  タイプ: 文字列

  説明: (必須) タスクが起動に失敗した Amazon ECS クラスターの名前。
- CloudwatchRetentionPeriod

  タイプ: 整数

  説明: (オプション) Lambda 関数ログが Amazon CloudWatch Logs に保存されるまでの保持期間 (日単位)。これが必要なのは、分析の結果、ネットワーク接続をテストする必要があると判断された場合のみです。

  有効な値: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

  デフォルト: 30
- TaskId

  タイプ: 文字列

説明: (必須) 失敗したタスクの ID。最後に失敗したタスクを使用してください。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeScript - 自動化を開始したユーザーまたはロールに必要な IAM 権限があることを確認します。このランブックを使用するための十分な権限がない場合は、不足している必須権限が自動化の出力に含まれます。
- aws:branch - ランブックに必要なすべてのアクションに対する権限があるかどうかに基づいて分岐させます。
- aws:executeScript - 分析によりネットワーク接続をテストする必要があると判断された場合は、VPC に Lambda 関数を作成します。
- aws:branch - 前のステップの結果に基づいて分岐させます。
- aws:executeScript - タスクの起動に失敗した潜在的原因を分析します。
- aws:executeScript - この自動化によって作成されたリソースを削除します。
- aws:executeScript - 分析結果をコンソールに返すように自動化の出力をフォーマットします。このステップの後、自動化が完了する前に分析を確認できます。

- aws:branch - Lambda 関数と関連リソースが作成され、削除する必要があるかどうかに基づいて分岐させます。
- aws:sleep - 30 分間スリープ状態になるため、Lambda 関数の エラスティックネットワークインターフェイスを削除できます。
- aws:executeScript - Lambda 関数のネットワークインターフェイスを削除します。
- aws:executeScript - Lambda 関数のネットワークインターフェイス削除ステップの出力をフォーマットします。

AWS-UpdateAmazonECSAgent

説明

AWS-UpdateAmazonECSAgent ランブックでは、指定した Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上の Amazon Elastic Container Service (Amazon ECS) エージェントを更新します。このランブックは、Amazon Linux および Amazon Linux 2 インスタンスのみをサポートします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム

(ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ClusterARN

  タイプ: StringList

  説明: (必須) コンテナインスタンスが登録されている Amazon ECS クラスターの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetCommandInvocation
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeImage
- ec2:DescribeInstance
- ec2:DescribeInstanceAttribute
- ecs:DescribeContainerInstances
- ecs:DescribeClusters
- ecs:ListContainerInstances
- ecs:UpdateContainerAgent

ドキュメントステップ

aws:executeScript - ClusterARN パラメータで指定した Amazon ECS クラスターの Amazon ECS エージェントを更新します。

出力

UpdateAmazonECSAgent.UpdatedContainers - Amazon ECS エージェントの更新が成功したインスタンスの ID。

UpdateAmazonECSAgent.FailedContainers - Amazon ECS エージェントの更新が失敗したインスタンスの ID。

UpdateAmazonECSAgent.InProgressContainers - Amazon ECS エージェントの更新が進行中のインスタンスの ID。

Amazon EFS

AWS Systems Manager 自動化は、Amazon Elastic File System 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-CheckAndMountEFS

AWSSupport-CheckAndMountEFS

説明

AWSSupport-CheckAndMountEFS ランブックでは、Amazon Elastic File System (Amazon EFS) ファイルシステムをマウントするための前提条件を確認し、指定した Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにファイルシステムをマウントします。このランブックでは、Amazon EFS ファイルシステムをマウントする際に、DNS 名、またはマウントのターゲットとなる IP アドレスを使用することができます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- アクション

  タイプ: 文字列

  有効な値: Check | CheckAndMount

  説明: (必須) ランブックが前提条件のみを確認するのか、前提条件を確認した後でファイルシステムをマウントするのかを決定します。

- EfsId

  タイプ: 文字列

  説明: (必須) マウントするファイルシステムの ID。

- InstanceId

  タイプ: 文字列

  説明: (必須) ファイルシステムをマウントする Amazon EC2 インスタンスの ID。

- MountOptions

  タイプ: 文字列

  説明: (オプション) ファイルシステムのマウントに使用する Amazon EFS マウントヘルパーでサポートされるオプション。`tls` オプションを指定する場合は、ターゲットのインスタンスで stunnel がアップグレードされていることを確認します。

- MountPoint

  タイプ: 文字列

  説明: (オプション) ファイルシステムをマウントするディレクトリ。`Action` パラメータで `Check` 値を指定する場合は、このパラメータを指定しないでください。

- MountTargetIP

タイプ: 文字列

説明: (オプション) マウントのターゲットとなる IP アドレス。IP アドレスによるマウントは、DNS ホスト名が無効化されている仮想プライベートクラウド (VPC) などの、DNS が無効な環境で機能します。また、Amazon Route 53 (Route 53) 以外の DNS プロバイダーを使用している環境でも、このオプションを使用できます。

- リージョン

タイプ: 文字列

説明: (必須) Amazon EC2 インスタンスとファイルシステム AWS リージョン がある 。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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:*

ドキュメントステップ

- aws:executeScript - InstanceId パラメータで指定された Amazon EC2 インスタンスの詳細を収集します。
- aws:executeScript - EfsId パラメータで指定されたファイルシステムの詳細を収集します。
- aws:executeScript - ファイルシステムに関連付けられたセキュリティグループが、InstanceId パラメータで指定された Amazon EC2 インスタンスからのポート 2049 でのトラフィックを許可しているかを確認します。
- aws:assertAwsResourceProperty - InstanceId パラメータで指定した Amazon EC2 インスタンスが Systems Manager によって管理されており、ステータスが Online であることを確認します。
- aws:branch - Action パラメータで指定した値に基づいて分岐させます。
- aws:runCommand - EfsId パラメータで指定されたファイルシステムをマウントするための前提条件を確認します。
- aws:runCommand - EfsId パラメータで指定されたファイルシステムをマウントするための前提条件を確認し、このファイルシステムを、InstanceId パラメータで指定された Amazon EC2 インスタンスにマウントします。

Amazon EKS

AWS Systems Manager Automation は、Amazon Elastic Kubernetes Service 用の事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- 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

説明

AWSSupport-CollectEKSInstanceLogs ランブックは、一般的な問題のトラブルシューティングに役立つように、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスからオペレーティングシステムと Amazon Elastic Kubernetes Service (Amazon EKS) に関連するログファイルを収集します。自動化によって関連するログファイルが収集される間、一時ディレクトリの作成、ログファイルの一時ディレクトリへのコピー、ログファイルのアーカイブへの圧縮など、ファイルシステム構造が変更されます。このアクティビティにより、EC2 インスタンスで CPUUtilization が増加する可能性があります。CPUUtilization の詳細については、Amazon CloudWatch ユーザーガイドの「インスタンスメトリクス」を参照してください。

LogDestination パラメータの値を指定すると、指定した Amazon Simple Storage Service (Amazon S3) バケットのポリシーステータスが自動化によって評価されます。EC2 インスタンスから収集されたログのセキュリティを支援するために、ポリシーステータス isPublic が true に設定されている場合、またはアクセスコントロールリスト (ACL) が All Users Amazon S3 事前定義済みグループに READ|WRITE アクセス許可を付与している場合、ログはアップロードされません。Amazon S3 の定義済みグループの詳細については、Amazon Simple Storage Service ユーザーガイドの「Amazon S3 の定義済みグループ」を参照してください。

> **Note**
>
> このオートメーションでは、EC2 インスタンスにアタッチされたルート Amazon Elastic Block Store (Amazon EBS) ボリュームの空きディスク容量の 10% 以上が必要です。ルートボリュームに十分な空きディスク容量がない場合、自動化は停止します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- EKSInstanceId

  タイプ: 文字列

  説明: (必須) ログを収集する元の Amazon EKS EC2 インスタンスの ID。
- LogDestination

  タイプ: 文字列

  説明: (オプション) アーカイブされたログをアップロードするアカウントの S3 バケット。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

このコマンドを受信する EC2 インスタンスには、[AmazonSSMManagedInstanceCore] Amazon 管理ポリシーがアタッチされた IAM ロールがあることが推奨されます。LogDestination パラメータで指定した S3 バケットにログアーカイブをアップロードするには、s3:PutObject アクセス許可を追加する必要があります。

ドキュメントステップ

- aws:assertAwsResourceProperty - EKSInstanceId パラメータで指定された値のオペレーティングシステムが Linux であることを確認します。
- aws:runCommand - オペレーティングシステムおよび Amazon EKS に関連するログファイルを収集し、/var/log ディレクトリ内のアーカイブに圧縮します。
- aws:branch - LogDestination パラメータに値が指定されたかどうかを確認します。
- aws:runCommand - LogDestination パラメータで指定した S3 バケットにログアーカイブをアップロードします。

AWS-CreateEKSClusterWithFargateProfile

説明

AWS-CreateEKSClusterWithFargateProfile ランブックは、 を使用して Amazon Elastic Kubernetes Service (Amazon EKS) クラスターを作成します AWS Fargate。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ClusterName

  タイプ: 文字列

  説明: (必須) クラスターの一意の名前。

- ClusterRoleArn

  タイプ: 文字列

  説明: (必須) Kubernetes コントロールプレーンがユーザーに代わって AWS API オペレーションを呼び出すためのアクセス許可を提供する IAM ロールの ARN。

- FargateProfileName

  タイプ: 文字列

  説明: (必須) Fargate プロファイルの名前。

- FargateProfileRoleArn

  タイプ: 文字列

  説明: (必須) Amazon EKS Pod 実行 IAM ロールの ARN。

- FargateProfileSelectors

  タイプ: 文字列

  説明: (必須) ポッドを Fargate プロファイルに一致させるセレクタ。

- SubnetIds

  タイプ: StringList

  説明: (必須) Amazon EKS クラスターに使用するサブネットの IDs。Amazon EKS は、ノードと Kubernetes コントロールプレーン間の通信のために、これらのサブネットに Elastic Network Interface を作成します。少なくとも 2 つのサブネット ID を指定する必要があります。

- EKSEndpointPrivateAccess

型: ブール値

デフォルト: True

説明: (オプション) この値を に設定`True`して、クラスターの Kubernetes API サーバーエンドポイントへのプライベートアクセスを許可します。プライベートアクセスを有効にした場合、クラスターの VPC 内からの Kubernetes API リクエストは、プライベート VPC エンドポイントを使用します。プライベートアクセスを無効にし、クラスターにノードまたはポッドがある場合は、ノードまたは Fargate AWS Fargate ポッドとの通信に必要な CIDR ブロックが `publicAccessCidrs`に含まれていることを確認してください。

- EKSEndpointPublicAccess

  型: ブール値

  デフォルト: False

  説明: (オプション) この値を に設定`False`して、クラスターの Kubernetes API サーバーエンドポイントへのパブリックアクセスを無効にします。パブリックアクセスを無効にすると、クラスターの Kubernetes API サーバーは、起動した VPC 内からのみリクエストを受信できます。

- PublicAccessCIDRs

  タイプ: StringList

  説明: (オプション) クラスターのパブリック Kubernetes API サーバーエンドポイントへのアクセスが許可されている CIDR ブロック。指定した CIDR ブロック外のアドレスからエンドポイントへの通信は拒否されます。プライベートエンドポイントアクセスを無効にしていて、クラスターにノードまたは Fargate ポッドがある場合は、必要な CIDR ブロックを指定していることを確認してください。

- SecurityGroupIds

  タイプ: StringList

  説明: (オプション) Amazon EKS によってアカウントで作成された Elastic Network Interface に関連付ける 1 つ以上のセキュリティグループを指定します。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- CreateEKSCluster (aws:executeAwsApi) - Amazon EKS クラスターを作成します。
- VerifyEKSClusterIsActive (aws:waitForAwsResourceProperty) - クラスターの状態が であることを確認しますACTIVE。
- CreateFargateProfile (aws:executeAwsApi) - クラスターの Fargate を作成します。
- VerifyFargateProfileIsActive (aws:waitForAwsResourceProperty) - Fargate プロファイルの状態がであることを確認しますACTIVE。

出力

CreateEKSCluster.CreateClusterResponse

説明: CreateCluster API コールから受信したレスポンス。

CreateFargateProfile.CreateFargateProfileResponse

説明: CreateFargateProfile API コールから受信したレスポンス。

AWS-CreateEKSClusterWithNodegroup

説明

AWS-CreateEKSClusterWithNodegroup ランブックは、容量のノードグループを使用して Amazon Elastic Kubernetes Service (Amazon EKS) クラスターを作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ClusterName

  タイプ: 文字列

  説明: (必須) クラスターの一意の名前。
- ClusterRoleArn

  タイプ: 文字列

  説明: (必須) Kubernetes コントロールプレーンがユーザーに代わって AWS API オペレーションを呼び出すためのアクセス許可を提供する IAM ロールの ARN。

- NodegroupName

  タイプ: 文字列

  説明: (必須) ノードグループの一意の名前。

- NodegroupRoleArn

  タイプ: 文字列

  説明: (必須) ノードグループに関連付ける IAM ロールの ARN。Amazon EKS ワーカーノード kubelet デーモンは、ユーザーに代わって APIs を AWS 呼び出します。ノードは、IAM インスタンスプロファイルおよび関連ポリシーを通じて、これらの API コールのアクセス許可を受け取ります。ノードを起動してクラスターに登録する前に、起動するときに使用するノード用の IAM ロールを作成する必要があります。

- SubnetIds

  タイプ: StringList

  説明: (必須) Amazon EKS クラスターに使用するサブネットの IDs。Amazon EKS は、ノードと Kubernetes コントロールプレーン間の通信のために、これらのサブネットに Elastic Network Interface を作成します。少なくとも 2 つのサブネット ID を指定する必要があります。

- EKSEndpointPrivateAccess

  型: ブール値

  デフォルト: True

  説明: (オプション) この値を に設定`True`して、クラスターの Kubernetes API サーバーエンドポイントへのプライベートアクセスを許可します。プライベートアクセスを有効にした場合、クラスターの VPC 内からの Kubernetes API リクエストは、プライベート VPC エンドポイントを使用します。プライベートアクセスを無効にし、クラスターにノードまたはポッドがある場合は、ノードまたは Fargate AWS Fargate ポッドとの通信に必要な CIDR ブロックが `publicAccessCidrs`に含まれていることを確認してください。

- EKSEndpointPublicAccess

  型: ブール値

  デフォルト: False

説明: (オプション) この値を に設定Falseして、クラスターの Kubernetes API サーバーエンドポイントへのパブリックアクセスを無効にします。パブリックアクセスを無効にすると、クラスターの Kubernetes API サーバーは、起動した VPC 内からのみリクエストを受信できます。

- PublicAccessCIDRs

  タイプ: StringList

  説明: (オプション) クラスターのパブリック Kubernetes API サーバーエンドポイントへのアクセスが許可されている CIDR ブロック。指定した CIDR ブロック外のアドレスからエンドポイントへの通信は拒否されます。プライベートエンドポイントアクセスを無効にしていて、クラスターにノードまたは Fargate ポッドがある場合は、必要な CIDR ブロックを指定していることを確認してください。

- SecurityGroupIds

  タイプ: StringList

  説明: (オプション) Amazon EKS によってアカウントで作成された Elastic Network Interface に関連付ける 1 つ以上のセキュリティグループを指定します。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSubnets
- eks:CreateCluster
- eks:CreateNodegroup
- eks:DescribeCluster
- eks:DescribeNodegroup
- iam:CreateServiceLinkedRole
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:PassRole

ドキュメントステップ

- CreateEKSCluster (aws:executeAwsApi) - Amazon EKS クラスターを作成します。
- VerifyEKSClusterIsActive (aws:waitForAwsResourceProperty) - クラスターの状態が であることを確認しますACTIVE。
- CreateNodegroup (aws:executeAwsApi) - クラスターのノードグループを作成します。
- VerifyNodegroupIsActive (aws:waitForAwsResourceProperty) - ノードグループの状態が であることを確認しますACTIVE。

出力

- `CreateEKSCluster.CreateClusterResponse`: `CreateCluster` API コールから受信したレスポンス。
- `CreateNodegroup.CreateNodegroupResponse`: `CreateNodegroup` API コールから受信したレスポンス。

AWS-DeleteEKSCluster

説明

このランブックは、ノードグループや Fargate プロファイルなど、Amazon EKS クラスターに関連付けられているリソースを削除します。必要に応じて、すべてのセルフマネージド型ノード、ノードの作成に使用される AWS CloudFormation スタック、クラスターの VPC CloudFormation スタックを削除できます。クラスターの削除の詳細については、Amazon EKS ユーザーガイドの「クラスターの削除」を参照してください。

> **Note**
>
> クラスター内にロードバランサーと関連付けられているアクティブなサービスがある場合は、クラスターを削除する前にそれらのサービスを削除する必要があります。これを行わない場合は、システムがロードバランサーを削除できなくなります。`AWS-DeleteEKSCluster` ランブックを実行する前にサービスを検索および削除するには、次の手順に従います。

クラスター内のサービスを検索して削除するには

1. Kubernetes コマンドラインユーティリティ kubectl をインストールします。詳細については、「Amazon EKS ユーザーガイド」の「kubectl のインストール」を参照してください。
2. クラスターで実行されているすべてのサービスを一覧表示するには、次のコマンドを実行します。

```
kubectl get svc --all-namespaces
```

3. EXTERNAL-IP 値が関連付けられているサービスをすべて削除するには、次のコマンドを実行します。これらのサービスの前面にはロードバランサーが置かれているため、そのロードバランサーや関連するリソースを適切に解放するためには、これらのサービスを Kubernetes から削除する必要があります。

```
kubectl delete svc
service-name
```

これで、AWS-DeleteEKSCluster ランブックを実行できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- EKSClusterName

  タイプ: 文字列

  説明: (必須) 削除される Amazon EKS クラスターの名前。

- VPCCloudFormationStack

  タイプ: 文字列

  説明: (オプション) 削除される EKS クラスターの VPC の AWS CloudFormation スタック名。これにより、VPC の AWS CloudFormation スタックと、スタックによって作成されたリソースが削除されます。

- VPCCloudFormationStackRole

  タイプ: 文字列

  説明: (オプション) VPC CloudFormation スタックを削除するために が AWS CloudFormation 引き受ける IAM ロールの ARN。 は、ロールの認証情報 AWS CloudFormation を使用してユーザーに代わって呼び出しを行います。

- SelfManagedNodeStacks

  タイプ: 文字列

  説明: (オプション) セルフマネージドノードの AWS CloudFormation スタック名のカンマ区切りリスト。これにより、セルフマネージドノードの AWS CloudFormation スタックが削除されます。

- SelfManagedNodeStacksRole

  タイプ: 文字列

  説明: (オプション) セルフマネージド型ノードスタックを削除するために が AWS CloudFormation 引き受ける IAM ロールの ARN。 は、ロールの認証情報 AWS CloudFormation を使用してユーザーに代わって呼び出しを行います。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- sts:AssumeRole
- eks:ListNodegroups
- eks:DeleteNodegroup
- eks:ListFargateProfiles
- eks:DeleteFargateProfile
- eks:DeleteCluster
- cfn:DescribeStacks
- cfn:DeleteStack

ドキュメントステップ

- aws:executeScript - DeleteNodeGroups: EKS クラスター内のすべてのノードグループを検索および削除します。
- aws:executeScript - DeleteFargateProfiles: EKS クラスター内のすべてのFargateプロファイルを検索および削除します。
- aws:executeScript - DeleteSelfManagedNodes: すべてのセルフマネージドノードと、それらノードの作成に使用された CloudFormation スタックを削除します。
- aws:executeScript - DeleteEKSCluster: EKS クラスターを削除します。
- aws:executeScript - DeleteVPCCloudFormationStack: VPC CloudFormation スタックを削除します。

AWS-MigrateToNewEKSSelfManagedNodeGroup

説明

AWS-MigrateToNewEKSSelfManagedNodeGroup ランブックは、既存のアプリケーションを移行する新しい Amazon Elastic Kubernetes Service (Amazon EKS) Linux ノードグループを作成するのに役立ちます。詳細については、「Amazon EKS ユーザーガイド」の「新しいノードグループへの移行」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- OldStackName

  タイプ: 文字列

  説明: (必須) 既存の AWS CloudFormation スタックの名前またはスタック ID。

- NewStackName

  タイプ: 文字列

  説明: (オプション) 新しいノードグループ用に作成された新しい AWS CloudFormation スタックの名前。このパラメータの値を指定しない場合、スタック名は の形式を使用して作成されますNewNodeGroup-*ClusterName*-*AutomationExecutionID*。

- ClusterControlPlaneSecurityGroup

  タイプ: 文字列

  説明: (オプション) ノードが Amazon EKS コントロールプレーンとの通信に使用するセキュリティグループの ID。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたセキュリティグループが使用されます。

- NodeInstanceType

タイプ: 文字列

説明: (オプション) 新しいノードグループに使用するインスタンスタイプ。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたインスタンスタイプが使用されます。

- NodeGroupName

  タイプ: 文字列

  説明: (オプション) 新しいノードグループの名前。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたノードグループ名が使用されます。

- NodeAutoScalingGroupDesiredCapacity

  タイプ: 文字列

  説明: (オプション) 新しいスタックの作成時にスケールするノードの必要数。この数値は、 NodeAutoScalingGroupMinSize 値以上、 以下である必要がありますNodeAutoScalingGroupMaxSize。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたノードグループの希望する容量が使用されます。

- NodeAutoScalingGroupMaxSize

  タイプ: 文字列

  説明: (オプション) ノードグループがスケールアウトできるノードの最大数。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたノードグループの最大サイズが使用されます。

- NodeAutoScalingGroupMinSize

  タイプ: 文字列

  説明: (オプション) ノードグループがスケールインできるノードの最小数。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたノードグループの最小サイズが使用されます。

- NodeImageId

  タイプ: 文字列

  説明: (オプション) ノードグループに使用する Amazon Machine Image (AMI) のID。

- NodeImageIdSSMParam

  タイプ: 文字列

  説明: (オプション) ノードグループに使用する AMI のパブリック Systems Manager パラメータ。

- NodeVolumeSize

  タイプ: 文字列

  説明: (オプション) GiB 単位のノードのルートボリュームのサイズ。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたノードボリュームサイズが使用されます。

- NodeVolumeType

  タイプ: 文字列

  説明: (オプション) ノードのルートボリュームに使用する Amazon EBS ボリュームのタイプ。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたボリュームタイプが使用されます。

- KeyName

  タイプ: 文字列

  説明: (オプション) ノードに割り当てるキーペア。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたキーペアが使用されます。

- サブネット

  タイプ: StringList

  説明: (オプション) 新しいノードグループに使用するサブネット IDs のカンマ区切りリスト。このパラメータの値を指定しない場合、既存の AWS CloudFormation スタックで指定されたサブネットが使用されます。

- DisableIMDSv1

  型: ブール値

  説明: (オプション) インスタンスメタデータサービスバージョン 1 (IMDSv1) を無効にするtrueには、 を指定します。デフォルトでは、ノードは IMDSv1 と IMDSv2 をサポートします。

- BootstrapArguments

タイプ: 文字列

説明: (オプション) ノードブートストラップスクリプトに渡す追加の引数。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- DetermineParameterValuesForNewNodeGroup (aws:executeScript) - 新しいノードグループに使用するパラメータ値を収集します。

- CreateStack (aws:createStack) - 新しいノードグループの AWS CloudFormation スタックを作成します。
- GetNewStackNodeInstanceRole (aws:executeAwsApi) - ノードインスタンスロールを取得します。
- GetNewStackSecurityGroup (aws:executeAwsApi) - ステップはノードセキュリティグループを取得します。
- AddIngressRulesToNewNodeSecurityGroup (aws:executeAwsApi) - 新しく作成されたセキュリティグループに進入ルールを追加し、以前のノードグループに割り当てられたものからのトラフィックを受け入れることができるようにします。
- AddIngressRulesToOldNodeSecurityGroup (aws:executeAwsApi) - イングレスルールを以前のセキュリティグループに追加し、新しく作成したノードグループに割り当てられたグループからのトラフィックを受け入れることができるようにします。
- VerifyStackComplete (aws:assertAwsResourceProperty) - 新しいスタックステータスが であることを確認しますCREATE_COMPLETE。

出力

DetermineParameterValuesForNewNodeGroup.NewStackParameters - 新しいスタックの作成に使用されるパラメータ。

GetNewStackNodeInstanceRole.NewNodeInstanceRole - 新しいノードグループのノードインスタンスロール。

GetNewStackSecurityGroup.NewNodeSecurityGroup - 新しいノードグループのセキュリティグループの ID。

DetermineParameterValuesForNewNodeGroup.NewStackName - 新しいノードグループの AWS CloudFormation スタック名。

CreateStack.StackId - 新しいノードグループの AWS CloudFormation スタック ID。

AWSPremiumSupport-TroubleshootEKSCluster

説明

AWSPremiumSupport-TroubleshootEKSCluster ランブックは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスター、基盤となるインフラストラクチャに関する一般的な問題を診断し、推奨される修復手順を提供します。

> **Important**
>
> AWSPremiumSupport-* ランブックにアクセスするには、エンタープライズサポートまたはビジネスサポートサブスクリプションが必要です。詳細については、AWS「サポートプランの比較」を参照してください。

S3BucketName パラメータの値を指定すると、指定した Amazon Simple Storage Service (Amazon S3) バケットのポリシーステータスが自動化によって評価されます。EC2 インスタンスから収集されたログのセキュリティを支援するために、ポリシーステータス isPublic が true に設定されている場合、またはアクセスコントロールリスト (ACL) が All Users Amazon S3 事前定義済みグループに READ|WRITE アクセス許可を付与している場合、ログはアップロードされません。Amazon S3 の定義済みグループの詳細については、Amazon Simple Storage Service ユーザーガイドの「Amazon S3 の定義済みグループ」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ClusterName

タイプ: 文字列

説明: (必須) トラブルシューティングする Amazon EKS クラスターの名前。

- S3BucketName

タイプ: 文字列

説明: (必須) ランブックによって生成されたレポートをアップロードするプライベート Amazon S3 バケットの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

さらに、オートメーションを開始するユーザーまたはロールにアタッチされた AWS Identity and Access Management (IAM) ポリシーでは、ワーカーノードに推奨される最新の Amazon EKS Amazon Machine Image (AMI) を取得するために、次のパブリック AWS Systems Manager パラメータへの ssm:GetParameter オペレーションを許可する必要があります。

- 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

ランブックによって生成されたレポートを Amazon S3 バケットにアップロードするには、指定した Amazon S3 バケットに次の権限が必要です。

- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:PutObject

ドキュメントステップ

- aws:executeAwsApi - 指定した Amazon EKS クラスターの詳細を収集します。
- aws:executeScript - Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、Auto Scaling グループ、AMI および Amazon EC2 GPU グラフィックインスタンスのタイプの詳細を収集します。
- aws:executeScript - Amazon EKS クラスターの仮想プライベートクラウド (VPC)、サブネット、ネットワークアドレス変換 (NAT) ゲートウェイ、サブネットルート、セキュリティグループ、ネットワークアクセスコントロールリスト (ACL) の詳細を収集します。
- aws:executeScript - アタッチされた IAM インスタンスプロファイルとロールポリシーの詳細を収集します。

- aws:executeScript - S3BucketName パラメータで指定した Amazon S3 バケットの詳細を収集します。
- aws:executeScript - Amazon VPC サブネットをパブリックまたはプライベートに分類します。
- aws:executeScript - Amazon EKS クラスターの一部として必要なタグが Amazon VPC サブネットにないかを確認します。
- aws:executeScript - Elastic Load Balancing サブネットに必要なタグが Amazon VPC サブネット にないかを確認します。
- aws:executeScript - ワーカーノードの Amazon EC2 インスタンスが最新の Amazon EKS の最適化された AMI を使用しているかどうかを確認します
- aws:executeScript - Amazon VPC セキュリティグループがワーカーノードにアタッチされているか、必要なタグがあるかどうかを確認します。
- aws:executeScript - Amazon EKS クラスターとワーカーノードの Amazon VPC セキュリティグループのルールをチェックして、Amazon EKS クラスターへの推奨進入ルールを確認します。
- aws:executeScript - Amazon EKS クラスターとワーカーノードの Amazon VPC セキュリティグループのルールをチェックして、Amazon EKS クラスターへの推奨退出ルールを確認します。
- aws:executeScript - Amazon VPC サブネットのネットワーク ACL 設定をチェックします。
- aws:executeScript - ワーカーノードの Amazon EC2 インスタンスに必要な管理ポリシーがあるかどうかを確認します。
- aws:executeScript - Auto Scaling グループにクラスターの自動スケーリングに必要なタグがあるかどうかを確認します。
- aws:executeScript - ワーカーノードの Amazon EC2 インスタンスがインターネットに接続されているかどうかを確認します。
- aws:executeScript - 前のステップの出力に基づいてレポートを生成します。S3BucketName パラメータに値を指定すると、生成されたレポートが Amazon S3 バケットにアップロードされます。

AWSSupport-TroubleshootEKSWorkerNode

説明

AWSSupport-TroubleshootEKSWorkerNode ランブックは、Amazon Elastic Compute Cloud (Amazon EC2) ワーカーノードと Amazon Elastic Kubernetes Service (Amazon EKS) クラスターを分析し、ワーカーノードがクラスターに参加できない一般的な原因を特定してトラブルシューティン

グするのに役立ちます。ランブックには、特定されたあらゆる問題の解決に役立つガイダンスが出力されます。

> **Important**
>
> この自動化を正常に実行するには、Amazon EC2 ワーカーノードの状態は `running` で、Amazon EKS クラスターの状態は `ACTIVE` でなければなりません。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ClusterName

  タイプ: 文字列

  説明: (必須) Amazon EKS クラスターの名前。
- WorkerID

  タイプ: 文字列

説明: (必須) クラスターへの参加に失敗した Amazon EC2 ワーカーノードの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:assertAwsResourceProperty - ClusterName パラメータで指定した Amazon EKS クラスターが存在し、ACTIVE 状態にあることを確認します。
- aws:assertAwsResourceProperty - WorkerID パラメータで指定した Amazon EC2 ワーカーノードが存在し、running 状態にあることを確認します。
- aws:executeScript - ワーカーノードがクラスターに参加できない潜在的原因を特定するのに役立つ Python スクリプトを実行します。

AWS-UpdateEKSCluster

説明

AWS-UpdateEKSCluster ランブックは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターを、使用する Kubernetes バージョンに更新するのに役立ちます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ClusterName

タイプ: 文字列

説明: (必須) Amazon EKS クラスターの名前。

- バージョン

タイプ: 文字列

説明: (必須) クラスターを更新する Kubernetes バージョン。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- eks:DescribeUpdate
- eks:UpdateClusterVersion

ドキュメントステップ

- aws:executeAwsApi - Amazon EKS クラスターで使用される Kubernetes バージョンを更新します。
- aws:waitForAwsResourceProperty - 更新ステータスが になるまで待ちますSuccessful。

AWS-UpdateEKSManagedNodeGroup

説明

AWS-UpdateEKSManagedNodeGroup ランブックは、Amazon Elastic Kubernetes Service (Amazon EKS) マネージドノードグループを更新するのに役立ちます。Version または Configuration の更新を選択できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ClusterName

  タイプ: 文字列

  説明: (必須) 更新するノードグループを持つクラスターの名前。

- NodeGroupName

  タイプ: 文字列

  説明: (必須) 更新するノードグループの名前。

- UpdateType

  タイプ: 文字列

  有効値: [ノードグループバージョンの更新] | [ノードグループ構成の更新]

  デフォルト: ノードグループバージョンの更新

  説明: (必須) ノードグループで実行する更新のタイプ。

以下のパラメーターは `Version` の更新タイプにのみ適用されます。

- AMIReleaseVersion

  タイプ: 文字列

説明: (オプション) 使用する Amazon EKS の最適化された AMI のバージョン。デフォルトでは、最新バージョンが使用されます。

- ForceUpgrade

  型: ブール値

  説明: (オプション) この値が true の場合は、Pod の中断時に予算違反があった場合でも、アップグレードが失敗することはありません。

- KubernetesVersion

  タイプ: 文字列

  説明: (オプション) ノードグループを更新する Kubernetes バージョン。

- LaunchTemplateId

  タイプ: 文字列

  説明: (オプション) 起動テンプレートの ID。

- LaunchTemplateName

  タイプ: 文字列

  説明: (オプション) 起動テンプレートの名前。

- LaunchTemplateVersion

  タイプ: 文字列

  説明: (オプション) Amazon Elastic Compute Cloud (Amazon EC2) がテンプレートバージョンを起動します。このパラメーターは、ノードグループが起動テンプレートから作成された場合にのみ有効です。

以下のパラメーターは `Configuration` の更新タイプにのみ適用されます。

- AddOrUpdateNodeGroupLabels

  型: StringMap

  説明: (オプション) 追加または更新する Kubernetes ラベル。

- AddOrUpdateKubernetesTaintsEffect

タイプ: StringList

説明: (オプション) 追加または更新する Kubernetes テイント。

- MaxUnavailableNodeGroups

  タイプ: 整数

  デフォルト: 0

  説明: (オプション) バージョン更新中に一度に使用不可となるノードの最大数。

- MaxUnavailablePercentageNodeGroup

  タイプ: 整数

  デフォルト: 0

  説明: (オプション) バージョン更新中に使用できないノードの割合。

- NodeGroupDesiredSize

  タイプ: 整数

  デフォルト: 0

  説明: (オプション) マネージド型ノードグループが保持する必要があるノードの数。

- NodeGroupMaxSize

  タイプ: 整数

  デフォルト: 0

  マネージド型ノードグループがスケールアウトできるノードの最大数。

- NodeGroupMinSize

  タイプ: 整数

  デフォルト: 0

  説明: (オプション) マネージド型ノードグループがスケールインできるノードの最小数。

- RemoveKubernetesTaintsEffect

タイプ: StringList

説明: (オプション) 削除する Kubernetes テイント。

- RemoveNodeGroupLabels

  タイプ: StringList

  説明: (オプション) 削除するラベルのコンマ区切りのリスト。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- eks:UpdateNodegroupConfig
- eks:UpdateNodegroupVersion

ドキュメントステップ

- aws:executeScript - ランブックの入力パラメータに指定した値に従って Amazon EKS クラスターノードグループを更新します。
- aws:waitForAwsResourceProperty - クラスターの更新ステータスが Successful になるのを待ちます。

AWS-UpdateEKSSelfManagedLinuxNodeGroups

説明

AWS-UpdateEKSSelfManagedLinuxNodeGroups ランブックは、 AWS CloudFormation スタックを使用することで、Amazon Elastic Kubernetes Service (Amazon EKS) クラスター内の自己管理型の管理型ノードグループを更新します。

クラスターで自動スケーリングを使用している場合は、このランブックを使用する前にデプロイを 2 つのレプリカにスケールダウンすることをお勧めします。

デプロイでのレプリカを 2 にスケールするには

1. Kubernetes コマンドラインユーティリティ kubectl をインストールします。詳細については、Amazon EKS ユーザーガイドの「kubectl のインストール」を参照してください。
2. 以下のコマンドを実行してください。

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. AWS-UpdateEKSSelfManagedLinuxNodeGroups ランブックを実行してください。
4. デプロイを必要な数のレプリカにスケールバックする際は、次のコマンドを実行します。

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ClusterName

  タイプ: 文字列

説明: (必須) Amazon EKS クラスターの名前。

- NodeGroupName

  タイプ: 文字列

  説明: (必須) マネージド型ノードグループの名前。

- ClusterControlPlaneSecurityGroup

  タイプ: 文字列

  説明: (必須) コントロールプレーンセキュリティグループの ID。

- DisableIMDSv1

  型: ブール値

  説明: (オプション) インスタンスメタデータサービスバージョン 1 (IMDSv1) および IMDSv2 を許可するかどうかを決定します。

- KeyName

  タイプ: 文字列

  説明: (オプション) インスタンスのキーの名前。

- NodeAutoScalingGroupDesiredCapacity

  タイプ: 文字列

  説明: (オプション) ノードグループが保持する必要があるノードの数。

- NodeAutoScalingGroupMaxSize

  タイプ: 文字列

  説明: (オプション) ノードグループがスケールアウトできるノードの最大数。

- NodeAutoScalingGroupMinSize

  タイプ: 文字列

  説明: (オプション) ノードグループがスケールインできるノードの最小数。

- NodeInstanceType

タイプ: 文字列

デフォルト: t3.large

説明: (オプション) ノードグループに使用するインスタンスタイプ。

- NodeImageId

  タイプ: 文字列

  説明: (オプション) ノードグループに使用する Amazon Machine Image (AMI) のID。

- NodeImageIdSSMParam

  タイプ: 文字列

  デフォルト: /aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

  説明: (オプション) ノードグループに使用する AMI のパブリック Systems Manager パラメータ。

- StackName

  タイプ: 文字列

  説明: (必須) ノードグループの更新に使用される AWS CloudFormation スタックの名前。

- サブネット

  タイプ: 文字列

  説明: (必須) クラスターに使用させるサブネットの ID をカンマ区切りにしたリスト。

- VpcId

  タイプ: 文字列

  デフォルト: Default

  説明: (必須) クラスターがデプロイされている仮想プライベートクラウド (VPC)。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- eks:CreateCluster
- eks:CreateNodegroup
- eks:DeleteNodegroup
- eks:DeleteCluster
- eks:DescribeCluster
- eks:DescribeNodegroup
- eks:ListClusters
- eks:ListNodegroups
- eks:UpdateClusterConfig
- eks:UpdateNodegroupConfig

ドキュメントステップ

- aws:executeScript - ランブックの入力パラメータに指定した値に従って Amazon EKS クラスターノードグループを更新します。
- aws:waitForAwsResourceProperty - AWS CloudFormation スタックの更新ステータスが返されるのを待ちます。

AWSSupport-SetupK8sApiProxyForEKS

説明

AWSSupport-SetupK8sApiProxyForEKS オートメーションランブックは、Amazon Elastic Kubernetes Service クラスターエンドポイントへのコントロールプレーン API コールを行うためのプロキシとして機能する AWS Lambda 関数を作成する方法を提供します。これは、タスクを自動化し、Amazon EKS クラスターの問題をトラブルシューティングするためにコントロールプレーン API コールを行う必要があるランブックの構成要素として機能します。

> **Important**
>
> この自動化によって作成されたすべてのリソースにはタグが付けられ、簡単に見つけることができます。使用されるタグは次のとおりです。
>
> - AWSSupport-SetupK8sApiProxyForEKS: true

> **Note**
>
> - オートメーションはヘルパーランブックであり、スタンドアロンランブックとして実行することはできません。これは、Amazon EKS クラスターへのコントロールプレーン API コールを必要とするランブックの子オートメーションとして呼び出されます。
> - 不要なコストが発生しないように、使用後に必ずCleanupオペレーションを実行してください。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ClusterName

  タイプ: 文字列

  説明: (必須) Amazon Elastic Kubernetes Service クラスターの名前。
- Operation

  タイプ: 文字列

説明: (必須) 実行するオペレーション: アカウントで Lambda 関数をSetupプロビジョニングし、セットアップフェーズの一部として作成されたリソースのプロビジョニングを解除Cleanupします。

使用できる値: Setup | Cleanup

デフォルト: セットアップ

- LambdaRoleArn

  タイプ: 文字列

  説明: (オプション) 関数が必要な AWS のサービスとリソースにアクセスできるようにする AWS Lambda IAM ロールの ARN。ロールが指定されていない場合、この Systems Manager Automation は、管理ポリシー Automation-K8sProxy-Role-<ExecutionId> AWSLambdaBasicExecutionRoleと を含む名前で、アカウントに Lambda の IAM ロールを 1 つ作成しますAWSLambdaVPCAccessExecutionRole。

動作の仕組み

ランブックは次のステップを実行します。

- オートメーションが子実行として実行されていることを確認します。ランブックは、スタンドアロンランブックとして呼び出されると機能しません。これは、ランブックが単独で意味のある作業を実行しないためです。
- 指定されたクラスターのプロキシ Lambda 関数の既存の AWS CloudFormation スタックをチェックします。
  - スタックが存在する場合、既存のインフラストラクチャは再作成せずに再利用されます。
  - リファレンスカウンターは、同じクラスターの別のランブックによって再利用されている場合、ランブックがインフラストラクチャを削除しないようにタグを使用して維持されます。
- 呼び出しに指定されたオペレーションタイプ (Setup/Cleanup) を実行します。
  - セットアップ： 既存のリソースを作成または記述します。

    クリーンアップ： インフラストラクチャが他のランブックで使用されていない場合、プロビジョニングされたリソースを削除します。

必要な IAM アクセス許可

AutomationAssumeRole パラメータには、渡 LambdaRoleArnされないという以下のアクセス許可が必要です。

- 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

LambdaRoleArn が指定されている場合、オートメーションはロールを作成する必要はなく、次のアクセス許可を除外できます。

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

が渡されない場合に必要なアクセス許可を示すポリシーの例
AutomationAssumeRoleLambdaRoleArnを次に示します。

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

が渡された場合LambdaRoleArnは、パブリッククラスター用に AWSLambdaBasicExecutionRole ポリシーがアタッチされていること、さらにプライベートクラスター用に AWSLambdaVPCAccessExecutionRole がアタッチされていることを確認してください。

作成されたリソース

Setup オペレーション中に次のリソースが作成されます。

1. AWS Lambda 関数
2. IAM ロール: 指定されていない場合は Lambda 実行ロール。
3. CloudWatch ロググループ (Lambda ログ)

Lambda 関数と実行ロールは、*Cleanup*オペレーションが実行されるまで保持されます。Lambda ロググループは 30 日間、または手動で削除されるまで保持されます。

指示

ランブックは、子オートメーションとして他のランブック内から実行されるように設計されたヘルパーユーティリティです。これにより、親ランブックが Amazon EKS K8s コントロールプレーン API コールを実行できるようにするインフラストラクチャの作成が容易になります。ランブックを使用するには、親オートメーションのコンテキストから以下のステップに従います。

1. セットアップフェーズ: オペレーションを に設定して Amazon EKS K8s コントロールプレーン API コールを行うランブックから aws:executeAutomationアクションオペレーションを使用してオートメーションを呼び出しますSetup。

   入力パラメータの例：

   ```
   {
     "AutomationAssumeRole": "<role-arn>",
   ```

```
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Setup"
}
```

aws:executeAutomation ステップの出力には、プロキシ Lambda 関数の ARN が含まれます。

2. Lambda プロキシの使用: API コールパスとベアラートークンのリスト Lambda.Client.invoke(...)を含む boto3の を使用して、aws:executeScriptアクション内で Lambda 関数を呼び出します。Lambda 関数は、ベアラートークンを認可ヘッダーの一部として渡すことで、指定されたパスへの HTTP GET呼び出しを実行します。

   Lambda 呼び出しイベントの例：

```
{
    "ApiCalls": ["/api/v1/pods/", ...],
    "BearerToken": "..."
}
```

> **Note**
>
> ベアラートークンは、親オートメーションスクリプトの一部として生成する必要があります。親ランブックを実行するプリンシパルに、指定された Amazon EKS クラスターへの読み取り専用アクセス許可があることを確認する必要があります。

3. クリーンアップフェーズ: オペレーションを に設定して Amazon EKS K8s コントロールプレーン API コールを行うランブックから aws:executeAutomationアクションオペレーションを使用してオートメーションを呼び出しますCleanup。

   入力パラメータの例：

```
{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Cleanup"
}
```

自動化ステップ

1. ValidateExecution

- オートメーションがスタンドアロン実行として実行されていないことを確認します。

2. CheckForExistingStack
   - 指定されたクラスター名に対して AWS CloudFormation スタックが既にプロビジョニングされているかどうかを確認します。
   - スタックの存在ステータスと、削除しても安全かどうかを返します。
3. BranchOnIsStackExists
   - スタックの存在に基づいて分岐する決定ステップ。
   - 既存のスタック名を更新するか、オペレーションの分岐に進むルート。
4. UpdateStackName
   - `StackName` 変数を既存のスタックの名前で更新します。
   - スタックが既に存在する場合にのみ実行されます。
5. BranchOnOperation
   - `Operation` パラメータ (`Setup`/) に基づいてオートメーションをルーティングしますCleanup。
   - の場合Setup: 新しいスタックを作成するか、既存のリソースを記述するようにルーティングします。
   - の場合Cleanup: 安全に削除できる場合、スタックの削除に進みます。
6. GetClusterNetworkConfig
   - VPC 設定を取得するための Amazon EKS クラスターについて説明します。
   - エンドポイント、VPC ID、サブネット IDs、セキュリティグループ ID、CA データを取得します。
7. ProvisionResources
   - 必要なリソースを持つ AWS CloudFormation スタックを作成します。
   - 必要なネットワーク設定で Lambda 関数をプロビジョニングします。
   - 追跡と管理のためにすべてのリソースにタグを付けます。
8. DescribeStackResources
   - 作成済み/既存のスタックに関する情報を取得します。
   - プロビジョニングされた Lambda 関数の ARN を取得します。
9. BranchOnIsLambdaDeploymentRequired
   - Lambda コードのデプロイが必要かどうかを判断します。
   - 新しく作成されたスタックのデプロイのみに進みます。

10DeployLambdaFunctionCode

- デプロイパッケージを使用して Lambda 関数コードをデプロイします。
- プロキシ実装で関数を更新します。

11AssertLambdaAvailable

- Lambda 関数コードの更新が成功したことを確認します。
- 関数が `Successful`状態になるまで待ちます。

12PerformStackCleanup

- AWS CloudFormation スタックと関連するリソースを削除します。
- `Cleanup` オペレーション中または `Setup`オペレーションの失敗時に実行されます。

出力

LambdaFunctionArn: プロキシ Lambda 関数の ARN

リファレンス

Systems Manager Automation

- オートメーションを実行する
- オートメーションの設定
- 自動化ワークフローのサポート

AWSSupport-TroubleshootEbsCsiDriversForEks

説明

`AWSSupport-TroubleshootEbsCsiDriversForEks` ランブックは、Amazon Elastic Kubernetes Service (Amazon EKS) および Amazon EBS Container Storage Interface (CSI) ドライバーの問題における Amazon Elastic Block Store ボリュームマウントに関する問題のトラブルシューティングに役立ちます。

> **Important**
>
> 現在、 で実行されている Amazon EBS CSI ドライバー AWS Fargate はサポートされていません。

動作の仕組み

ランブックは、以下の大まかなステップAWSSupport-TroubleshootEbsCsiDriversForEksを実行します。

- ターゲット Amazon EKS クラスターが存在し、アクティブ状態になっているかどうかを確認します。
- アドオンが Amazon EKS マネージドかセルフマネージドかに基づいて、Kubernetes API コールを実行するために必要な認証リソースをデプロイします。
- Amazon EBS CSI コントローラーのヘルスチェックと診断を実行します。
- ノードロールとサービスアカウントロールに対して IAM アクセス許可チェックを実行します。
- 指定されたアプリケーションポッドの永続的なボリューム作成の問題を診断します。
- node-to-podスケジューリングを確認し、ポッドイベントを調べます。
- 関連する Kubernetes ログとアプリケーションログを収集し、指定された Amazon S3 バケットにアップロードします。
- ノードのヘルスチェックを実行し、Amazon EC2 エンドポイントとの接続を検証します。
- 永続的なボリュームブロックデバイスのアタッチメントとマウントステータスを確認します。
- トラブルシューティング中に作成された認証インフラストラクチャをクリーンアップします。
- すべての診断結果を組み合わせた包括的なトラブルシューティングレポートを生成します。

> **Note**
>
> - Amazon EKS クラスターの認証モードは、 APIまたは に設定する必要がありますAPI_AND_CONFIG_MAP。Amazon EKS Access エントリを使用することをお勧めします。ランブックには、必要な API コールを実行するための Kubernetes ロールベースのアクセスコントロール (RBAC) アクセス許可が必要です。
> - Lambda 関数の IAM ロール (LambdaRoleArn パラメータ) を指定しない場合、オートメーションはAutomation-K8sProxy-Role-<ExecutionId>アカウントに という名前のロールを作成します。このロールには、 管理ポリシーAWSLambdaBasicExecutionRoleと が含まれますAWSLambdaVPCAccessExecutionRole。
> - 一部の診断ステップでは、Amazon EKS ワーカーノードを Systems Manager マネージドインスタンスにする必要があります。ノードが Systems Manager マネージドインスタン

スでない場合、Systems Manager アクセスを必要とするステップはスキップされますが、他のチェックは続行されます。

- 自動化には、認証インフラストラクチャリソースを削除するクリーンアップステップが含まれています。このクリーンアップステップは、前のステップが失敗しても実行され、AWS アカウント内の孤立したリソースを防ぐのに役立ちます。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

/

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

指示

次の手順に従って自動化を設定します。

1. TroubleshootEbsCsiDriversForEks-SSM-Role アカウントに SSM 自動化ロールを作成します。信頼関係に以下のポリシーが含まれていることを確認します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 以下のポリシーを IAM ロールにアタッチして、指定されたリソースで指定されたアクションを実行するために必要なアクセス許可を付与します。

- 同じ AWS リージョンの Amazon S3 バケットに実行ログとリソースログをアップロードする場合は、 の を自分の arn:{partition}:s3:::BUCKET_NAME/* として置き換えますOptionalRestrictPutObjects。
  - Amazon S3 バケットは正しい Amazon S3 バケットを指す必要があります。 S3BucketName
  - を指定しない場合、このアクセス許可はオプションです。 S3BucketName
  - Amazon S3 バケットはプライベートで、SSM オートメーションを実行するのと同じ AWS リージョンにある必要があります。

```
{
    "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. Amazon EKS クラスター RBAC (ロールベースのアクセスコントロール) に必要なアクセス許可を付与します。推奨されるアプローチは、Amazon EKS クラスターでアクセスエントリを作成することです。

Amazon EKS コンソールで、クラスターに移動します。Amazon EKS アクセスエントリの場合は、アクセス設定が API_AND_CONFIG_MAPまたは に設定されていることを確認しますAPI。アクセスエントリの認証モードを設定する手順については、「アクセスエントリの設定」を参照してください。

[アクセスエントリの作成] を選択してください。

- IAM プリンシパル ARN で、前のステップで SSM 自動化用に作成した IAM ロールを選択します。
- [タイプ] では、Standard[] を選択します。

4. アクセスポリシーを追加します。
   - アクセススコープで、 を選択しますCluster。
   - ポリシー名 で、 を選択しますAmazonEKSAdminViewPolicy。

   [Add policy] を選択します。

   アクセスエントリを使用して Kubernetes API アクセス許可を管理していない場合は、ConfigMap aws-auth を更新し、IAM ユーザーまたはロール間にロールバインディングを作成する必要があります。IAM エンティティに次の読み取り専用 Kubernetes API アクセス許可があることを確認します。
   - 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. オートメーション AWSSupport-TroubleshootEbsCsiDriversForEks を実行する (コンソール)
6. [Execute automation] (オートメーションを実行) を選択します。

7. 入力パラメータには、次のように入力します。

- AutomationAssumeRole (オプション):
  - 説明: (オプション) SSM Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。Kubernetes API コールを許可するには、ロールを Amazon EKS クラスターアクセスエントリまたは RBAC アクセス許可に追加する必要があります。
  - 型: `AWS::IAM::Role::Arn`
  - 例: `TroubleshootEbsCsiDriversForEks-SSM-Role`
- EksClusterName:
  - 説明: ターゲット Amazon Elastic Kubernetes Service (Amazon EKS) クラスターの名前。
  - 型: `String`
- ApplicationPodName:
  - 説明: Amazon EBS CSI ドライバーに問題がある Kubernetes アプリケーションポッドの名前。
  - 型: `String`
- ApplicationNamespace:
  - 説明: Amazon EBS CSI ドライバーに問題があるアプリケーションポッドの Kubernetes 名前空間。
  - 型: `String`
- EbsCsiControllerDeploymentName (オプション):
  - 説明: (オプション) Amazon EBS CSI コントローラーポッドのデプロイ名。
  - 型: `String`
  - デフォルト: `ebs-csi-controller`
- EbsCsiControllerNamespace (オプション):
  - 説明: (オプション) Amazon EBS CSI コントローラーポッドの Kubernetes 名前空間。
  - 型: `String`
  - デフォルト: `kube-system`
- S3BucketName (オプション):
  - 説明: (オプション) トラブルシューティングログがアップロードされるターゲット Amazon S3 バケット名。
  - 型: `AWS::S3::Bucket::Name`

- LambdaRoleArn (オプション):
  - 説明: (オプション) AWS Lambda 関数が必要な AWS サービスとリソースにアクセスできるようにする IAM ロールの ARN。
  - 型: `AWS::IAM::Role::Arn`

[実行] を選択します。

8. 完了したら、出力セクションで実行の詳細な結果を確認します。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- オートメーションワークフローのサポート

Amazon EBS CSI ドライバーの詳細については、「Amazon EBS CSI ドライバー」を参照してください。

Elastic Beanstalk

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Elastic Beanstalk。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-CollectElasticBeanstalkLogs
- AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming
- AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications
- AWSSupport-TroubleshootElasticBeanstalk

AWSSupport-CollectElasticBeanstalkLogs

説明

AWSSupport-CollectElasticBeanstalkLogs ランブックは、一般的な問題のトラブルシューティングに役立つように、Elastic Beanstalk によって起動された Amazon Elastic Compute Cloud (Amazon EC2) Windows Server インスタンスから AWS Elastic Beanstalk に関連するログファイルを収集します。自動化によって関連するログファイルが収集される間、一時ディレクトリの作成、ログファイルの一時ディレクトリへのコピー、ログファイルのアーカイブへの圧縮など、ファイルシステム構造が変更されます。このアクティビティにより、Amazon EC2 インスタンスで CPUUtilization が増加する可能性があります。CPUUtilization の詳細については、Amazon CloudWatch ユーザーガイドの「インスタンスメトリクス」を参照してください。

S3BucketName パラメータの値を指定すると、指定した Amazon Simple Storage Service (Amazon S3) バケットのポリシーステータスが自動化によって評価されます。Amazon EC2 インスタンスから収集されたログのセキュリティを支援するために、ポリシーステータス isPublic が true に設定されている場合、またはアクセスコントロールリスト (ACL) が All Users Amazon S3 事前定義済みグループに READ|WRITE アクセス許可を付与している場合、ログはアップロードされません。Amazon S3 の定義済みグループの詳細については、Amazon Simple Storage Service ユーザーガイドの「Amazon S3 の定義済みグループ」を参照してください。

S3BucketName パラメータの値を指定しない場合、自動化は、オートメーションを実行する場所 AWS リージョン のデフォルトの Elastic Beanstalk Amazon S3 バケットにログバンドルをアップロードします。ディレクトリは、 elasticbeanstalk- *region* - *accountID* の構造に従って名前が付けられます。*#####*および *accountID* の値は、オートメーションを実行するリージョンおよび AWS アカウント によって異なります。ログバンドルは resources/environments/logs/bundle/ *environmentID* / *instanceID* ディレクトリに保存されます。*environmentID* と *instanceID* の値は、Elastic Beanstalk 環境と、ログを収集している Amazon EC2 インスタンスによって異なります。

デフォルトでは、Elastic Beanstalk 環境の Amazon EC2 インスタンスにアタッチされた AWS Identity and Access Management (IAM) インスタンスプロファイルには、環境のデフォルトの Elastic Beanstalk Amazon S3 バケットにバンドルをアップロードするために必要なアクセス許可があります。S3BucketName パラメータの値を指定する場合、Amazon EC2 インスタンスにアタッチされたインスタンスプロファイルは、指定した Amazon S3 バケットとパスの s3:GetBucketAcl、s3:GetBucketPolicy、s3:GetBucketPolicyStatus および s3:PutObject アクションを許可する必要があります。

> **Note**
>
> この自動化では、Amazon EC2 インスタンスにアタッチされたルート Amazon Elastic Block Store (Amazon EBS) ボリュームの空きディスク容量 500 MB 以上が必要です。ルートボリュームに十分な空きディスク容量がない場合、自動化は停止します。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- EnvironmentId

  タイプ: 文字列

  説明: (必須) ログバンドルを収集する Elastic Beanstalk 環境の ID。
- InstanceId

  タイプ: 文字列

  (必須) ログバンドルを収集する Elastic Beanstalk 環境の Amazon EC2 インスタンスの ID。

- S3BucketName

  タイプ: 文字列

  (オプション) アーカイブされたログをアップロードする Amazon S3 バケット。

- S3BucketPath

  タイプ: 文字列

  (オプション) ログバンドルをアップロードする Amazon S3 バケット。このパラメータは、S3BucketName パラメータの値を指定していない場合は無視されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:SendCommand
- ssm:DescribeInstanceInformation
- ec2:DescribeInstances

ドキュメントステップ

- aws:assertAwsResourceProperty - InstanceId パラメータで指定した Amazon EC2 インスタンスが AWS Systems Managerによって管理されていることを確認します。
- aws:assertAwsResourceProperty - InstanceId パラメータで指定した Amazon EC2 インスタンスが Windows Server インスタンスであることを確認します。
- aws:runCommand - インスタンスが Elastic Beanstalk 環境の一部であるかどうか、ログをバンドルするのに十分なディスク容量があるかどうか、ログのアップロード先となる Amazon S3 バケットがパブリックかどうかをチェックします。
- aws:runCommand - ログファイルを収集し、S3BucketName パラメータで指定された Amazon S3 バケット、または値が指定されていない場合は Elastic Beanstalk 環境のデフォルトバケットにアーカイブをアップロードします。

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

説明

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ランブックは、指定した AWS Elastic Beanstalk (Elastic Beanstalk) 環境で口グ記録を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- EnvironmentId

  タイプ: 文字列

  説明: (必須) 口グ記録を有効にする Elastic Beanstalk 環境の ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution

- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

ドキュメントステップ

- aws:executeAwsApi - EnvironmentId パラメータで指定された Elastic Beanstalk 環境での口グ記録を有効にします。
- aws:waitForAwsResourceProperty - 環境のステータスが Ready に変わるまで待機します。
- aws:executeScript - Elastic Beanstalk 環境で口グ記録が有効化されていることを確認します。

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

説明

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications ランブックは、指定した AWS Elastic Beanstalk (Elastic Beanstalk) 環境の通知を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- EnvironmentId

  タイプ: 文字列

  説明: (必須) 通知を有効にする Elastic Beanstalk 環境の ID。

- TopicArn

  タイプ: 文字列

  説明: (必須) 通知を送信する Amazon Simple Notification Service (Amazon SNS) トピックの ARN。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticbeanstalk:DescribeConfigurationSettings
- elasticbeanstalk:DescribeEnvironments
- elasticbeanstalk:UpdateEnvironment

ドキュメントステップ

- aws:executeAwsApi - EnvironmentId パラメータで指定した Elastic Beanstalk 環境の通知を有効にします。
- aws:waitForAwsResourceProperty - 環境のステータスが Ready に変わるまで待機します。
- aws:executeScript - 通知が Elastic Beanstalk 環境で有効になっていることを確認します。

AWSSupport-TroubleshootElasticBeanstalk

説明

AWSSupport-TroubleshootElasticBeanstalk ランブックは、 AWS Elastic Beanstalk 環境が Degradedまたは Severe状態にある潜在的な理由のトラブルシューティングに役立ちます。このオートメーションは、Elastic Beanstalk 環境に関連付けられている次の AWS リソースをチェックします。

- ロードバランサー、 AWS CloudFormation スタック、Amazon EC2 Auto Scaling グループ、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、仮想プライベートクラウド (VPC) の設定詳細。
- サブネットに関連付けられているセキュリティグループのルール、ルートテーブル、ネットワークアクセスコントロールリスト (ACL) に関するネットワーク設定の問題。
- Elastic Beanstalk エンドポイントへの接続とパブリックインターネットアクセスを検証します。
- ロードバランサーのステータスを検証します。
- Amazon EC2 インスタンスのステータスを確認します。
- Elastic Beanstalk 環境からログバンドルを取得し、オプションでファイルを にアップロードします サポート。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ApplicationName

  タイプ: 文字列

  説明: (必須) Elastic Beanstalk アプリケーションの名前。

- EnvironmentName

  タイプ: 文字列

  説明: (必須) Elastic Beanstalk 環境の名前。

- AWSS3UploaderLink

  タイプ: 文字列

  説明: (オプション) Elastic Beanstalk 環境からログバンドルをアップロード サポート するために から提供される URL。このオプションは、 サポート プランを購入し、サポートケースを開いたお客様のみが使用できます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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*

ドキュメントステップ

- aws:executeScript - 自動化を開始した AWS Identity and Access Management (IAM) プリンシパルに、ランブックで定義されているすべてのアクションを実行するために必要なアクセス許可があることを確認します。
- aws:branch - 前のステップの結果に基づいてワークフローを分岐させます。
- aws:executeScript - ロードバランサー、 AWS CloudFormation スタック、Auto Scaling グループ、Amazon EC2 インスタンス、VPC 設定など、Elastic Beanstalk 環境に関する情報を収集します。
- aws:executeScript - VPC 内のサブネットに関連付けられているルートテーブルと ACL のネットワーク接続の問題を確認します。
- aws:executeScript - Amazon EC2 インスタンスに関連するセキュリティグループルールのネットワーク接続の問題をチェックします。
- aws:executeScript - Amazon EC2 インスタンスのステータスチェックを確認します。
- aws:executeScript - Elastic Beanstalk 環境のログバンドルのリンクを生成します。
- aws:executeScript - ログバンドルを にアップロードします サポート。
- aws:executeScript - Elastic Beanstalk 環境のステータスに影響を与える可能性のある問題のトラブルシューティングに役立つアクションアイテムのレポートを出力します。

エラスティックロードバランシング

AWS Systems Manager Automation は、Elastic Load Balancing 用の事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-DropInvalidHeadersForALB
- AWS-EnableCLBAccessLogs
- AWS-EnableCLBConnectionDraining
- AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing
- AWSConfigRemediation-EnableELBDeletionProtection
- AWSConfigRemediation-EnableLoggingForALBAndCLB
- AWSSupport-TroubleshootCLBConnectivity
- AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing
- AWS-UpdateALBDesyncMitigationMode
- AWS-UpdateCLBDesyncMitigationMode

AWSConfigRemediation-DropInvalidHeadersForALB

説明

AWSConfigRemediation-DropInvalidHeadersForALB ランブックは、無効なヘッダーを含む HTTP ヘッダーを削除できるように、指定した Application Load Balancer を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- LoadBalancerArn

  タイプ: 文字列

  説明: (必須) 無効なヘッダーを削除するロードバランサーの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

ドキュメントステップ

- aws:executeAwsApi - LoadBalancerArn パラメータで指定したロードバランサーの無効なヘッダーの削除設定を有効にします。
- aws:executeScript - LoadBalancerArn パラメータで指定したロードバランサーで無効なヘッダーの削除設定が有効になっていることを確認します。

AWS-EnableCLBAccessLogs

説明

AWS-EnableCLBAccessLogs ランブックは、Classic Load Balancer のアクセスログを有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- EmitInterval

  タイプ: 整数

  有効な値: 5 | 60

  デフォルト: 60

  説明: (オプション) アクセスログを数分で発行する間隔。
- LoadBalancerNames

  タイプ: 文字列

  説明: (必須) アクセスログを有効にする Classic Load Balancer のカンマ区切りリスト。
- S3BucketName

  タイプ: 文字列

  説明: (必須) アクセスログが保存されている Amazon Simple Storage Service (Amazon S3) バケットの名前。
- S3BucketPrefix

タイプ: 文字列

説明: (オプション) Amazon S3 バケット用に作成した論理階層。例: my-bucket-prefix/prod。プレフィックスが指定されていない場合、ログはバケットのルートレベルに配置されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- elasticloadbalancing:ModifyLoadBalancerAttributes

ドキュメントステップ

- aws:executeAwsApi - LoadBalancerNamesパラメータで指定した Classic Load Balancer のアクセスログを有効にします。

出力

EnableCLBAccessLogs.SuccessesLoadBalancers - アクセスログが正常に有効になったロードバランサー名のリスト。

EnableCLBAccessLogs.FailedLoadBalancers - アクセスログの有効化が失敗したロードバランサー名の MapList と、失敗した理由。

AWS-EnableCLBConnectionDraining

説明

AWS-EnableCLBConnectionDraining ランブックは、指定されたタイムアウト値への Classic Load Balancer (CLB) の接続ドレインを有効にします。Connection Draining を使用すると、CLB は、登録解除中のリクエストや異常なリクエストを完了できます。指定したタイムアウトは、インスタンスが登録解除として報告される前に接続が存続している時間です。CLBs、Classic Load Balancer ユーザーガイドの「Classic Load Balancer の接続ドレイニングを設定する」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- LoadBalancerName

  タイプ: 文字列

  説明: (必須) Connection Draining を有効にするロードバランサーの名前。
- [ConnectionTimeout]

  タイプ: 整数

  有効な値: 1 ~ 3600

  デフォルト: 300

  説明: (必須) ロードバランサーの接続タイムアウト値。タイムアウト値は 1 ~ 3600 秒の間で設定できます。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

ドキュメントステップ

- ModifyLoadBalancerConnectionDraining (aws:executeAwsApi): 接続ドレインを有効にし、指定したロードバランサーの指定されたタイムアウト値を設定します。
- VerifyLoadBalancerConnectionDrainingEnabled (aws:assertAwsResourceProperty): ロードバランサーで Connection Draining が有効になっていることを確認します。
- VerifyLoadBalancerConnectionDrainingTimeout (aws:assertAwsResourceProperty): ロードバランサーの接続タイムアウト値が、指定した値と一致することを確認します。

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

説明

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing ランブックは、指定した Classic Load Balancer (CLB) のクロスゾーン負荷分散を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- LoadBalancerName

  タイプ: 文字列

  説明: (必須) クロスゾーン負荷分散を有効にする NLB の名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elb:DescribeLoadBalancerAttributes
- elb:ModifyLoadBalancerAttributes

ドキュメントステップ

- aws:executeAwsApi - LoadBalancerName パラメータで指定した CLB のクロスゾーンロードバランシングを有効にします。
- aws:assertAwsResourceProperty - クロスゾーン負荷分散が CLB で有効になっていることを確認します。

AWSConfigRemediation-EnableELBDeletionProtection

説明

AWSConfigRemediation-EnableELBDeletionProtection ランブックは、指定した Elastic Load Balancing (ELB) の削除保護を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- LoadBalancerArn

  タイプ: 文字列

  説明: (必須) 削除保護を有効にする ELB の Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

ドキュメントステップ

- `aws:executeScript` - `LoadBalancerArn` パラメータで指定した ELB で削除保護を有効にします。

AWSConfigRemediation-EnableLoggingForALBAndCLB

説明

AWSConfigRemediation-EnableLoggingForALBAndCLB ランブックは、指定された AWS Application Load Balancer または Classic Load Balancer (CLB) のログ記録を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- LoadBalancerId

  タイプ: 文字列

  説明: (必須) Classic Load Balancer 名または Application Load Balancer ARN。
- S3BucketName

  タイプ: 文字列

  説明: (必須) Amazon S3 バケット名。
- S3BucketPrefix

  タイプ: 文字列

説明: (オプション) 例えば、Amazon Simple Storage Service (Amazon S3) バケット用に作成した論理階層 (my-bucket-prefix/prod など)。プレフィックスが指定されていない場合、ログはバケットのルートレベルに配置されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

ドキュメントステップ

- aws:executeScript - Classic Load Balancer または Application Load Balancer のログ記録を有効にし、検証します。

AWSSupport-TroubleshootCLBConnectivity

説明

AWSSupport-TroubleshootCLBConnectivity ランブックは、Classic Load Balancer (CLB) と Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの間の接続の問題をトラブルシューティングするのに役立ちます。また、クライアントと CLB 間の接続の問題についてもレビューします。このランブックでは、CLB のヘルスチェックのレビュー、ベストプラクティスが守られていることの確認、トラブルシューティングダッシュボードの作成も行います。オプションで、Amazon Simple Storage Service (Amazon S3) バケットに自動化の出力をアップロードできます。ただし、このランブックは、パブリックにアクセスできる S3 バケットへの出力のアップロードをサポートしていません。この自動化用に一時的な S3 バケットを作成することをお勧めします。

> **Important**
>
> このランブックを使用すると、作成したダッシュボードの料金が発生する可能性があります。詳細については、Amazon CloudWatch 料金表をご覧ください。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InvestigationType

  タイプ: 文字列

  有効な値: ベストプラクティス | 接続問題 | トラブルシューティングダッシュボード

  説明: (必須) ランブックに実行する操作。
- LoadBalancerName

  タイプ: 文字列

  説明: (必須) CLB の名前。
- S3Location

  タイプ: 文字列

  説明: (オプション) 自動化の結果を送信する S3 バケットの名前。パブリックにアクセス可能なバケットはサポートされません。S3 バケットがサーバー側の暗号化を使用している場

合、このオートメーションを実行するユーザーまたはロールには AWS KMS キーに対する kms:GenerateDataKey 権限が必要です。

- S3LocationPrefix

  タイプ: 文字列

  説明: (オプション) 自動化出力をアップロードする Amazon S3 キープレフィックス (サブフォルダ)。形式出力は、amzn-s3-demo-bucket/*S3LocationPrefix*/{{*InvestigationType*}}_{{automation:*EXECUTION_ID*}}.txt の形式で保存されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeScript - LoadBalancerName パラメータで指定した CLB が存在することを確認します。
- aws:branch - InvestigationType パラメータで指定した値に基づいて分岐させます。
- aws:executeScript - CLB への接続チェックを実行します。
- aws:executeScript - CLB 設定が Elastic Load Balancing のベストプラクティスに準拠していることを確認します。
- aws:executeScript - CLB 用の Amazon CloudWatch ダッシュボードを作成します。
- aws:executeScript - 自動化の結果を含むテキストファイルを作成し、S3Location パラメータで指定した Amazon S3 バケットにアップロードします。

出力

RunBestPractices.Summary

RunConnectivityChecks.Summary

CreateTroubleshootingDashboard.Output

UploadOutputToS3.Output

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

説明

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing ランブックは、指定した Network Load Balancer (NLB) のクロスゾーン負荷分散を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- LoadBalancerArn

  タイプ: 文字列

  説明: (必須) クロスゾーン負荷分散を有効にする NLB の Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

ドキュメントステップ

- aws:executeAwsApi - LoadBalancerArn パラメータで指定した NLB のクロスゾーンロードバランシングを有効にします。
- aws:executeScript - クロスゾーン負荷分散が NLB で有効になっていることを確認します。

AWS-UpdateALBDesyncMitigationMode

説明

AWS-UpdateALBDesyncMitigationMode ランブックは、Application Load Balancer (ALB) の非同期緩和モードを指定された緩和モードに更新します。非同期緩和モードは、ロードバランサーがアプリケーションにセキュリティリスクをもたらす可能性のあるリクエストを処理する方法を決定します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- LoadBalancerArn

  タイプ: 文字列

説明: (必須) 非同期緩和モードを変更する ALB の Amazon リソースネーム (ARN)。

- DesyncMitigationMode

  タイプ: 文字列

  有効な値: monitor | defensive | strictest

  説明: (必須) ALB で使用する緩和モード。非同期緩和モードの詳細については、Application Load Balancer ユーザーガイドの「非同期緩和モード」を参照してください。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

ドキュメントステップ

- VerifyLoadBalancerType (aws:assertAwsResourceProperty) - 次のステップに進む前に、`LoadBalancerArn`入力パラメータに指定された値がアプリケーションロードバランサー用であることを確認します。
- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - 指定された を使用するように ALB を更新します`DesyncMitigationMode`。
- VerifyLoadBalancerDesyncMitigationMode (aws:executeScript) - ターゲット ALB の非同期緩和モードが更新されていることを確認します。

出力

VerifyLoadBalancerDesyncMitigationMode.ModificationResult - ALB への変更を検証するスクリプトのメッセージペイロード。

AWS-UpdateCLBDesyncMitigationMode

説明

AWS-UpdateCLBDesyncMitigationMode ランブックは、Classic Load Balancer (CLB) の非同期緩和モードを指定された緩和モードに更新します。非同期緩和モードは、ロードバランサーがアプリケーションにセキュリティリスクをもたらす可能性のあるリクエストを処理する方法を決定します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- LoadBalancerName

  タイプ: 文字列

  説明: (必須) 非同期緩和モードを変更する CLB の名前。

- DesyncMitigationMode

  タイプ: 文字列

有効な値: monitor | defensive | strictest

説明: (必須) CLB で使用する緩和モード。非同期緩和モードの詳細については、Application Load Balancer ユーザーガイドの「非同期緩和モード」を参照してください。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:ModifyLoadBalancerAttributes

ドキュメントステップ

- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - 指定された を使用するように CLB を更新しますDesyncMitigationMode。
- VerifyLoadBalancerDesyncMitigationMode (aws:executeScript) - ターゲット CLB の非同期緩和モードが更新されていることを確認します。

出力

VerifyLoadBalancerDesyncMitigationMode.ModificationResult - CLB への変更を検証するスクリプトのメッセージペイロード。

Amazon EMR

AWS Systems Manager 自動化は、Amazon EMR 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-AnalyzeEMRLogs
- AWSSupport-DiagnoseEMRLogsWithAthena

AWSSupport-AnalyzeEMRLogs

説明

このランブックは、Amazon EMR クラスターでジョブを実行しているときのエラーを特定するのに役立ちます。このランブックは、ファイルシステム上の定義済みログのリストを分析し、定義済みのキーワードのリストを探します。これらのログエントリは Amazon CloudWatch Events イベントの作成に使用されるため、イベントに基づいて必要なアクションを実行できます。オプションで、ランブックは、選択した Amazon CloudWatch Logs ロググループにログエントリを公開します。このランブックは現在、ログファイル内の以下のエラーとパターンを検索しています。

- container_out_of_memory – YARN コンテナがメモリ不足になったため、実行中のジョブが失敗する可能性があります。
- yarn_nodemanager_health: コアノードまたはタスクノードのディスク容量が少なくなっているため、タスクを実行できなくなります。
- node_state_change: マスターノードはコアノードまたはタスクノードにアクセスできません。
- step_failure: EMR ステップが失敗しました。
- no_core_nodes_running: 現在実行中の CORE ノードはありません。クラスターは異常です。
- hdfs_missing_blocks: HDFS ブロックが不足しているため、データが失われる可能性があります。
- hdfs_high_util: HDFS の使用率が高いため、ジョブやクラスターの状態に影響する可能性があります。
- instance_controller_restart: インスタンスコントローラープロセスが再起動しました。このプロセスはクラスターの健全性にとって不可欠です。
- instance_controller_restart_legacy: インスタンスコントローラープロセスが再起動しました。このプロセスはクラスターの健全性にとって不可欠です。
- high_load: 高い負荷平均が検出されました。ノードのヘルスレポートに影響を与えたり、タイムアウトや速度低下の原因になる場合があります。
- yarn_node_blacklisted: コアノードまたはタスクノードが YARN によって実行中のタスクからブラックリストに登録されました。
- yarn_node_lost: コアノードまたはタスクノードが YARN によって LOST とマークされました。接続に問題がある可能性があります。

指定した `ClusterID` に関連するインスタンスは、 AWS Systems Managerで管理する必要があります。この自動化は 1 回実行することも、特定の時間間隔で実行するようにスケジュールするこ

とも、自動化によって以前に作成されたスケジュールを削除することもできます。このランブックは、Amazon EMR リリースバージョン 5.20 ~ 6.30 をサポートします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ClusterID

  タイプ: 文字列

  説明: (必須) 分析するノードログを持つクラスターの ID。
- Operation

  タイプ: 文字列

  有効な値: 1 回実行 | スケジュール | スケジュール削除

  説明: (必須) クラスターで実行する操作。
- IntervalTime

  タイプ: 文字列

有効な値: 5 分 | 10 分 | 15 分

説明: (オプション) オートメーションを実行する間の期間。このパラメータは、Operation パラメータの Schedule を指定した場合にのみ適用されます。

- LogToCloudWatchLogs

  タイプ: 文字列

  有効な値: はい | いいえ

  説明: (オプション) このパラメータの値を yes に指定すると、自動化は CloudWatchLogGroup パラメータで指定された名前で CloudWatch Logs ロググループを作成し、一致するログエントリを保存します。

- CloudwatchLogGroup

  タイプ: 文字列

  説明: (オプション) 一致するログエントリを保存する CloudWatch Logs ロググループの名前。このパラメータは、LogToCloudWatchLogs パラメータの yes を指定した場合にのみ適用されます。

- CreateLogInsightsDashboard

  タイプ: 文字列

  有効な値: はい | いいえ

  説明: (オプション) yes に指定すると、CloudWatch ダッシュボードがまだ存在していない場合は CloudWatch ダッシュボードが作成されます。このパラメータは、LogToCloudWatchLogs パラメータの yes を指定した場合にのみ適用されます。

- CreateMetricFilters

  タイプ: 文字列

  有効な値: はい | いいえ

  説明: (オプション) CloudWatch Logs ロググループのメトリクスフィルタを作成するかどうかについて yes を指定します。このパラメータは、LogToCloudWatchLogs パラメータの yes を指定した場合にのみ適用されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeAwsApi - ClusterID パラメータで指定された Amazon EMR クラスターに関する情報を収集します。
- aws:branch - 入力に基づいて分岐させます。
  - 指定した操作が Run Once または Schedule の場合:
    - aws:assertAwsResourceProperty - クラスターが使用可能であることを確認します。
    - aws:executeAwsApi - クラスター内で実行されているすべてのインスタンスの ID を収集します。
    - aws:assertAwsResourceProperty - SSM Agent がクラスター内のすべてのインスタンスで実行されていることを確認します。
    - aws:branch - 自動化を 1 回実行するように指定したか、スケジュールに従って実行するように指定したかに基づいて分岐させます。
      - 指定した操作が Run Once の場合:
        - aws:branch - LogToCloudWatchLogs パラメータで指定した値に基づいて分岐させます。
          - LogToCloudWatchLogs 値が yes の場合:
            - aws:executeScript - パラメータ CloudWatchLogGroup で指定された名前の CloudWatch Logs ロググループが既に存在するかどうかを確認します。存在しない場合、グループは指定された名前で作成されます。
            - aws:branch - CreateMetricFilters パラメータで指定した値に基づいて分岐させます。
              - CreateMetricFilters 値が yes の場合:
                - aws:executeAwsApi - メトリクスフィルターごとに 12 ステップが実行されます。
                - aws:branch - CreateLogInsightsDashboard パラメータで指定した値に基づいて分岐させます。
                  - CreateLogInsightsDashboard 値が yes の場合:

- aws:executeAwsApi - CloudWatchLogGroup パラメータで指定されたものと同じ名前で CloudWatch ダッシュボードを作成します (まだ存在しない場合)。
- CreateLogInsightsDashboard 値が no の場合:
- aws:runCommand - シェルスクリプトを実行して、クラスター内の各インスタンスのログパターンを検索します。
- CreateMetricFilters 値が no の場合:
- aws:branch - CreateLogInsightsDashboard パラメータで指定した値に基づいて分岐させます。
- CreateLogInsightsDashboard 値が yes の場合:
- aws:executeAwsApi - CloudWatchLogGroup パラメータで指定されたものと同じ名前で CloudWatch ダッシュボードを作成します (まだ存在しない場合)。
- CreateLogInsightsDashboard 値が no の場合:
- aws:runCommand - シェルスクリプトを実行して、クラスター内の各インスタンスのログパターンを検索します。
- LogToCloudWatchLogs 値が no の場合:
- aws:executeAwsApi - シェルスクリプトを実行して、クラスター内の各インスタンスのログパターンを検索します。
- 指定した操作が Schedule の場合:
- aws:createStack - このランブックをターゲットとする Amazon EventBridge イベントを作成します。
- 指定した操作が Remove Schedule の場合:
- aws:executeAwsApi - クラスターのスケジュールが存在することを確認します。
- aws:deleteStack - スケジュールを削除します。

出力

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstances.InstanceIDs

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists.output

FindLogPatternOnEMRNode.CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

説明

AWSSupport-DiagnoseEMRLogsWithAthena ランブックは、 AWS Glue Data Catalog との統合で Amazon Athena を使用して Amazon EMR ログを診断するのに役立ちます。Amazon Athena は、コンテナ、ノードログ、またはその両方について Amazon EMR ログファイルをクエリするために使用されます。特定の日付範囲またはキーワードベースの検索のオプションパラメータも指定します。

ランブックは、既存のクラスターの Amazon EMR ログの場所を自動的に取得することも、Amazon S3 ログの場所を指定することもできます。ログを分析するために、ランブックは次の操作を行います。

- AWS Glue データベースを作成し、Amazon EMR Amazon S3 ログの場所に対して Amazon Athena データ定義言語 (DDL) クエリを実行して、クラスターログのテーブルと既知の問題のリストを作成します。 Amazon S3
- データ操作言語 (DML) クエリを実行して、Amazon EMR ログ内の既知の問題パターンを検索します。クエリは、検出された問題のリスト、それらの出現数、および Amazon S3 ファイルパスで一致したキーワードの数を返します。
- 結果は、プレフィックス で指定した Amazon S3 バケットにアップロードされますsaw_diagnose_EMR_known_issues。
- ランブックは Amazon Athena クエリ結果を返します。結果、推奨事項、および事前定義されたサブセットから取得された Amazon ナレッジセンター (KC) 記事への参照が強調表示されます。
- 完了または失敗すると、 AWS Glue データベースと Amazon S3 バケットにアップロードされた既知の問題ファイルが削除されます。

動作の仕組み

は、Amazon Athena を使用して Amazon EMR ログの分析AWSSupport-DiagnoseEMRLogsWithAthenaを実行し、エラーを検出し、検出結果、推奨事項、関連するナレッジセンターの記事を強調します。

ランブックは次のステップを実行します。

- クラスター ID または Amazon S3 の場所を入力して Amazon EMR クラスターログの場所を取得し、ログの場所とサイズを取得します。
- ログの場所のサイズに基づいて Athena のコスト見積もりを提供します。
- Athena クエリを実行し、次のステップに進む前に、指定された IAM プリンシパルに承認をリクエストして、続行の承認を取得します。
- 指定された Amazon S3 バケットに既知の問題をアップロードし、 AWS Glue データベースとテーブルを作成します。
- Amazon EMR ログデータに対して Athena クエリを実行します。クエリは、日付範囲、キーワード、両方の基準で検索することも、提供された入力に基づいてフィルターなしで実行することもできます。
- 結果を分析して、検出結果、推奨事項、関連する KC 記事を強調します。
- Amazon Athena DML クエリ結果の出力リンク。
- 作成したデータベース、テーブル、アップロードされた既知の問題を削除して、環境をクリーンアップします。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

/

AutomationAssumeRole パラメータでは、ランブックを正常に使用するには、次のアクションが必要です。

- athena:GetQueryExecution
- athena:StartQueryExecution
- athena:GetPreparedStatement
- athena:CreatePreparedStatement
- glue:GetDatabase
- glue:CreateDatabase
- glue:DeleteDatabase

- glue:CreateTable
- glue:GetTable
- glue:DeleteTable
- elasticmapreduce:DescribeCluster
- s3:ListBucket
- s3:GetBucketVersioning
- s3:ListBucketVersions
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetObject
- s3:GetBucketLocation
- 料金:GetProducts
- 料金:GetAttributeValues
- 料金:DescribeServices
- 料金:ListPriceLists

Important

この自動化に必要なリソースのみにアクセスを制限するには、SSM サービスを信頼する IAM ロールに次のポリシーをアタッチします。パーティション、リージョン、アカウントを、実行ブックが実行されるパーティション、リージョン、およびアカウント番号の適切な値に置き換えます。

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

指示

次の手順に従って自動化を設定します。

1. 「 ドキュメント AWS Systems Manager 」のAWSSupport-DiagnoseEMRLogsWithAthena」に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 次の入力パラメータを入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指

定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ClusterID (必須):

  Amazon EMR クラスター ID。

- S3LogLocation (オプション):

  Amazon S3 Amazon EMR ログの場所。パス形式の URL Amazon S3 の場所を入力します。例: `s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/`。Amazon EMR クラスターが 30日以上終了している場合は、このパラメータを指定します。

- S3BucketName (必須):

  既知の問題のリストをアップロードする Amazon S3 バケット名、および Amazon Athena クエリの出力。バケットでは、ブロックパブリックアクセスが有効で、Amazon EMR クラスターと同じ AWS リージョンとアカウントにある必要があります。

- 承認者 (必須):

  アクションを承認または拒否できる AWS 認証済みプリンシパルのリスト。プリンシパルは、ユーザー名、ユーザー ARN、IAM ロール ARN、または IAM 継承ロール ARN のいずれかの形式を使用して指定できます。承認者の最大数は 10 です。

- FetchNodeLogsOnly (オプション):

  に設定すると`true`、オートメーションは Amazon EMR アプリケーションコンテナログを診断します。デフォルト値は `false` です。

- FetchContainersLogsOnly (オプション):

  に設定すると`true`、オートメーションは Amazon EMR コンテナログを診断します。デフォルト値は `false` です。

- EndSearchDate (オプション):

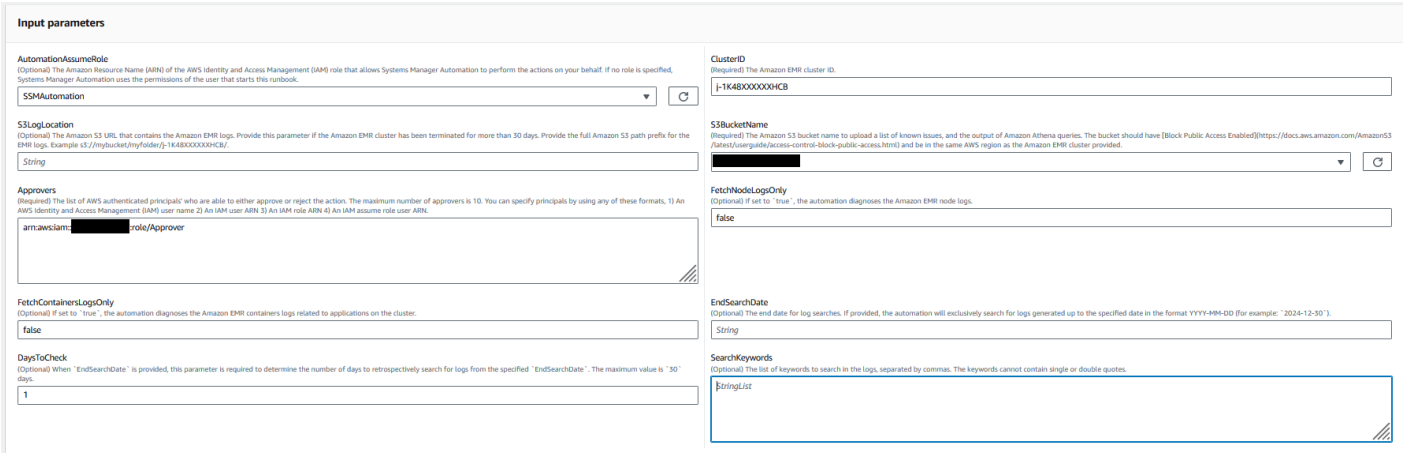
  ログ検索の終了日。指定した場合、オートメーションは指定された日付までに生成されたログを YYYY-MM-DD 形式でのみ検索します (例: `2024-12-30`) 。

- DaysToCheck (オプション):

  `EndSearchDate` が指定されている場合、このパラメータは、指定された から`EndSearchDate`ログを遡及的に検索する日数を決定するために必要です。最大値は `30` 日です。デフォルト値は `1` です。

- SearchKeywords (オプション):

  ログで検索するキーワードのリスト。カンマで区切られています。キーワードに一重引用符または二重引用符を含めることはできません。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。

   - getLogLocation:

     指定された Amazon S3 ログの場所を取得します。オートメーションが Amazon EMR クラスター ID からログの場所をクエリできない場合、ランブックは S3LogLocation入力パラメータを使用します。

   - branchOnValidLog:

     Amazon EMR ログの場所を確認します。ロケーションが有効な場合は、Amazon EMR ログでクエリを実行する際の Amazon Athena の潜在的なコストの見積もりに進みます。

   - estimateAthenaCosts:

     Amazon EMR ログのサイズを決定し、ログデータセットで Athena スキャンを実行するためのコスト見積もりを提供します。非商用リージョン (非AWS パーティション) の場合、このステップではコストを見積もることなくログサイズを提供します。コストは、指定されたリージョンの Athena 料金ドキュメントを使用して計算できます。

   - approveAutomation:

     指定された IAM プリンシパルの承認が自動化の次のステップに進むのを待ちます。承認通知には、Amazon EMR ログに対する Amazon Athena スキャンの推定コストと、自動化によってプロビジョニングされるリソースに関する詳細が含まれます。

- uploadKnownIssuesExecuteAthenaQueries:

  S3BucketName パラメータで指定された Amazon S3 バケットに事前定義された既知の問題をアップロードします。 AWS Glue データベースとテーブルを作成します。入力パラメータに基づいて AWS Glue 、データベースで Amazon Athena クエリを実行します。

- getQueryExecutionStatus:

  Amazon Athena クエリの実行が SUCCEEDED状態になるまで待ちます。Amazon Athena DML クエリは、Amazon EMR クラスターログのエラーと例外を検索します。

- analyzeAthenaResults:

  Amazon Athena の結果を分析し、事前定義されたマッピングセットから取得した検出結果、レコメンデーション、ナレッジセンター (KC) の記事を提供します。

- getAnalyzeResultsQuery1ExecutionStatus:

  クエリの実行が SUCCEEDED状態になるまで待ちます。Amazon Athena DML クエリは、前の DML クエリの結果を分析します。この分析クエリは、解決と KC 記事で一致した例外を返します。

- getAnalyzeResultsQuery2ExecutionStatus:

  クエリの実行が SUCCEEDED状態になるまで待ちます。Amazon Athena DML クエリは、前の DML クエリの結果を分析します。この分析クエリは、各 Amazon S3 ログパスで検出された例外/エラーのリストを返します。

- printAthenaQueriesMessage:

  Amazon Athena DML クエリ結果のリンクを出力します。

- cleanupResources:

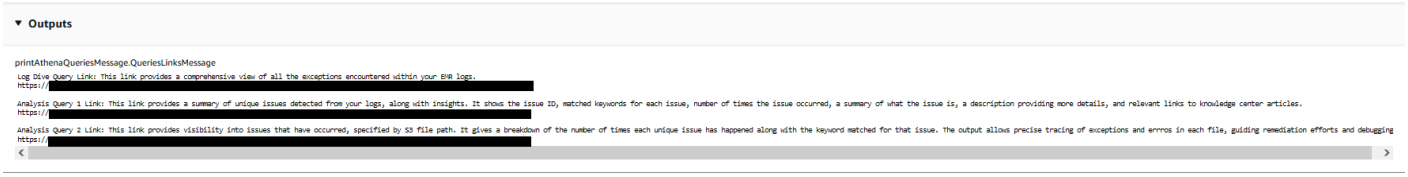
  作成された AWS Glue データベースを削除し、Amazon EMR ログバケットで作成された既知の問題ファイルを削除することで、リソースをクリーンアップします。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

   出力には、Athena クエリ結果の 3 つのリンクがあります。

- Amazon EMR クラスターログで見つかったすべてのエラーと頻繁に発生する例外のリストと、対応するログの場所 (Amazon S3 プレフィックス) 。
- Amazon EMR ログで一致した一意の既知の例外の概要と、トラブルシューティングに役立つ推奨される解決策と KC 記事。

- 詳細な診断をサポートするために、Amazon S3 ログパスに特定のエラーと例外が表示される場所に関する詳細。



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスドキュメント

- 詳細については、「Amazon EMR クラスターのトラブルシューティング」を参照してください。

Amazon OpenSearch Service

AWS Systems Manager Automation は、Amazon OpenSearch Service 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-DeleteOpenSearchDomain
- AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain
- AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups
- AWSSupport-TroubleshootOpenSearchRedYellowCluster
- AWSSupport-TroubleshootOpenSearchHighCPU

AWSConfigRemediation-DeleteOpenSearchDomain

説明

AWSConfigRemediation-DeleteOpenSearchDomain ランブックは DeleteDomain API を使用して指定された Amazon OpenSearch Service のドメインを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- DomainName

  タイプ: 文字列

  許容値: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  説明: (必須) 削除する Amazon OpenSearch Service ドメインの名前。
- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DeleteDomain
- es:DescribeDomain

ドキュメントステップ

- aws:executeScript - Amazon OpenSearch Service ドメイン名を入力として受け入れ、それを削除し、削除を検証します。

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

説明

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain ランブックは UpdateDomainConfig APIを使用して指定された Amazon OpenSearch Service ドメインで EnforceHTTPS を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- DomainName

  タイプ: 文字列

  許容値: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  説明: (必須) HTTPS を強制するために使用する Amazon OpenSearch Service ドメインの名前。

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

ドキュメントステップ

- aws:executeScript - DomainName パラメータで指定された Amazon OpenSearch Service ドメインの EnforceHTTPS エンドポイントオプションを有効にします。

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

説明

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups ランブックは UpdateDomainConfig API を使用して指定された Amazon OpenSearch Service ドメインでセキュリティグループ設定を更新します。

> **Note**
>
> AWS セキュリティグループは、Amazon Virtual Private Cloud (VPC) アクセス用に設定された Amazon OpenSearch Service ドメインにのみ適用でき、パブリックアクセス用に設定された Amazon OpenSearch Service ドメインには適用されません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- DomainName

  タイプ: 文字列

  説明: (必須) セキュリティグループの更新に使用する Amazon OpenSearch Service ドメインの名前。
- SecurityGroupList

  タイプ: StringList

  説明: (必須) Amazon OpenSearch Service ドメインの割り当てに使用するセキュリティグループの ID。
- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

- es:DescribeDomain
- es:UpdateDomainConfig

ドキュメントステップ

- aws:executeScript - DomainName パラメータで指定した Amazon OpenSearch Service ドメイン上のセキュリティグループ設定を更新します。

AWSSupport-TroubleshootOpenSearchRedYellowCluster

説明

AWSSupport-TroubleshootOpenSearchRedYellowCluster オートメーションランブックは、赤または黄色のクラスターのヘルスステータスの原因を特定し、クラスターを緑に戻す手順を説明するために使用されます。

動作の仕組み

ランブックは、赤または黄色のクラスターの原因のトラブルシューティングAWSSupport-TroubleshootOpenSearchRedYellowClusterに役立ち、クラスター設定とリソース使用率を分析して、この問題を解決するための次のステップを提供します。

ランブックは次のステップを実行します。

- ターゲットドメインに対して DescribeDomain API を呼び出して、クラスター設定を取得します。
- OpenSearch Service ドメインがインターネットベース (パブリック) か Amazon Virtual Private Cloud (VPC) ベースかを確認します。
- クラスター設定に応じて、パブリックまたは Amazon VPC ベースの AWS Lambda 関数を作成します。注: Lambda 関数には、クラスターに対して OpenSearch Service APIs を実行し、クラスターが赤または黄色の状態である理由を判断するトラブルシューティングコードが含まれています。
- Lambda 関数を削除します。
- 赤または黄色のクラスターの問題を解決するために実行されたチェックと、次に推奨されるステップを表示します。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ランブックを正常に使用するには、 LambdaExecutionRoleパラメータに次のアクションが必要です。

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface

LambdaExecutionRole ポリシーの概要：

以下は、このランブックに必要な AWS サービスおよびリソースにアクセスするためのアクセス許可を関数に付与する Lambda 関数の実行ロール (AWS Identity and Access Management (IAM) ロールの例です。詳細については、「Lambda 実行ロール」を参照してください。

> **Note**
>
> ec2:DescribeNetworkInterfaces、ec2:CreateNetworkInterface、および ec2:DeleteNetworkInterfaceは、Lambda 関数が Amazon VPC ネットワークインターフェイスを作成および管理できるようにするために、OpenSearch Service クラスターが Amazon VPC ベースである場合にのみ必要です。 https://docs.aws.amazon.com/opensearch-service/latest/developerguide/vpc.html詳細については、「Amazon VPC のリソースへのアウトバウンドネットワークの接続」および「Lambda 実行ロール」を参照してください。

```
        {
            "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"
                }

            ]
        }
```

指示

次の手順に従って自動化を設定します。

1. コンソールで AWSSupport-TroubleshootOpenSearchRedYellowCluster AWS Systems Manager に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 次の入力パラメータを入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- LambdaExecutionRole (必須):

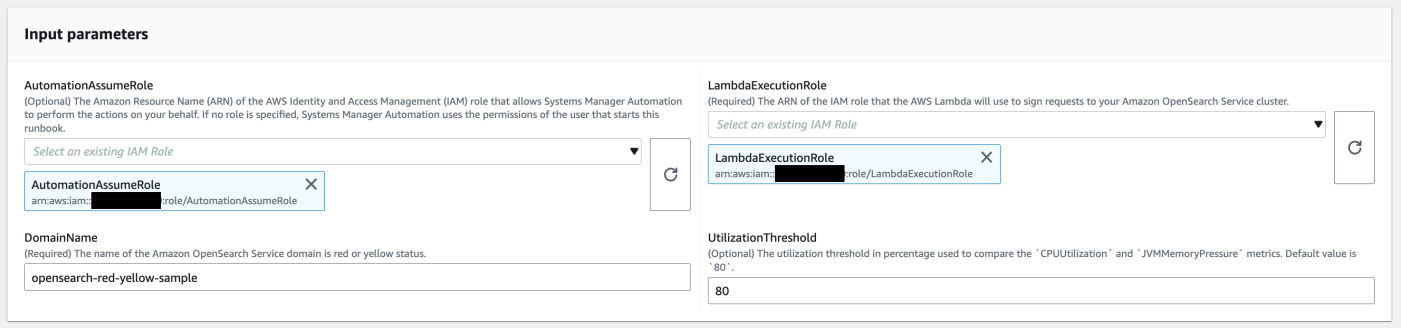
  Lambda が Amazon OpenSearch Service クラスターへのリクエストに署名するために使用する IAM ロールの ARN。

- DomainName (必須):

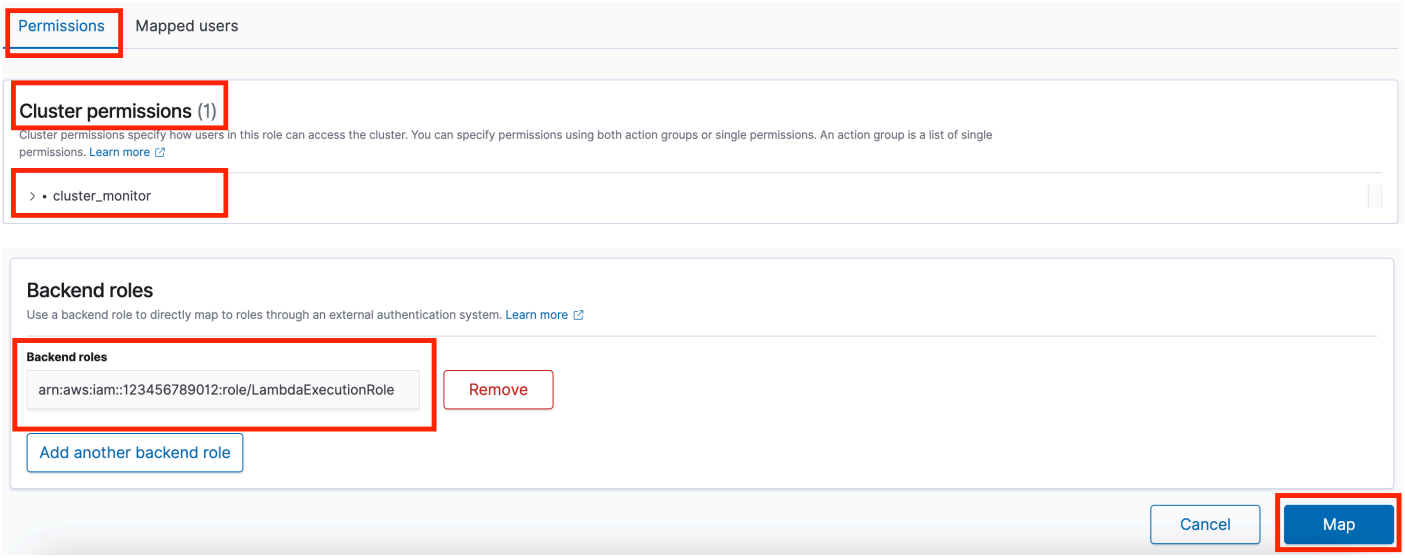
  赤または黄色のクラスターヘルスステータスを持つ OpenSearch Service ドメインの名前。

- UtilizationThreshold (オプション):

  CPUUtilization メトリクスと JVMMemoryPressure メトリクスの比較に使用される使用率のしきい値の割合。デフォルト値は 80 です。



4. OpenSearch Service クラスターできめ細かなアクセスコントロールを有効にしている場合は、`LambdaExecutionRole`ロール ARN が少なくとも アクセス`cluster_monitor`許可を持つロールにマッピングされていることを確認してください。



5. [実行] を選択します。
6. 自動化が開始されます。
7. 自動化ランブックは以下のステップを実行します。

- GetClusterConfiguration:

  OpenSearch Service クラスター設定を取得します。

- CreateAWSLambdaFunctionStack:

  を使用して、アカウントに一時的な Lambda 関数を作成します AWS CloudFormation。Lambda 関数は、OpenSearch Service APIs を実行するために使用されます。

- WaitForAWSLambdaFunctionStack:

  CloudFormation スタックが完了するまで待ちます。

- GetClusterMetricsFromCloudWatch:

  Amazon CloudWatch ClusterStatus、CPUUtilization、JVMMemoryPressure OpenSearch Service クラスター関連のメトリクスとその作成日を取得します。

- RunOpenSearchAPIs:

  Lambda 関数を使用して OpenSearch Service APIs、クラスターメトリクスデータを分析して、赤または黄色のクラスターステータスの原因を診断します。

- DeleteAWSLambdaFunctionStack:

  アカウントでこのオートメーションによって作成された Lambda 関数を削除します。

8. 完了したら、出力セクションで詳細な実行結果を確認します。

   - RootCause:

     クラスターの状態が赤または黄色になる原因として特定されたものの概要を示します。

   - IssueDescription:

     クラスターが赤または黄色の状態である理由の詳細と、クラスターを緑の状態に戻すためのステップについて説明します。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスドキュメント

- 詳細については、「Amazon OpenSearch Service のトラブルシューティング」を参照してください。

AWSSupport-TroubleshootOpenSearchHighCPU

説明

AWSSupport-TroubleshootOpenSearchHighCPU ランブックは、Amazon OpenSearch Service ドメインから診断データを収集し、CPU の高い問題をトラブルシューティングする自動化されたソリューションを提供します。

動作の仕組み

AWSSupport-TroubleshootOpenSearchHighCPU ランブックは、Amazon OpenSearch Service ドメインの CPU 使用率が高い場合のトラブルシューティングに役立ちます。

ランブックは次のステップを実行します。

- 指定された Amazon OpenSearch Service ドメインに対して DescribeDomain API を実行して、クラスターメタデータを取得します。
- Amazon OpenSearch Service ドメインがパブリックか Amazon VPC ベースかを確認し AWS CloudFormation、 の助けを借りてパブリックまたは Amazon VPC ベースの AWS Lambda 関数を作成します。
- Lambda 関数は、Amazon OpenSearch Service ドメインから診断データを取得します。
- AWS Step Functions ステートマシンを使用して複数の Lambda 関数の実行を調整し、より包括的なデータを収集します。
- デフォルトでは、収集されたデータを Amazon CloudWatch ロググループに 24 時間保存します。
- CloudWatch ロググループを除く、作成されたリソースを削除します。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ランブックを正常に使用するには、 LambdaExecutionRoleパラメータに次のアクションが必要です。

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface
- logs:CreateLogStream
- logs:PutLogEvents

Lambda 実行ロールは、このランブックに必要な AWS サービスとリソースにアクセスするためのアクセス許可を関数に付与します。詳細については、「Lambda 実行ロール」を参照してください。

> **Note**
>
> ec2:DescribeNetworkInterfaces、ec2:CreateNetworkInterface、および ec2:DeleteNetworkInterfaceは、Lambda 関数が Amazon VPC ネットワークイン

ターフェイスを作成および管理できるようにするために、OpenSearch Service クラスターが Amazon VPC ベースである場合にのみ必要です。 https://docs.aws.amazon.com/opensearch-service/latest/developerguide/vpc.html詳細については、「Amazon VPC のリソースへのアウトバウンドネットワークの接続」および「Lambda 実行ロール」を参照してください。

指示

次の手順に従って自動化を設定します。

1. コンソールで AWSSupport-TroubleshootOpenSearchHighCPU AWS Systems Manager に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 次の入力パラメータを入力します。
   - AutomationAssumeRole (オプション):

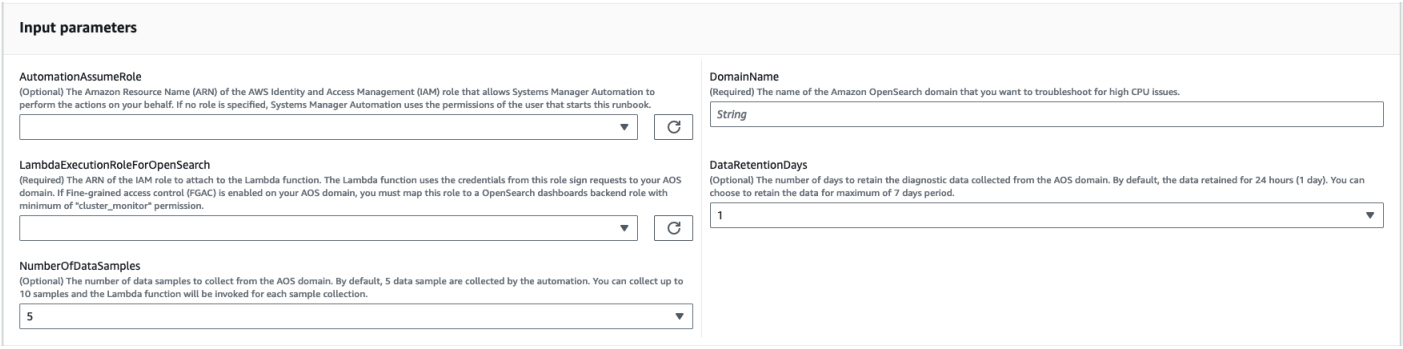
     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
   - DomainName (必須):

     CPU の大きな問題についてトラブルシューティングする Amazon OpenSearch Service ドメインの名前。
   - LambdaExecutionRoleForOpenSearch (必須):

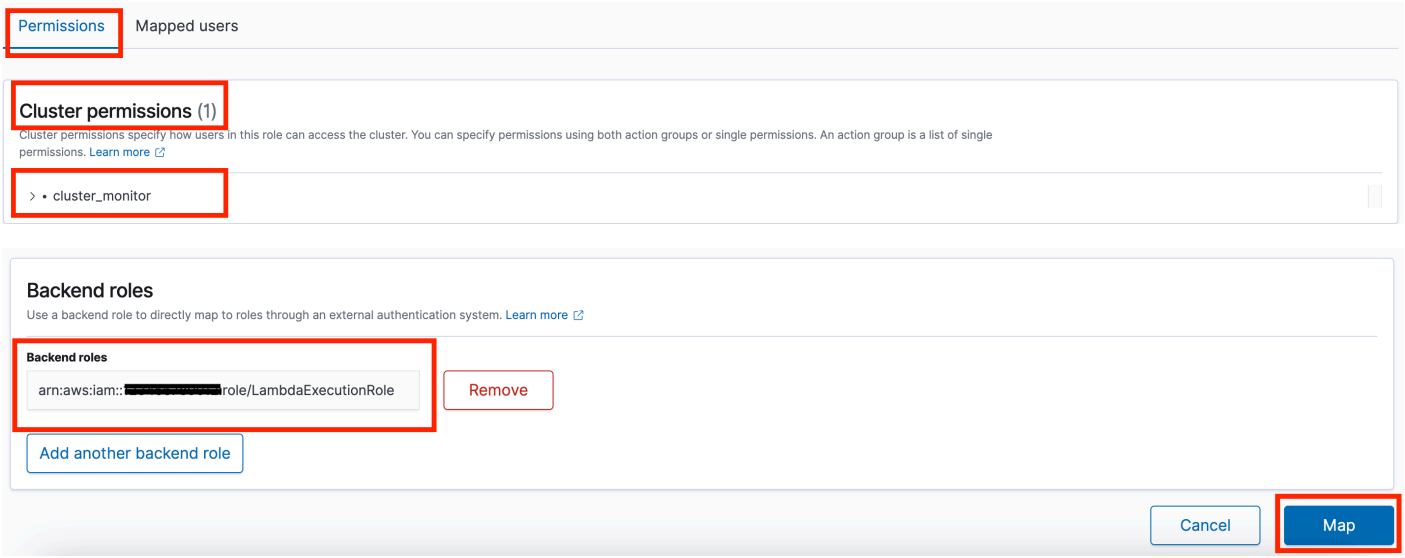
     Lambda 関数にアタッチする IAM ロールの ARN。Lambda 関数は、このロールの認証情報を使用して Amazon OpenSearch Service ドメインへのリクエストに署名します。Amazon OpenSearch Service ドメインできめ細かなアクセスコントロールが有効になっている場合は、このロールを「cluster_monitor」以上のアクセス許可を持つ OpenSearch Service Dashboards バックエンドロールにマッピングする必要があります。
   - DataRetentionDays (オプション):

     Amazon OpenSearch Service ドメインから収集された診断データを保持する日数。デフォルトでは、データは 24 時間 (1 日) 保持されます。データは最大 30 日間保持できます。
   - NumberOfDataSamples (オプション):

Amazon OpenSearch Service ドメインから収集するデータサンプルの数。デフォルトでは、5 つのデータサンプルが収集されます。最大 10 個のサンプルを収集でき、サンプルコレクションごとに Lambda 関数が呼び出されます。



4. OpenSearch Service クラスターできめ細かなアクセスコントロールを有効にしている場合は、`LambdaExecutionRole`ロール ARN が少なくとも アクセス`cluster_monitor`許可を持つロールにマッピングされていることを確認してください。



5. [実行] を選択します。
6. 自動化が開始されます。
7. 自動化ランブックは以下のステップを実行します。
   - checkConcurrency:

     指定された Amazon OpenSearch Service ドメインを対象とするこのランブックの実行が 1 つだけであることを確認します。ランブックが同じドメイン名をターゲットとする別の実行を検出すると、エラーが返され、終了します。
   - getDomainConfig:

ターゲット OpenSearch Service ドメインの設定の詳細を取得します。

- provisionResources:

  を使用してデータ収集用のリソースをプロビジョニングします AWS CloudFormation。

- waitForStackCreation:

  AWS CloudFormation スタックが完了するまで待ちます。

- describeStackResources:

  AWS CloudFormation スタックを記述し、ステートマシンの ARN を取得します。

- runStateMachine:

  Step Functions ステートマシンを実行して、データコレクターの Lambda 関数を 1 回以上呼び出します。

- describeErrorsFromStackEvents:

  AWS CloudFormation スタックのエラーについて説明します。

- unstageOpenSearchHighCPUAutomation:

  `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation スタックを削除します。

- describeErrorsFromStackDeletion:

  AWS CloudFormation スタックの削除中に発生したエラーについて説明します。

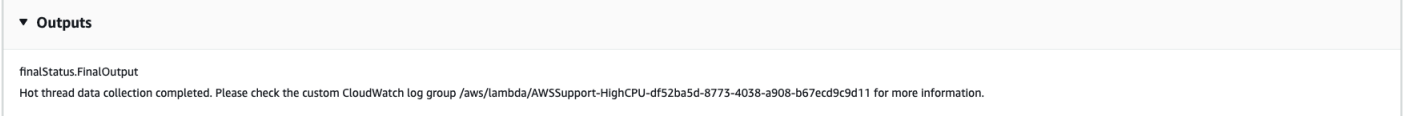
- finalStatus:

  `AWSSupport-TroubleshootOpenSearchHighCPU` ランブックの最終出力を返します。

8. 完了したら、出力セクションで詳細な実行結果を確認します。

   - finalStatus.FinalOutput:

     診断データが保存されている CloudWatch ロググループを提供します。



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスドキュメント

- 詳細については、「Amazon OpenSearch Service のトラブルシューティング」を参照してください。

EventBridge

AWS Systems Manager Automation は、Amazon EventBridge 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-AddOpsItemDedupStringToEventBridgeRule
- AWS-DisableEventBridgeRule

AWS-AddOpsItemDedupStringToEventBridgeRule

説明

AWS-AddOpsItemDedupStringToEventBridgeRule ランブックは、Amazon EventBridge ルールに関連付けられたすべての AWS Systems Manager OpsItems に重複排除文字列を追加します。ルールが既に適用されている場合、このランブックはこのルールに対して重複解除文字列を追加しません。重複排除文字列と OpsItems の詳細については、「AWS Systems Manager ユーザーガイド」の「重複する OpsItems の削減」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- DedupString

  タイプ: 文字列

  説明: (必須) ルールに追加する重複排除文字列。
- RuleName

  タイプ: 文字列

  説明: (必須) 重複排除文字を追加するルールの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- events:ListTargetsByRule
- events:PutTargets

ドキュメントステップ

- aws:executeScript - RuleName パラメータで指定した EventBridge ルールに重複排除文字列を追加します。

AWS-DisableEventBridgeRule

説明

AWS-DisableEventBridgeRule ランブックは、指定した Amazon EventBridge ルールを無効にします。EventBridge ルールの詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge ルール」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- EventBusName

  タイプ: 文字列

  デフォルト: default

  説明: (オプション) 無効にするルールに関連付けられたイベントバス。

- RuleName

  タイプ: 文字列

  説明: (必須) 削除されるルールの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- events:DisableRule

ドキュメントステップ

- aws:executeAwsApi - RuleName パラメータで指定した EventBridge ルールを無効にします。

AWS Glue

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Glue。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-TroubleshootGlueConnection

AWSSupport-TroubleshootGlueConnection

説明

AWSSupport-TroubleshootGlueConnections ランブックは、 AWS Glue 接続の問題のトラブルシューティングに役立ちます。テストされた接続のターゲットは JDBC 接続を介して到達する必要があり、Amazon Relational Database Service (Amazon RDS) クラスター/インスタンス、Amazon Redshift クラスター、または JDBC を介してアクセス可能なその他のターゲットのいずれかになります。最初の 2 つのケースでは、Reachability Analyzer ツールを使用して、ソース (AWS Glue) と

ターゲット (Amazon RDS または Amazon Redshift) 間の接続が付与されているかどうかを判断します。

接続のターゲットが Amazon RDS でも Amazon Redshift でもない場合、接続と同じサブネット (ネットワークポイントオブプレゼンス) に AWS Lambda 関数を作成し、ターゲット名が解決可能かどうか、およびターゲットポートで到達可能かどうかをチェックすることで、 AWS Glue 接続がテストされます。

Important

Reachability Analyzer チェックを実行するために、Elastic Network Interface は接続の各データソースサブネットに作成されます。これらのサブネットに十分な空き IPs があり、1 つの IP を消費しても、この自動化を実行する前にワークロードに影響しないことを確認してください。

Important

この自動化によって作成されたすべてのリソースにはタグが付けられ、簡単に見つけることができます。使用されるタグは次のとおりです。

- `AWSSupport-TroubleshootGlueConnection`: true
- `AutomationExecutionId`: *`Amazon EC2 Systems Manager ## ID`*

動作の仕組み

ランブックは次のステップを実行します。

- AWS Glue 接続チェックのソース情報 (サブネットとセキュリティグループ) を取得するための接続について説明します。
- JDBC URL で参照されているデータソース、または存在する場合は お よび `DatasourceSubnets`パラメータからターゲット情報 (サブネット`DatasourceSecurityGroups`とセキュリティグループ) を取得します。
- JDBC URL に存在するデータソースが Amazon RDS インスタンスまたはクラスター、または Amazon Redshift クラスターの場合、この自動化は、前のステップで収集されたソース情報とターゲット情報の両方を使用して ENIs を作成し、Reachability Analyzer を使用してそれらの間の接続チェックを実行します。

- Lambda 関数 (この自動化のコンテキストではネットワーク上の存在ポイント) を使用して、L4 接続と名前解決のチェックを実行します。
- 同じ Lambda 関数を使用して、Amazon S3 エンドポイントに対してチェックを実行します。
- Policy Simulator は、接続で使用される IAM ロールに必要なアクセス許可があるかどうかを判断するために使用されます。
- 自動化は、接続で使用されるセキュリティグループが想定された設定になっているかどうかを確認します。
- テスト接続オペレーションの失敗の考えられる原因、および/または実行された成功したテストを含むレポートが生成されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

/

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `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**
>
> 上記のアクションに加えて、 には AmazonVPCReachabilityAnalyzerFullAccessPolicy をアタッチされた管理ポリシーとして設定し、Reachability Analyzer テストが正常に実行されるようにAutomationAssumeRoleする必要があります。

に付与できるポリシーの例を次に示します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"
                }
            }
        }
    ]
}
```

指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager AWSSupport-TroubleshootGlueConnectionで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - TestConnectionRole (必須)

     接続テスト中に使用される IAM ロールの Amazon リソースネーム (ARN)。
   - ConnectionName (必須)

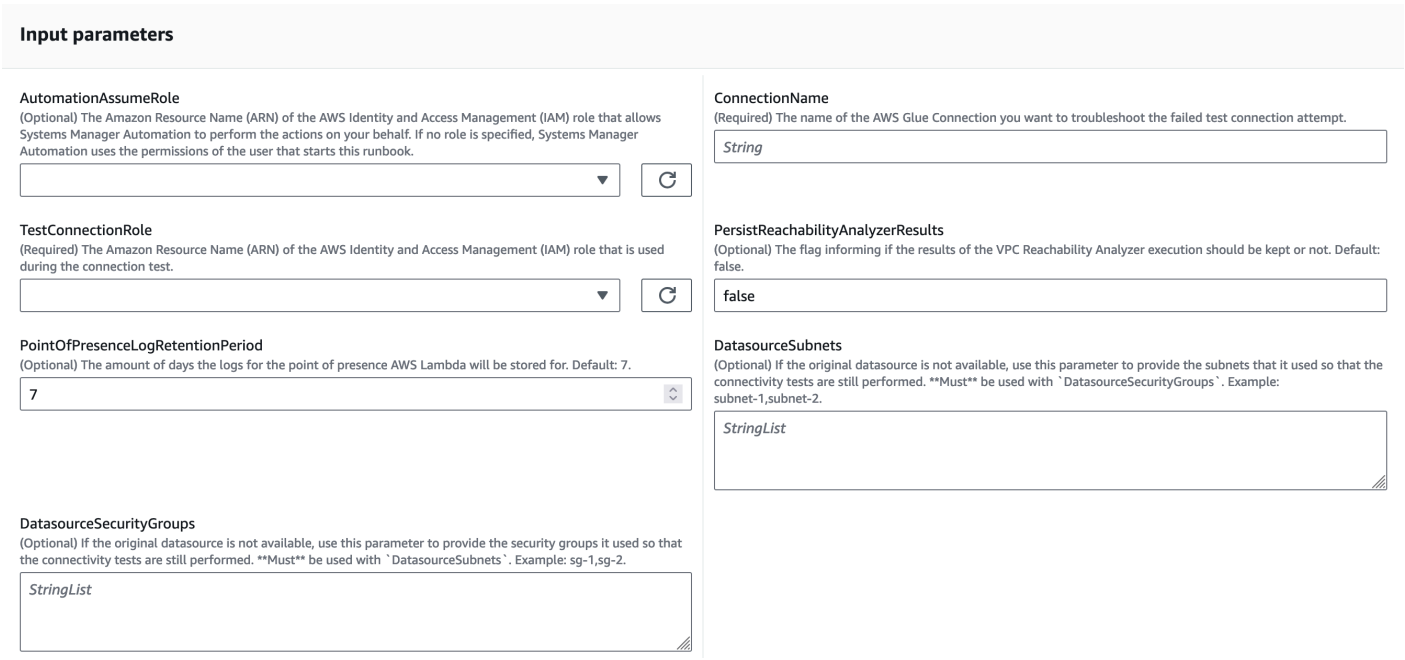
     AWS Glue トラブルシューティングするテスト接続名が失敗しました。
   - PersistReachabilityAnalyzerResults (オプション)

     Reachability Analyzer の実行結果を保持するかどうかを通知するフラグ。デフォルト: `false`.
   - PointOfPresenceLogRetentionPeriod (オプション)

     Lambda のプレゼンスポイントのログが保存される日数。デフォルト: 7。
   - DatasourceSubnets (オプション)

     元のデータソースが使用できない場合は、このパラメータを使用して、接続テスト がまだ実行されるように使用したサブネットを指定します。で使用する必要がありますDatasourceSecurityGroups。例えば、`subnet-1,subnet-2` などです。
   - DatasourceSecurityGroups (オプション)

     元のデータソースが使用できない場合は、このパラメータを使用して、接続テストがまだ実行されるように、使用したセキュリティグループを指定します。と一緒に使用する必要がありますDatasourceSubnets。例えば、`sg-1,sg-2` などです。



4. [実行] を選択します。
5. 自動化が開始されます。
6. 自動化ランブックは以下のステップを実行します。
   - ParseInputs:

     このステップでは、入力の組み合わせを検証します。DatasourceSecurityGroups と の両方DatasourceSubnetsが指定されている場合、それらは有効であり、そのまま返されます。何も指定しない場合、2 つの空のリストが返されます。そのうちの 1 つだけが指定されている場合、ステップは を生成しますValueException。
   - GetConnectionDetails:

     このステップは、提供された AWS Glue 接続の詳細を返します。
   - ParseSecurityGroupList:

     このステップは、このオートメーションSecurityGroupIdListで将来の使用Stringのために の を連結するために使用されます。
   - GetConnectionData:

     JDBC URL、、、 RedShift RdsInstance RdsCluster 間の接続のタイプに基づいて決定しますOther。さらに、 は JDBC 接続で使用されるドメインとポート、接続の Amazon VPC とそのドメインネームサーバーを返します。
   - GetNetworkDetails:

Amazon RDS または Amazon Redshift ターゲットからサブネットとセキュリティグループ情報を取得します。

- CreateENITemplate:

  接続のテストに使用されるネットワークインターフェイスの作成に使用される AWS CloudFormation テンプレートを生成します。これは Reachability Analyzer ツールを実行するために必要です。

- CreateENIStack:

  前のステップで作成したテンプレートから AWS CloudFormation スタックを作成します。

- GetStackDetails:

  前の AWS CloudFormation スタックで作成されたスタックを記述し`SourceNetworkInterface`、`TargetNetworkInterfaces`情報を取得します。

- RunSourceToTargetCheck:

  Reachability Analyzer ツールを使用して、前のステップで作成したソース ENIs の間でチェックを実行します。

- DeleteENIStack:

  ネットワークインターフェイスを作成する AWS CloudFormation スタックを削除します。

- CreateNetworkPointOfPresence:

  AWS CloudFormation は、ネットワークのプレゼンスポイントとして使用される Lambda 関数を作成します。

- GetFunctionName:

  describe AWS CloudFormation スタック API コールを実行して、前のステップで作成した Lambda 関数の名前を取得します。

- RunEndpointChecks:

  JDBC 接続に存在するエンドポイントが、宣言されたポートで解決可能かつ到達可能かどうかを判断するために、ネットワーク上のプレゼンスポイントを使用します。

- CheckS3Connectivity:

  Amazon S3 サービス AWS Glue への接続からのネットワーク接続を確認します。

- DeletePointOfPresence:

ネットワークポイントオブプレゼンス Lambda を作成する AWS CloudFormation スタックを削除します。

- TestIAMRolePermissions:

  テストに使用される IAM ロールに、テストの実行に必要なアクセス許可があるかどうかを確認します。

- CheckConnectionSecurityGroupReferencingRule:

  AWS Glue 接続で使用されるセキュリティグループが、それ自体からのすべての受信トラフィックを許可しているかどうかを確認します。このルールがない場合、セキュリティグループのリストが返されます。

- GenerateReport:

  検出結果のリスト (接続テストの失敗の考えられる理由) と次のステップ (接続テストの失敗の解決を試みます) を含むレポートを生成します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

   - 自動化の結果

     このセクションでは、テスト接続オペレーションが失敗する原因 (検出結果) と、それらを修正する方法 (次のステップ) を説明するシナリオを示します。自動化がテストの失敗の原因を特定できない場合は、このセクションにも通知されます。

   - 成功したテスト

     このセクションでは、この自動化によって正常にテストされた内容を示すシナリオを示します。成功したテストは、自動化がテスト接続の失敗の原因を特定できない場合に役立ちます。これは、問題の原因となっていないものを通知することで、調査の範囲を狭めるためです。

   - 自動化エラー

     このセクションでは、自動化中に発生した問題を説明するシナリオを示します。このシナリオでは、自動化が実行できるテストの数が制限されている可能性があります。シナリオの説明は、失敗したステップを通知します。

```
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.
```

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

Amazon FSx

AWS Systems Manager Automation は、Amazon FSx 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-ValidateFSxWindowsADConfig

AWSSupport-ValidateFSxWindowsADConfig

説明

AWSSupport-ValidateFSxWindowsADConfig ランブックは、Amazon FSx for Windows File Server のセルフマネージド Active Directory (AD) 設定を検証するために使用されます。

動作の仕組み

ランブックは、Amazon FSx サブネットのランブックによって起動された一時的な Amazon Elastic Compute Cloud (Amazon EC2) Windows インスタンスで Amazon FSx 検証スクリプトAWSSupport-ValidateFSxWindowsADConfigを実行します。このスクリプトは複数のチェックを実行して、セルフマネージド AD/DNS サーバーへのネットワーク接続と Amazon FSx サービスアカウントのアクセス許可を検証します。ランブックは、失敗した、または誤って設定された Amazon FSx for Windows File Server を検証したり、セルフマネージド AD を使用して新しい Amazon FSx for Windows File Server を作成したりできます。

デフォルトでは、ランブックは Amazon FSx サブネット AWS CloudFormation で を使用して、Amazon EC2 Windows インスタンス、 (SSM) アクセスのセキュリティグループ AWS Systems Manager 、 AWS Identity and Access Management (IAM) ロール、およびポリシーを作成します。既存の Amazon EC2 インスタンスでスクリプトを実行する場合は、パラメータ で ID を指定しますInstanceId。正常に実行されると、CloudFormation リソースが削除されます。ただし、リソースを保持するには、 RetainCloudFormationStackパラメータを に設定しますtrue。

CloudFormation テンプレートは、Amazon EC2 インスタンスにアタッチして Amazon FSx 検証スクリプトを実行するために必要なアクセス許可を持つ IAM ロールをユーザーに代わって作成します。一時インスタンスの既存の IAM インスタンスプロファイルを指定するには、InstanceProfileNameパラメータを使用します。関連付けられた IAM ロールには、次のアクセス許可が含まれている必要があります。

- ec2:DescribeSubnets および のec2:DescribeVpcsアクセス許可と Amazon 管理ポリシーAmazonSSMManagedInstanceCore。
- GetSecretValue API を呼び出して Systems Manager から Amazon FSx サービスアカウントのユーザー名とパスワードを取得するアクセス許可。
- スクリプト出力の Amazon Simple Storage Service (Amazon S3) バケットにオブジェクトを配置するアクセス許可。

前提条件

SSM Run Command を使用してAmazonFSxADValidationスクリプトを実行するには AWS Systems Manager、一時的な Amazon EC2 インスタンスが作成されるサブネット (またはInstanceIdパラメータで提供される既存のインスタンス) で、、 AWS Secrets Manager、および Amazon S3 エンドポイントへのアクセスを許可する必要があります。

AWS Secrets Manager セットアップ

検証スクリプトは、Secrets Manager へのランタイム呼び出しを使用して Amazon FSx サービスアカウントのユーザー名とパスワードを取得することで、Microsoft AD ドメインに接続します。「AWS Secrets Manager シークレットを作成する」の手順に従って、新しい Secrets Manager シークレットを作成します。ユーザー名とパスワードが 形式のキーと値のペアを使用して保存されていることを確認します{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}"。シークレットへのアクセスを保護する方法については、「 の認証とアクセスコントロール AWS Secrets Manager」を参照してください。

ツールの詳細については、AmazonFSxADValidation README.mdファイルのTROUBLESHOOTING.mdおよび ファイルを参照してください。

ランブックの実行

Amazon FSx ID または AD パラメータを使用してランブックを実行します。ランブックのワークフローは次のとおりです。

- Amazon FSx ID からパラメータを取得するか、入力 AD パラメータを使用します。
- Amazon FSx サブネット上の一時的な検証 Amazon EC2 Windows インスタンス、SSM アクセスのセキュリティグループ、CloudFormation を使用した IAM ロールとポリシー (条件付き) を作成します。InstanceId パラメータを指定すると、パラメータが使用されます。
- Amazon FSx プライマリサブネットのターゲット Amazon EC2 インスタンスで検証スクリプトをダウンロードして実行します。
- 自動化出力に AD 検証結果コードを提供します。さらに、完全なスクリプト出力が Amazon S3 バケットにアップロードされます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

自動化引き受けロールの IAM ポリシーの例

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

指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager [AWSSupport-ValidateFSxWindowsADConfig](#)で に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 既存の失敗した、または誤って設定された Amazon FSx でセルフマネージド AD を検証するには、次のパラメータを入力します。

- AutomationAssumeRole (オプション):

  Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。

- FSxId (条件付き):

  Amazon FSx for Windows File Server ID。これは、既存の失敗した、または誤って設定された Amazon FSx を検証するために必要です。

- SecretArn (必須):

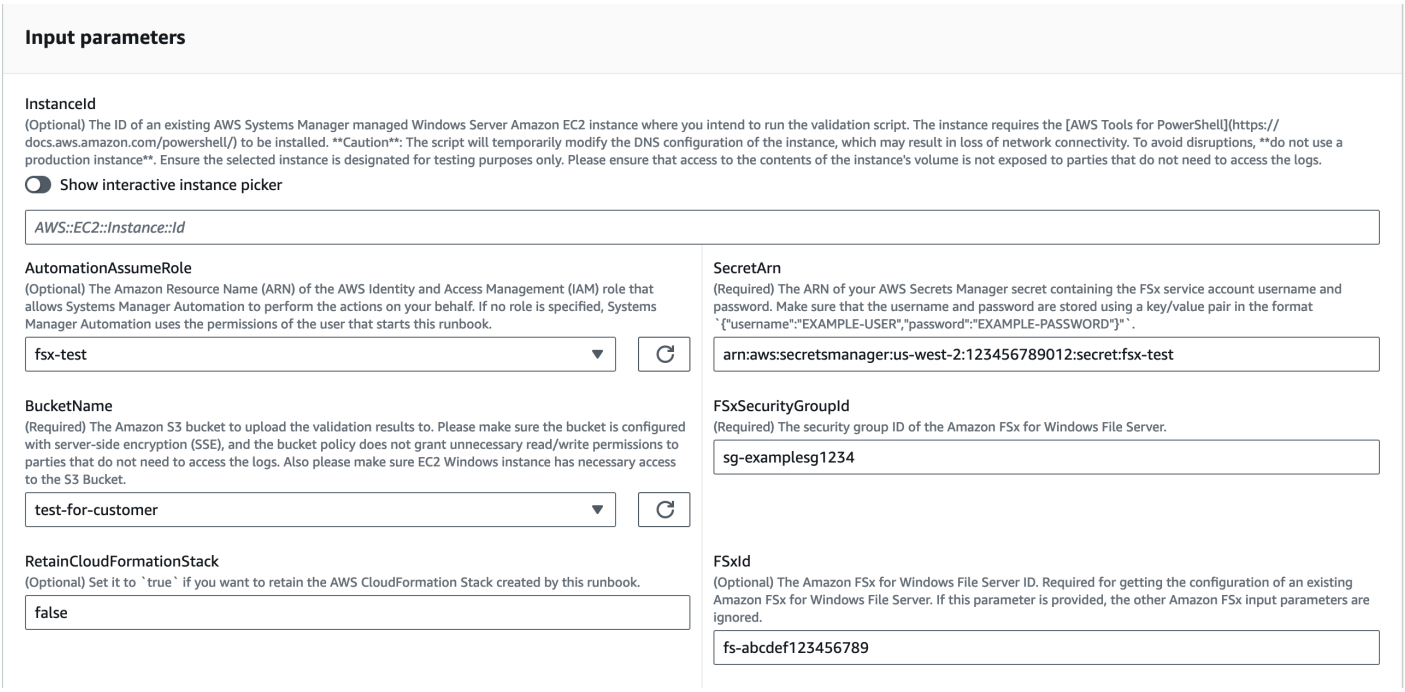
  Amazon FSx サービスアカウントのユーザー名とパスワードを含む Secrets Manager シークレットの ARN。ユーザー名とパスワードが 形式のキーと値のペアを使用して保存されていることを確認します`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`。CloudFormation スタックは、`GetSecretValue`この ARN に対して実行するアクセス許可を持つ検証インスタンスを作成します。

- FSxSecurityGroupId (必須):

  Amazon FSx for Windows File Server のセキュリティグループ ID。

- BucketName (必須):

  検証結果をアップロードする Amazon S3 バケット。バケットがサーバー側の暗号化 (SSE) で設定されており、バケットポリシーがログにアクセスする必要がないユーザーに不要な読み取り/書き込みアクセス許可を付与していないことを確認します。また、Amazon EC2 Windows インスタンスが Amazon S3 バケットに必要なアクセス権を持っていることを確認します。



4. 新しい Amazon FSx 作成のセルフマネージド AD 設定を検証するには、次のパラメータを入力します。

   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。

   - SecretArn (必須):

     Amazon FSx サービスアカウントのユーザー名とパスワードを含む Secrets Manager シークレットの ARN。ユーザー名とパスワードが 形式のキーと値のペアを使用して保存されていることを確認します`{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}`。CloudFormation スタックは、`GetSecretValue`この ARN に対して実行するアクセス許可を持つ検証インスタンスを作成します。

   - FSxSecurityGroupId (必須):

     Amazon FSx for Windows File Server のセキュリティグループ ID。

   - BucketName (必須):

     検証結果をアップロードする Amazon S3 バケット。バケットがサーバー側の暗号化 (SSE) で設定されており、バケットポリシーがログにアクセスする必要がないユーザーに不要な読み取

り/書き込みアクセス許可を付与していないことを確認します。また、Amazon EC2 Windows インスタンスが Amazon S3 バケットに必要なアクセス権を持っていることを確認します。

- FSxPreferredSubnetId (条件付き):

  Amazon FSx for Windows File Server の優先サブネット。

- DomainName (条件付き):

  セルフマネージド Microsoft AD ドメインの完全修飾ドメイン名。

- DnsIpAddresses (条件付き):

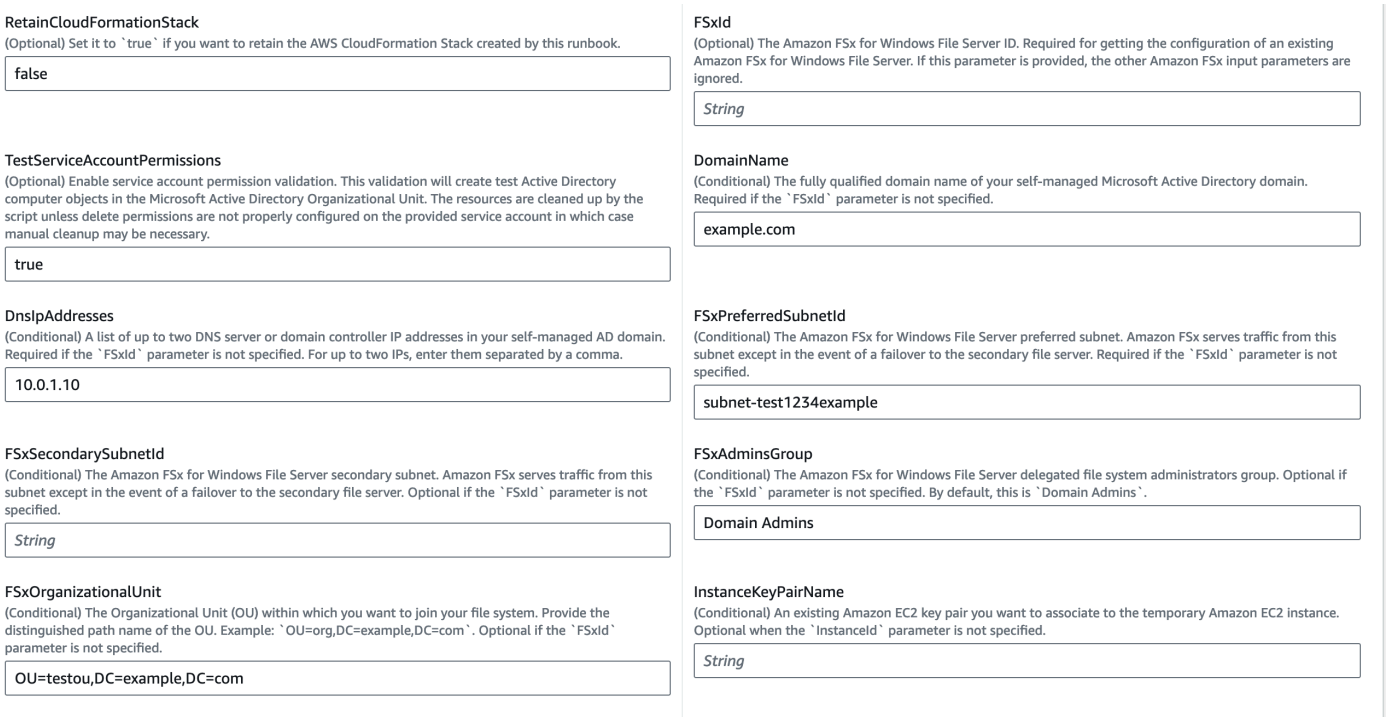
  セルフマネージド AD ドメイン内の最大 2 つの DNS サーバーまたはドメインコントローラーの IP アドレスのリスト。最大 2 つの IPs、カンマで区切って入力します。

- FSxAdminsGroup (条件付き):

  Amazon FSx for Windows File Server の委任ファイルシステム管理者グループ。デフォルトでは、これは `Domain Admins` です。

- FSxOrganizationalUnit (条件付き):

  ファイルシステムに参加する組織単位 (OU)。OU の識別パス名を指定します。例えば、`OU=org,DC=example,DC=com` などです。



5. [実行] を選択します。

6. 自動化が開始されます。
7. ドキュメントは以下のステップを実行します。
   - CheckBucketPublicStatus (aws:executeScript):

     ターゲット Amazon S3 バケットがオブジェクトへの読み取り/書き込みパブリックアクセスを許可する可能性があるかどうかを確認します。
   - BranchOnInputParameters (aws:branch):

     Amazon FSx ID や Amazon FSx パラメータなど、指定された入力パラメータのブランチ。
   - AssertFileSystemTypeIsWindows (aws:assertAwsResourceProperty):

     Amazon FSx ID が指定されている場合、 はファイルシステムタイプが Amazon FSx for Windows File Server であることを確認します。
   - GetValidationInputs (aws:executeScript):

     Amazon EC2 インスタンスを作成するために CloudFormation テンプレートに必要なセルフマネージド Microsoft AD 設定を返します。
   - BranchOnInstanceId (aws:branch):

     指定された入力 のブランチ`InstanceId`。が指定されている場合、検証スクリプト`InstanceId`はオートメーション からターゲット Amazon EC2 インスタンスで実行されます`step:RunValidationScript`。
   - CreateEC2InstanceStack (aws:createStack):

     `AmazonFSxADValidation` ツールが実行される AWS CloudFormation を使用して、任意のサブネットに Amazon EC2 インスタンスを作成します。
   - DescribeStackResources (aws:executeAwsApi):

     一時的な Amazon EC2 インスタンス ID を取得するための CloudFormation スタックについて説明します。
   - WaitForEC2InstanceToBeManaged (aws:waitForAwsResourceProperty):

     SSM Run Command を使用して検証スクリプトを実行するために、Amazon EC2 インスタンスが Systems Manager によって管理されるまで待ちます。
   - GetAmazonFSxADValidationAttachment (aws:executeAwsApi):

     ランブックアタッチメントから`AmazonFSxADValidation`ツール URL を取得します。

- RunValidationScript (aws:runCommand):

  一時的な Amazon EC2 インスタンスでAmazonFSxADValidationツールを実行し、BucketNameパラメータで指定された Amazon S3 バケットに結果を保存します。

- DescribeErrorsFromStackEvents (aws:executeScript):

  ランブックがスタックの作成に失敗した場合の CloudFormation スタックイベントについて説明します。

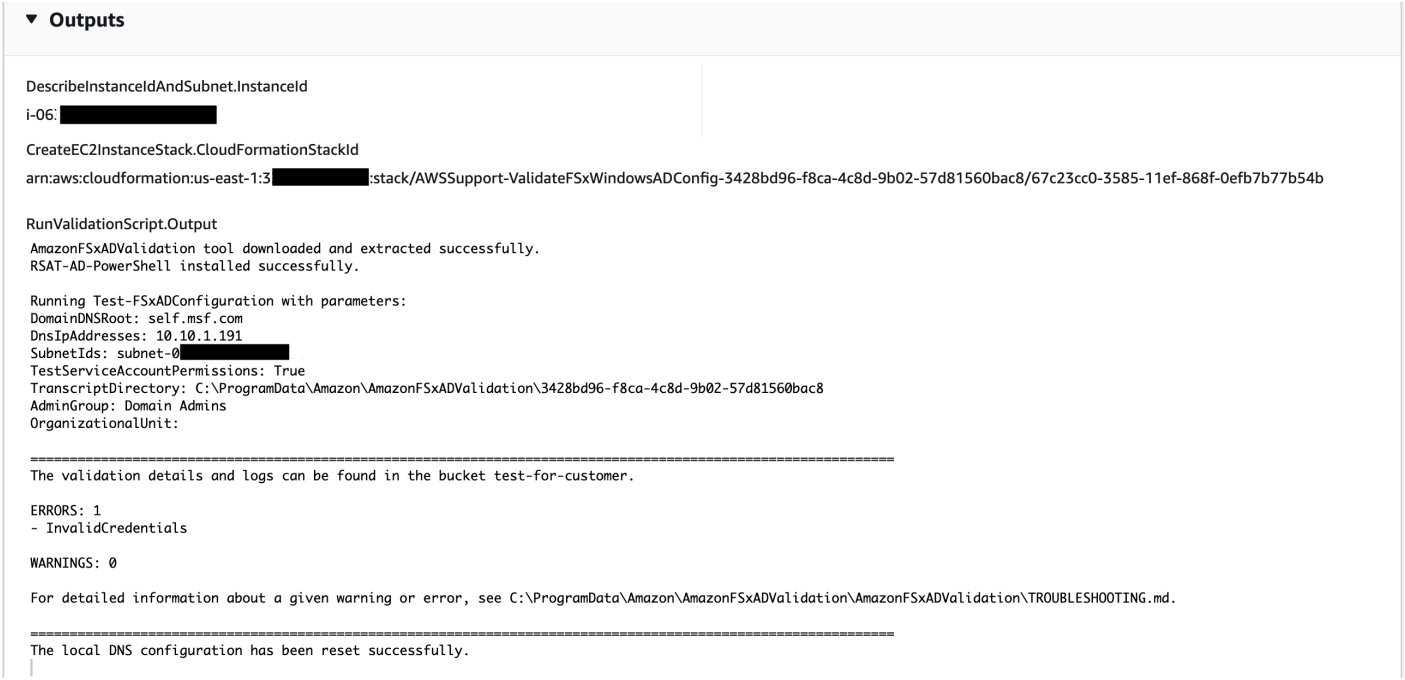
- BranchOnRetainCloudFormationStack (aws:branch):

  CloudFormation スタックを削除するかどうかを判断するために、RetainCloudFormationStack および InstanceIdパラメータで分岐します。

- DeleteCloudFormationStack (aws:deleteStack):

  AWS CloudFormation スタックを削除します。

8. 完了したら、出力セクションで実行結果を確認します。



ランブックは、検証スクリプトの実行結果を Amazon S3 バケットにアップロードします。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスドキュメント

- Amazon FSx for Windows File Server とは
- Amazon FSx for Windows File Server のセルフマネージド AD 設定の検証

GuardDuty

AWS Systems Manager Automation は、Amazon GuardDuty 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-CreateGuardDutyDetector

AWSConfigRemediation-CreateGuardDutyDetector

説明

AWSConfigRemediation-CreateGuardDutyDetector ランブックは、オートメーション AWS リージョン を実行する に Amazon GuardDuty (GuardDuty) ディテクターを作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `guardduty:CreateDetector`
- `guardduty:GetDetector`

ドキュメントステップ

- `aws:executeAwsApi` - GuardDuty ディテクターを作成します。
- `aws:assertAwsResourceProperty` - ディテクターの `Status` が `ENABLED` かどうかを確認します。

IAM

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Identity and Access Management。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- 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

説明

AWSSupport-TroubleshootIAMAccessDeniedEvents オートメーションランブックは、 AWS Identity and Access Management (IAM) アクセス拒否問題のトラブルシューティングに役立ちます。ランブックは、指定された IAM エンティティと AWS サービスイベントソースに関連する最近のアクセス拒否イベントを CloudTrail にクエリします。最大 24 時間の設定可能な時間枠内でイベントを分析し、実行ごとに最大 10 個のイベントを処理します。識別された各アクセス拒否イベントは、拒否のコンテキストと試行されたアクションを理解するのに役立ちます。自動化は、アイデンティティベースの IAM ポリシーとリソースベースの IAM ポリシーの両方を分析します。ID ベースのポリシーでは、IAM エンティティにアタッチされたインラインポリシーとマネージドポリシーを調べます。リソースベースのポリシーでは、Amazon Simple Storage Service (Amazon S3)、 AWS Key Management Service （ AWS KMS ）、Amazon Simple Notification Service (Amazon SNS) AWS Lambda、Amazon Elastic Container Registry (Amazon ECR)、Amazon API Gateway、CodeArtifact、Amazon Elastic File System (Amazon EFS)、Amazon Simple Queue Service (Amazon SQS) AWS Cloud9、Amazon OpenSearch Service、 AWS Signer AWS Serverless Application Repository、および AWS を含む複数のサービスにわたってポリシーを評価します AWS Secrets Manager。

ランブックは IAM ポリシーシミュレーション機能を使用して、CloudTrail イベントで見つかった拒否されたアクションに対してこれらのポリシーを評価します。ランブックは、IAM ユーザー向け

の SimulatePrincipalPolicy と IAM ロール向けの SimulateCustomPolicy の両方を通じて IAM のポリシーシミュレーション機能を活用して、CloudTrail イベントで見つかった拒否されたアクションに対してこれらのポリシーを評価します。自動化は、拒否された特定のアクションを識別し、暗黙的な拒否と明示的な拒否を区別し、アクセス拒否を担当するポリシーを一覧表示し、各拒否の説明を提供するのに役立つレポートを出力します。このレポートは、欠落している許可ステートメントや競合する拒否ステートメントの特定など、潜在的な解決策も提案します。

動作の仕組み

ランブックは次のステップを実行します。

- (RequesterARNロールまたはユーザー) を記述して検証し、IAM エンティティタイプや IAM ID などの情報を取得します。
- 指定されたResourceARN場合は、RequesterARN、、EventSourceおよび に関連付けられた CloudTrail イベントを取得します。
- CloudTrail イベントを分析して、アクセス拒否エラーが返されたときに実行されたアクションを取得し、IAM エンティティにアタッチされたインラインポリシーやマネージドポリシー、リソースベースのポリシーなど、すべての IAM ポリシーを調べます。次に、問題の CloudTrail イベントからのアクセス拒否エラーで見つかったアクションに対してこれらのポリシーをシミュレートして、エラーの原因を特定します。
- アクセス拒否エラーのタイプ、エラーの原因となっているポリシーを決定するレポートを出力し、エラーに対する潜在的な解決策を提案します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

/

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ポリシーの例：

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

指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager AWSSupport-TroubleshootIAMAccessDeniedEvents でに移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):
     - 説明: (オプション) SSM Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。Kubernetes API コールを許可するには、ロールを Amazon EKS クラスターアクセスエントリまたは RBAC アクセス許可に追加する必要があります。
     - 型: `AWS::IAM::Role::Arn`
   - RequesterARN (必須):
     - 説明: (必須) 特定の AWS リソースに対するアクセス許可を調査する IAM ユーザーまたはロールの ARN。
     - タイプ: 文字列
     - 許可パターン: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$`
   - ResourceARN (オプション):
     - 説明: (オプション) アクセス拒否が評価される AWS リソースの ARN。 AWS ターゲットリソースは、オートメーションランブックが実行されるのと同じリージョンに存在する必要があります。

  - タイプ: 文字列
  - 許可パターン: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):([a-zA-Z0-9\\-]{1,63}):([a-z0-9\\-]{0,63})?:(\\d{12})?:([a-zA-Z0-9\\-_/:.]{1,1024})$`
- EventSource (必須):
  - 説明: (必須) CloudTrail イベントが発生した Amazon API エンドポイント。例: `s3.amazonaws.com`。
  - タイプ: 文字列
  - 許可パターン: `^([a-zA-Z0-9.-]+)\\.amazonaws\\.com$`
- EventName (オプション):
  - 説明: (オプション) CloudTrail イベントに関連付けられた Amazon API アクション名。例: `s3:CreateBucket`。
  - タイプ: 文字列
  - 許可パターン: `^$|^[a-z0-9]+:[A-Za-z0-9]+$`
- LookBackHours (オプション):
  - 説明: (オプション) イベントを検索するときに CloudTrail `Access Denied`イベントをさかのぼる時間数。有効な範囲: `1 ~ 24`時間。
  - タイプ: 整数
  - 許可パターン: `^([1-9]|1[0-9]|2[0-4])$`
  - デフォルト: 12
- MaxEvents (オプション):
  - 説明: (オプション) `Access Denied`イベントの検索時に返される CloudTrail イベントの最大数。有効範囲: `1 ~ 5`イベント。
  - タイプ: 整数
  - 許可パターン: `^([1-9]|1[0-9]|2[0-4])$`
  - デフォルト: 3
- UseContextEntries (オプション):
  - 説明: (オプション) を指定すると`true`、オートメーションは CloudTrail イベントから API リクエストのコンテキストに関する詳細を抽出し、IAM ポリシーシミュレーションに含めます。
  - 型: ブール値
  - 許可パターン: `^([1-9]|1[0-9]|2[0-4])$`

- デフォルト: 3

4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - ValidateRequesterArn

     `RequesterArn` ARN を検証および分解し、ターゲット IAM ユーザーまたはロールに関する情報を取得します。
   - GetCloudTrailEventsWithAccessDeniedError

     指定された IAM エンティティと AWS サービスに関連する最近のイベントの CloudTrail `Access Denied`イベントをクエリします`EventSource`。
   - EvaluateIAMRequesterPolicies

     CloudTrail イベントからのアクションに対してリクエスタ IAM エンティティの IAM アクセス許可を評価します。この評価には、リクエスタに関連付けられたアイデンティティベースのポリシーとリソースベースのポリシーの両方の分析が含まれます。自動化では、IAM のポリシーシミュレーション機能を使用して、CloudTrail イベントで特定された拒否されたアクションのコンテキストでこれらのポリシーを評価します。
7. 完了したら、出力セクションで実行の詳細な結果を確認します。
   - PermissionEvaluationResults

     暗黙的な拒否と明示的な拒否を区別して、拒否された特定のアクションを識別するのに役立つレポートを出力します。また、アクセス拒否を担当するポリシーを一覧表示し、各拒否の説明を提供します。このレポートは、欠落している許可ステートメントや競合する拒否ステートメントの特定など、潜在的な解決策も提案します。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS-AttachIAMToInstance

説明

AWS Identity and Access Management (IAM) ロールをマネージドインスタンスにアタッチします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- ForceReplace

  型: ブール値

  説明: (オプション) 既存の IAM プロファイルを置き換えるかどうかを指定するためのフラグ。

  デフォルト: true
- InstanceId

  タイプ: 文字列

  説明: (必須) IAM ロールを割り当てるインスタンスの ID。
- RoleName

タイプ: 文字列

説明: (必須) マネージドインスタンスに追加する IAM ロール名。

ドキュメントステップ

1. aws:executeAwsApi - EC2 インスタンスにアタッチされた IAM インスタンスプロファイルを検索します。
2. aws:branch - CheckInstanceProfileAssociations - EC2 インスタンスにアタッチされた IAM インスタンスプロファイルを確認します。
   a. IAM インスタンスプロファイルがアタッチされており、ForceReplace が true に設定されている場合:
      i. aws:executeAwsApi - DisassociateIamInstanceProfile - IAM インスタンスプロファイルと EC2 インスタンスの関連付けを解除します。
   b. aws:executeAwsApi - ListInstanceProfilesForRole - アタッチされている IAM ロールのインスタンスプロファイルを一覧表示します。
   c. aws:branch - CheckInstanceProfileCreated - アタッチされている IAM ロールに、インスタンスプロファイルが関連付けられているかどうかを確認します。
      i. IAM ロールにインスタンスプロファイルが関連付けられている場合:
         A. aws:executeAwsApi - AttachIAMProfileToInstance - IAM インスタンスプロファイルロールを EC2 インスタンスにアタッチします。
      i. IAM ロールにインスタンスプロファイルが関連付けられていない場合:
         A. aws:executeAwsApi - CreateInstanceProfileForRole - 指定された IAM ロールのインスタンスプロファイルロールを作成します。
         B. aws:executeAwsApi - AddRoleToInstanceProfile - インスタンスプロファイルロールを指定された IAM ロールにアタッチします。
         C. aws:executeAwsApi - GetInstanceProfile - 指定された IAM ロールのインスタンスプロファイルデータを取得します。
         D. aws:executeAwsApi - AttachIAMProfileToInstanceWithRetry - IAM インスタンスプロファイルを EC2 インスタンスにアタッチします。

出力

AttachIAMProfileToInstanceWithRetry.AssociationId

GetInstanceProfile.InstanceProfileName

GetInstanceProfile.InstanceProfileArn

AttachIAMProfileToInstance.AssociationId

ListInstanceProfilesForRole.InstanceProfileName

ListInstanceProfilesForRole.InstanceProfileArn

AWS-DeleteIAMInlinePolicy

説明

AWS-DeleteIAMInlinePolicy ランブックは、指定した IAM ID にアタッチされたすべての AWS Identity and Access Management (IAM) インラインポリシーを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- IamArns

  タイプ: 文字列

説明: (必須) インラインポリシーを削除する IAM ID の ARNs のカンマ区切りリスト。このリストには、IAM ユーザー、グループ、またはロールを含めることができます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- iam:DeleteGroupPolicy
- iam:DeleteRolePolicy
- iam:DeleteUserPolicy
- iam:ListGroupPolicies
- iam:ListRolePolicies
- iam:ListUserPolicies

ドキュメントステップ

- aws:executeScript - ターゲット IAM ID にアタッチされた IAM インラインポリシーを削除します。

AWSConfigRemediation-DeleteIAMRole

説明

AWSConfigRemediation-DeleteIAMRole ランブックは指定した AWS Identity and Access Management (IAM) ロールを削除します。このオートメーションでは、IAM ロールまたはサービスリンクロールに関連付けられたインスタンスプロファイルは削除されません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- IAMRoleID

  タイプ: 文字列

  説明: (必須) 削除される IAM ロールの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListInstanceProfilesForRole
- iam:ListRolePolicies
- iam:ListRoles
- iam:RemoveRoleFromInstanceProfile

ドキュメントステップ

- aws:executeScript - IAMRoleID パラメータで指定した IAM ロールの名前を収集します。

- aws:executeScript - IAM ロールに関連付けられたポリシーとインスタンスプロファイルを収集します。
- aws:executeScript - アタッチされたポリシーを削除します。
- aws:executeScript - IAM ロールを削除し、ロールが削除されたことを確認します。

AWSConfigRemediation-DeleteIAMUser

説明

AWSConfigRemediation-DeleteIAMUser ランブックは指定した AWS Identity and Access Management (IAM) ユーザーを削除します。このオートメーションは、IAM ユーザーに関連付けられた次のリソースを削除またはデタッチします。

- アクセスキー
- アタッチされた管理ポリシー
- Git 認証情報
- IAM グループメンバーシップ
- IAM ユーザーパスワード
- インラインポリシー
- 多要素認証 (MFA) デバイス
- 証明書への署名
- SSH 公開キー

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- IAMUserId

  タイプ: 文字列

  説明: (必須) 削除される IAM ユーザーの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeScript - IAMUserId パラメータで指定する IAM ユーザーのユーザー名を収集します。
- aws:executeScript - IAM ユーザーに関連付けられたアクセスキー、証明書、認証情報、MFA デバイス、SSH キーを収集します。
- aws:executeScript - IAM ユーザーのグループメンバーシップとポリシーを収集します。
- aws:executeScript - IAM ユーザーに関連付けられたアクセスキー、証明書、認証情報、MFA デバイス、SSH キーを削除します。
- aws:executeScript - IAM ユーザーのグループメンバーシップとポリシーを削除します。
- aws:executeScript - IAM ユーザーを削除し、ユーザーが削除されたことを確認します。

AWSConfigRemediation-DeleteUnusedIAMGroup

説明

AWSConfigRemediation-DeleteUnusedIAMGroup ランブックは、任意のユーザーを含まない IAM グループを削除します。

AWSConfigRemediation-DeleteUnusedIAMGroup ランブックは、任意のユーザーを含まない IAM グループを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- GroupName

  タイプ: 文字列

  説明: (必須) 削除する IAM グループの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:DeleteGroup
- iam:DeleteGroupPolicy
- iam:DetachGroupPolicy

ドキュメントステップ

- aws:executeScript - ターゲット IAM グループにアタッチされている管理およびインライン IAM ポリシーを削除してから、IAM グループを削除します。

AWSConfigRemediation-DeleteUnusedIAMPolicy

説明

AWSConfigRemediation-DeleteUnusedIAMPolicy ランブックは、任意のユーザー、グループ、またはロールにアタッチされていない AWS Identity and Access Management (IAM) ポリシーを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- IAMResourceId

  タイプ: 文字列

  説明: (必須) 削除する IAM ポリシーのリソース識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

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

- iam:DeletePolicy
- iam:DeletePolicyVersion
- iam:GetPolicy
- iam:ListEntitiesForPolicy
- iam:ListPolicyVersions

ドキュメントステップ

- aws:executeScript - IAMResourceId パラメータで指定するポリシーを削除し、ポリシーが削除されたことを確認します。

AWSConfigRemediation-DetachIAMPolicy

説明

AWSConfigRemediation-DetachIAMPolicy ランブックは、指定した AWS Identity and Access Management (IAM) ポリシーをデタッチします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- IAMResourceId

  タイプ: 文字列

  説明: (必須) デタッチする IAM ポリシーの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- config:ListDiscoveredResources
- iam:DetachGroupPolicy
- iam:DetachRolePolicy
- iam:DetachUserPolicy
- iam:GetPolicy
- iam:ListEntitiesForPolicy

ドキュメントステップ

- aws:executeScript - すべてのリソースから IAM ポリシーをデタッチします。

AWSConfigRemediation-EnableAccountAccessAnalyzer

説明

AWSConfigRemediation-EnableAccountAccessAnalyzer ランブックは、 に AWS Identity and Access Management (IAM) Access Analyzer を作成します AWS アカウント。Access Analyzer の詳細については、「IAM ユーザーガイド」の「 AWS IAM Access Analyzer の使用」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AnalyzerName

  タイプ: 文字列

  説明: (必須) 作成するアナライザーの名前。
- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- access-analyzer:CreateAnalyzer
- access-analyzer:GetAnalyzer

ドキュメントステップ

- aws:executeAwsApi - アカウントで Access Analyzer を作成します。
- aws:waitForAwsResourceProperty - Access Analyzer のステータスが ACTIVE になるまで待機します。

- aws:assertAwsResourceProperty - Access Analyzer の状態が ACTIVE であることを確認します。

AWSSupport-GrantPermissionsToIAMUser

説明

このランブックは、指定されたアクセス許可を IAM グループ (新規または既存) に付与し、既存の IAM ユーザーを追加します。選択できるポリシー: 請求またはサポート。IAM の請求へのアクセスを有効にするには、「IAM ユーザーおよびフェデレーションユーザーの請求およびコンソールマネジメントページへのアクセス」を有効にすることも忘れないでください。

> **Important**
>
> 既存の IAM グループを提供する場合、グループ内のすべての現行 IAM ユーザーは新しいアクセス権限を受け取ります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- IAMGroupName

  タイプ: 文字列

  デフォルト: ExampleSupportAndBillingGroup

  説明: (必須) 新規または既存のグループにすることができます。IAM エンティティの名前の制限に準拠する必要があります。

- IAMUserName

  タイプ: 文字列

  デフォルト: ExampleUser

  説明: (必須) 既存のユーザーである必要があります。

- LambdaAssumeRole

  タイプ: 文字列

  説明: (オプション) Lambda によって引き受けられたロールの ARN。

- アクセス許可

  タイプ: 文字列

  有効な値: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

  デフォルト: SupportAndBillingFullAccess

  説明: (必須) 次のいずれかを選択します。SupportFullAccess はサポートセンターへのフルアクセスを許可します。BillingFullAccess は請求ダッシュボードへのフルアクセスを許可します。SupportAndBillingFullAccess はサポートセンターと請求ダッシュボードの両方へのフルアクセスを許可します。ドキュメント詳細のポリシーに関する詳細。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

必要なアクセス許可は、AWSSupport-GrantPermissionsToIAMUser の実行方法によって異なります。

現在ログインしているユーザーまたはロールとして実行

AmazonSSMAutomationRole Amazon 管理ポリシーを添付し、Lambda 関数と IAM ロールを作成して Lambda に渡すための以下の追加のアクセス権限を有効にすることをお勧めします。

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

AutomationAssumeRole および LambdaAssumeRole の使用

ユーザーは、ランブックに対する ssm:StartAutomationExecution アクセス権限と AutomationAssumeRole および LambdaAssumeRole として渡された IAM ロールの iam:PassRole を保持している必要があります。各 IAM ロールに必要なアクセス権限を次に示します。

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

ドキュメントステップ

1. aws:createStack - AWS CloudFormation テンプレートを実行して Lambda 関数を作成します。
2. aws:invokeLambdaFunction - Lambda を実行して IAM アクセス許可を設定します。
3. aws:deleteStack - CloudFormation テンプレートを削除します。

出力

configureIAM.Payload

AWSConfigRemediation-RemoveUserPolicies

説明

AWSConfigRemediation-RemoveUserPolicies ランブックは、 AWS Identity and Access Management (IAM) インラインポリシーを削除し、指定したユーザーにアタッチされたすべての管理ポリシーをデタッチします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- IAMUserID

タイプ: 文字列

説明: (必須) ポリシーを削除するユーザーの ID。

- PolicyType

  タイプ: 文字列

  有効な値: すべて | インライン | 管理

  デフォルト: All

  説明: (必須) ユーザーから削除する IAM ポリシーのタイプ。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:DeleteUserPolicy
- iam:DetachUserPolicy
- iam:ListAttachedUserPolicies
- iam:ListUserPolicies
- iam:ListUsers

ドキュメントステップ

- aws:executeScript - IAM ポリシーを削除し、IAMUserID パラメータで指定したユーザーからデタッチします。

AWSConfigRemediation-ReplaceIAMInlinePolicy

説明

AWSConfigRemediation-ReplaceIAMInlinePolicy ランブックは、インライン AWS Identity and Access Management (IAM) ポリシーをレプリケートされたマネージド IAM ポリシーに置き換え

ます。ユーザー、グループ、またはロールにアタッチされたインラインポリシーの場合、インラインポリシーのアクセス許可のクローンが管理 IAM ポリシーに作成されます。マネージド IAM ポリシーがリソースに追加され、インラインポリシーが削除されます。このオートメーションを実行する AWS リージョン で を有効にする AWS Config 必要があります。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- InlinePolicyName

  タイプ: StringList

  説明: (必須) 置き換える IAM インラインポリシー。
- ResourceId

  タイプ: 文字列

  説明: (必須) インラインポリシーを置き換える IAM ユーザー、グループ、またはロールの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeScript - インライン IAM ポリシーを、指定したリソースで AWS レプリケートされたポリシーに置き換えます。

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

説明

AWSConfigRemediation-RevokeUnusedIAMUserCredentials ランブックは、未使用の AWS Identity and Access Management (IAM) パスワードとアクティブなアクセスキーを取り消します。このランブックでは、期限切れのアクセスキーも非アクティブ化され、期限切れのログインプロファイルも削除されます。このオートメーションを実行する AWS リージョン では、 を有効にする AWS Config 必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- IAMResourceId

  タイプ: 文字列

  説明: (必須) 未使用の認証情報を取り消す IAM リソースの ID。
- MaxCredentialUsageAge

  タイプ: 文字列

  デフォルト: 90

  説明: (必須) 認証情報を使用する必要がある日数。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:ListDiscoveredResources
- iam:DeleteAccessKey
- iam:DeleteLoginProfile

- iam:GetAccessKeyLastUsed
- iam:GetLoginProfile
- iam:GetUser
- iam:ListAccessKeys
- iam:UpdateAccessKey

ドキュメントステップ

- aws:executeScript - IAMResourceId パラメータで指定されたユーザーの IAM 認証情報を取り消します。期限切れのアクセスキーが非アクティブ化され、期限切れのログインプロファイルは削除されます。

> **Note**
>
> この修復アクションの MaxCredentialUsageAgeパラメータは、このアクションのトリガーに使用する AWS Config ルールの maxAccessKeyAgeパラメータと一致するように設定してください: access-keys-rotated。

AWSConfigRemediation-SetIAMPasswordPolicy

説明

AWSConfigRemediation-SetIAMPasswordPolicy ランブックは、ユーザーの AWS アカウントで、 AWS Identity and Access Management (IAM) ユーザーパスワードポリシーを設定します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- AllowUsersToChangePassword

  型: ブール値

  デフォルト: false

  説明: (オプション) に設定すると`true`、 内のすべての IAM ユーザーが AWS Management Console AWS アカウント を使用してパスワードを変更できます。

- HardExpiry

  型: ブール値

  デフォルト: false

  説明: (オプション) この値を `true` に設定した場合、IAM ユーザは、既に有効期限切れとなったパスワードをリセットできなくなります。

- MaxPasswordAge

  タイプ: 整数

  デフォルト: 0

  説明: (オプション) IAM ユーザーのパスワードが有効な日数。

- MinimumPasswordLength

  タイプ: 整数

  デフォルト: 6

  説明: (オプション) IAM ユーザーのパスワードに最小限必要な文字数。

- PasswordReusePrevention

  タイプ: 整数

デフォルト: 0

説明: (オプション) IAM ユーザーが再使用できない以前のパスワードの数。

- RequireLowercaseCharacters

  型: ブール値

  デフォルト: false

  説明: (オプション) この値を `true` に設定した場合は、IAM ユーザーのパスワードには、ISO 基本ラテンアルファベット (a ~ z) の小文字を含める必要があります。

- RequireNumbers

  型: ブール値

  デフォルト: false

  説明: (オプション) この値を `true` に設定した場合、IAM ユーザーのパスワードには数字 (0 ~ 9) を含める必要があります。

- RequireSymbols

  型: ブール値

  デフォルト: false

  説明: (オプション) この値を `true` に設定した場合、IAM ユーザーのパスワードには英数字以外の文字を含める必要があります (! @ # $ % ^ * ( ) _ + - = [ ] { } | ')。

- RequireUppercaseCharacters

  型: ブール値

  デフォルト: false

  説明: (オプション) この値を `true` に設定した場合、IAM ユーザーのパスワードには、ISO 基本ラテンアルファベット (A ~ Z) の大文字を含める必要があります。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:GetAccountPasswordPolicy
- iam:UpdateAccountPasswordPolicy

ドキュメントステップ

- aws:executeScript - AWS アカウントのランブックパラメータで指定された値に基づいて、IAM ユーザーパスワードポリシーを設定します。

AWSSupport-ContainIAMPrincipal

説明

セキュリティインシデントが発生した場合、または AWS Identity and Access Management (IAM) ユーザー/ロールまたは AWS アイデンティティセンター (IDC) ユーザーの侵害が疑われる場合は、調査のために設定を保持しながら、影響を受ける ID を迅速に分離することが重要です。AWSSupport-ContainIAMPrincipal ランブックは、侵害された IAM または IDC ID を含めるための構造化された可逆的なアプローチを提供し、 AWS リソースへのアクセスを効果的にブロックし、侵害の拡散を防止します。

この自動化されたプロセスにより、アイデンティティの設定を永続的に変更することなく調査が可能になり、適切であると判断された場合に通常のアクセスを復元できます。封じ込めプロセスは、IAM 内のユーザーまたはロール、または IDC 内のユーザーを維持し、すべてのネットワークアクティビティから効果的に分離します。この分離により、含まれている ID リソースが Amazon Virtual Private Cloud 内のリソースと通信したり、インターネットリソースにアクセスしたりできなくなります。封じ込めは元に戻すように設計されており、適切であると判断された場合は通常のアクセスを復元できます。

動作の仕組み

AWSSupport-ContainIAMPrincipal ランブックは、IAM ユーザー、ロール、および Identity Center ユーザー向けの包括的な封じ込めプロセスを実装します。Contain モードで実行すると、まずすべての入力パラメータを検証し、指定された Amazon S3 バケットでセキュリティチェックを

実行します。次に、ターゲット IAM プリンシパルに関する詳細情報を収集し、プリンシパルタイプに基づいて適切な封じ込め対策を適用します。IAM ユーザーの場合、アクセスキーを無効にし、コンソールアクセスを削除して、拒否ポリシーをアタッチします。IAM ロールの場合、封じ込め前に作成されたセッションのアクセス許可を取り消す拒否ポリシーがアタッチされます。Identity Center ユーザーの場合、アクセス許可セット、グループメンバーシップを削除し、拒否ポリシーを適用します。このプロセスを通じて、ランブックは元の設定を Amazon S3 バケットにバックアップし、復元の可能性に備えます。`Restore` モードで実行すると、バックアップされた設定を使用してプリンシパルをコンテナ前の状態に戻そうとします。ランブックには、変更を適用せずにプレビューする`DryRun`オプションが含まれており、成功したオペレーションシナリオと失敗シナリオの両方に関する包括的なレポートを提供します。

Important

- 昇格された権限の使用： この SSM ドキュメントは、IAM および IDC ID ポリシーの変更や隔離設定の適用など、昇格された権限を必要とするさまざまなオペレーションを実行します。これらのアクションは、特権の エスカレーションや、ターゲット ID に依存する他のワークロードに影響を与える可能性があります。`AutomationAssumeRole` パラメータで指定されたロールに付与されたアクセス許可を確認し、それらが意図したユースケースに適していることを確認する必要があります。IAM アクセス許可の詳細については、次の AWS ドキュメントを参照してください。
  - Identity and Access Management (IAM) のアクセス許可
  - AWS Systems Manager Automation のアクセス許可
- ワークロードの可用性低下のリスク： この Systems Manager ドキュメントは、ワークロードの可用性の低下や中断を引き起こす可能性のある分離アクションを実行します。セキュリティイベント中に実行されると、指定された IAM および IDC ID から AWS API アクセス許可を取り消すことで、影響を受けるリソースへのアクセスが制限され、 AWS API コールやアクションが行われなくなります。これは、これらの ID に依存するアプリケーションまたはサービスに影響を与える可能性があります。
- 追加リソースの作成： オートメーションドキュメントは、実行パラメータに応じて、Amazon Simple Storage Service (Amazon S3) バケットやそこに保存されている Amazon S3 オブジェクトなどの追加リソースを条件付きで作成することがあります。これらのリソースには、 AWS 使用量に基づいて追加料金が発生します。
- 復元リスク： Action パラメータが `Restore` に設定されている場合、この SSM ドキュメントは IAM または IDC ID 設定を元の状態に復元しようとします。ただし、復元プロセスが失敗し、IAM または IDC アイデンティティが一貫性のない状態になるリスクがあります。ドキュメントには、このような障害が発生した場合の手動復元の手順が記載されてい

ますが、復元プロセス中に発生する可能性のある問題に対処する準備を整えておく必要があります。

本番環境で実行する前に、ランブックを徹底的に確認し、その潜在的な影響を理解し、非本番環境でテストすることをお勧めします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

/

必要な IAM アクセス許可

ランブックを正常に使用するには、 `AutomationAssumeRole`パラメータに次のアクセス許可が必要です。

- s3:GetBucketLocation
- s3:GetBucket
- s3:ListBucket
- s3:GetBucketPublicAccessBlocks
- s3:GetAccountPublicAccessBlocks
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:GetObject
- s3:CreateBucket
- s3:PutObject
- 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
- organizations:ListAccounts

- sso:ListPermissionSetsProvisionedToAccount
- sso:GetInlinePolicyForPermissionSet
- sso:ListInstances
- sso-directory:SearchUsers
- sso:ListPermissionSets
- sso:ListAccountAssignments
- sso-directory:DescribeUser
- identitystore:ListUsers
- identitystore:ListGroups
- identitystore:IsMemberInGroups
- identitystore:ListGroupMemberships
- secretsmanager:CreateSecret
- secretsmanager:DeleteSecret
- sso:DeleteAccountAssignment
- sso:PutInlinePolicyToPermissionSet
- sso:CreateAccountAssignment
- sso:DeleteInlinePolicyFromPermissionSet
- sso:TagResource
- sso:UntagResource
- identitystore:DeleteGroupMembership
- identitystore:CreateGroupMembership

に必要なアクセス許可を付与する IAM ポリシーの例を次に示します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": "*"
        }
    ]
}
```

指示

次の手順に従って自動化を設定します。

1. AWS Systems Manager コンソールで AWSSupport-ContainIAMPrincipal に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):
     - 説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
     - 型: `AWS::IAM::Role::Arn`
   - PrincipalType (必須):
     - 説明: (必須) IAM AWS プリンシパルタイプ: IAM ユーザー、IAM ロール、または Identity Center ユーザー。
     - タイプ: 文字列
     - 使用できる値: `IAM user|IAM role|Identity Center user`
   - PrincipalName (必須):
     - 説明: (必須) IAM プリンシパルの名前。Identity Center ユーザーの場合は、ユーザー名を入力します。
     - タイプ: 文字列
     - 許可されたパターン: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/+=,@]{1,1024}$`

- アクション (必須):
  - 説明: (必須) ターゲット IAM プリンシパルをContain分離Restoreするか、IAM プリンシパルを以前のバックアップから元の設定に復元しようとします。
  - タイプ: 文字列
  - 使用できる値: Contain|Restore
- DryRun (オプション):
  - 説明: (オプション) に設定するとtrue、オートメーションはターゲット IAM プリンシパルに変更を加えません。代わりに、変更を試みた内容が出力され、各ステップの詳細が表示されます。デフォルト値: true。
  - 型: ブール値
  - 使用できる値: true|false
- ActivateDisabledKeys (条件付き):
  - 説明: (条件付き) 入力パラメータ Action が に設定Restoreされ、PrincipalType が IAM ユーザーに設定されている場合、このオプションは、このオートメーションが非アクティブ化された場合に関連付けられたアクセスキーをアクティブ化しようとするかどうかを決定します。侵害されたアクセスキーの整合性は検証できないことに注意してください。 AWS では、侵害されたキーの再アクティブ化を強くお勧めします。代わりに、新しいキーを生成することをお勧めします。デフォルト値: false。
  - 型: ブール値
  - 使用できる値: true|false
- BackupS3BucketName (条件付き):
  - 説明: (条件付き) アクションが に設定されている場合に IAM プリンシパル設定をバックアップする Amazon S3 バケット、Containまたはアクションが に設定されている場合に から設定を復元する Amazon S3 バケットRestore。指定されたアクションが Containで、ランブックがバケットにアクセスできない場合、または値が指定されていない場合、アカウントに という名前の新しいバケットが作成されますawssupport-containiamprincipal-<random-string>。DryRun が に設定されている場合、trueこのパラメータは必須です。
  - 型: AWS::S3::Bucket::Name
- BackupS3KeyName (条件付き):
  - 説明: (条件付き) Action が に設定されている場合Restore、オートメーションが IAM プリンシパル設定の復元を試みるために使用する Amazon S3 キーを指定します。Amazon S3 キーは通常、 の形式に従います{year}/{month}/{day}/{hour}/{minute}/

{automation_execution_id}.json。キーは、前の封じ込め自動化実行の出力から取得できます。

- タイプ: 文字列
- 許可されたパターン: ^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$

- BackupS3BucketAccess (条件付き):
  - 説明: (条件付き) 封じ込めアクションを実行した後にバックアップ Amazon S3 バケットへのアクセスを許可する IAM ユーザーまたはロールの ARN。このパラメータは、アクションがの場合に必要ですContain。AutomationAssumeRole、または自動化が実行されているコンテキストのユーザーが存在しない場合は、自動的にリストに追加されます。
  - タイプ: StringList
  - 許可されたパターン: ^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$
- TagIdentifier (オプション):
  - 説明: (オプション) 次の形式を使用して、IAM プリンシパルに任意のタグを付けます。Key=<EXAMPLE_KEY>,Value=<EXAMPLE_VALUE>このオプションを使用すると、このランブックの対象となる IAM プリンシパルを追跡できます。注： タグキーと値は大文字と小文字が区別されます。
  - タイプ: 文字列
  - 許可されたパターン: ^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\._\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\._\\:\\/@a-zA-Z0-9]{0,128}$

4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - ValidateRequiredInputs

     Action 指定された に基づいて、必要なオートメーション入力パラメータを検証します。
   - CheckBackupS3BucketName

     ターゲット Amazon Amazon S3 バケットがオブジェクトへのwriteパブリックアクセスを許可readしている可能性があるかどうかを確認します。封じ込めワークフローの場合、バケットが存在しない場合、新しい Amazon S3 BackupS3BucketNameバケットが作成されます。
   - BranchOnAction

指定された の値に基づいてオートメーションを分岐しますAction。

- BranchOnPrincipalTypeAndDryRun

  IAM プリンシパルのタイプ (IAM ユーザー、IAM ロール、または Identity Center ユーザー) と、DryRun モードで実行されているかどうかに基づいてオートメーションを分岐します。

- BranchOnPrincipalTypeForContain

  Contain アクションベースのオートメーションと、入力で指定された IAM プリンシパルタイプ (IAM ユーザー、IAM ロール、または Identity Center ユーザー) を分岐します。

- GetIAMUser

  ターゲット IAM ユーザーの作成時刻とユーザー名を取得します。

- GetIAMUserDetails

  インラインポリシー、 管理ポリシー、アクセスキー、MFA デバイス、ログインプロファイルなど、ターゲット IAM ユーザーの設定を取得して保存します。

- UpdateS3KeyForUser

  ステップ の出力からオートメーション 'S3Key' 変数を更新しますGetIAMUserDetails。

- GetIAMRole

  ターゲット IAM ロールの作成時刻、ロール名、パスを取得します。

- GetIAMRoleDetails

  ロールにアタッチされたインラインポリシーや管理ポリシーなど、ターゲット IAM ロールの設定を取得して保存します。

- UpdateS3KeyForRole

  ステップ の出力からオートメーション 'S3Key' 変数を更新しますGetIAMRoleDetails。

- GetIdentityStoreId

  AWS アカウントに関連付けられた AWS IAM Identity Center インスタンスの ID を取得します。

- GetIDCUser

  Identity Store ID を使用して、ターゲット Identity Center ユーザーのユーザー ID を取得します。

- GatherIDCUserDetails

アカウント割り当て、関連するアクセス許可セット、インラインポリシーなど、ターゲット Identity Center ユーザーの設定を取得して保存します。

- UpdateS3KeyForIDCUser

  ステップ の出力からオートメーション 'S3Key' 変数を更新しますGatherIDCUserDetails。

- BranchOnIdentityContain

  アクションの値DryRunと IAM プリンシパルタイプに基づいてオートメーションを分岐しますContain。

- BranchOnDisableAccessKeys

  IAM ユーザーが無効化する必要があるアクセスキーを持っているかどうかに基づいて自動化を分岐します。

- DisableAccessKeys

  アクティブな IAM ユーザーアクセスキーを無効にします。

- BranchOnDisableConsoleAccess

  IAM ユーザーが AWS マネジメントコンソールへのアクセスを有効にしているかどうかに基づいて分岐します。

- DisableConsoleAccess

  IAM ユーザーの AWS マネジメントコンソールへのパスワードベースのアクセスを削除します。

- AttachInlineDenyPolicyToUser

  古いセッショントークンのアクセス許可を取り消す拒否ポリシーを IAM ユーザーにアタッチします。

- AttachInlineDenyPolicyToRole

  古いセッショントークンのアクセス許可を取り消す拒否ポリシーを IAM ロールにアタッチします。

- RemovePermissionSets

  Identity Center ユーザーに関連付けられたアクセス許可セットを削除します。

- RemoveIDCUserFromIDCGroups

Identity Center グループから Identity Center ユーザーを削除します。

- AttachInlineDenyPolicyToPermissionSet

  Identity Center ユーザーに関連付けられたアクセス許可セットに拒否ポリシーをアタッチします。

- BranchOnReactivateKeys

  復元プロセス中に `ActivateDisabledKeys`パラメータに基づいてオートメーションを分岐します。

- DetachInlineDenyPolicy

  封じ込めプロセス中に IAM ロールにアタッチされた拒否ポリシーを削除します。

- DetachInlineDenyPolicyFromPermissionSet

  封じ込めプロセス中にアクセス許可セットにアタッチされた拒否ポリシーを削除します。

- ReportContain

  `DryRun` が に設定されている場合に実行される封じ込めアクションに関する詳細情報を出力しますTrue。

- ReportRestore

  `DryRun` が に設定されている場合に実行される復元アクションに関する詳細情報を出力しますTrue。

- ReportContainFailure

  封じ込めワークフローの失敗シナリオ中に IAM プリンシパルの元の設定を手動で復元する包括的な手順を提供します。

- ReportRestoreFailure

  復元ワークフローの失敗シナリオ中に IAM プリンシパルの元の設定の復元を手動で完了する詳細な手順を示します。

7. 実行が完了したら、出力セクションで実行の詳細な結果を確認します。

- ContainIAMPrincipal.Output

  Action が Contain に設定され、DryRun が False に設定されている場合に実行される封じ込めアクションに関する詳細情報を提供します。バックアップの場所、適用された拒否ポリシー、および変更された設定に関する情報が含まれます。

- RestoreIAMPrincipal.Output

  Action が Restore に設定され、DryRun が False に設定されている場合に実行される復元アクションに関する詳細情報を提供します。復元された設定と、復元中に発生した問題に関する情報が含まれます。

- ReportContain.Output

  Action が Contain に設定され、DryRun が True に設定されている場合に実行される封じ込めアクションに関する詳細情報を出力します。現在の設定と封じ込め後の設定の比較が含まれます。

- ReportRestore.Output

  Action が Restore に設定され、DryRun が True に設定されている場合に実行される復元アクションに関する詳細情報を出力します。復元される現在の設定と元の設定を表示します。

- ReportContainFailure.Output

  封じ込めワークフローの失敗シナリオ中に IAM プリンシパルの元の設定を手動で復元する包括的な手順を提供します。

- ReportRestoreFailure.Output

  復元ワークフローの失敗シナリオ中に IAM プリンシパルの元の設定の復元を手動で完了する詳細な手順を示します。

出力

実行が完了したら、出力セクションで詳細な結果を確認します。

- ContainIAMPrincipal.Output

  Action が Contain に設定され、DryRun が False に設定されている場合に実行される封じ込めアクションに関する詳細情報を提供します。バックアップの場所、適用された拒否ポリシー、および変更された設定に関する情報が含まれます。

- RestoreIAMPrincipal.Output

  Action が Restore に設定され、DryRun が False に設定されている場合に実行される復元アクションに関する詳細情報を提供します。復元された設定と、復元中に発生した問題に関する情報が含まれます。

- ReportContain.Output

Action が Contain に設定され、DryRun が True に設定されている場合に実行される封じ込めアクションに関する詳細情報を出力します。現在の設定と封じ込め後の設定の比較が含まれます。

- ReportRestore.Output

  Action が Restore に設定され、DryRun が True に設定されている場合に実行される復元アクションに関する詳細情報を出力します。復元される現在の設定と元の設定を表示します。

- ReportContainFailure.Output

  封じ込めワークフローの失敗シナリオ中に IAM プリンシパルの元の設定を手動で復元する包括的な手順を提供します。

- ReportRestoreFailure.Output

  復元ワークフローの失敗シナリオ中に IAM プリンシパルの元の設定の復元を手動で完了する詳細な手順を示します。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- シンプルなオートメーションワークフローを実行する
- 自動化のセットアップ
- オートメーションワークフローのサポート

Amazon Kinesis Data Streams

AWS Systems Manager Automation は、Amazon Kinesis Data Streams 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-EnableKinesisStreamEncryption

AWS-EnableKinesisStreamEncryption

説明

AWS-EnableKinesisStreamEncryption ランブックは、Amazon Kinesis Data Streams (Kinesis Data Streams) で暗号化を有効にします。暗号化されたストリームに書き込むプロデューサーアプリケーションは、 AWS Key Management Service （ AWS KMS) キーにアクセスできない場合にエラーが発生します。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- KinesisStreamName

  タイプ: 文字列

  説明: (必須) 暗号化を有効にするストリームの名前。
- KeyId

  タイプ: 文字列

  デフォルト: alias/aws/kinesis

  説明: (必須) 暗号化に使用するカスタマーマネージド AWS KMS キー。この値は、グローバルに一意の識別子、エイリアスまたはキーへの ARN、または「alias/」というプレフィックスが付いたエ

イリアス名にすることができます。パラメータのデフォルト値を使用して、 AWS マネージドキーを使用することもできます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- kinesis:DescribeStream
- kinesis:StartStreamEncryption
- kms:DescribeKey

ドキュメントステップ

- VerifyKinesisStreamStatus (aws:waitforAwsResourceProperty) - Kinesis Data Streams のステータスを確認します。
- EnableKinesisStreamEncryption (aws:executeAwsApi) - Kinesis Data Streams の暗号化を有効にします。
- VerifyKinesisStreamUpdateComplete (aws:waitForAwsResourceProperty) - Kinesis Data Streams のステータスが に戻るのを待ちますACTIVE。
- VerifyKinesisStreamEncryption (aws:assertAwsResourceProperty) - Kinesis Data Streams で暗号化が有効になっていることを確認します。

AWS KMS

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Key Management Service。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-CancelKeyDeletion
- AWSConfigRemediation-EnableKeyRotation

AWSConfigRemediation-CancelKeyDeletion

説明

AWSConfigRemediation-CancelKeyDeletion ランブックは、指定した AWS Key Management Service（ AWS KMS) カスタマーマネージドキーの削除をキャンセルします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- KeyId

  タイプ: 文字列

  説明: (必須) 削除をキャンセルするカスタマーマネージドキーの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- kms:CancelKeyDeletion
- kms:DescribeKey

ドキュメントステップ

- aws:executeAwsApi - KeyId パラメータで指定したカスタマーマネージドキーの削除をキャンセルします。
- aws:assertAwsResourceProperty - カスタマーマネージドキーでキーの削除が無効になっていることを確認します。

AWSConfigRemediation-EnableKeyRotation

説明

AWSConfigRemediation-EnableKeyRotation ランブックは、symmetric AWS Key Management Service（ AWS KMS) カスタマーマネージドキーの自動キーローテーションを有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- KeyId

  タイプ: 文字列

  説明: (必須) 自動キーローテーションを有効にするカスタマーマネージドキーの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:EnableKeyRotation
- kms:GetKeyRotationStatus

ドキュメントステップ

- aws:executeAwsApi - KeyId パラメータで指定されたカスタマーマネージドキーの自動キーローテーションを有効にします。
- aws:assertAwsResourceProperty - カスタマーマネージドキーで自動キーローテーションが有効になっていることを確認します。

Lambda

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Lambda。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing
- AWSConfigRemediation-DeleteLambdaFunction
- AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK
- AWSConfigRemediation-MoveLambdaToVPC
- AWSSupport-RemediateLambdaS3Event

- AWSSupport-TroubleshootLambdaInternetAccess
- AWSSupport-TroubleshootLambdaS3Event

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

説明

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing ランブックは、FunctionNameパラメータで指定した AWS Lambda 関数で AWS X-Ray ライブトレースを有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- FunctionName

  タイプ: 文字列

  説明: (必須) トレースを有効にする Lambda 関数の名前または ARN。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- lambda:UpdateFunctionConfiguration
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

ドキュメントステップ

- aws:executeAwsApi - FunctionName パラメータで指定された Lambda 関数で X-Ray トレースを有効にします。
- aws:assertAwsResourceProperty - Lambda 関数で X-Ray トレースが有効になっているかを確認します。

出力

UpdateLambdaConfig.UpdateFunctionConfigurationResponse - UpdateFunctionConfiguration API コールからの応答。

AWSConfigRemediation-DeleteLambdaFunction

説明

AWSConfigRemediation-DeleteLambdaFunction ランブックは指定した AWS Lambda 機能を削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- LambdaFunctionName

  タイプ: 文字列

  説明: (必須) 削除される Lambda 関数の名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:DeleteFunction
- lambda:GetFunction

ドキュメントステップ

- aws:executeAwsApi - LambdaFunctionName パラメータで指定された Lambda 関数を削除します。
- aws:executeScript - Lambda 関数が削除されたことを確認します。

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

説明

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK ランブックは、AWS Key Management Service () カスタマーマネージドキーを使用して、指定した AWS Lambda

(Lambda AWS KMS) 関数の環境変数を保管時に暗号化します。このランブックは、推奨される最小限セキュリティのベストプラクティスに従って Lambda 関数の環境変数が暗号化されるようにするための、ベースラインとしてのみ使用するようにします。複数の関数は、それぞれ異なるカスタマーマネージドキーを使用して暗号化することをお勧めします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- FunctionName

  タイプ: 文字列

  説明: (必須) 暗号化する環境変数を持つ Lambda 関数の名前または ARN。
- KMSKeyArn

  タイプ: 文字列

  説明: (必須) Lambda 関数の環境変数の暗号化に使用する AWS KMS カスタマーマネージドキーの ARN。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:GetFunctionConfiguration
- lambda:UpdateFunctionConfiguration

ドキュメントステップ

- aws:waitForAwsResourceProperty - LastUpdateStatus プロパティが Successful になるのを待ちます。
- aws:executeAwsApi - FunctionNameパラメータで指定した AWS KMS カスタマーマネージドキーを使用して、 KMSKeyArnパラメータで指定した Lambda 関数の環境変数を暗号化します。
- aws:assertAwsResourceProperty - Lambda 関数の環境変数の暗号化が有効になっていることを確認します。

AWSConfigRemediation-MoveLambdaToVPC

説明

AWSConfigRemediation-MoveLambdaToVPC ランブックは、 AWS Lambda (Lambda) 関数を Amazon Virtual Private Cloud (Amazon VPC) に移動します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- FunctionName

  タイプ: 文字列

  説明: (必須) Amazon VPC に移動する Lambda 関数の名前。
- SecurityGroupIds

  タイプ: 文字列

  説明: (必須) Lambda 関数に関連付けられた Elastic Network Interface (ENI) に割り当てるセキュリティグループ ID。
- SubnetIds

  タイプ: 文字列

  説明: (必須) Lambda 関数に関連付けられた Elastic Network Interface (ENI) を作成するサブネット ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

ドキュメントステップ

- aws:executeAwsApi - FunctionName パラメータで指定した Lambda 関数の Amazon VPC 設定を更新します。
- aws:waitForAwsResourceProperty - Lambda 関数 LastUpdateStatus が successful になるのを待ちます。
- aws:executeScript - Lambda 関数の Amazon VPC 設定が正常に更新されたことを確認します。

AWSSupport-RemediateLambdaS3Event

説明

AWSSupport-TroubleshootLambdaS3Event ランブックは、 AWS ナレッジセンターの記事Amazon S3 イベント通知が Lambda 関数をトリガーしないのはなぜですか？」および「次の送信先設定を検証できない」というエラーが、Lambda 関数をトリガーする Amazon S3 イベント通知を作成するときに表示されるのはなぜですか？」で説明されている手順の自動ソリューションを提供します。このランブックは、Amazon Simple Storage Service (Amazon S3) イベント通知が指定した AWS Lambda 関数のトリガーに失敗した理由を特定して修正するのに役立ちます。ランブックの出力で Lambda 関数の同時実行の検証と設定が提案されている場合は、「非同期呼び出し」と「AWS Lambda 関数のスケーリング」を参照してください。

> **Note**
>
> Amazon Simple Notification Service (Amazon SNS) と Amazon Simple Queue Service (Amazon SQS) Amazon S3 イベントの設定が正しくないために、「以下の送信先設定を検証できません」というエラーが発生する可能性もあります。このランブックは Lambda 関数の設定のみをチェックします。ランブックを使用した後も「以下の送信先設定を検証できません」というエラーが表示される場合は、既存の Amazon SNS および Amazon SQS Amazon S3 イベント設定を確認してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- LambdaFunctionArn

  タイプ: 文字列

  説明: (必須) Lambda 関数の ARN。

- S3BucketName

  タイプ: 文字列

  説明: (必須) イベント通知が Lambda 関数をトリガーする Amazon S3 バケットの名前。

- アクション

  タイプ: 文字列

  有効な値: トラブルシューティング | 修復

  説明: (必須) ランブックで実行したいアクション。この `Troubleshoot` オプションは問題の特定に役立ちますが、問題を解決するための変更アクションは実行しません。この `Remediate` オプションは問題を特定し、ユーザーに代わって解決を試行する上で役立ちます。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`

- ssm:GetDocument
- ssm:ListDocuments
- ssm:DescribeAutomationExecutions
- ssm:DescribeAutomationStepExecutions
- ssm:GetAutomationExecution
- lambda:GetPolicy
- lambda:AddPermission
- s3:GetBucketNotification

ドキュメントステップ

- aws:branch - Action パラメータで指定した入力に基づいて分岐させます。

  指定した値が Troubleshoot である場合:

  - aws:executeAutomation - AWSSupport-TroubleshootLambdaS3Event ランブックを実行します。
  - aws:executeAwsApi - 前のステップで実行した AWSSupport-TroubleshootLambdaS3Event ランブックの出力を確認します。

  指定した値が Remediate である場合:

  - aws:executeScript - Amazon S3 イベント通知で Lambda 関数がトリガーされないのはなぜですか?および、Lambda 関数をトリガーする Amazon S3 イベント通知を作成するときに「以下の送信先設定を検証できません」というエラーが表示されるのはなぜですか?で説明されている問題を修正するためのスクリプトを実行します。ナレッジセンターの記事。

出力

checkoutput.Output

remediatelambdas3event.Output

AWSSupport-TroubleshootLambdaInternetAccess

説明

AWSSupport-TroubleshootLambdaInternetAccess ランブックは、Amazon Virtual Private Cloud (Amazon VPC) で起動された AWS Lambda 関数のインターネットアクセスに関する問題の

トラブルシューティングに役立ちます。サブネットルート、セキュリティグループルール、ネットワークアクセスコントロールリスト (ACL) ルールなどのリソースを確認して、アウトバウンドのインターネットアクセスが許可されていることを確認します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- FunctionName

  タイプ: 文字列

  説明: (必須) インターネットアクセスのトラブルシューティングを行う Lambda 関数の名前。
- destinationIp

  タイプ: 文字列

  説明: (必須) アウトバウンド接続を確立する宛先 IP アドレス。
- destinationPort

  タイプ: 文字列

デフォルト: 443

説明: (オプション) アウトバウンド接続を確立する宛先ポート。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- lambda:GetFunction
- ec2:DescribeRouteTables
- ec2:DescribeNatGateways
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkAcls

ドキュメントステップ

- aws:executeScript - Lambda 関数が起動された VPC 内のさまざまなリソースの設定を検証します。
- aws:branch - 指定された Lambda 関数が VPC 内にあるかどうかに基づいて分岐させます。
- aws:executeScript - Lambda 関数が起動されたサブネットのルートテーブルルートを確認し、ネットワークアドレス変換 (NAT) ゲートウェイとインターネットゲートウェイへのルートが存在することを確認します。Lambda 関数がパブリックサブネットにないことを確認します。
- aws:executeScript - destinationIp および destinationPort パラメータに指定された値に基づいて、Lambda 関数に関連付けられたセキュリティグループがアウトバウンドインターネットアクセスを許可していることを確認します。
- aws:executeScript - destinationIp および destinationPort パラメータに指定された値に基づいて、Lambda 関数のサブネットに関連付けられた ACL ルールと NAT ゲートウェイがアウトバウンドインターネットアクセスを許可していることを確認します。

出力

checkVpc.vpc - Lambda 関数が起動された VPC の ID。

checkVpc.subnet - Lambda 関数が起動された サブネットの ID。

checkVpc.securityGroups - Lambda 関数に関連付けられたセキュリティグループ。

checkNACL.NACL - リソース名を含む分析メッセージ。LambdaIp とは、Lambda 関数の エラスティックネットワークインターフェイスのプライベート IP アドレスを指します。LambdaIpRules オブジェクトは NAT ゲートウェイへのルートがあるサブネットに対してのみ生成されます。次のコンテンツは出力の例です。

```
{
   "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 - Lambda 関数に関連付けられているセキュリティグループの分析。次のコンテンツは出力の例です。

```
{
   "sg-123456789":{
      "Status":"Allowed",
      "Analysis":"This security group has allowed destintion IP and port in its
 outbuond rule."
   }
```

```
}
```

checkSubnet.subnets - Lambda 関数に関連付けられた VPC 内のサブネットの分析。次のコンテンツは出力の例です。

```
{
   "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

説明

AWSSupport-TroubleshootLambdaS3Event ランブックは、 AWS ナレッジセンターの記事Amazon S3 イベント通知が Lambda 関数をトリガーしないのはなぜですか？」および「次の送信先設定を検証できない」というエラーが、Lambda 関数をトリガーする Amazon S3 イベント通知を作成するときに表示されるのはなぜですか？」で説明されている手順の自動ソリューションを提供します。 このランブックは、Amazon Simple Storage Service (Amazon S3) イベント通知が指定した AWS Lambda 関数のトリガーに失敗した理由を特定するのに役立ちます。ランブックの出力で Lambda 関数の同時実行の検証と設定が提案されている場合は、「非同期呼び出し」と「AWS Lambda 関数のスケーリング」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- LambdaFunctionArn

  タイプ: 文字列

  説明: (必須) Amazon S3 イベント通知がトリガーする Lambda 関数 の ARN。
- S3BucketName

  タイプ: 文字列

  説明: (必須) イベント通知が Lambda 関数をトリガーする Amazon S3 バケットの名前。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

ドキュメントステップ

- `aws:executeScript` - Amazon S3 イベント通知の構成設定を検証するスクリプトを実行します。Lambda 関数のリソースベースの IAM ポリシーを検証し、必要なアクセス許可がポリシーにない場合に必要なアクセス許可を追加する AWS Command Line Interface （ AWS CLI) コマンドを生成します。同じ S3 バケットのイベント通知の一部である他の Lambda 関数リソースポリシーを検証し、必要なアクセス許可がない場合は出力として AWS CLI コマンドを生成します。

出力

lambdaS3Event.output

Amazon Managed Workflows for Apache Airflow

AWS Systems Manager Automation は、Amazon Managed Workflows for Apache Airflow 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-TroubleshootMWAAEnvironmentCreation

AWSSupport-TroubleshootMWAAEnvironmentCreation

説明

AWSSupport-TroubleshootMWAAEnvironmentCreation ランブックには、Amazon Managed Workflows for Apache Airflow (Amazon MWAA) の環境作成の問題をデバッグし、障害の特定に役立つよう、文書化された理由とともにチェックを実行するための情報が記載されています。

動作の仕組み

ランブックは次のステップを実行します。

- Amazon MWAA 環境の詳細を取得します。
- 実行ロールのアクセス許可を検証します。
- 環境がログ記録に指定された AWS KMS キーを使用するアクセス許可を持っているかどうか、および必要な CloudWatch ロググループが存在するかどうかを確認します。
- 指定されたロググループのログを解析して、エラーを見つけます。
- ネットワーク設定をチェックして、Amazon MWAA 環境が必要なエンドポイントにアクセスできるかどうかを確認します。
- 結果を含むレポートを生成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

/

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

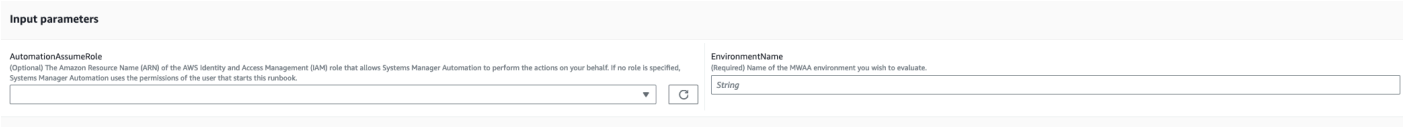
指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager AWSSupport-TroubleshootMWAAEnvironmentCreationで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - EnvironmentName (必須):

     評価する Amazon MWAA 環境の名前。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - **GetMWAAEnvironmentDetails:**

     Amazon MWAA 環境の詳細を取得します。このステップが失敗すると、自動化プロセスは停止し、 と表示されますFailed。
   - **CheckIAMPermissionsOnExecutionRole:**

実行ロールに Amazon MWAA、Amazon S3、CloudWatch Logs、CloudWatch、Amazon SQS リソースに必要なアクセス許可があることを確認します。カスタマーマネージド AWS Key Management Service（ AWS KMS) キーが検出されると、オートメーションはキーに必要なアクセス許可を検証します。このステップでは、 `iam:SimulateCustomPolicy` API を使用して、自動化実行ロールがすべての必要なアクセス許可を満たしているかどうかを確認します。

- **CheckKMSPolicyOnKMSKey:**

  AWS KMS キーポリシーで、Amazon MWAA 環境で CloudWatch Logs の暗号化にキーの使用が許可されているかどうかを確認します。 AWS KMS キーが AWS管理されている場合、オートメーションはこのチェックをスキップします。

- **CheckIfRequiredLogGroupsExists:**

  Amazon MWAA 環境に必要な CloudWatch ロググループが存在するかどうかを確認します。そうでない場合、自動化は CloudTrail で `CreateLogGroup`および `DeleteLogGroup`イベントをチェックします。このステップでは、 `CreateLogGroup`イベントもチェックします。

- **BranchOnLogGroupsFindings:**

  Amazon MWAA 環境に関連する CloudWatch ロググループの存在に基づいて分岐します。少なくとも 1 つのロググループが存在する場合、自動化はそれを解析してエラーを見つけます。ロググループが存在しない場合、オートメーションは次のステップをスキップします。

- **CheckForErrorsInLogGroups:**

  CloudWatch ロググループを解析してエラーを見つけます。

- **GetRequiredEndPointsDetails:**

  Amazon MWAA 環境で使用されるサービスエンドポイントを取得します。

- **CheckNetworkConfiguration:**

  Amazon MWAA 環境のネットワーク設定が、セキュリティグループ、ネットワーク ACLs、サブネット、ルートテーブル設定のチェックなどの要件を満たしていることを確認します。

- **CheckEndpointsConnectivity:**

  `AWSSupport-ConnectivityTroubleshooter` 子オートメーションを呼び出して、必要なエンドポイントへの Amazon MWAA の接続を検証します。

- **CheckS3BlockPublicAccess:**

Amazon MWAA 環境の Amazon S3 バケットBlock Public Accessが有効になっているかどうかを確認し、アカウントの全体的な Amazon S3 パブリックアクセスブロック設定も確認します。

- **GenerateReport:**

  オートメーションから情報を収集し、各ステップの結果または出力を出力します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。
   - Amazon MWAA 環境実行ロールのアクセス許可の確認：

     実行ロールに Amazon MWAA、Amazon S3、CloudWatch Logs、CloudWatch、Amazon SQS リソースに必要なアクセス許可があるかどうかを検証します。カスタマーマネージド AWS KMS キーが検出されると、オートメーションはキーに必要なアクセス許可を検証します。
   - Amazon MWAA 環境 AWS KMS キーポリシーの確認：

     実行ロールが Amazon MWAA、Amazon S3、CloudWatch Logs、CloudWatch、Amazon SQS リソースに必要なアクセス許可を持っているかどうかを確認します。さらに、カスタマーマネージド AWS KMS キーが検出されると、オートメーションはキーに必要なアクセス許可をチェックします。
   - Amazon MWAA 環境の CloudWatch ロググループの確認：

     Amazon MWAA 環境に必要な CloudWatch Log Groups が存在するかどうかを確認します。そうでない場合、自動化は CloudTrail をチェックして CreateLogGroupおよび DeleteLogGroupイベントを見つけます。
   - Amazon MWAA 環境のルートテーブルの確認：

     Amazon MWAA 環境の Amazon VPC ルートテーブルが正しく設定されているかどうかを確認します。
   - Amazon MWAA 環境のセキュリティグループの確認：

     Amazon MWAA 環境の Amazon VPC セキュリティグループが正しく設定されているかどうかを確認します。
   - Amazon MWAA 環境のネットワーク ACLs の確認：

     Amazon MWAA 環境の Amazon VPC セキュリティグループが正しく設定されているかどうかを確認します。
   - Amazon MWAA 環境サブネットの確認：

Amazon MWAA 環境のサブネットがプライベートかどうかを確認します。

- Amazon MWAA 環境に必要なエンドポイント接続の確認：

  Amazon MWAA 環境が必要なエンドポイントにアクセスできるかどうかを確認します。この目的のために、オートメーションはAWSSupport-ConnectivityTroubleshooterオートメーションを呼び出します。

- Amazon MWAA 環境の Amazon S3 バケットの確認：

  Amazon MWAA 環境の Amazon S3 バケットBlock Public Accessが有効になっているかどうかを確認し、アカウントの Amazon S3 パブリックアクセスブロック設定も確認します。

- Amazon MWAA 環境の CloudWatch ロググループのエラーを確認する：

  Amazon MWAA 環境の既存の CloudWatch ロググループを解析してエラーを見つけます。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

Neptune

AWS Systems Manager 自動化は、Amazon Neptune 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-EnableNeptuneDbAuditLogsToCloudWatch
- AWS-EnableNeptuneDbBackupRetentionPeriod
- AWS-EnableNeptuneClusterDeletionProtection

AWS-EnableNeptuneDbAuditLogsToCloudWatch

説明

AWS-EnableNeptuneDbAuditLogsToCloudWatch ランブックは、Amazon Neptune DB クラスターの監査ログを Amazon CloudWatch Logs に送信するのに役立ちます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム

(ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- DbClusterResourceId

  タイプ: 文字列

  説明: (必須) 監査ログを有効にする Neptune DB クラスターのリソース ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

ドキュメントステップ

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Neptune DB クラスターの ID を返します。
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty) - Neptune DB エンジンタイプがであることを確認しますneptune。
- EnableNeptuneDbAuditLogs (aws:executeAwsApi) - Neptune DB クラスターの監査ログを CloudWatch Logs に送信できるようにします。
- VerifyNeptuneDbStatus (aws:waitAwsResourceProperty) - Neptune DB クラスターのステータスが であることを確認しますavailable。
- VerifyNeptuneDbAuditLogs (aws:executeScript) - 監査ログが CloudWatch Logs に送信するように正常に設定されていることを確認します。

AWS-EnableNeptuneDbBackupRetentionPeriod

説明

AWS-EnableNeptuneDbBackupRetentionPeriod ランブックは、Amazon Neptune DB クラスターのバックアップ保持期間を 7～35 日として自動バックアップを有効にするのに役立ちます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- DbClusterResourceId

  タイプ: 文字列

  説明: (必須) バックアップを有効にする Neptune DB クラスターのリソース ID。

- BackupRetentionPeriod

  タイプ: 整数

  有効な値: 7～35

説明: (必須) バックアップが保持される日数。

- PreferredBackupWindow

  タイプ: 文字列

  説明: (オプション) バックアップが作成されるまでの 1 日あたりの 30 分以上の期間。値は協定世界時 (UTC) で、 の形式を使用する必要がありますhh24:mm-hh24:mm。バックアップ保持期間は、希望するメンテナンスウィンドウと競合できません。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

ドキュメントステップ

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Neptune DB クラスターの ID を返します。
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty) - Neptune DB エンジンタイプがであることを確認しますneptune。
- VerifyNeptuneDbStatus (aws:waitAwsResourceProperty) - Neptune DB クラスターのステータスが であることを確認しますavailable。
- ModifyNeptuneDbRetentionPeriod (aws:executeAwsApi) - Neptune DB クラスターの保持期間を設定します。
- VerifyNeptuneDbBackupsEnabled (aws:executeScript) - 保持期間とバックアップウィンドウが正常に設定されたことを確認します。

AWS-EnableNeptuneClusterDeletionProtection

説明

AWS-EnableNeptuneClusterDeletionProtection ランブックは、指定した Amazon Neptune クラスターの削除保護を有効にします。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- DbClusterResourceId

  タイプ: 文字列

  説明: (必須) 削除保護を有効にする Neptune クラスターの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:GetAutomationExecution

- ssm:StartAutomationExecution
- neptune:DescribeDBCluster
- neptune:ModifyDBCluster
- rds:DescribeDBClusters
- rds:ModifyDBCluster

ドキュメントステップ

- GetNeptuneDbClusterIdentifier (aws:executeAwsApi) - Neptune DB クラスターの ID を返します。
- VerifyNeptuneDbEngine (aws:assertAwsResourceProperty) - 指定された DB クラスターのエンジンタイプが であることを確認しますneptune。
- VerifyNeptuneStatus (aws:waitForAwsResourceProperty) - クラスターのステータスが であることを確認しますavailable。
- EnableNeptuneDbDeletionProtection (aws:executeAwsApi) - Neptune DB クラスターの削除保護を有効にします。
- VerifyNeptuneDbDeletionProtection (aws:assertAwsResourceProperty) - DB クラスターで削除保護が有効になっていることを確認します。

出力

- EnableNeptuneDbDeletionProtection.EnableNeptuneDbDeletionProtectionResponse - API オペレーションからの出力。

Amazon RDS

AWS Systems Manager Automation は、Amazon Relational Database Service 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- 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

説明

AWS-CreateEncryptedRdsSnapshot ランブックは、暗号化されていない Amazon Relational Database Service (Amazon RDS) インスタンスから暗号化されたスナップショットを作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- DB インスタンス識別子

  タイプ: 文字列

  説明: (必須) スナップショットを作成する Amazon RDS インスタンスの ID。
- DBSnapshotIdentifier

  タイプ: 文字列

  説明: (オプション) Amazon RDS スナップショットの名前テンプレート。デフォルトの名前テンプレートは *DBInstanceIdentifier-yyyymmddhhmmss* です。
- EncryptedDBSnapshotIdentifier

  タイプ: 文字列

  説明: (オプション) 暗号化されたスナップショットの名前。デフォルト名は、 に追加された `DBSnapshotIdentifier`パラメータに指定した値です`-encrypted`。

- InstanceTags

  タイプ: 文字列

  説明: (オプション) DB インスタンスに追加するタグ。 (例: Key=tagKey1,Value=tagValue1;Key=tagKey2,Value=tagValue2)'
- KmsKeyId

  タイプ: 文字列

  デフォルト: `alias/aws/rds`

  説明: (オプション) スナップショットの暗号化に使用するカスタマーマネージドキーの ARN、キー ID、またはキーエイリアス。
- SnapshotTags

  タイプ: 文字列

  説明: (オプション) スナップショットに追加するタグ。 (例: Key=tagKey1,Value=tagValue1;Key=tagKey2,Value=tagValue2)'

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds:CreateDBSnapshot`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

ドキュメントステップ

- `aws:executeScript` - `DBInstanceIdentifier`パラメータで指定した DB インスタンスのスナップショットを作成します。
- `aws:executeScript` - 前のステップで作成したスナップショットが存在し、 であることを確認します`available`。

- aws:executeScript - 以前に作成したスナップショットを暗号化されたスナップショットにコピーします。
- aws:executeScript - 前のステップで作成した暗号化されたスナップショットが存在することを確認します。

出力

CopyRdsSnapshotToEncryptedRdsSnapshot.EncryptedSnapshotId - 暗号化された Amazon RDS スナップショットの ID。

AWS-CreateRdsSnapshot

説明

Amazon RDS インスタンスの Amazon Relational Database Service (Amazon RDS) スナップショットを作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- DB インスタンス識別子

  タイプ: 文字列

  説明: (必須) スナップショットの作成元の RDS インスタンスの DBInstanceId ID です。
- DBSnapshotIdentifier

  タイプ: 文字列

  説明: (オプション) 作成する RDS スナップショットの DBSnapshotIdentifier ID です。
- InstanceTags

  タイプ: 文字列

  説明: (オプション) インスタンス用に作成するタグです。
- SnapshotTags

  タイプ: 文字列

  説明: (オプション) スナップショット用に作成するタグです。

ドキュメントステップ

createRDSSnapshot – RDS スナップショット を作成し、スナップショット ID を返します。

verifyRDSSnapshot – 前のステップで作成したスナップショットが存在することを確認します。

出力

createRDSSnapshot.SnapshotId – 作成されたスナップショットの ID です。

AWSConfigRemediation-DeleteRDSCluster

説明

AWSConfigRemediation-DeleteRDSCluster ランブックは、指定した Amazon Relational Database Service (Amazon RDS) クラスターを削除します。このオートメーションを実行する AWS リージョン で を有効にする AWS Config 必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DBClusterId

  タイプ: 文字列

  説明: (必須) 削除保護を有効にする DB クラスターのリソース識別子。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DeleteDBCluster`
- `rds:DeleteDBInstance`
- `rds:DescribeDBClusters`

ドキュメントステップ

- aws:executeScript - DBClusterId パラメータで指定した DB クラスターを削除します。

AWSConfigRemediation-DeleteRDSClusterSnapshot

説明

AWSConfigRemediation-DeleteRDSClusterSnapshot ランブックは、指定された Amazon Relational Database Service (Amazon RDS) クラススナップショットを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DBClusterSnapshotId

  タイプ: 文字列

  説明: (必須) 削除する Amazon RDS クラススナップショット識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DeleteDBClusterSnapshot
- rds:DescribeDBClusterSnapshots

ドキュメントステップ

- aws:branch - クラススナップショットが available 状態にあるかどうかを確認します。使用できない場合、フローは終了します。
- aws:executeAwsApi - データベース (DB) クラススナップショット識別子を使用して、指定された Amazon RDS クラススナップショットを削除します。
- aws:executeScript - 指定された Amazon RDS クラススナップショットが削除されたことを検証します。

AWSConfigRemediation-DeleteRDSInstance

説明

AWSConfigRemediation-DeleteRDSInstance ランブックは、指定した Amazon Relational Database Service (Amazon RDS) インスタンスを削除します。データベース (DB) インスタンスを削除すると、そのインスタンスの自動バックアップはすべて削除され、復旧することはできません。手動 DB スナップショットは削除されません。削除する DB インスタンスが failed、incompatible-network または incompatible-restore 状態の場合は、SkipFinalSnapshot パラメータを true に設定する必要があります。

> **Note**
>
> 削除する DB インスタンスが Amazon Aurora DB クラスターにある場合に、そのインスタンスがリードレプリカで DB クラスター内の唯一のインスタンスである場合には、ランブックは DB インスタンスを削除しません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- DbiResourceId

  タイプ: 文字列

  説明: (必須) 削除する DB インスタンスのリソース識別子。

- SkipFinalSnapshot

  型: ブール値

  デフォルト: false

  説明: (オプション) `true` に設定すると、DB インスタンスが削除されるまで最終的なスナップショットは作成されません。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBInstance`
- `rds:DescribeDBInstances`

ドキュメントステップ

- aws:executeAwsApi - DbiResourceId パラメータで指定した値から DB インスタンス名を収集します。
- aws:branch - SkipFinalSnapshot パラメータで指定した値に基づいて分岐させます。
- aws:executeAwsApi - DbiResourceId パラメータで指定した DB インスタンスを削除します。
- aws:executeAwsApi - 最終的なスナップショットが作成された後、DbiResourceId パラメータで指定した DB インスタンスを削除します。
- aws:assertAwsResourceProperty - DB インスタンスが削除されたことを確認します。

AWSConfigRemediation-DeleteRDSInstanceSnapshot

説明

AWSConfigRemediation-DeleteRDSInstanceSnapshot ランブックは、指定した Amazon Relational Database Service (Amazon RDS) インスタンススナップショットを削除します。available 状態のスナップショットのみが削除されます。このランブックでは、Amazon Aurora データベースインスタンスのスナップショットの削除はサポートされていません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- DbSnapshotId

  タイプ: 文字列

  説明: (必須) 削除されるスナップショットの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DeleteDBSnapshot
- rds:DescribeDBSnapshots

ドキュメントステップ

- aws:executeAwsApi - DbSnapshotId パラメータで指定されたスナップショットの状態を収集します。
- aws:assertAwsResourceProperty - スナップショットの状態が available であることを確認します。
- aws:executeAwsApi - DbSnapshotId パラメータで指定されたスナップショットを削除します。
- aws:executeScript - スナップショットが削除されたことを確認します。

AWSConfigRemediation-DisablePublicAccessToRDSInstance

説明

AWSConfigRemediation-DisablePublicAccessToRDSInstance ランブックは、指定した Amazon Relational Database Service (Amazon RDS) データベース (DB) インスタンスのパブリックアクセシビリティを無効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DbiResourceId

  タイプ: 文字列

  説明: (必須) パブリックアクセシビリティを無効にする DB インスタンスのリソース識別子。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

ドキュメントステップ

- aws:executeAwsApi - DB インスタンスリソース識別子から DB インスタンス識別子を収集します。
- aws:assertAwsResourceProperty - DB インスタンスが AVAILABLE の状態にあることを確認します。
- aws:executeAwsApi - DB インスタンスでのパブリックアクセシビリティを無効にします。
- aws:waitForAwsResourceProperty - DB インスタンスの状態が MODIFYING に変更されるまで待機します。
- aws:waitForAwsResourceProperty - DB インスタンスの状態が AVAILABLE に変更されるまで待機します。
- aws:assertAwsResourceProperty - DB インスタンスでパブリックアクセシビリティが無効になっていることを確認します。

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

説明

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster ランブックは、指定した Amazon Relational Database Service (Amazon RDS) クラスターの CopyTagsToSnapshot 設定を有効にします。この設定を有効にすると、DB クラスターから、その DB クラスターのスナップショットに対し、すべてのタグがコピーされます。デフォルトでは、これらをコピーしません。このオートメーションを実行する AWS リージョン で を有効にする AWS Config 必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- ApplyImmediately

  型: ブール値

  デフォルト: false

  説明: (オプション) このパラメータで `true` を指定した場合、DBクラスターの `PreferredMaintenanceWindow` 設定に関係なく、当該のリクエストのための変更ならびに保留中の変更は、できるだけ迅速に、かつ非同期的に適用されます。
- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DbClusterResourceId

  タイプ: 文字列

  説明: (必須) `CopyTagsToSnapshot` 設定を有効にする DB クラスターのリソース識別子。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

ドキュメントステップ

- `aws:executeAwsApi` - DB クラスターリソース識別子から DB クラスター識別子を収集します。
- `aws:assertAwsResourceProperty` - DB クラスターの状態が `AVAILABLE` であることを確認します。
- `aws:executeAwsApi` - DB クラスターの `CopyTagsToSnapshot` 設定を有効にします。

- aws:assertAwsResourceProperty - DB クラスターで CopyTagsToSnapshot 設定が有効になっていることを確認します。

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

説明

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance ランブックは、指定した Amazon Relational Database Service (Amazon RDS) インスタンスの CopyTagsToSnapshot 設定を有効にします。この設定を有効にすることで、DB インスタンスのすべてのタグが、そのインスタンスのスナップショットにコピーされるようになります。デフォルトでは、これらをコピーしません。このオートメーションを実行する AWS リージョン で を有効にする AWS Config 必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- ApplyImmediately

  型: ブール値

  デフォルト: false

  説明: (オプション) このパラメータで true を指定した場合、DB インスタンスの PreferredMaintenanceWindow 設定に関係なく、当該のリクエストのための変更ならびに保留中の変更は、できるだけ迅速に、かつ非同期的に適用されます。
- AutomationAssumeRole

タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- DbiResourceId

  タイプ: 文字列

  説明: (必須) CopyTagsToSnapshot 設定を有効にする DB インスタンスのリソース識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds:DescribeDBInstances
- rds:ModifyDBInstance

ドキュメントステップ

- aws:executeAwsApi - DB インスタンスリソース識別子から DB インスタンス識別子を収集します。
- aws:assertAwsResourceProperty - DB インスタンスの状態が AVAILABLE であることを確認します。
- aws:executeAwsApi - DB インスタンスの CopyTagsToSnapshot 設定を有効にします。
- aws:assertAwsResourceProperty - DB インスタンスで CopyTagsToSnapshot 設定が有効になっていることを確認します。

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

説明

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance ランブックは、ユーザーにより指定された Amazon RDS データベースインスタンスの拡張モニタリングを有効化します。拡張モニタリングの詳細については、「Amazon RDS ユーザーガイド」の「拡張モニタリング」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- MonitoringInterval

  タイプ: 整数

  有効な値: 1 | 5 | 10 | 15 | 30 | 60

  説明: (必須) DB インスタンスから拡張モニタリングメトリクスが収集される間隔 (秒単位)。
- MonitoringRoleArn

  タイプ: 文字列

  説明: (必須) Amazon RDS が Amazon CloudWatch Logs に拡張モニタリングメトリクスを送信することを許可する IAM ロールの Amazon リソースネーム (ARN)。
- ResourceId

  タイプ: 文字列

説明: (必須) 拡張モニタリングを有効にする DB インスタンスのリソース識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

ドキュメントステップ

- aws:executeAwsApi - DB インスタンスリソース識別子から DB インスタンス識別子を収集します。
- aws:assertAwsResourceProperty - DB インスタンスの状態が AVAILABLE であることを確認します。
- aws:executeAwsApi - DB インスタンスで拡張モニタリングを有効にします。
- aws:executeScript - DB インスタンスで拡張モニタリングが有効になっていることを確認します。

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

説明

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS ランブックは、指定した Amazon RDS データベースインスタンスの AutoMinorVersionUpgrade 設定を有効にします。この設定を有効にすると、メンテナンスの時間帯に DB インスタンスに自動的にマイナーバージョンアップグレードが適用されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DbiResourceId

  タイプ: 文字列

  説明: (必須) AutoMinorVersionUpgrade 設定を有効にする DB インスタンスのリソース識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

ドキュメントステップ

- aws:executeAwsApi - DB インスタンスリソース識別子から DB インスタンス識別子を収集します。
- aws:assertAwsResourceProperty - DB インスタンスの状態が AVAILABLE であることを確認します。

- aws:executeAwsApi - DB インスタンスの AutoMinorVersionUpgrade 設定を有効にします。
- aws:executeScript - DB インスタンスで AutoMinorVersionUpgrade 設定が有効になっていることを確認します。

AWSConfigRemediation-EnableMultiAZOnRDSInstance

説明

AWSConfigRemediation-EnableMultiAZOnRDSInstance ランブックでは、Amazon Relational Database Service (Amazon RDS) データベース (DB) インスタンスがマルチ AZ 配置に変更されます。この設定を変更しても機能は停止しません。ApplyImmediately パラメータで true を設定していない限り、この変更は次のメンテナンス期間中に適用されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- ApplyImmediately

  型: ブール値

  デフォルト: false

  説明: (オプション) このパラメータで true を指定した場合、DB インスタンスの PreferredMaintenanceWindow 設定に関係なく、当該のリクエストのための変更ならびに保留中の変更は、できるだけ迅速に、かつ非同期的に適用されます。
- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- DbiResourceId

  タイプ: 文字列

  説明: (必須) MultiAZ設定を有効にするための DB インスタンスの AWS リージョン一意でイミュータブルな識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- rds:DescribeDBInstances
- rds:ModifyDBInstance
- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

ドキュメントステップ

- aws:executeAwsApi - DBInstanceId パラメータで指定された値を使用して DB インスタンス名を取得します。
- aws:executeAwsApi - DBInstanceStatus は available であることを確認します。
- aws:branch - DbiResourceId パラメータで指定された DB インスタンスで、MultiAZ がすでに true に設定済みであるかを確認します。
- aws:executeAwsApi - DbiResourceId パラメータで指定された DB インスタンスの MultiAZ 設定を true に変更します。
- aws:assertAwsResourceProperty - DbiResourceId パラメータで指定された DB インスタンスの MultiAZ が true に設定されていることを確認します。

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

説明

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance ランブックは、ユーザーにより指定された Amazon RDS DB インスタンスの Performance Insights を有効化します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DbiResourceId

  タイプ: 文字列

  説明: (必須) Performance Insights を有効にする DB インスタンスのリソース識別子。
- PerformanceInsightsKMSKeyId

  タイプ: 文字列

  デフォルト: `alias/aws/rds`

  説明: (オプション) Performance Insights で機密データの暗号化に使用する Amazon リソースネーム (ARN)、キー ID、または AWS Key Management Service （ AWS KMS) カスタマーマネージドキーのキーエイリアス。このパラメータのキーエイリアスを入力する場合は、値の前に **alias/** を付けます。このパラメータの値を指定しない場合、 AWS マネージドキー が使用されます。
- PerformanceInsightsRetentionPeriod

タイプ: 整数

有効な値: 7、731

デフォルト: 7

説明: (オプション) Performance Insights のデータを保持する日数。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:CreateGrant
- kms:DescribeKey
- rds:DescribeDBInstances
- rds:ModifyDBInstance

ドキュメントステップ

- aws:executeAwsApi - DB インスタンスリソース識別子から DB インスタンス識別子を収集します。
- aws:assertAwsResourceProperty - DB インスタンスのステータスが available であることを確認します。
- aws:executeAwsApi - PerformanceInsightsKMSKeyIdパラメータで指定された AWS KMS カスタマーマネージドキーの ARN を収集します。
- aws:branch - DB インスタンスの PerformanceInsightsKMSKeyId プロパティに、値が既に割り当てられているかどうかをチェックします。
- aws:executeAwsApi - DbiResourceId パラメータで指定された DB インスタンスで Performance Insights を有効にします。
- aws:assertAwsResourceProperty - DB インスタンスの Performance Insights による暗号化を有効にするために、PerformanceInsightsKMSKeyId パラメータで指定された値が使用されたことを確認します。

- `aws:assertAwsResourceProperty` - DB インスタンスで Performance Insights が有効になっていることを確認します。

AWSConfigRemediation-EnableRDSClusterDeletionProtection

説明

`AWSConfigRemediation-EnableRDSClusterDeletionProtection` ランブックは、指定した Amazon Relational Database Service (Amazon RDS) クラスターの削除保護を有効にします。このオートメーションを実行する AWS リージョン で を有効にする AWS Config 必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- ClusterId

  タイプ: 文字列

  説明: (必須) 削除保護を有効にする DB クラスターのリソース識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- config:GetResourceConfigHistory
- rds:DescribeDBClusters
- rds:ModifyDBCluster

ドキュメントステップ

- aws:executeAwsApi - DB クラスターリソース識別子から DB クラスター名を収集します。
- aws:assertAwsResourceProperty - DB クラスターのステータスが available であることを確認します。
- aws:executeAwsApi - ClusterId パラメータで指定した DB クラスターで削除保護を有効にします。
- aws:assertAwsResourceProperty - DB クラスターで削除保護が有効化済みであることを確認します。

AWSConfigRemediation-EnableRDSInstanceBackup

説明

AWSConfigRemediation-EnableRDSInstanceBackup ランブックは、指定した Amazon Relational Database Service (Amazon RDS) データベースインスタンスのバックアップを有効にします。このランブックでは、Amazon Aurora データベースインスタンスのバックアップの有効化はサポートしていません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- ApplyImmediately

  型: ブール値

  デフォルト: false

  説明: (オプション) このパラメータで `true` を指定した場合、DB インスタンスの `PreferredMaintenanceWindow` 設定に関係なく、当該のリクエストのための変更ならびに保留中の変更は、できるだけ迅速に、かつ非同期的に適用されます。
- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- BackupRetentionPeriod

  タイプ: 整数

  有効な値: 1 ~ 35

  説明: (必須) バックアップが保持される日数。
- DbiResourceId

  タイプ: 文字列

  説明: (必須) バックアップを有効にする DB インスタンスのリソース識別子。
- PreferredBackupWindow

  タイプ: 文字列

  説明: (オプション) バックアップが作成される毎日の時間範囲 (UTC)。

  制約:

  - `hh24:mi-hh24:mi` 形式であることが必要です。

- 時間は協定世界時 (UTC) である必要があります。
- 必要なメンテナンス期間と競合してはいけません。
- 少なくとも 30 分以上必要です。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

ドキュメントステップ

- aws:executeScript - DB インスタンスリソース識別子から DB インスタンス識別子を収集します。DB インスタンスのバックアップを有効にします。DB インスタンスでバックアップが有効になっていることを確認します。

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

説明

AWSConfigRemediation-EnableRDSInstanceDeletionProtection ランブックは、指定した Amazon RDS データベースインスタンスの削除保護を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- ApplyImmediately

  型: ブール値

  デフォルト: false

  説明: (オプション) このパラメータで `true` を指定した場合、DB インスタンスの `PreferredMaintenanceWindow` 設定に関係なく、当該のリクエストのための変更ならびに保留中の変更は、できるだけ迅速に、かつ非同期的に適用されます。
- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DbInstanceResourceId

  タイプ: 文字列

  説明: (必須) 削除保護を有効にする DB インスタンスのリソース識別子。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

ドキュメントステップ

- `aws:executeAwsApi` - DB インスタンスリソース識別子から DB インスタンス識別子を収集します。

- aws:executeAwsApi - DB インスタンスの削除保護を有効にします。
- aws:assertAwsResourceProperty - DB インスタンスで削除保護が有効になっていることを確認します。

AWSConfigRemediation-ModifyRDSInstancePortNumber

説明

AWSConfigRemediation-ModifyRDSInstancePortNumber ランブックは、Amazon Relational Database Service (Amazon RDS) インスタンスが接続を受け入れるポート番号を変更します。このオートメーションを実行すると、データベースが再起動されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- PortNumber

  タイプ: 文字列

  説明: (オプション) DB インスタンスに接続を受け入れさせるポート番号。
- RDSDBInstanceResourceId

  タイプ: 文字列

説明: (必須) インバウンドポート番号を変更する DB インスタンスのリソース識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBInstances
- rds:ModifyDBInstance

ドキュメントステップ

- aws:executeAwsApi - DB インスタンスリソース識別子から DB インスタンス識別子を収集します。
- aws:assertAwsResourceProperty - DB インスタンスの状態が AVAILABLE であることを確認します。
- aws:executeAwsApi - DB インスタンスが接続を受け入れるインバウンドポートの番号を変更します。
- aws:waitForAwsResourceProperty - DB インスタンスの状態が MODIFYING になるまで待機します。
- aws:waitForAwsResourceProperty - DB インスタンスの状態が AVAILABLE になるまで待機します。

AWSSupport-ModifyRDSSnapshotPermission

説明

AWSSupport-ModifyRDSSnapshotPermission ランブックは、複数の Amazon Relational Database Service (Amazon RDS) スナップショットに対するアクセス許可を変更するのに役立ちます。このランブックを使用すると、Public または Private スナップショットを作成したり、他の AWS アカウントと共有したりできます。デフォルトの KMS キーで暗号化されたスナップショットは、このランブックを使用する他のアカウントと共有することはできません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- AccountIds

  タイプ: StringList

  デフォルト: なし

  説明: (オプション) スナップショットを共有するアカウントの ID。このパラメータは、`Private` パラメータの値に `No` を入力する場合に必須です。
- AccountPermissionOperation

  タイプ: 文字列

  有効な値: 追加 | 削除

  デフォルト: なし

  説明: (オプション) 実行するオペレーションの種類。
- プライベート

タイプ: 文字列

有効な値: はい | いいえ

説明: (必須) スナップショットを特定のアカウントと共有する場合、この値に No を入力します。

- SnapshotIdentifiers

  タイプ: StringList

  説明: (必須) アクセス許可を変更する Amazon RDS スナップショットの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- rds:DescribeDBSnapshots
- rds:ModifyDBSnapshotAttribute

ドキュメントステップ

1. aws:executeScript - SnapshotIdentifiers パラメータで指定されたスナップショットの ID を検証します ID を確認した後、スクリプトは暗号化されたスナップショットを確認し、見つかった場合はリストを出力します。
2. aws:branch - Private パラメータで入力した値に基づいて自動化を分岐させます。
3. aws:executeScript - 指定したスナップショットの権限を変更して、指定したアカウントと共有します。
4. aws:executeScript - スナップショットの権限を Public から Private に変更します。

出力

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Result

MakePrivate.Result

MakePrivate.Commands

AWSPremiumSupport-PostgreSQLWorkloadReview

説明

AWSPremiumSupport-PostgreSQLWorkloadReview ランブックは、Amazon Relational Database Service (Amazon RDS) PostgreSQL データベースの使用統計の複数のスナップショットをキャプチャします。キャプチャされた統計は、 サポート Proactive Services のエキスパートが運用レビューを実行するために必要です。統計は一連のカスタム SQL とシェルスクリプトを使用して収集されます。これらのスクリプトは、このランブックによって作成された の一時的な Amazon Elastic Compute Cloud (Amazon EC2) AWS アカウント インスタンスにダウンロードされます。ランブックでは、ユーザー名とパスワードのキーと値のペアを含む AWS Secrets Manager シークレットを使用して認証情報を提供する必要があります。ユーザー名は、標準の PostgreSQL 統計ビューと関数を照会する許可を持っている必要があります。

このランブックは、 AWS CloudFormation スタック AWS アカウント を使用して に次の AWS リソースを自動的に作成します。スタックの作成は AWS CloudFormation コンソールを使用して監視できます。

- 仮想プライベートクラウド (VPC) と Amazon EC2 インスタンスは VPC のプライベートサブネットで起動され、オプションで NAT ゲートウェイを使用してインターネットに接続できます。
- Secrets Manager シークレット値を取得するアクセス許可を持つ一時的な Amazon EC2 インスタンスにアタッチされた AWS Identity and Access Management (IAM) ロール。このロールには、選択した Amazon Simple Storage Service (Amazon S3) バケットにファイルをアップロードするアクセス許可も付与され、オプションで サポート ケースにアップロードするアクセス許可も付与されます。
- DB インスタンスと一時的な Amazon EC2 インスタンス間の接続を可能にする VPC ピアリング接続。
- 一時的な VPC にアタッチされているシステムマネージャ、シークレットマネージャ、および Amazon S3 VPC エンドポイント。
- 一時的な Amazon EC2 インスタンスの起動と停止、データ収集スクリプトの実行、Amazon S3 バケットへのファイルのアップロードを定期的に行う登録済みのタスクを含むメンテナンスウィンドウ。登録されたタスクを実行する権限を付与する IAM ロールもメンテナンスウィンドウ用に作成されます。

ランブックが完了すると、必要な AWS リソースの作成に使用される AWS CloudFormation スタックが削除され、レポートは選択した Amazon S3 バケットにアップロードされ、オプションで サポート ケースにアップロードされます。

> **Note**
>
> デフォルトでは、一時的な Amazon EC2 インスタンスのルート Amazon EBS ボリュームは保持されます。このオプションは、`EbsVolumeDeleteOnTermination` パラメータを `true` に設定することで上書きできます。

前提条件

- エンタープライズサポートサブスクリプション このランブックとプロアクティブサービスワークロード診断およびレビューには、エンタープライズサポートサブスクリプションが必要です。このランブックを使用する前に、テクニカルアカウントマネージャー (TAM) またはスペシャリスト TAM (STAM) に指示を求めてください。詳細については、「サポート プロアクティブサービス」を参照してください。
- アカウントと AWS リージョン クォータ このランブックを使用するアカウントとリージョンで作成できる Amazon EC2 インスタンスまたは VPCs の最大数に達していないことを確認してください。制限の引き上げをリクエストするには、サービスの制限緩和フォームをご覧ください。
- データベース設定

  1. `DatabaseName` パラメータで指定するデータベースには、`pg_stat_statements` 拡張子が設定されている必要があります。`shared_preload_libraries` で `pg_stat_statements` を設定していない場合は、DB パラメータグループの値を編集し、変更を適用する必要があります。`shared_preload_libraries` パラメータを変更すると、DB インスタンスを再起動する必要があります。詳細については、「パラメータグループの操作」を参照してください。`pg_stat_statements` を `shared_preload_libraries` に追加すると、パフォーマンスのオーバーヘッドがいくらか増加します。ただし、これは個々のステートメントのパフォーマンスを追跡する場合に役立ちます。`pg_stat_statements` の拡張の詳細については、PostgreSQL のドキュメントを参照してください。`pg_stat_statements` 拡張を設定していない場合や、統計収集に使用されているデータベースに拡張が存在しない場合、ステートメントレベルの分析は運用レビューに表示されません。
  2. `track_counts` および `track_activities` パラメータがオフになっていないことを確認してください。DB パラメータグループでこれらのパラメータがオフになっていると、意味のある統計は得られません。これらのパラメータを変更するには、DB インスタンスの再起動が必要にな

ります。詳しくは、「Amazon RDS for PostgreSQL DB インスタンスでのパラメータの使用」を参照してください。

3. track_io_timing パラメータをオフにすると、I/O レベルの統計は運用レビューに含まれません。track_io_timing を変更すると DB インスタンスを再起動する必要があり、DB インスタンスのワークロードによっては追加のパフォーマンスオーバーヘッドが発生します。重要なワークロードにはパフォーマンスオーバーヘッドがかかりますが、このパラメータはクエリごとの I/O 時間に関する有用な情報を提供します。

請求と料金 このオートメーションの実行中に一時的な Amazon EC2 インスタンス、関連付けられた Amazon EBS ボリューム、NAT ゲートウェイ、転送されたデータに関連するコストが課金 AWS アカウント されます。デフォルトでは、このランブックは t3.micro Amazon Linux 2 インスタンスを作成して統計を収集します。ランブックはコストを削減するためにステップの合間にインスタンスを起動および停止します。

データセキュリティとガバナンス このランブックは、PostgreSQLの統計ビューと関数をクエリして統計を収集します。SecretId パラメータにおいて指定する認証情報では、統計ビューと関数に対する読み取り専用権限のみを許可するようにしてください。自動化の一環として、収集スクリプトは Amazon S3 バケットにアップロードされ、s3://*amzn-s3-demo-bucket*/*automation execution id*/queries/ に配置されます。

これらのスクリプトは、 AWS スペシャリストがオブジェクトレベルで主要なパフォーマンス指標を確認するために使用するデータを収集します。このスクリプトは、テーブル名、スキーマ名、インデックス名などの情報を収集します。この情報に収益指標、ユーザー名、メールアドレス、その他の個人を特定できる情報などの機密情報が含まれている場合は、このワークロードレビューを中止することをお勧めします。 AWS TAM に連絡して、ワークロードレビューの代替アプローチについて話し合います。

このオートメーションで収集された統計とメタデータを と共有するために必要な承認と許可があることを確認してください AWS。

セキュリティ上の考慮事項 UpdateRdsSecurityGroup パラメータを yes に設定すると、ランブックは DB インスタンスに関連付けられているセキュリティグループを更新して、一時的な Amazon EC2 インスタンスのプライベート IP アドレスからのインバウンドトラフィックを許可します。

UpdateRdsRouteTable パラメータを yes に設定すると、ランブックは DB インスタンスが実行されているサブネットに関連付けられたルートテーブルを更新して、VPC ピアリング接続を介して一時的な Amazon EC2 インスタンスへのトラフィックを許可します。

ユーザー作成 収集スクリプトが Amazon RDS データベースに接続できるようにするには、統計ビューを読み取る権限を持つユーザーを設定する必要があります。また、認証情報は Secrets Manager に保存する必要があります。この自動化には、新しい専用ユーザーを作成することをお勧めします。別のユーザーを作成すると、この自動化によって実行されるアクティビティを監査および追跡できます。

1. 新しいユーザーを作成します。

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "CREATE USER <user_name> PASSWORD '<password>';"
   ```

2. このユーザーは読み取り専用接続しか行えないようにしてください。

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "ALTER USER <user_name> SET default_transaction_read_only=true;"
   ```

3. ユーザーレベルの制限を設定します。

   ```
   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. 新しいユーザーに DB 統計にアクセスできる pg_monitor 権限を付与します。(pg_monitor ロールは pg_read_all_settings、pg_read_all_stats および pg_stat_scan_table のメンバーです)。

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "GRANT pg_monitor to <user_name>;"
   ```

この Systems Manager 自動化によって一時的な Amazon EC2 インスタンスプロファイルに追加される権限 一時的な Amazon EC2 インスタンスに関連付けられた IAM ロールには、次の権限が追加されます。AmazonSSMManagedInstanceCore 管理ポリシーは IAM ロールにも関連付けられているため、Amazon EC2 インスタンスを Systems Manager で管理できるようになります。

```
{
```

```
    "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"
        }
    ]
}
```

この Systems Manager 自動化によって一時的なメンテナンスウィンドウに追加される権限 次の権限は、メンテナンスウィンドウタスクに関連付けられた IAM ロールに自動的に追加されます。メンテナンスウィンドウタスクは一時的な Amazon EC2 インスタンスを開始、停止し、このインスタンスにコマンドを送信します。

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

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- DB インスタンス識別子

  タイプ: 文字列

  説明: (必須) DB インスタンスの ID。

- DatabaseName

タイプ: 文字列

説明: (必須) DB インスタンスにホストされているデータベース名。

- SecretId

  タイプ: 文字列

  説明: (必須) ユーザー名とパスワードのキーと値のペアを含む Secrets Manager シークレットの ARN。 AWS CloudFormation スタックは、この ARN に対する `GetSecretValue`オペレーションのアクセス許可を持つ IAM ポリシーを作成します。認証情報を使用して、一時的なインスタンスがデータベース統計を収集できるようにします。TAM または STAM に問い合わせて、最低限必要な権限について相談してください。

- 了解

  タイプ: 文字列

  説明: (必須) このランブックが DB インスタンスから統計情報を収集するための一時的なリソースをアカウントに作成することを承認する場合、**yes** を入力してください。このオートメーションを実行する前に TAM または STAM に連絡することをお勧めします。

- SupportCase

  タイプ: 文字列

  説明: (オプション) TAM または STAM によって提供される サポート ケース番号。指定した場合、ランブックはケースを更新し、収集したデータをアタッチします。このオプションでは、 サポート API エンドポイントにアクセスするために、一時的な Amazon EC2 インスタンスにインターネット接続が必要です。`AllowVpcInternetAccess` パラメータを `true` に設定する必要があります。ケースの件名には `AWSPremiumSupport-PostgreSQLWorkloadReview` という語句が含まれている必要があります。

- S3BucketName

  タイプ: 文字列

  説明: (必須) 自動化によって収集されたデータをアップロードするアカウントの Amazon S3 バケット名。バケットポリシーが、バケットのコンテンツにアクセスする必要がないプリンシパルに不必要な読み取りまたは書き込みアクセス許可を付与していないことを確認します。この自動化を目的として一時的な Amazon S3 バケットを新規作成することをお勧めします。ランブックは、一時的な Amazon EC2 インスタンスにアタッチされた IAM ロールに `s3:PutObject` API オペレー

ションの許可を提供します。アップロードされたファイルは s3://*bucket name*/*automation execution id*/ にあります。

- InstanceType

  タイプ: 文字列

  説明: (オプション) カスタム SQL とシェルスクリプトを実行する一時的な Amazon EC2 インスタンスのタイプ。

  有効な値: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large

  デフォルト: t3.micro

- VpcCidr

  タイプ: 文字列

  説明: (オプション) 新しい VPC の CIDR 表記の IP アドレス範囲 (例: 172.31.0.0/16)。DB インスタンスに接続できる既存の VPC と重複しない、または一致しない CIDR を選択してください。作成できる最小の VPC は /28 サブネットマスクを使用し、最大の VPC は /16 サブネットマスクを使用します。

  デフォルト: 172.31.0.0/16

- StackResourcesNamePrefix

  タイプ: 文字列

  説明: (オプション) AWS CloudFormation スタックリソース名のプレフィックスとタグ。ランブックは、リソースに適用される名前とタグの一部として、このプレフィックスを使用して AWS CloudFormation スタックリソースを作成します。タグのキーバリューペアの構造は *StackResourcesNamePrefix*:{{automation:EXECUTION_ID}} です。

  デフォルト: AWSPostgreSQLWorkloadReview

- スケジュール

  タイプ: 文字列

  説明: (オプション) メンテナンスウィンドウのスケジュール。メンテナンスウィンドウでタスクを実行する頻度を指定します。デフォルト値は True です 1 hour。

  有効な値: 15 分 | 30 分 | 1 時間 | 2 時間 | 4 時間 | 6 時間 | 12 時間 | 1 日 | 2 日 | 4 日

デフォルト: 1 時間

- 期間

  タイプ: 整数

  説明: (オプション) オートメーションを実行できる最大時間 (分) 。サポートされる最大時間は 8,640 分 (6 日間) です。デフォルト値は 4,320 分 (3 日間) です。

  有効な値: 30 ~ 8640

  デフォルト: 4320

- UpdateRdsRouteTable

  タイプ: 文字列

  説明: (オプション) `true` に設定すると、ランブックは DB インスタンスが実行されているサブネットに関連付けられたルートテーブルを更新します。IPv4 ルートが追加され、新しく作成された VPC ピアリング接続を介して一時的な Amazon EC2 インスタンスのプライベート IPV4 アドレスにトラフィックがルーティングされます。

  有効な値: true | false

  デフォルト: false

- AllowVpcInternetAccess

  タイプ: 文字列

  説明: (オプション) に設定すると`true`、ランブックは サポート API エンドポイントと通信するための一時的な Amazon EC2 インスタンスへのインターネット接続を提供する NAT ゲートウェイを作成します。ランブックが出力を Amazon S3 バケットにアップロードすることだけを望む場合、このパラメータを `false` のままにしておくことができます。

  有効な値: true | false

  デフォルト: false

- UpdateRdsSecurityGroup

  タイプ: 文字列

説明: (オプション) true に設定すると、ランブックは DB インスタンスに関連付けられているセキュリティグループを更新し、一時インスタンスのプライベート IP アドレスからのトラフィックを許可します。

有効な値: false/true

デフォルト: false

- EbsVolumeDeleteOnTermination

  タイプ: 文字列

  説明: (オプション) に設定するとtrue、ランブックが AWS CloudFormation スタックを完了して削除した後、一時的な Amazon EC2 インスタンスのルートボリュームが削除されます。

  有効な値: false/true

  デフォルト: false

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

1. aws:assertAwsResourceProperty - DB インスタンスの状態が available であることを確認します。
2. aws:executeAwsApi - DB インスタンスの詳細を収集します。
3. aws:executeScript - S3BucketName で指定されている Amazon S3 バケットが、匿名またはパブリックの読み取りまたは書き込みアクセス権限を許可しているかどうかを確認します。
4. aws:executeScript - に一時 AWS リソースを作成するために使用される Automation ランブックアタッチメントから AWS CloudFormation テンプレートコンテンツを取得します AWS アカウント。
5. aws:createStack - AWS CloudFormation スタックリソースを作成します。
6. aws:waitForAwsResourceProperty - AWS CloudFormation テンプレートによって作成された Amazon EC2 インスタンスが実行されるまで待ちます。
7. aws:executeAwsApi - 一時的な Amazon EC2 インスタンスと、 AWS CloudFormationによって作成された VPC ピアリング接続の ID を取得します。
8. aws:executeAwsApi - 一時的な Amazon EC2 インスタンスの IP アドレスを取得して DB インスタンスとの接続を設定します。
9. aws:executeAwsApi - 一時的な Amazon EC2 インスタンスにアタッチされた Amazon EBS ボリュームにタグを付けます。
10. aws:waitForAwsResourceProperty - 一時的な Amazon EC2 インスタンスがステータスチェックに合格するまで待ちます。
11. aws:waitForAwsResourceProperty - 一時的な Amazon EC2 インスタンスが Systems Manager によって管理されるまで待ちます。このステップがタイムアウトになったり失敗したりすると、ランブックはインスタンスを再起動します。
    a. aws:executeAwsApi - 前のステップが失敗したりタイムアウトになった場合、一時的な Amazon EC2 インスタンスを再起動します。
    b. aws:waitForAwsResourceProperty - 一時的な Amazon EC2 インスタンスが再起動後に Systems Manager によって管理されるまで待ちます。

12. aws:runCommand - メタデータコレクターのアプリケーション要件を一時的な Amazon EC2 インスタンスにインストールします。
13. aws:runCommand - 一時的な Amazon EC2 インスタンスに設定ファイルを作成することで、DB インスタンスへのアクセスを設定します。
14. aws:executeAwsApi - Run Command を使用してメタデータコレクターアプリケーションを定期的に実行するためのメンテナンスウィンドウを作成します。メンテナンスウィンドウは、コマンドの合間にインスタンスを起動および停止します。
15. aws:waitForAwsResourceProperty - AWS CloudFormation テンプレートによって作成されたメンテナンスウィンドウの準備ができるまで待ちます。
16. aws:executeAwsApi - によって作成されたメンテナンスウィンドウと変更力レンダーIDs を取得します AWS CloudFormation。
17. aws:sleep - メンテナンスウィンドウの終了日まで待機します。
18. aws:executeAwsApi - メンテナンスウィンドウをオフにします。
19. aws:executeScript - メンテナンスウィンドウ中に実行されたタスクの結果を取得します。
20. aws:waitForAwsResourceProperty - メンテナンスウィンドウが最後のタスクを終了した後に続行するまで待機します。
21. aws:branch - SupportCase パラメータに値を指定したかどうかに応じてワークフローを分岐します。
    a. aws:changeInstanceState - 一時的な Amazon EC2 インスタンスを起動し、ステータスチェックに合格するのを待ってからレポートをアップロードします。
    b. aws:waitForAwsResourceProperty - 一時的な Amazon EC2 インスタンスが Systems Manager によって管理されるまで待ちます。このステップがタイムアウトになったり失敗したりすると、ランブックはインスタンスを再起動します。
        i. aws:executeAwsApi - 前のステップが失敗したりタイムアウトになった場合、一時的な Amazon EC2 インスタンスを再起動します。
        ii. aws:waitForAwsResourceProperty - 一時的な Amazon EC2 インスタンスが再起動後に Systems Manager によって管理されるまで待ちます。
    c. aws:runCommand - SupportCase パラメータに値を指定した場合、メタデータレポートを サポート ケースにアタッチします。このスクリプトは、レポートを 5 MB のファイルに圧縮して分割します。スクリプトが サポート ケースにアタッチするファイルの最大数は 12 です。
22. aws:changeInstanceState - AWS CloudFormation スタックの削除に失敗した場合に備えて、一時的な Amazon EC2 インスタンスを停止します。

23.aws:executeAwsApi - ランブックが AWS CloudFormation スタックの作成または更新に失敗した場合の AWS CloudFormation スタックイベントを記述します。

24.aws:waitForAwsResourceProperty - AWS CloudFormation スタックがターミナルステータスになるまで待ってから削除します。

25.aws:executeAwsApi - メンテナンスウィンドウを除く AWS CloudFormation スタックを削除します。EbsVolumeDeleteOnTermination パラメータ値が false に設定された場合、一時的な Amazon EC2 インスタンスに関連付けられているルート Amazon EBS ボリュームは保持されます。

AWS-RebootRdsInstance

説明

AWS-RebootRdsInstance ランブックは、Amazon Relational Database Service (Amazon RDS) DB インスタンスがまだ再起動されていない場合は、そのインスタンスを再起動します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

タイプ: 文字列

説明: (必須) 再起動する Amazon RDS DB インスタンスの ID。

ドキュメントステップ

RebootInstance - DB インスタンスをまだ再起動していない場合は、再起動します。

WaitForAvailableState - DB インスタンスが再起動プロセスを完了するのを待ちます。

出力

このオートメーションには出力がありません。

AWSSupport-ShareRDSSnapshot

説明

AWSSupport-ShareRDSSnapshot ランブックは、ナレッジセンター記事「暗号化された Amazon RDS DB スナップショットを別のアカウントと共有する方法を教えてください。」で説明されている手順についての、自動化されたソリューションを提供します。Amazon Relational Database Service (Amazon RDS) スナップショットがデフォルトを使用して暗号化されている場合 AWS マネージドキー、スナップショットを共有することはできません。この場合、カスタマーマネージドキーを使用してスナップショットをコピーしてから、スナップショットをターゲットアカウントと共有する必要があります。このオートメーションでは、SnapshotName パラメータで指定した値、または選択した Amazon RDS DB インスタンスまたはクラスターで見つかった最新のスナップショットを使用して、これらのステップが実行されます。

> **Note**
>
> KMSKey パラメータの値を指定しない場合、オートメーションはスナップショットの暗号化に使用される新しい AWS KMS カスタマーマネージドキーをアカウントに作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AccountIds

  タイプ: StringList

  説明: (必須) スナップショットを共有するアカウント ID のカンマ区切りリスト。

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- データベース

  タイプ: 文字列

  説明: (必須) スナップショットを共有する Amazon RDS DB インスタンスまたはクラスターの名前。`SnapshotName` パラメータの値を指定する場合、このパラメータはオプションです。

- KMSKey

  タイプ: 文字列

  説明: (オプション) スナップショットの暗号化に使用される AWS KMS カスタマーマネージドキーの完全な Amazon リソースネーム (ARN)。

- SnapshotName

  タイプ: 文字列

  説明: (オプション) 使用する DB クラスターまたはインスタンススナップショットの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- rds:DescribeDBInstances
- rds:DescribeDBSnapshots
- rds:CopyDBSnapshot
- rds:ModifyDBSnapshotAttribute

AutomationAssumeRole では、DB クラスターでランブックを正常に起動するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- rds:DescribeDBClusters
- rds:DescribeDBClusterSnapshots
- rds:CopyDBClusterSnapshot
- rds:ModifyDBClusterSnapshotAttribute

オートメーションの実行に使用される IAM ロールは、ARNKmsKey パラメータで指定された KMS キーを使用するためにキーユーザーとして追加する必要があります。KMS キーへのキーユーザーの追加については、AWS Key Management Service デベロッパーガイドの「キーポリシーの変更」を参照してください。

KMSKey パラメータで値を指定していない場合、AutomationAssumeRole には、ランブックを正常に実行するために以下のような追加アクションが必要です。

- kms:CreateKey
- kms:ScheduleKeyDeletion
- kms:CreateGrant
- kms:DescribeKey

ドキュメントステップ

1. aws:executeScript - KMSKeyパラメータに値が指定されたかどうかを確認し、値が見つからない場合は AWS KMS カスタマーマネージドキーを作成します。

2. aws:branch - SnapshotName パラメータに値が指定されたかどうかをチェックし、それに応じて分岐します。
3. aws:executeAwsApi - 提供されたスナップショットが DB インスタンスのものであるかどうかをチェックします。
4. aws:executeScript - コロンをハイフンに置き換える SnapshotName パラメータをフォーマットします。
5. aws:executeAwsApi - 指定した KMSKey を使用してスナップショットをコピーします。
6. aws:waitForAwsResourceProperty - コピースナップショットの操作が完了するまで待機します。
7. aws:executeAwsApi - 新しいスナップショットを指定した AccountIds と共有します。
8. aws:executeAwsApi - 提供されたスナップショットが DB クラスターのものであるかどうかをチェックします。
9. aws:executeScript - コロンをハイフンに置き換える SnapshotName パラメータをフォーマットします。
10. aws:executeAwsApi - 指定した KMSKey を使用してスナップショットをコピーします。
11. aws:waitForAwsResourceProperty - コピースナップショットの操作が完了するまで待機します。
12. aws:executeAwsApi - 新しいスナップショットを指定した AccountIds と共有します。
13. aws:executeAwsApi - Database パラメータに指定された値が DB インスタンスであるかどうかをチェックします。
14. aws:executeAwsApi - Database パラメータに指定された値が DB クラスターであるかどうかをチェックします。
15. aws:executeAwsApi - 指定された Database のスナップショットのリストを取得します。
16. aws:executeScript - 前のステップでアセンブルされたリストから使用可能な最新のスナップショットを決定します。
17. aws:executeAwsApi - 指定した KMSKey を使用して DB インスタンスのスナップショットをコピーします。
18. aws:waitForAwsResourceProperty - コピースナップショットの操作が完了するまで待機します。
19. aws:executeAwsApi - 新しいスナップショットを指定した AccountIds と共有します。
20. aws:executeAwsApi - 指定された Database のスナップショットのリストを取得します。
21. aws:executeScript - 前のステップでアセンブルされたリストから使用可能な最新のスナップショットを決定します。

22aws:executeAwsApi - 指定した KMSKey を使用して DB インスタンスのスナップショットをコピーします。

23aws:waitForAwsResourceProperty - コピースナップショットの操作が完了するまで待機します。

24aws:executeAwsApi - 新しいスナップショットを指定した AccountIds と共有します。

25aws:executeScript - KMSKeyパラメータの値を指定せず、オートメーションが失敗した場合、オートメーションによって作成された AWS KMS カスタマーマネージドキーを削除します。

AWS-StartRdsInstance

説明

Amazon Relational Database Service (Amazon RDS) インスタンスの起動

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

説明: (必須) 起動する Amazon RDS インスタンスの ID。

AWS-StartStopAuroraCluster

説明

このランブックは、Amazon Aurora クラスターを起動または停止します。

> **Note**
>
> クラスターを起動するには、`stopped`クラスターのステータスが である必要があります。クラスターを停止するには、 `available`ステータスである必要があります。このランブックを使用して、Aurora Serverless クラスター、Aurora マルチマスタークラスター、Aurora グローバルデータベースの一部、または Aurora 並列クエリを使用するクラスターであるクラスターを起動または停止することはできません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- ClusterName

  タイプ: 文字列

  説明: (必須) 停止または開始する Aurora クラスターの名前。
- アクション

  タイプ: 文字列

  有効な値: Start | Stop

  デフォルト: 開始

  説明: (必須) 停止または開始する Aurora クラスターの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- rds:DescribeDBClusters
- rds:StartDBCluster
- rds:StopDBCluster

ドキュメントステップ

- aws:executeScript - に指定した値に基づいてクラスターを開始または停止します。

出力

StartStopAuroraCluster.ClusterName - Aurora クラスターの名前

StartStopAuroraCluster.CurrentStatus - Aurora クラスターの現在のステータス

StartStopAuroraCluster.Message - オートメーションの詳細

AWS-StopRdsInstance

説明

Amazon Relational Database Service (Amazon RDS) インスタンスを停止します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: 文字列

  説明: (必須) 停止する Amazon RDS インスタンスの ID。

AWSSupport-TroubleshootConnectivityToRDS

説明

AWSSupport-TroubleshootConnectivityToRDS ランブックは、EC2 インスタンスと Amazon Relational Database Service インスタンスの間の接続の問題を診断します。このオートメーションにより、DB インスタンスが使用可能であることが確認され、関連付けられているセキュリティグループのルール、ネットワークアクセスコントロールリスト (ネットワーク ACL)、ルートテーブルの潜在的な接続の問題がチェックされます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- DB インスタンス識別子

  タイプ: 文字列

  説明: (必須) 接続をテストする接続先の DB インスタンスの ID。
- SourceInstance

  タイプ: 文字列

  使用できるパターン: ^i-[a-z0-9]{8,17}$

  説明: (必須) 接続をテストする EC2 インスタンスの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ec2:DescribeInstances
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- rds:DescribeDBInstances

ドキュメントステップ

- aws:assertAwsResourceProperty - DB インスタンスのステータスがavailable であることを確認します。
- aws:executeAwsApi - DB インスタンスに関する情報を取得します。
- aws:executeAwsApi - DB インスタンスのネットワーク ACL に関する情報を取得します。
- aws:executeAwsApi - DB インスタンスのサブネットの CIDR を取得します。
- aws:executeAwsApi - EC2 インスタンスに関する情報を取得します。
- aws:executeAwsApi - EC2 インスタンスのネットワーク ACL に関する情報を取得します。
- aws:executeAwsApi - EC2 インスタンスに関連付けられているセキュリティグループに関する情報を取得します。
- aws:executeAwsApi - DB インスタンスに関連付けられているセキュリティグループに関する情報を取得します。
- aws:executeAwsApi - EC2 インスタンスに関連付けられているルートテーブルに関する情報を取得します。
- aws:executeAwsApi - EC2 インスタンスの Amazon VPC に関連付けられているメインルートテーブルに関する情報を取得します。
- aws:executeAwsApi - DB インスタンスに関連付けられているルートテーブルに関する情報を取得します。
- aws:executeAwsApi - DB インスタンスの Amazon VPC に関連付けられているメインルートテーブルに関する情報を取得します。
- aws:executeScript - セキュリティグループのルールを評価します。
- aws:executeScript - ネットワーク ACL を評価します。
- aws:executeScript - ルートテーブルを評価します。
- aws:sleep - 自動化を終了します。

出力

getRDSInstanceProperties.DBInstanceIdentifier - オートメーションで使用された DB インスタンス。

getRDSInstanceProperties.DBInstanceStatus - DB インスタンスの現在のステータス。

evalSecurityGroupRules.SecurityGroupEvaluation - `SourceInstance` セキュリティグループのルールと DB インスタンスのセキュリティグループのルールを比較した結果。

evalNetworkAclRules.NetworkAclEvaluation - `SourceInstance` ネットワーク ACL と DB インスタンスのネットワーク ACL を比較した結果。

evalRouteTableEntries.RouteTableEvaluation - `SourceInstance` ルートテーブルと DB インスタンスのルートを比較した結果。

AWSSupport-TroubleshootRDSIAMAuthentication

説明

は、Amazon RDS for PostgreSQL、Amazon RDS for MySQL、Amazon RDS for MariaDB、Amazon Aurora PostgreSQL、および Amazon Aurora MySQL インスタンスの AWS Identity and Access Management (IAM) 認証のトラブルシューティング`AWSSupport-TroubleshootRDSIAMAuthentication`に役立ちます。このランブックを使用して、Amazon RDS インスタンスまたは Aurora クラスターでの IAM 認証に必要な設定を確認します。また、Amazon RDS インスタンスまたは Aurora クラスターへの接続の問題を修正する手順も示します。

> **Important**
>
> このランブックは、Amazon RDS for Oracle または Amazon RDS for Microsoft SQL Server をサポートしていません。

> **Important**
>
> ソース Amazon EC2 インスタンスが提供され、ターゲットデータベースが Amazon RDS の場合、子オートメーション`AWSSupport-TroubleshootConnectivityToRDS`が呼び出され、TCP 接続のトラブルシューティングが行われます。出力には、IAM 認証を使用して Amazon RDS インスタンスに接続するために Amazon EC2 インスタンスまたはソースマシンで実行できるコマンドも用意されています。

動作の仕組み

このランブックは 6 つのステップで構成されています。

- ステップ 1: validateInputs: オートメーションへの入力を検証します。
- ステップ 2: branchOnSourceEC2Provided: 入力パラメータでソース Amazon EC2 インスタンス ID が指定されているかどうかを確認します。
- ステップ 3: validateRDSConnectivity: ソース Amazon EC2 インスタンスから Amazon RDS 接続が提供されている場合は検証します。
- ステップ 4: validateRDSIAMAuthentication: IAM 認証機能が有効になっているかどうかを検証します。
- ステップ 5: validateIAMPolicies: 指定された IAM ユーザー/ロールに必要な IAM アクセス許可が存在するかどうかを確認します。
- ステップ 6: generateReport: 以前に実行したステップの結果のレポートを生成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- RDSType

タイプ: 文字列

説明: (必須): 接続および認証しようとしているリレーショナルデータベースのタイプを選択します。

使用できる値: Amazon RDSまたは Amazon Aurora Cluster.

- DB インスタンス識別子

  タイプ: 文字列

  説明: (必須) ターゲット Amazon RDS データベースインスタンスまたは Aurora データベースクラスターの識別子。

  許可されたパターン: ^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$

  最大文字数: 63

- SourceEc2InstanceIdentifier

  型: AWS::EC2::Instance::Id

  説明: (オプション) 同じアカウントとリージョンで実行されている Amazon EC2 インスタンスから Amazon RDS データベースインスタンスに接続する場合の Amazon EC2 インスタンス ID。ソースが Amazon EC2 インスタンスでない場合、またはターゲットの Amazon RDS タイプが Aurora データベースクラスターである場合は、このパラメータを指定しないでください。

  デフォルト: ""

- DBIAMRoleName

  タイプ: 文字列

  説明: (オプション) IAM ベースの認証に使用される IAM ロール名。パラメータが指定されDBIAMUserNameていない場合にのみ を指定し、指定しない場合は空のままにします。DBIAMRoleName または を指定DBIAMUserNameする必要があります。

  許可されたパターン: ^[a-zA-Z0-9+=,.@_-]{1,64}$|^$

  最大文字数: 64

  デフォルト: ""

- DBIAMUserName

タイプ: 文字列

説明: (オプション) IAM ベースの認証に使用される IAM ユーザー名。DBIAMRoleName パラメータが指定されていない場合にのみ を指定し、指定しない場合は空のままにします。DBIAMRoleName または を指定DBIAMUserNameする必要があります。

許可されたパターン: ^[a-zA-Z0-9+=,.@_-]{1,64}$|^$

最大文字数: 64

デフォルト: ""

- DBUserName

  タイプ: 文字列

  説明: (オプション) データベース内の IAM ベースの認証用に IAM ロール/ユーザーにマッピングされたデータベースユーザー名。デフォルトのオプションでは、データベース内のすべてのユーザーに アクセスrds-db:connect許可が付与されているかどうか*を評価します。

  許可されたパターン: ^[a-zA-Z0-9+=,.@*_-]{1,64}$

  最大文字数: 64

  デフォルト: *

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

指示

1. AWS Systems Manager コンソールで AWSSupport-TroubleshootRDSIAMAuthentication に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 次の入力パラメータを入力できます。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
   - RDSType (必須):

     接続および認証しようとしている Amazon RDS のタイプを選択します。2 つの許可された値から選択します。 `Amazon RDS` または `Amazon Aurora Cluster.`
   - DBInstanceIdentifier (必須):

     接続しようとしているターゲット Amazon RDS データベースインスタンスまたは Aurora クラスターの識別子を入力し、認証に IAM 認証情報を使用します。
   - SourceEc2InstanceIdentifier (オプション):

     同じアカウントとリージョンに存在する Amazon EC2 インスタンスから Amazon RDS データベースインスタンスに接続する場合は、Amazon EC2 インスタンス ID を指定します。ソースが

Amazon EC2 でない場合、またはターゲットの Amazon RDS タイプが Aurora クラスターの場合は空白のままにします。

- DBIAMRoleName (オプション):

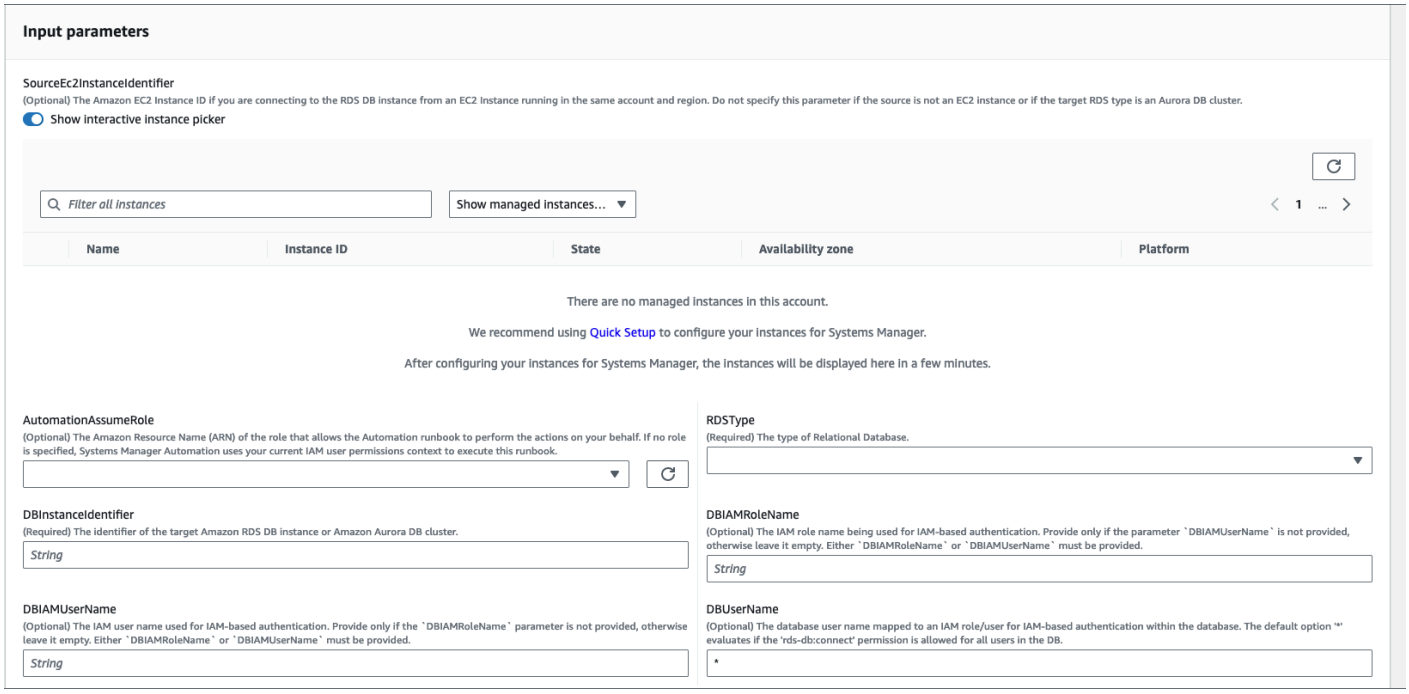
  IAM ベースの認証に使用される IAM ロール名を入力します。DBIAMUserName が指定されていない場合にのみ を指定します。それ以外の場合は空白のままにします。DBIAMRoleName または を指定DBIAMUserNameする必要があります。

- DBIAMUserName (オプション):

  IAM ベースの認証に使用される IAM ユーザーを入力します。DBIAMRoleName が指定されていない場合は のみを指定し、それ以外の場合は空白のままにします。DBIAMRoleName または を指定DBIAMUserNameする必要があります。

- DBUserName (オプション):

  データベース内の IAM ベースの認証用に IAM ロール/ユーザーにマッピングされたデータベースユーザーを入力します。デフォルトのオプション*は評価に使用されます。このフィールドには何も表示されません。



4. [実行] を選択します。
5. オートメーションが開始されることに注意してください。
6. ドキュメントは以下のステップを実行します。

   - ステップ 1: validateInputs:

オートメーションへの入力を検証します - SourceEC2InstanceIdentifier (オプション)、DBInstanceIdentifier、ClusterID、DBIAMRoleNameまたは DBIAMUserName。入力した入力パラメータがアカウントとリージョンに存在するかどうかを確認します。また、ユーザーが IAM パラメータ (DBIAMRoleNameや など) のいずれかを入力したかどうかも確認しますDBIAMUserName。さらに、言及されたデータベースが使用可能ステータスであるかどうかなど、他の検証も実行します。

- ステップ 2: branchOnSourceEC2Provided済み :

  ソース Amazon EC2 が入力パラメータで提供され、データベースが Amazon RDS であることを確認します。「はい」の場合、ステップ 3 に進みます。そうでない場合、Amazon EC2-Amazon RDS 接続検証であるステップ 3 をスキップし、ステップ 4 に進みます。

- ステップ 3: validateRDSConnectivity:

  ソース Amazon EC2 が入力パラメータで提供され、データベースが Amazon RDS である場合、ステップ 2 はステップ 3 を開始します。このステップでは、ソース Amazon EC2 から Amazon RDS 接続を検証するために、子オートメーションAWSSupport-TroubleshootConnectivityToRDSが呼び出されます。子オートメーションランブックAWSSupport-TroubleshootConnectivityToRDSは、Amazon EC2 インスタンスから Amazon RDS インスタンスに接続できるように、必要なネットワーク設定 (Amazon Virtual Private Cloud [Amazon VPC]、セキュリティグループ、ネットワークアクセスコントロールリスト [NACL]、Amazon RDS の可用性) が設定されているかどうかを確認します。

- ステップ 4: validateRDSIAMAuthentication:

  Amazon RDS インスタンスまたは Aurora クラスターで IAM 認証機能が有効になっているかどうかを検証します。

- ステップ 5: validateIAMPolicies:

  IAM 認証情報が指定されたデータベースユーザー (存在する場合) の Amazon RDS インスタンスを認証できるように、渡された IAM ユーザー/ロールに必要な IAM アクセス許可が存在するかどうかを確認します。

- ステップ 6: generateReport:

  前のステップからすべての情報を取得し、各ステップの結果または出力を出力します。また、IAM 認証情報を使用して Amazon RDS インスタンスに接続するために参照して実行する手順も示します。

7. 自動化が完了したら、出力セクションで詳細な結果を確認します。

- データベースに接続するための IAM ユーザー/ロールのアクセス許可の確認：

  IAM 認証情報が指定されたデータベースユーザー (存在する場合) の Amazon RDS インスタンスに対して認証できるように渡された IAM ユーザー/ロールに必要な IAM アクセス許可が存在するかどうかを確認します。

- データベースの IAM ベースの認証属性の確認：

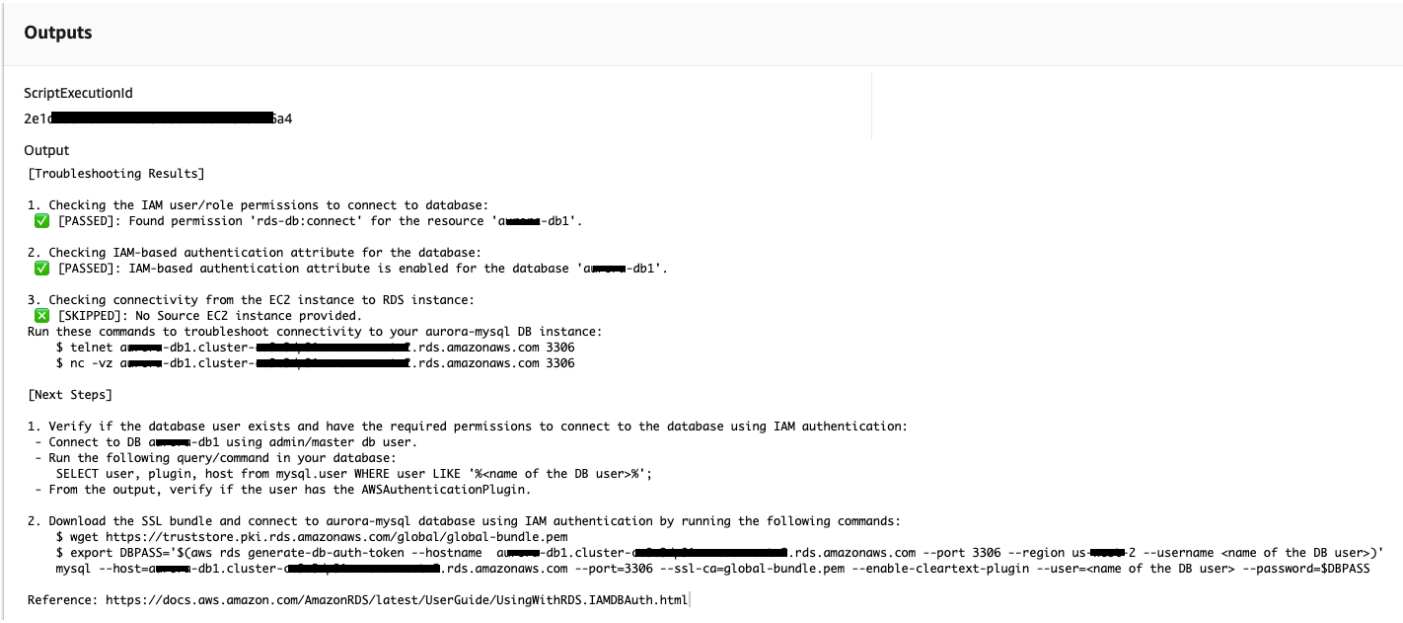
  指定された Amazon RDS データベース/Aurora クラスターで IAM 認証の機能が有効になっているかどうかを確認します。

- Amazon EC2 インスタンスから Amazon RDS インスタンスへの接続の確認：

  Amazon EC2 インスタンスから Amazon RDS インスタンスに接続できるように、必要なネットワーク設定 (Amazon VPC、セキュリティグループ、NACL、Amazon RDS の可用性) が設定されているかどうかを確認します。

- 次のステップ:

  IAM 認証情報を使用して Amazon RDS インスタンスに接続するために参照および実行するコマンドとステップを一覧表示します。



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
```

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)

- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWSSupport-ValidateRdsNetworkConfiguration

説明

AWSSupport-ValidateRdsNetworkConfiguration オートメーションは、ModifyDBInstance または StartDBInstanceオペレーションを実行する前に、既存の Amazon Relational Database Service (Amazon RDS) / Amazon Aurora / Amazon DocumentDB インスタンスの互換性のないネットワーク状態を回避するのに役立ちます。インスタンスがすでに互換性のないネットワーク状態である場合、ランブックは理由を提供します。

動作の仕組み

このランブックは、Amazon RDS データベースインスタンスが互換性のないネットワーク状態になるかどうか、または存在する場合は、互換性のないネットワーク状態である理由を決定します。

ランブックは、Amazon RDS データベースインスタンスに対して次のチェックを実行します。

- リージョンあたりの Amazon Elastic Network Interface (ENI) クォータ。
- データベースサブネットグループ内のすべてのサブネットが存在します。
- サブネット (複数可) に十分な空き IP アドレスがあります。
- (パブリックにアクセス可能な Amazon RDS インスタンスの場合) VPC 属性の設定 (enableDnsSupport および enableDnsHostnames) 。

> **Important**
>
> Amazon Aurora/Amazon DocumentDB クラスターに対してこのドキュメントを使用する場合は、 DBInstanceIdentifierの代わりに を使用してくださいClusterIdentifier。そうしないと、ドキュメントは最初のステップで失敗します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- rds:DescribeDBInstances
- servicequotas:GetServiceQuota
- ec2:DescribeNetworkInterfaces
- ec2:DescribeVpcAttribute
- ec2:DescribeSubnets

ポリシーの例:

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

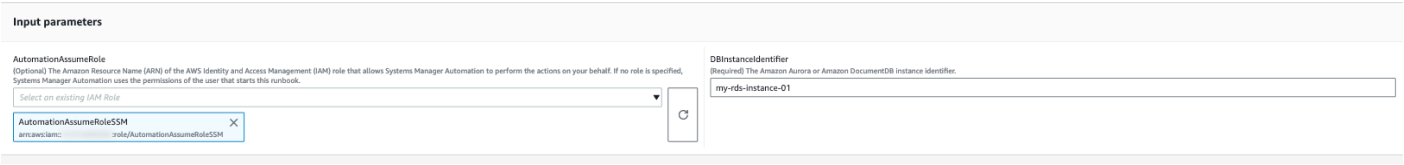
```
        }
```

指示

1. AWS Systems Manager コンソールで AWSSupport-ValidateRdsNetworkConfiguration に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 次の入力パラメータを入力できます。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
   - DBInstanceIdentifier (必須):

     Amazon Relational Database Service インスタンス識別子を入力します。



4. [実行] を選択します。
5. オートメーションが開始されることに注意してください。
6. ドキュメントは以下のステップを実行します。
   - ステップ 1: assertRdsState:

     指定されたインスタンス識別子が存在し、、、`available`、`stopped`または のいずれかの状態になっているかどうかを確認します`incompatible-network`。
   - ステップ 2: gatherRdsInformation:

     オートメーションの後半で使用する Amazon RDS インスタンスに関する必須情報を収集します。
   - ステップ 3: checkEniQuota:

     リージョンで現在利用可能な Amazon ENI のクォータを確認します。
   - ステップ 4: validateVpcAttributes:

Amazon VPC の DNS パラメータ (enableDnsSupport および enableDnsHostnames) が true に設定されていることを確認します (Amazon RDS インスタンスが の場合は設定しませんPubliclyAccessible) 。

- ステップ 5: validateSubnetAttributes:

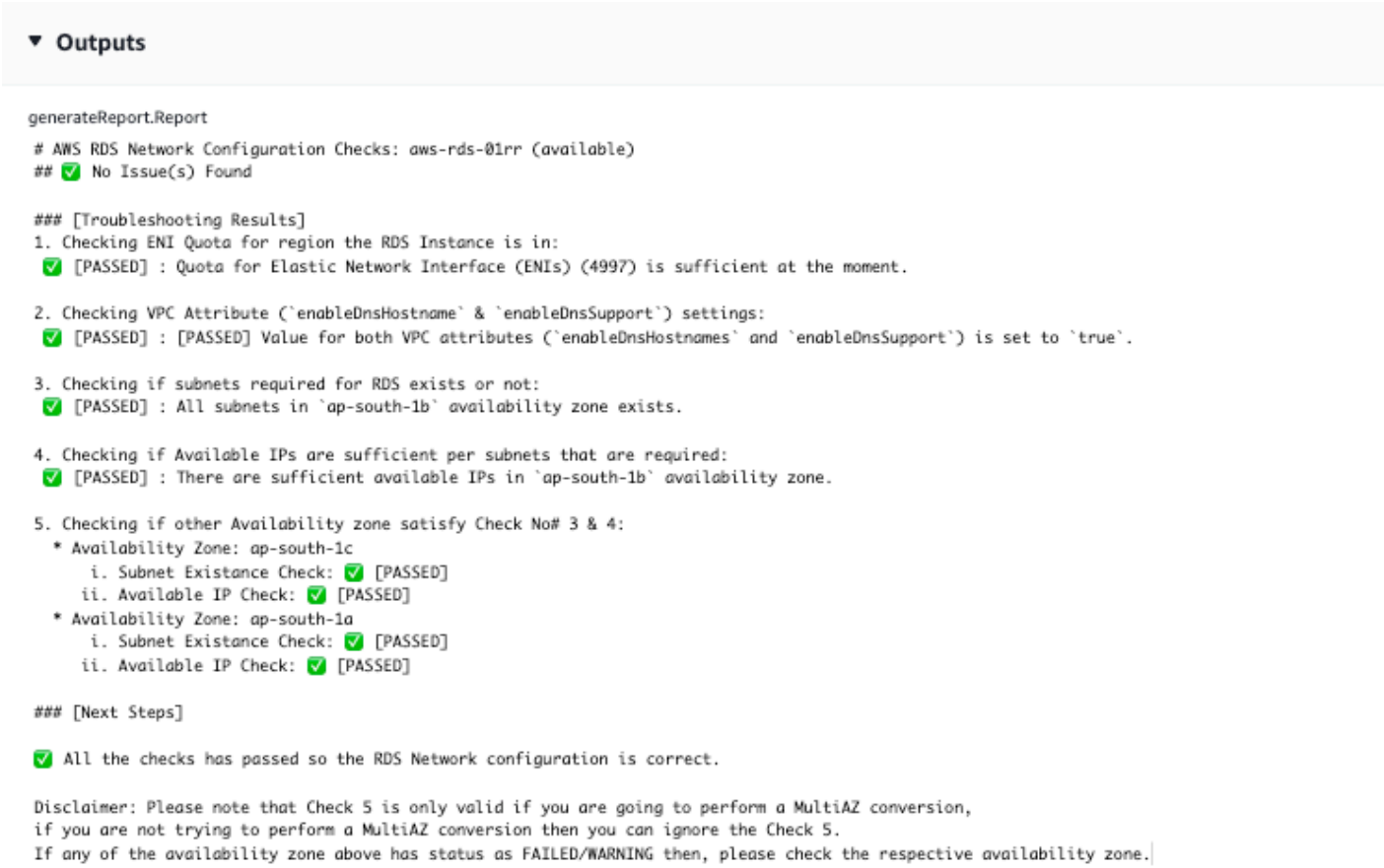
  内のサブネットの存在を検証DBSubnetGroupし、各サブネットで使用可能な IPsをチェックします。

- ステップ 6: generateReport:

  前のステップからすべての情報を取得し、各ステップの結果または出力を出力します。また、IAM 認証情報を使用して Amazon RDS インスタンスに接続するために参照して実行する手順も示します。

7. 自動化が完了したら、出力セクションで詳細な結果を確認します。

   有効なネットワーク設定を持つ Amazon RDS インスタンス :



ネットワーク設定が正しくない Amazon RDS インスタンス (VPC 属性 enableDnsHostnames が false に設定されています) 。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスドキュメント

- 互換性のないネットワーク状態にある Amazon RDS データベースの問題を解決するにはどうすればよいですか？
- 互換性のないネットワーク状態にある Amazon DocumentDB インスタンスの問題を解決するにはどうすればよいですか？

Amazon Redshift

AWS Systems Manager Automation は、Amazon Redshift 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-DeleteRedshiftCluster
- AWSConfigRemediation-DisablePublicAccessToRedshiftCluster
- AWSConfigRemediation-EnableRedshiftClusterAuditLogging
- AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot
- AWSConfigRemediation-EnableRedshiftClusterEncryption
- AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting
- AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster
- AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings
- AWSConfigRemediation-ModifyRedshiftClusterNodeType

AWSConfigRemediation-DeleteRedshiftCluster

説明

AWSConfigRemediation-DeleteRedshiftCluster ランブックは、ユーザーにより指定された Amazon Redshift クラスターを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- ClusterIdentifier

  タイプ: 文字列

  説明: (必須) 削除する Amazon Redshift クラスターの ID。
- SkipFinalClusterSnapshot

  型: ブール値

  デフォルト: false

  説明: (オプション) この値を `false` に設定した場合、オートメーションは Amazon Redshift クラスターを削除する前に、そのスナップショットを作成します。この値を `true` に設定すると、クラスターの最終的なスナップショットは作成されません。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DeleteCluster`
- `redshift:DescribeClusters`

ドキュメントステップ

- `aws:branch` - `SkipFinalClusterSnapshot` パラメータで指定した値に基づいて分岐させます。

- aws:executeAwsApi - ClusterIdentifier パラメータで指定された Amazon Redshift クラスターを削除します。
- aws:assertAwsResourceProperty - Amazon Redshift クラスターが削除されたことを確認します。

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

説明

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster ランブックは、指定した Amazon Redshift クラスターのパブリックアクセシビリティを無効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- ClusterIdentifier

  タイプ: 文字列

  説明: (必須) パブリックアクセシビリティを無効にするクラスターの一意の識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

ドキュメントステップ

- aws:executeAwsApi - ClusterIdentifier パラメータで指定されたクラスターのパブリックアクセシビリティを無効にします。
- aws:waitForAwsResourceProperty - クラスターの状態が available に変わるまで待機します。
- aws:assertAwsResourceProperty - クラスターでパブリックアクセシビリティ設定が無効になっていることを確認します。

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

説明

AWSConfigRemediation-EnableRedshiftClusterAuditLogging ランブックは、指定した Amazon Redshift クラスターの監査ログ記録を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- BucketName

  タイプ: 文字列

  説明: (必須) ログをアップロードする Amazon Simple Storage Service (Amazon S3) バケットの名前。
- ClusterIdentifier

  タイプ: 文字列

  説明: (必須) 監査ログ記録を有効にするクラスターの一意の識別子。
- S3KeyPrefix

  タイプ: 文字列

  説明: (オプション) ログをアップロードする Amazon S3 キープレフィックス (サブフォルダ)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

ドキュメントステップ

- aws:branch - S3KeyPrefix パラメータに値が指定されたかどうかに基づいて分岐させます。
- aws:executeAwsApi - ClusterIdentifier パラメータで指定されたクラスターで監査ログ記録を有効にします。
- aws:assertAwsResourceProperty - 監査ログ記録がクラスターで有効化されたことを確認します。

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

説明

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot ランブックは、ユーザーにより指定された Amazon Redshift クラスターの、自動スナップショットを有効化します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- AutomatedSnapshotRetentionPeriod

  タイプ: 整数

  有効な値: 1 ~ 35

説明: (必須) 自動スナップショットが保持される日数。

- ClusterIdentifier

  タイプ: 文字列

  説明: (必須) 自動スナップショットを有効にするクラスターの一意の識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

ドキュメントステップ

- aws:executeAwsApi - ClusterIdentifier パラメーターで指定されたクラスターで自働スナップショットを有効にします。
- aws:waitForAwsResourceProperty - クラスターの状態が available に変わるまで待機します。
- aws:executeScript - クラスターで自動スナップショットが有効化されたことを確認します。

AWSConfigRemediation-EnableRedshiftClusterEncryption

説明

AWSConfigRemediation-EnableRedshiftClusterEncryption ランブックは、 AWS Key Management Service （ AWS KMS) カスタマーマネージドキーを使用して指定した Amazon Redshift クラスターで暗号化を有効にします。このランブックは、推奨される最小限セキュリティのベストプラクティスに従って Amazon Redshift クラスターが暗号化されるようにするための、ベースラインとしてのみ使用するようにします。複数のクラスターは、それぞれ異なるカスタマーマネージドキーを使用して暗号化することをお勧めします。このランブックは、既に暗号化されているクラスターで使用されている AWS KMS カスタマーマネージドキーを変更することはできません。クラスターの

暗号化に使用される AWS KMS カスタマーマネージドキーを変更するには、まずクラスターの暗号化を無効にする必要があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- ClusterIdentifier

  タイプ: 文字列

  説明: (必須) 暗号化を有効にするクラスターの一意の識別子。
- KMSKeyARN

  タイプ: 文字列

  説明: (必須) クラスターのデータの暗号化に使用する AWS KMS カスタマーマネージドキーの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`

- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

ドキュメントステップ

- aws:executeAwsApi - ClusterIdentifier パラメータで指定された Amazon Redshift クラスターで暗号化を有効にします。
- aws:assertAwsResourceProperty - クラスターで暗号化が有効になっているかを確認します。

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

説明

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting ランブックは、指定された Amazon Redshift クラスターの、拡張仮想プライベートクラウド (VPC)ルーティングを有効にします。拡張 VPC ルーティングの詳細については、Amazon Redshift 管理ガイドの「Amazon Redshift 拡張 VPC ルーティング」を参照してください 。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- ClusterIdentifier

  タイプ: 文字列

  説明: (必須) 拡張 VPC ルーティングを有効にするクラスターの一意の識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

ドキュメントステップ

- aws:executeAwsApi - ClusterIdentifier パラメータで指定されたクラスターの、拡張 VPC ルーティングを有効にします。
- assertAwsResourceProperty - 拡張 VPC ルーティングがクラスターで有効化されたことを確認します。

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

説明

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster ランブックは、指定した Amazon Redshift クラスターで SSL を使用する着信接続を要求します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- ClusterIdentifier

  タイプ: 文字列

  説明: (必須) 拡張 VPC ルーティングを有効にするクラスターの一意の識別子。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:DescribeClusterParameters
- redshift:ModifyClusterParameterGroup

ドキュメントステップ

- aws:executeAwsApi - ClusterIdentifier パラメータで指定されたクラスターからパラメータの詳細を収集します。

- aws:executeAwsApi - ClusterIdentifier パラメータで指定されたクラスターの require_ssl 設定を有効にします。
- aws:assertAwsResourceProperty - クラスターで require_ssl 設定が有効になったことを確認します。
- aws:executeScript - クラスターの require_ssl 設定を検証します。

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

説明

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings ランブックは、指定した Amazon Redshift クラスターのメンテナンス設定を変更します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AllowVersionUpgrade

  型: ブール値

  説明: (必須) true に設定すると、メンテナンス期間中にメジャーバージョンアップグレードがクラスターに自動的に適用されます。

- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- AutomatedSnapshotRetentionPeriod

  タイプ: 整数

  有効な値: 1 ~ 35

  説明: (必須) 自動スナップショットが保持される日数。

- ClusterIdentifier

  タイプ: 文字列

  説明: (必須) 拡張 VPC ルーティングを有効にするクラスターの一意の識別子。

- PreferredMaintenanceWindow

  タイプ: 文字列

  説明: (必須) 週 1 回のシステムメンテナンスを実行できる時間帯 (UTC)

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- redshift:DescribeClusters
- redshift:ModifyCluster

ドキュメントステップ

- aws:executeAwsApi - ClusterIdentifier パラメータで指定されたクラスターのメンテナンス設定を変更します。
- aws:assertAwsResourceProperty - 変更されたメンテナンス設定がクラスターに対して設定されたことを確認します。

AWSConfigRemediation-ModifyRedshiftClusterNodeType

説明

AWSConfigRemediation-ModifyRedshiftClusterNodeType ランブックは、指定した Amazon Redshift クラスターのノードタイプとノード数を変更します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

データベース

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- クラシック

  型: ブール値

  説明: (オプション) true に設定した場合、サイズ変更操作では従来のサイズ変更プロセスが使用されます。
- ClusterIdentifier

  タイプ: 文字列

  説明: (必須) 変更するノードタイプのクラスターの一意の識別子。
- ClusterType

タイプ: 文字列

有効な値: single-node | multi-node

説明: (必須) クラスターに割り当てるクラスターのタイプ。

- NodeType

  タイプ: 文字列

  有効な値: ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

  説明: (必須) クラスターに割り当てるノードのタイプ。

- NumberOfNodes

  タイプ: 整数

  有効な値: 2 ~ 100

  説明: (オプション) クラスターに割り当てるノードの数。クラスターが `single-node` タイプの場合は、このパラメータの値を指定しないでください。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

ドキュメントステップ

- `aws:executeScript` - `ClusterIdentifier` パラメータで指定されたクラスターのノードタイプとノード数を変更します。

Amazon S3

AWS Systems Manager Automation は、Amazon Simple Storage Service 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- 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

説明

AWS-ArchiveS3BucketToIntelligentTiering ランブックは、指定した Amazon Simple Storage Service (Amazon S3) バケットのインテリジェント階層設定を作成または置き換えます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- BucketName

  タイプ: 文字列

  説明: (必須) インテリジェント階層設定を作成する S3 バケットの名前。

- ConfigurationId

  タイプ: 文字列

  説明: (必須) インテリジェント階層化設定の ID。これは、新しい設定 ID でも、既存の設定の ID でもかまいません。

- NumberOfDaysToArchive

  タイプ: 文字列

  有効な値: 90 ~ 730

  説明: (必須) バケット内のオブジェクトがアーカイブアクセス階層に移行できる連続日数。

- NumberOfDaysToDeepArchive

  タイプ: 文字列

  有効な値: 180 ~ 730

説明: (必須) バケット内のオブジェクトが Deep Archive アクセス階層に移行できる連続日数。

- S3Prefix

  タイプ: 文字列

  説明: (オプション) 設定を適用するオブジェクトのキー名のプレフィックス。

- [タグ]

  タイプ: MapList

  説明: (オプション) 設定を適用するオブジェクトに割り当てられたメタデータ。タグはユーザー定義のキーと値で構成されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:GetIntelligentTieringConfiguration
- s3:PutIntelligentTieringConfiguration

ドキュメントステップ

- PutsBucketIntelligentTieringConfiguration (aws:executeScript) - 指定されたバケットの Amazon S3 Intelligent-Tiering 設定を作成または更新します。
- VerifyBucketIntelligentTieringConfiguration (aws:assertAwsResourceProperty) - S3 バケットインテリジェント設定が指定されたバケットに適用されていることを確認します。

AWS-ConfigureS3BucketLogging

説明

Amazon Simple Storage Service (Amazon S3) バケットのログ記録を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- BucketName

  タイプ: 文字列

  説明: (必須) ログ記録を設定する Amazon S3 バケットの名前。
- GrantedPermission

  タイプ: 文字列

  有効な値: FULL_CONTROL | READ | WRITE

  説明: (必須) バケットの被付与者に割り当てられたログ記録のアクセス許可。
- GranteeEmailAddress

  タイプ: 文字列

  (オプション) 被付与者の E メールアドレス。
- GranteeId

  タイプ: 文字列

説明: (オプション) 被付与者の正規ユーザー ID。

- GranteeType

  タイプ: 文字列

  有効な値: CanonicalUser | AmazonCustomerByEmail | Group

  説明: (必須) 被付与者のタイプ。

- GranteeUri

  タイプ: 文字列

  説明: (オプション) 被付与者グループの URI。

- TargetBucket

  タイプ: 文字列

  説明: (必須) Amazon S3 がサーバーアクセスログを保存するバケットを指定します。ログは、所有するあらゆるバケットに配信することができます。また、複数のバケットのログを1つのバケットに配信するよう設定することもできます。この場合、配信されたログファイルをキーで区別できるように、配信元バケットごとに異なる TargetPrefix を選択する必要があります。

- TargetPrefix

  タイプ: 文字列

  デフォルト: /

  説明: (オプション) ログファイルを格納するキーのプレフィックスを指定します。

AWS-ConfigureS3BucketVersioning

説明

Amazon Simple Storage Service (Amazon S3) バケットのバージョニングを設定します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- BucketName

  タイプ: 文字列

  説明: (必須) バージョン設定する Amazon S3 バケットの名前。
- VersioningState

  タイプ: 文字列

  有効な値: Enabled | Suspended

  デフォルト: Enabled

  説明: (オプション) VersioningConfiguration.Status に適用されます。"Enabled" に設定すると、このプロセスはバケット内のオブジェクトのバージョン管理を有効にし、バケットに追加されたすべてのオブジェクトは一意のバージョン ID を受け取ります。Suspended に設定すると、このプロセスはバケット内のオブジェクトのバージョニングを無効にします。バケットに追加されたすべてのオブジェクトは、バージョン ID null を受け取ります。

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

説明

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock ランブックは、ランブックパラメータで指定された値に基づいて、Amazon Simple Storage Service (Amazon S3) バケットの Amazon S3 パブリックアクセスブロック設定を構成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- BlockPublicAcls

  型: ブール値

  デフォルト: true

  説明: (オプション) この値を true に設定すると、S3 バケットのパブリックアクセスコントロールリスト (ACL) と、BucketName パラメータで指定された S3 バケットに格納されているオブジェクトが、Amazon S3 によりブロックされます。
- BlockPublicPolicy

  型: ブール値

  デフォルト: true

  説明: (オプション) この値を true に設定すると、BucketName パラメータで指定された S3 バケットのパブリックバケットポリシーが、Amazon S3 によりブロックされます。

- BucketName

  タイプ: 文字列

  説明: (必須) 設定する S3 バケットの名前。

- IgnorePublicAcls

  型: ブール値

  デフォルト: true

  説明: (オプション) この値を `true` に設定すると、`BucketName` パラメータで指定された S3 バケットのための、すべてのパブリック ACL が Amazon S3 により無視されます。

- RestrictPublicBuckets

  型: ブール値

  デフォルト: true

  説明: (オプション) この値を `true` に設定すると、`BucketName` パラメータで指定された S3 バケットのパブリックバケットポリシーが、Amazon S3 により制限されます。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

ドキュメントステップ

- `aws:executeAwsApi` - `BucketName` パラメータで指定された S3 バケットの `PublicAccessBlock` 設定を作成または変更します。

- aws:executeScript - BucketName パラメータで指定された S3 バケットの PublicAccessBlock 設定を返し、ランブックパラメータで指定された値に基づいて変更が正常に行われているかを確認します。

AWSConfigRemediation-ConfigureS3PublicAccessBlock

説明

AWSConfigRemediation-ConfigureS3PublicAccessBlock ランブックは、ランブックパラメータで指定した値に基づいて、 AWS アカウントの Amazon Simple Storage Service (Amazon S3) パブリックアクセスブロック設定を構成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AccountId

  タイプ: 文字列

  説明: (必須) 設定する S3 バケットを所有 AWS アカウント する の ID。
- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- BlockPublicAcls

型: ブール値

デフォルト: true

説明: (オプション) に設定するとtrue、Amazon S3 は、 AccountIdパラメータで AWS アカウント 指定した が所有する S3 バケットのパブリックアクセスコントロールリスト (ACLs) をブロックします。

- BlockPublicPolicy

  型: ブール値

  デフォルト: true

  説明: (オプション) に設定するとtrue、Amazon S3 は AccountIdパラメータで AWS アカウント 指定した が所有する S3 バケットのパブリックバケットポリシーをブロックします。

- IgnorePublicAcls

  型: ブール値

  デフォルト: true

  説明: (オプション) に設定するとtrue、Amazon S3 は、 AccountIdパラメータで AWS アカウント 指定した が所有する S3 バケットのすべてのパブリック ACLs を無視します。

- RestrictPublicBuckets

  型: ブール値

  デフォルト: true

  説明: (オプション) に設定するとtrue、Amazon S3 は AccountIdパラメータで AWS アカウント 指定した が所有する S3 バケットのパブリックバケットポリシーを制限します。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution

- s3:GetAccountPublicAccessBlock
- s3:PutAccountPublicAccessBlock

ドキュメントステップ

- aws:executeAwsApi - AccountId パラメータで指定された AWS アカウント の PublicAccessBlock 設定を作成または変更します。
- aws:executeScript - AccountIdパラメータで AWS アカウント 指定された PublicAccessBlockの設定を返し、ランブックパラメータで指定された値に基づいて変更が正常に行われたことを確認します。

AWS-CreateS3PolicyToExpireMultipartUploads

説明

AWS-CreateS3PolicyToExpireMultipartUploads ランブックは、定義された日数後に進行中の不完全なマルチパートアップロードを期限切れにする、指定されたバケットのライフサイクルポリシーを作成します。このランブックは、新しいライフサイクルポリシーを、既に存在する既存のライフサイクルバケットポリシーとマージします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- BucketName

  タイプ: 文字列

  説明: (必須) 設定する S3 バケットの名前。

- DaysUntilExpire

  タイプ: 整数

  説明: (必須) Amazon S3 がアップロードのすべての部分を完全に削除するまで待機する日数。

- RuleId

  タイプ: 文字列

  説明: (必須) lifeycle バケットルールを識別するために使用される ID。これは一意の値である必要があります。

- S3Prefix

  タイプ: 文字列

  説明: (オプション) 設定を適用するオブジェクトのキー名のプレフィックス。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

ドキュメントステップ

- ConfigureExpireMultipartUploads (aws:executeScript) - バケットのライフサイクルポリシーを設定します。
- VerifyExpireMultipartUploads (aws:executeScript) - バケットにライフサイクルポリシーが設定されていることを確認します。

出力

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

AWS-DisableS3BucketPublicReadWrite

説明

Amazon Simple Storage Service (Amazon S3) `Block Public Access` を使用して、パブリック S3 バケットの読み取りおよび書き込みアクセスを無効にします。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 パブリックアクセスブロック」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム

(ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- S3BucketName

  タイプ: 文字列

  説明: (必須) アクセスを制限したい S3 バケット。

AWS-EnableS3BucketEncryption

説明

Amazon Simple Storage Service (Amazon S3) バケットにデフォルトの暗号化を設定する

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- BucketName

  タイプ: 文字列

説明: (必須) コンテンツを暗号化する S3 バケットの名前。

- SSEAlgorithm

  タイプ: 文字列

  デフォルト: AES256

  説明: (オプション) デフォルト暗号化に使用するサーバー側の暗号化アルゴリズム。

AWS-EnableS3BucketKeys

説明

AWS-EnableS3BucketKeys ランブックは、指定した Amazon Simple Storage Service (Amazon S3) バケットでバケットキーを有効にします。このバケットレベルのキーは、ライフサイクル中に新しいオブジェクトのデータキーを作成します。KmsKeyId パラメータの値を指定しない場合、Amazon S3 マネージドキー (SSE-S3) を使用したサーバー側の暗号化がデフォルトの暗号化設定に使用されます。

> **Note**
>
> Amazon S3 バケットキーは、 AWS Key Management Service （ AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) ではサポートされていません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- BucketName

  タイプ: 文字列

  説明: (必須) バケットキーを有効にする S3 バケットの名前。

- KMSKeyId

  タイプ: 文字列

  説明: (オプション) サーバー側の暗号化に使用する Amazon リソースネーム (ARN)、キー ID、または AWS Key Management Service （ AWS KMS) カスタマーマネージドキーのキーエイリアス。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

ドキュメントステップ

- ChooseEncryptionType (aws:branch) - `KmsKeyId`パラメータに指定された値を評価し、SSE-S3 (AES256) または SSE-KMS のどちらを使用するかを決定します。
- PutBucketKeysKMS (aws:executeAwsApi) - 指定された を使用して、指定された S3 バケットの `BucketKeyEnabled`プロパティを `true` に設定します`KmsKeyId`。

- PutBucketKeysAES256 (aws:executeAwsApi) - AES256 暗号化で指定された S3 バケットtrueの BucketKeyEnabledプロパティを に設定します。
- VerifyS3BucketKeysEnabled (aws:assertAwsResourceProperty) - ターゲット S3 バケットでバケットキーが有効になっていることを確認します。

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

説明

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy ランブックは、Amazon Simple Storage Service (Amazon S3) バケットポリシーから Allow アクションにワイルドカード (Principal: * または Principal: "AWS": *) を含むプリンシパルポリシーステートメントを削除します。条件を含むポリシーステートメントも削除されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- BucketName

  タイプ: 文字列

説明: (必須) ポリシーを変更する Amazon S3 バケットの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- s3:DeleteBucketPolicy
- s3:GetBucketPolicy
- s3:PutBucketPolicy

ドキュメントステップ

- aws:executeScript - バケットポリシーを変更し、ワイルドカードを含むプリンシパルポリシーステートメントが、BucketName パラメータで指定する Amazon S3 バケットから削除されていることを確認します。

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

説明

AWSConfigRemediation-RestrictBucketSSLRequestsOnly ランブックでは、指定した Amazon S3 バケットへの HTTP リクエストを明示的に拒否する Amazon Simple Storage Service (Amazon S3) バケットポリシーステートメントが作成されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- BucketName

  タイプ: 文字列

  説明: (必須) HTTP リクエストを拒否する S3 バケットの名前。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutEncryptionConfiguration`
- `s3:PutBucketPolicy`

ドキュメントステップ

- `aws:executeScript` - HTTP リクエストを明示的に拒否する `BucketName` パラメータで指定された S3 バケットのバケットポリシーを作成します。

AWSSupport-TroubleshootS3PublicRead

説明

AWSSupport-TroubleshootS3PublicRead ランブックは、S3BucketName パラメータで指定したパブリック Amazon Simple Storage Service (Amazon S3) バケットからのオブジェクトの読み取りに関する問題を診断します。S3 バケット内のオブジェクトについても、設定のサブセットが分析されます。

[このオートメーションを実行する (コンソール)]

制約事項

- この自動化では、オブジェクトへのパブリックアクセスを許可するアクセスポイントはチェックされません。
- この自動化では、S3 バケットポリシーの条件キーは評価されません。
- を使用している場合 AWS Organizations、この自動化は Amazon S3 へのアクセスが許可されていることを確認するためにサービスコントロールポリシーを評価しません。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- CloudWatchLogGroupName

  タイプ: 文字列

説明: (オプション) オートメーション出力を送信する Amazon CloudWatch Logs のロググループ。指定した値に一致するロググループが見つからない場合、自動化ではこのパラメータ値を使用してロググループが作成されます。この自動化によって作成されるロググループの保存期間は 14 日間です。

- CloudWatchLogStreamName

  タイプ: 文字列

  説明: (オプション) オートメーション出力を送信する CloudWatch Logs ログストリーム。指定した値に一致するログストリームが見つからない場合、自動化ではこのパラメータ値を使用してログストリームが作成されます。このパラメータに値を指定しない場合、自動化ではログストリームの名前に `ExecutionId` を使用します。

- HttpGet

  型: ブール値

  有効な値: true | false

  デフォルト: true

  説明: (オプション) このパラメータを `true` に設定すると、自動化では指定した `S3BucketName` のオブジェクトに部分的 HTTP リクエストを行います。Range HTTP ヘッダーを使用して、オブジェクトの最初のバイトのみが返されます。

- IgnoreBlockPublicAccess

  型: ブール値

  有効な値: true | false

  デフォルト: false

  説明: (オプション) このパラメータを `true` に設定すると、自動化では `S3BucketName` パラメータで指定した S3 バケットのパブリックアクセスブロック設定を無視します。このパラメータのデフォルト値を変更することは推奨されません。

- MaxObjects

  タイプ: 整数

  有効な値: 1 ~ 25

デフォルト: 5

説明: (オプション) S3BucketName パラメータで指定した S3 バケットで分析するオブジェクト数。

- S3BucketName

  タイプ: 文字列

  説明: (必須) トラブルシューティングする S3 バケットの名前。

- S3PrefixName

  タイプ: 文字列

  説明: (オプション) S3 バケットで分析するオブジェクトのキー名プレフィックス。詳細については、Amazon Simple Storage Service ユーザーガイドのオブジェクトキーを参照してください。

- StartAfter

  タイプ: 文字列

  説明: (オプション) 自動化で S3 バケット内のオブジェクトの分析を開始するオブジェクトキーの名前。

- ResourcePartition

  タイプ: 文字列

  有効な値: aws | aws-us-gov | aws-cn

  デフォルト: aws

  説明: (必須) S3 バケットがあるパーティション。

- 詳細

  型: ブール値

  有効な値: true | false

  デフォルト: false

  説明: (オプション) 自動化中に詳細情報を返すには、このパラメータを true に設定します。パラメータが false に設定されている場合、警告メッセージとエラーメッセージのみが返されます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

logs:CreateLogGroup、logs:CreateLogStream、およびlogs:PutLogEvents アクセス許可は、オートメーションでログデータを CloudWatch Logs に送信する場合にのみ必要です 。

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

ドキュメントステップ

- aws:assertAwsResourceProperty - S3 バケットが存在し、アクセス可能であることを確認します。
- aws:executeScript - S3 バケットの場所と正規ユーザー ID を返します。
- aws:executeScript - アカウントと S3 バケットのパブリックアクセスブロック設定を返します。
- aws:assertAwsResourceProperty - S3 バケットの支払者が BucketOwner に設定されていることを確認します。Requester Pays が S3 バケットで有効になっている場合、自動化は終了します。
- aws:executeScript - S3 バケットポリシーのステータスを返し、パブリックと見なされるかどうかを判断します。パブリック S3 バケットの詳細については、Amazon Simple Storage Service ユーザーガイドの「「パブリック」の意味」を参照してください。
- aws:executeAwsApi - S3 バケットポリシーを返します。
- aws:executeAwsApi - S3 バケットポリシーで見つかったすべてのコンテキストキーを返します。
- aws:assertAwsResourceProperty - GetObject API アクションの S3 バケットポリシーに明示的な拒否があるかどうかを確認します。
- aws:executeAwsApi - S3 バケットのアクセスコントロールリスト (ACL) を返します。
- aws:executeScript - CloudWatchLogGroupName パラメータの値を指定した場合、CloudWatch Logs ロググループとログストリームを作成します。
- aws:executeScript - ランブックの入力パラメータで指定された値に基づいて、オートメーション実行中に収集された S3 バケット設定のいずれかが、パブリックによるオブジェクトへのアクセスを妨げているのかどうかを評価します。このスクリプトは以下の関数を実行します。
  - パブリックアクセスブロック設定を評価する
  - MaxObjects、S3PrefixName、および StartAfter パラメータで指定した値に基づいて S3 バケットからオブジェクトを返します。

- S3 バケットから返されたオブジェクトのカスタム IAM ポリシーをシミュレートする S3 バケットポリシーを返します。
- HttpGet パラメータが true に設定されている場合、返されたオブジェクトに対して部分的 HTTP リクエストを実行します。Range HTTP ヘッダーを使用して、オブジェクトの最初のバイトのみが返されます。
- 返されたオブジェクトのキー名をチェックして、最後が 1 つか 2 つのピリオドになっているかどうかを確認します。ピリオドで終わるオブジェクトキー名は、Amazon S3 コンソールからダウンロードできません。
- 返されたオブジェクトの所有者が S3 バケットの所有者と一致するかどうかをチェックします。
- オブジェクトの ACL が匿名ユーザーに READ または FULL_CONTROL アクセス許可を付与するかどうかをチェックします。
- オブジェクトに関連付けられたタグを返します。
- シミュレートされた IAM ポリシーを使用して、GetObject API アクションの S3 バケットポリシーでこのオブジェクトに対する明示的な拒否があるかどうかを確認します。
- オブジェクトのメタデータを返し、ストレージクラスがサポートされていることを確認します。
- オブジェクトのサーバー側の暗号化設定をチェックして、オブジェクトが AWS Key Management Service（AWS KMS) カスタマーマネージドキーを使用して暗号化されているかどうかを確認します。

出力

AnalyzeObjects.bucket

AnalyzeObjects.object

AWSSupport-EmptyS3Bucket

説明

AWSSupport-EmptyS3Bucket オートメーションランブックは、ライフサイクルの有効期限設定ルールを使用して、既存の Amazon Simple Storage Service (Amazon S3) バケットを空にします。

> **Important**
>
> - 多要素認証 (MFA) が有効になっている Amazon S3 バケットはサポートされていません。

- このランブックによって変更されたライフサイクルルールは、指定された Amazon S3 バケット内のすべてのオブジェクトとそのバージョンを完全に削除します。削除されたオブジェクトを完全に復元することはできません。詳細については、「期限切れオブジェクト」を参照してください。

動作の仕組み

ランブックは、以下の大まかなステップAWSSupport-EmptyS3Bucketを実行します。

- 有効になっている場合、バケットのバージョニングを停止します。
- バケットポリシーを更新してs3:PutObject、API コールを拒否します (空になっている間に新しいアップロードを防ぐ) 。
- ライフサイクルルールを更新して、入力パラメータで指定された有効期限に従ってすべてのオブジェクトを削除します。

Note

- Amazon S3 オブジェクトロックで保護されたオブジェクトバージョンは、ライフサイクル設定によって削除または上書きされません。
- 削除プロセスは非同期であり、ランブックの実行が完了した後に完了するまでに時間がかかる場合があります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

/

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

AutomationAssumeRole パラメータでは、ランブックを正常に使用するには、次のアクションが必要です。

- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution
- s3:GetBucketVersioning
- s3:PutBucketVersioning
- s3:GetBucketPolicy
- s3:GetBucketLifecycleConfiguration
- s3:GetLifecycleConfiguration
- s3:PutBucketPolicy
- s3:PutBucketLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:DeleteBucketPolicy
- s3:DeleteBucketLifecycle

指示

次の手順に従って自動化を設定します。

1. Systems Manager AWSSupport-EmptyS3Bucketの ドキュメントで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - S3BucketName:

     空にする Amazon S3 バケットの名前。

- SNSTopicArn:

  承認通知用の Amazon SNS トピックの ARN を指定します。この Amazon SNS トピックは、オートメーション実行中に必要な 中に承認通知を送信するために使用されます。

- ApproverIAM:

  アクションを承認または拒否できる AWS 認証済みプリンシパルのリストを指定します。承認者の最大数は です10。これらの形式、 AWS Identity and Access Management (IAM) ユーザー名、IAM ユーザー ARN、IAM ロール ARN、または IAM 継承ロールユーザー ARN のいずれかを使用してプリンシパルを指定できます。

- MinimumRequiredApprovals (オプション):

  オートメーションが再開されるために必要な承認の最小数。値を指定しない場合、システムはデフォルトで になります1。このパラメータの値は、正の数にする必要があります。このパラメータの値は、ApproverIAM パラメータで定義された承認者の数を超えることはできません。

- NoncurrentVersionExpirationDays (オプション):

  以前のオブジェクトバージョンの有効期限が切れる日数を指定します。期限切れになると、Amazon S3 により、最新ではないオブジェクトのバージョンが完全に削除されます。

  - デフォルト: 1
  - 最大値: 365

- ExpirationDays (オプション):

  オブジェクトのライフサイクルの有効期限をフォーム日数で指定します。

  - デフォルト: 1
  - 最大値: 365

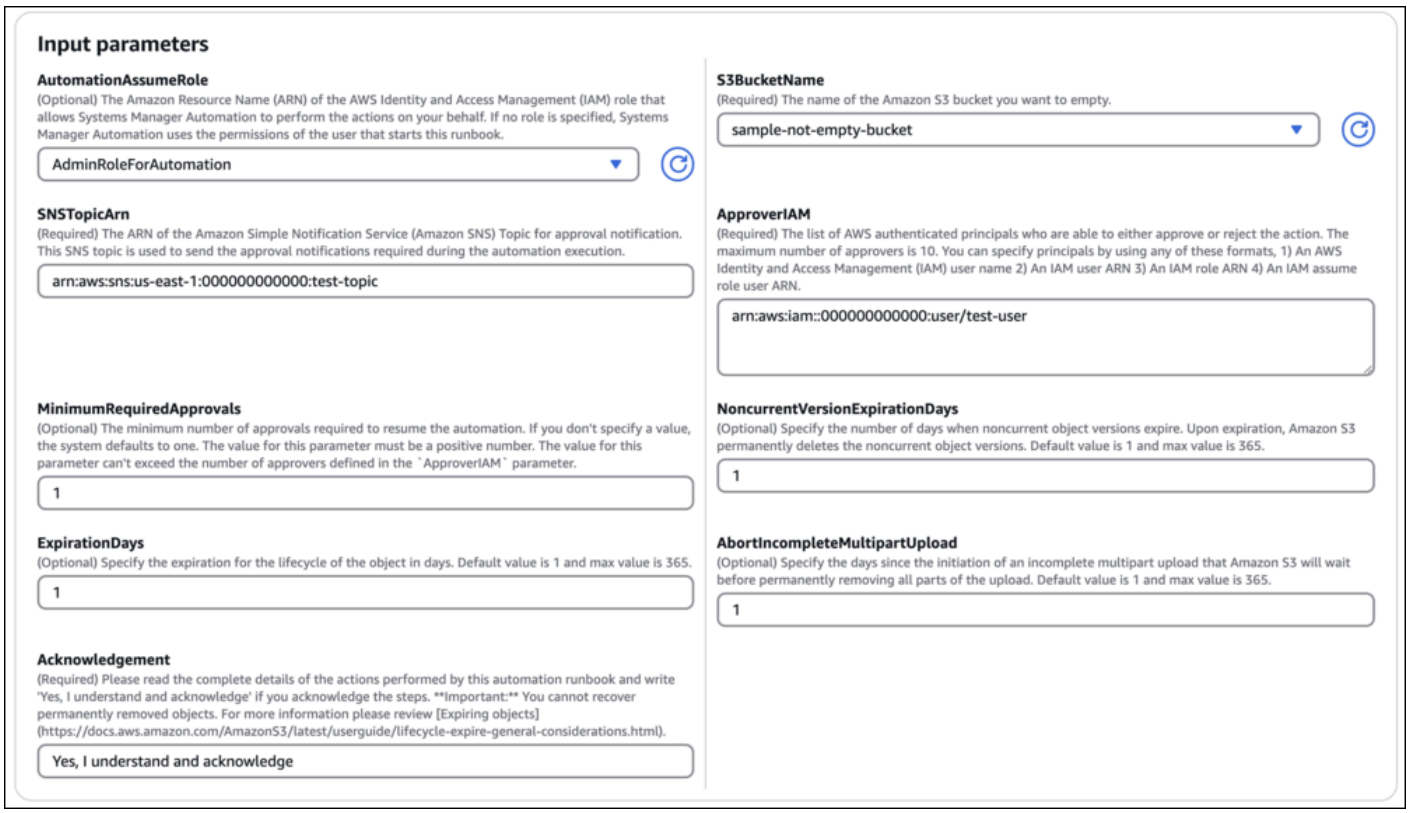
- AbortIncompleteMultipartUpload (オプション):

  Amazon S3 がアップロードのすべての部分を完全に削除するまで待機する、不完全なマルチパートアップロードの開始からの日数を指定します。

  - デフォルト: 1
  - 最大値: 365

- 確認 :

  このオートメーションランブックによって実行されるアクションの詳細をすべて読み、ステップに同意するYes, I understand and acknowledge場合は同意してください。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。

   - **checkConcurrency**:

     指定された Amazon S3 バケットをターゲットとするこのランブックの実行が 1 つだけであることを確認します。ランブックが同じバケット名をターゲットとする別の進行中の実行を検出した場合、エラーが返され、終了します。

   - **getBucketVersioningConfiguration**:

     指定された Amazon S3 バケットのバージョニングステータスを取得します。

   - **branchOnStoppingIfMFADeleteEnabled** (条件付き):

     指定した Amazon S3 バケットで多要素認証 (MFA) が有効になっている場合、オートメーションを停止します。

   - **approvalToMakeChangesToTheProvidedS3Bucket**:

     指定されたプリンシパルの承認がバケットのバージョニングを無効にし、指定された Amazon S3 バケットのバケットポリシーとライフサイクルルールの設定を更新するのを待ちます。

- **branchOnBucketVersioningStatus** (条件付き):

  指定された Amazon S3 バケットでバージョニングが有効になっている場合は、無効にします。それ以外の場合は、バケットポリシーとライフサイクル設定の更新を続行します。

- **suspendBucketVersioning**:

  指定された Amazon S3 バケットのバージョニング状態を停止します。

- **updateBucketPolicyAndLifeCycleConfiguration**:

  バケットポリシーを追加または更新してすべての`s3:PutObject`リクエストを拒否し、ユーザーが指定した入力パラメータに基づいてライフサイクル設定を更新してオブジェクトを期限切れにします。

- **branchOnFailingIfBucketPropertiesNotUpdated** (条件付き):

  `updateBucketPolicyAndLifeCycleConfiguration` ステップのステータスを確認し、オートメーションによって変更された場合、元のバケットのバージョニング状態を元に戻そうとします。

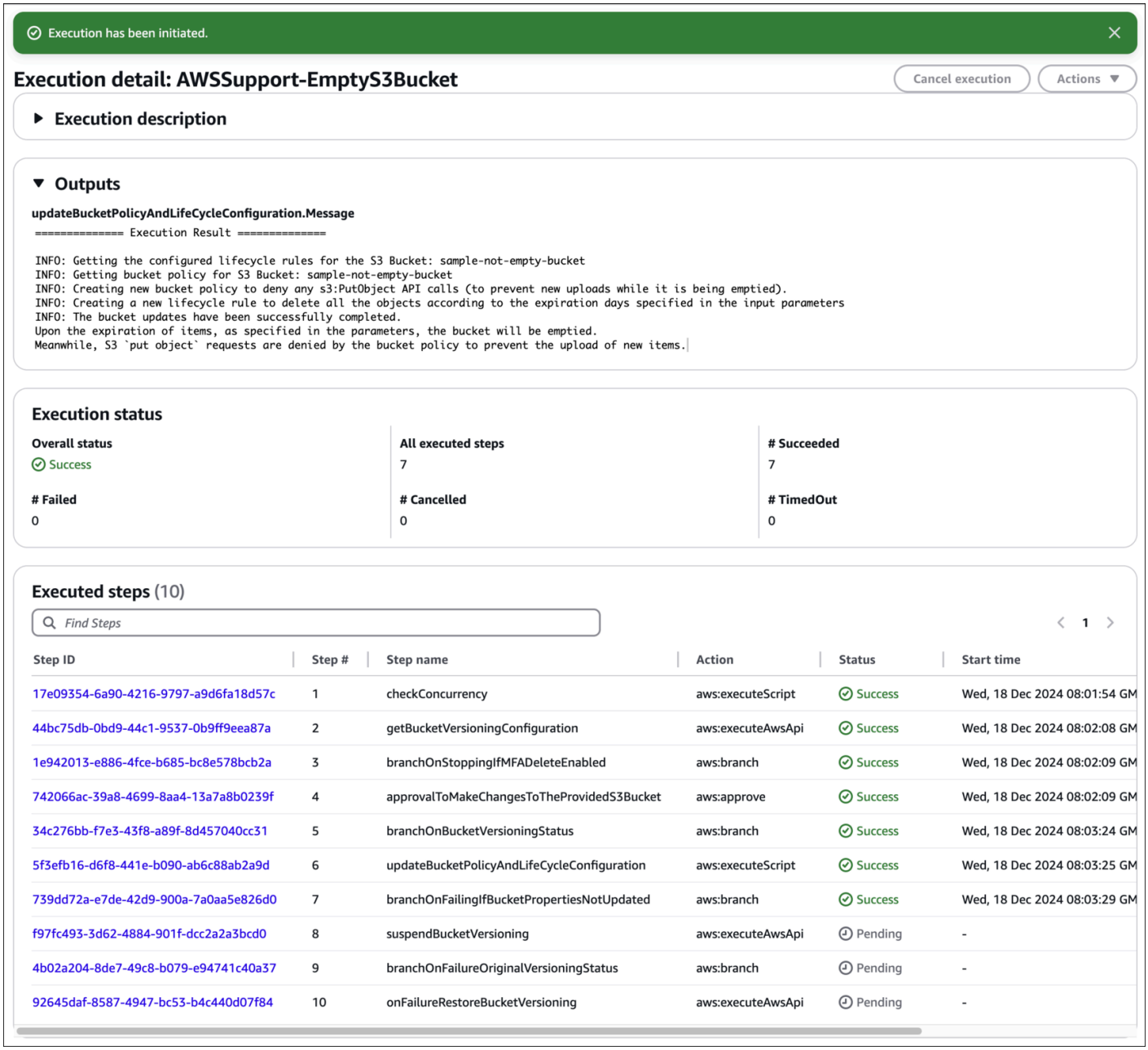
- **branchOnFailureOriginalVersioningStatus** (条件付き):

  失敗すると、 はブランチして元のバージョニングステータスを判断します。がこのオートメーションによって有効になり、停止された場合、 は再度有効にしようとします。

- **onFailureRestoreBucketVersioning**

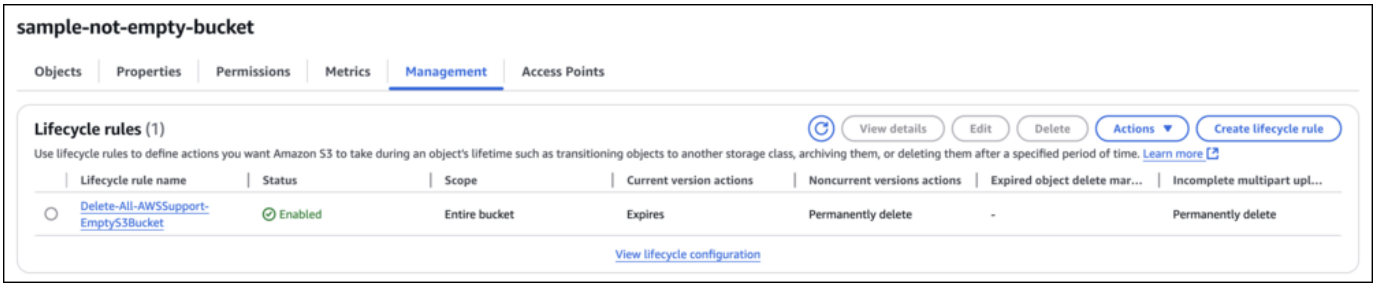
  指定された Amazon S3 バケットの有効なバージョニング状態を復元します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。



- 成功した実行

  このワークフローは、バケットのライフサイクルルールを更新します。オブジェクトはライフサイクルDelete-All-AWSSupport-EmptyS3-Bucketポリシーに従って削除されます。



- 失敗の実行

  部分的な削除は実行されません。実行が失敗すると、ライフサイクルおよびその他のバケット設定がロールバックされます。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- オートメーションワークフローのサポート

Amazon S3 バケットとオブジェクトの管理の詳細については、「バケットを空にする」を参照してください。

AWSSupport-TroubleshootS3EventNotifications

説明

AWSSupport-TroubleshootS3EventNotifications AWS Systems Manager オートメーションランブックは、 関数、Amazon Simple Notification Service (Amazon S3Amazon SNS) キューで AWS Lambda 設定された Amazon Simple Storage Service (Amazon S3) バケットイベント通知のトラブルシューティングに役立ちます。 Amazon SQS 送信先イベント通知として Amazon S3 バケットで設定されたさまざまなリソースの設定レポートを提供します。

動作の仕組み

ランブックは次のステップを実行します。

- Amazon S3 バケットAWSSupport-TroubleshootS3EventNotificationsが が実行されたのと同じアカウントに存在するかどうかを確認します。

- GetBucketNotificationConfiguration API を使用して、Amazon S3 バケットのイベント通知として設定された送信先リソース (AWS Lambda 関数、Amazon SNS トピック、または Amazon SQS キュー) を取得します。 Amazon S3
- 送信先リソースが存在することを検証し、送信先リソースのリソースベースのポリシーを確認して、Amazon S3 が送信先への発行を許可されているかどうかを確認します。
- 送信先を AWS Key Management Service （ AWS KMS) キーで暗号化した場合、キーポリシーがチェックされ、Amazon S3 アクセスが許可されているかどうかを確認します。
- すべての送信先リソースチェックのレポートを生成します。

> **Important**
>
> - このランブックは、Amazon S3 バケット所有者がオートメーションランブックが実行されている AWS アカウント 所有者と同じである場合にのみ、イベント通知設定を評価できます。
> - さらに、このランブックは、別の でホストされている送信先リソースのポリシーを評価することはできません AWS アカウント。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- S3BucketName

  型: `AWS::S3::Bucket::Name`

  説明: (必須) イベント通知で設定された Amazon S3 バケットの名前 (複数可) 。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `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`

自動化引き受けロールの IAM ポリシーの例

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

指示

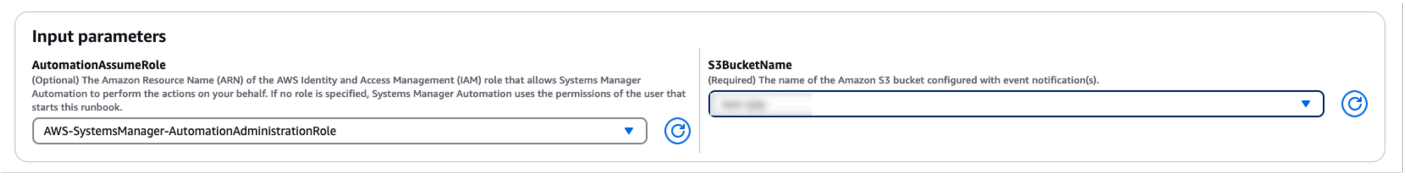
次の手順に従って自動化を設定します。

1. ドキュメントの下の Systems Manager [AWSSupport-TroubleshootS3EventNotifications]の に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。

3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - S3BucketName (必須):

     イベント通知で設定された Amazon S3 バケットの名前 (複数可) 。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - ValidateInputs

     提供された Amazon S3 バケットが、オートメーションが実行されているのと同じアカウントに属していることを検証し、バケットがホストされているリージョンを取得します。
   - GetBucketNotificationConfiguration

     `GetBucketNotificationConfiguration` API を呼び出して、Amazon S3 バケットで設定されたイベント通知を確認し、出力をフォーマットします。
   - BranchOnSQSResourcePolicy

     イベント通知に Amazon SQS リソースがあるかどうかを分岐させます。
   - ValidateSQSResourcePolicy

     Amazon SQS キュー属性のリソースポリシーに Amazon S3 の`sqs:SendMessage`アクセス許可があることを検証します。Amazon SQS リソースが暗号化されている場合、 は暗号化がデフォルト AWS KMS キーを使用していないことを確認します。つまり、 `aws/sqs` は AWS KMS キーポリシーに Amazon S3 のアクセス許可があることを確認します。
   - BranchOnSNSResourcePolicy

     イベント通知に Amazon SNS リソースがあるかどうかを分岐させます。

- ValidateSNSResourcePolicy

  Amazon SNS トピック属性のリソースポリシーに Amazon S3 のsns:Publishアクセス許可があることを検証します。Amazon SNS リソースが暗号化されている場合、 は暗号化がデフォルト AWS KMS キーを使用していないことを確認します。つまり、 aws/sns は AWS KMS キーポリシーに Amazon S3 のアクセス許可があることを確認します。

- BranchOnLambdaFunctionResourcePolicy

  イベント通知に AWS Lambda 関数があるかどうかを分岐させます。

- ValidateLambdaFunctionResourcePolicy

  AWS Lambda 関数に Amazon S3 のlambda:InvokeFunctionアクセス許可があるリソースポリシーを検証します。

- GenerateReport

  ランブックステップ出力の詳細と、Amazon S3 バケットで設定されたイベント通知の問題を解決するための推奨事項を返します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。

   - Amazon SQS イベント通知

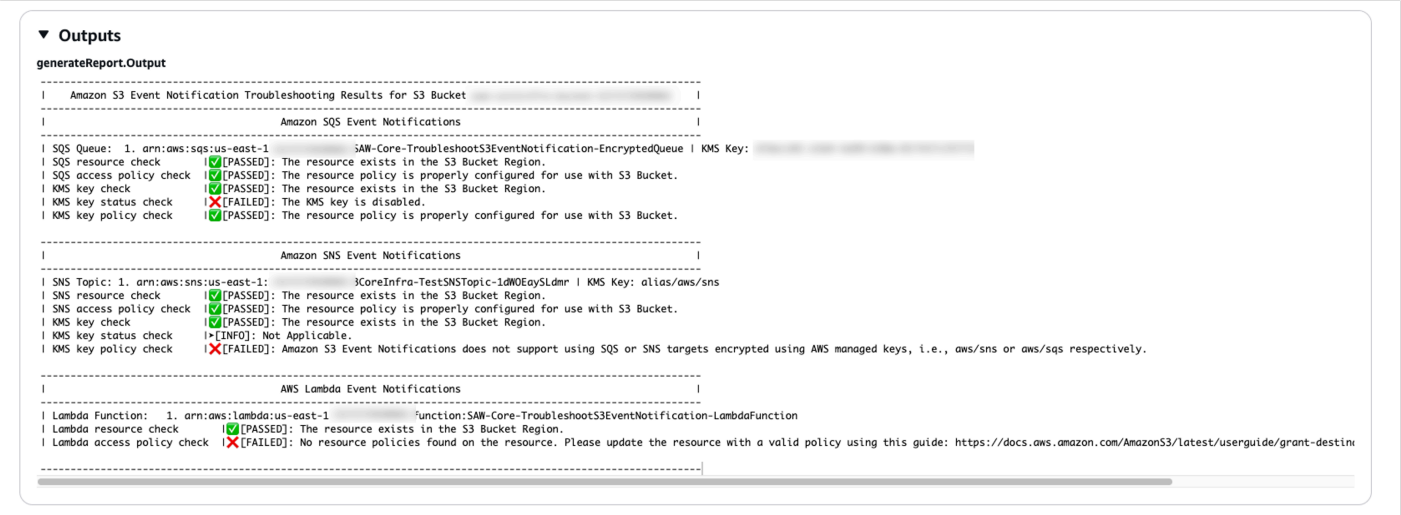
     Amazon S3 バケットで設定された Amazon SQS 送信先通知がある場合、Amazon SQS キューのリストがチェックの結果とともに表示されます。レポートには、Amazon SQS リソースチェック、Amazon SQS アクセスポリシーチェック、 AWS KMS キーチェック、 AWS KMS キーステータスチェック、および AWS KMS キーポリシーチェックが含まれます。

   - Amazon SNS イベント通知

     Amazon S3 バケットで設定された Amazon SNS 送信先通知がある場合、Amazon SNS トピックのリストがチェックの結果とともに表示されます。レポートには、Amazon SNS リソースチェック、Amazon SNS アクセスポリシーチェック、 AWS KMS キーチェック、 AWS KMS キーステータスチェック、および AWS KMS キーポリシーチェックが含まれます。

   - AWS Lambda イベント通知

     Amazon S3 バケットで設定された AWS Lambda 送信先通知がある場合、Lambda 関数のリストがチェックの結果とともに表示されます。レポートには、Lambda リソースチェックと Lambda アクセスポリシーチェックが含まれます。



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWSSupport-ContainS3Resource

説明

AWSSupport-ContainS3Resource ランブックは、記事「Support Automation Workflow (SAW) Runbook: Contain a compromised AWS Amazon S3 Bucket」で説明されている手順の自動化ソリューションを提供します。

Important

- このランブックは、Amazon S3 バケットポリシー、タグ、パブリックアクセス設定の変更など、昇格された権限を必要とするさまざまなオペレーションを実行します。これらのアクションは、特権のエスカレーションや、ターゲットの Amazon S3 バケットに依存する他のワークロードに影響を与える可能性があります。AutomationAssumeRole パラメータで指定されたロールに付与されたアクセス許可を確認し、それらが意図したユースケースに適していることを確認する必要があります。IAM アクセス許可の詳細について

は、次の AWS ドキュメントを参照してください: Identity and Access Management (IAM) Permissions AWS AWS Systems Manager Automation Permissions。

- このランブックは、ワークロードの可用性の低下や中断を引き起こす可能性のある変更アクションを実行します。具体的には、 Contain アクションは、 SecureRolesパラメータで指定されたロールを除き、指定された Amazon S3 バケットへのすべてのアクセスをブロックします。これは、ターゲットの Amazon S3 バケットに依存するアプリケーションまたはサービスに影響を与える可能性があります。
- Contain アクション中に、このランブックは追加の Amazon S3 バケット (BackupS3BucketNameパラメータで指定) を作成し、元のバケットの設定のバックアップがまだ存在しない場合は保存できます。
- Action パラメータが に設定されている場合Restore、このランブックは、バケットに保存されているバックアップに基づいて Amazon S3 BackupS3BucketNameバケットの設定を元の状態に復元しようとします。ただし、復元プロセスが失敗し、Amazon S3 バケットが整合性のない状態になるリスクがあります。ランブックには、このような障害が発生した場合の手動復元の手順が記載されていますが、復元プロセス中に発生する可能性のある問題に対処する準備を整えておく必要があります。

本番環境で実行する前に、ランブックを徹底的に確認し、その潜在的な影響を理解し、非本番環境でテストすることをお勧めします。

動作の仕組み

このランブックは、リソースタイプとアクションに基づいて動作が異なります。

- Amazon S3 汎用バケットContainmentの場合: オートメーションは、バケットへのパブリックアクセスをブロックし、ACL 設定を無効にし、バケット所有者オブジェクトの所有権を強制し、リストされた許可 IAM ロールを除くすべての Amazon S3 アクションを拒否する制限付きバケットポリシーをバケットに配置します。
- Amazon S3 汎用オブジェクト の場合Containment: オートメーションはバケットへのパブリックアクセスをブロックし、ACL 設定を無効にし、バケット所有者オブジェクトの所有権を強制し、リストされた許可 IAM ロールを除くオブジェクトに対するすべての Amazon S3 アクションを拒否する制限付きバケットポリシーを配置します。
- Amazon S3 ディレクトリバケットの場合Containment: オートメーションは、リストされた許可 IAM ロールを除くすべての Amazon S3 アクションを拒否する制限付きバケットポリシーをバケットに配置します。

- Amazon S3 汎用バケットの場合Restore: 自動化は、ブロックパブリックアクセス設定、バケット ACL 設定、バケット所有者オブジェクトの所有権、バケットポリシーを、封じ込め前の初期設定に復元します。
- Amazon S3 汎用オブジェクト の場合Restore: 自動化は、ブロックパブリックアクセス設定、バケット ACL 設定、オブジェクト ACL 設定、バケット所有者オブジェクトの所有権、バケットポリシーを格納前の初期設定に復元します。
- Amazon S3 Directory Bucket の場合Restore: 自動化は、格納前にバケットポリシーを初期設定に復元します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

プラットフォーム

/

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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
- s3express:CreateSession
- s3express:DeleteBucketPolicy
- s3express:GetBucketPolicy
- s3express:PutBucketPolicy
- ssm:DescribeAutomationExecutions

に必要なアクセス許可を付与する IAM ポリシーの例を次に示します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": "*"
        }
    ]
```

```
}
```

指示

次の手順に従って自動化を設定します。

1. ドキュメントの Systems Manager AWSSupport-ContainS3Resourceで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - BucketName (必須):
     - 説明: (必須) Amazon S3 バケットの名前。
     - 型: `AWS::S3::Bucket::Name`
   - アクション (必須):
     - 説明: (必須) Amazon S3 リソースを`Contain`分離`Restore`するか、リソース設定を以前のバックアップから元の状態に復元しようとします。
     - タイプ: 文字列
     - 使用できる値: `Contain|Restore`
   - DryRun (オプション):
     - 説明: (オプション) true に設定すると、オートメーションはターゲット Amazon S3 リソースを変更せず、変更しようとした内容を出力します。デフォルト値: true。
     - 型: ブール値
     - 使用できる値: `true|false`
   - BucketKeyName (オプション):
     - 説明: (オプション) 格納または復元する Amazon S3 オブジェクトのキー。オブジェクトレベルの格納中に使用されます。
     - タイプ: 文字列
     - 許可されたパターン: `^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$`
   - BucketRestrictAccess (条件付き):
     - 説明: (条件付き) 封じ込めアクションを実行した後にターゲット Amazon S3 リソースへのアクセスを許可する IAM ユーザーまたはロールの ARN。`Action` を `Contain` に設定した場合、このパラメータは必須です。
     - タイプ: StringList

- 許可されたパターン: ^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$

- TagIdentifier (オプション):
  - 説明: (オプション) 封じ込めワークフロー中にこのランブックによって作成または変更されたリソースに追加される Key=BatchId,Value=78925 形式のタグ。
  - タイプ: 文字列
  - 許可されたパターン: ^$|^[Kk][Ee][Yy]=[\\+\\-\\=\\._\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\._\\:\\/@a-zA-Z0-9]{0,128}$

- BackupS3BucketName (条件付き):
  - 説明: (条件付き) Actionが に設定されている場合にターゲットリソース設定をバックアップする Amazon S3 バケット、Containまたは Actionが に設定されている場合に から設定を復元する Amazon S3 バケットRestore。
  - 型: AWS::S3::Bucket::Name

- BackupS3KeyName (条件付き):
  - 説明: (条件付き) Actionが に設定されている場合Restore、オートメーションがターゲットリソース設定の復元を試みるために使用する Amazon S3 キーを指定します。
  - タイプ: 文字列
  - 許可されたパターン: ^[a-zA-Z0-9\\.\\-_\\\\!*'()/]{0,1024}$

- BackupS3BucketAccess (条件付き):
  - 説明: (条件付き) 封じ込めアクションを実行した後にバックアップ Amazon S3 バケットへのアクセスを許可する IAM ユーザーまたはロールの ARN。このパラメータは、 Actionが の場合に必要ですContain。
  - タイプ: StringList
  - 許可されたパターン: ^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z])?):iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,.@-]+$

- AutomationAssumeRole (オプション):
  - 説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする IAM ロールの Amazon リソースネーム (ARN)。
  - 型: AWS::IAM::Role::Arn

4. [実行] を選択します。

5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。

- validateRequiredInputs

  指定されたアクションに基づいて、必要な自動化入力パラメータを検証します。

- assertBucketExists

  ターゲット Amazon S3 バケットが存在し、アクセス可能かどうかを確認します。

- backupBucketPreChecks

  バックアップ Amazon S3 バケットがオブジェクトへのパブリック読み取りまたは書き込みアクセスを許可する可能性があるかどうかを確認します。

- backupTargetBucketMetadata

  ターゲット Amazon S3 バケットの現在の設定を記述し、指定されたバックアップ Amazon S3 バケットにバックアップをアップロードします。

- containBucket

  バケットレベルのオペレーションを実行して、ターゲット Amazon S3 バケットを含めます。

- BranchOnActionAndMode

  入力パラメータ Action と DryRun に基づいてオートメーションを分岐します。

- RestoreInstanceConfiguration

  バックアップから Amazon S3 バケット設定を復元します。

- containFinalOutput

  コンテナアクティビティを読み取り可能な形式で統合します。

- ReportContain

  封じ込めアクションのドライランの詳細を出力します。

- ReportRestore

  復元アクションのドライランの詳細を出力します。

- ReportRestoreFailure

  復元ワークフローの失敗シナリオ中に Amazon S3 バケットの元の設定を復元する手順について説明します。

- ReportContainmentFailure

  封じ込めワークフローの失敗シナリオ中に Amazon S3 バケットの元の設定を復元する手順について説明します。

- FinalOutput

  封じ込めアクションの詳細を出力します。

7. 実行が完了したら、出力セクションで実行の詳細な結果を確認します。

- ContainFinalOutput.Output

  が False にDryRun設定されている場合、このランブックによって実行される封じ込めアクションの詳細を出力します。

- RestoreFinalOutput.Output

  が False にDryRun設定されている場合、このランブックによって実行される復元アクションの詳細を出力します。

- ContainS3ResourceDryRun.Output

  が True にDryRun設定されている場合、このランブックによって実行される封じ込めアクションの詳細を出力します。

- RestoreS3ResourceDryRun.Output

  が True にDryRun設定されている場合、このランブックによって実行される復元アクションの詳細を出力します。

- ReportContainmentFailure.Output

  封じ込めワークフローの失敗シナリオ中に、ターゲット Amazon S3 リソースの元の設定を復元する手順について説明します。

- ReportRestoreFailure.Output

  復元ワークフローの失敗シナリオ中に、ターゲット Amazon S3 リソースの元の設定を復元する手順を示します。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)

- オートメーションを実行する
- オートメーションの設定
- 自動化ワークフローのサポート

Amazon SES

AWS Systems Manager Automation は、Amazon Simple Email Service 用の事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSSupport-AnalyzeSESMessageSendingStatus

AWSSupport-AnalyzeSESMessageSendingStatus

説明

AWSSupport-AnalyzeSESMessageSendingStatus 自動化ランブックは、未配信の E メールメッセージの E メール配信ステータスを要約し、未配信の理由を解決するためのアドバイスを提供します。ランブックは、Amazon SES によって公開された Amazon CloudWatch Logs グループに保存されている Amazon Simple Email Service (Amazon SES) の E メール送信イベントを取得します。Amazon SES イベント発行の詳細については、「Amazon Simple Email Service イベント発行を使用したモニタリング」を参照してください。ランブックには、E メール配信の概要とタイムライン、および未配信の E メールメッセージに影響を与える可能性のある推奨事項も記載されています。これらのメッセージは、各実行の出力セクションにあります。このランブックは、イベントストアのデプロイ後にのみイベントのトラブルシューティングを行うことができることに注意してください。

動作の仕組み

ランブックは次のステップを実行します。

- 同じ CloudWatch Logs グループの同時自動化実行をチェックします。

- オートメーションパラメータによって指定されたメッセージ IDs に対応する Amazon SES イベントを分析します。

- 配信の概要をオートメーション実行の出力セクションに出力します。

> **Important**
>
> - このランブックを実行する前に、 オートメーションパラメータで指定された CloudWatch Logs ロググループに公開された Amazon SES イベントを保存する必要があります。このランブックは、ロググループに保存されている Amazon SES イベントのみを分析します。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `logs:StartQuery`
- `logs:GetQueryResults`
- `ses:GetIdentityMailFromDomainAttributes`
- `ses:GetSendQuota`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

指示

次の手順に従って自動化を設定します。

1. Systems Manager AWSSupport-AnalyzeSESMessageSendingStatusの「 ドキュメント」でに移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - AutomationAssumeRole (オプション):

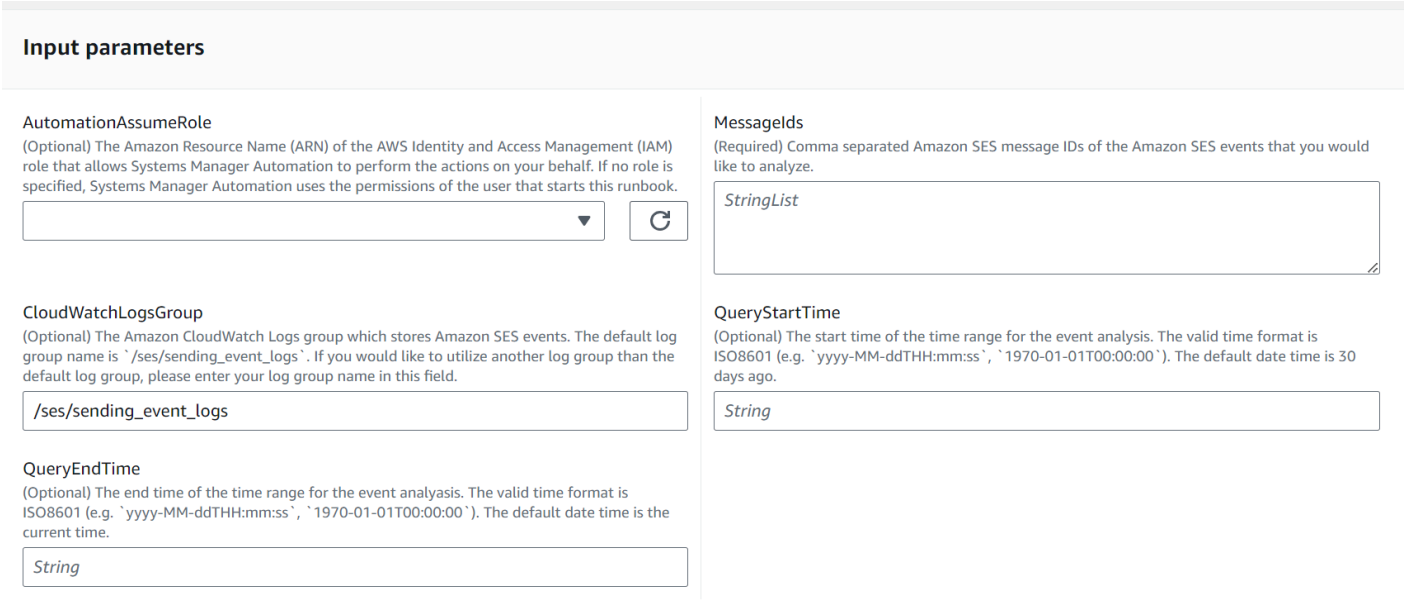
     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールが指定されていない場合、Systems Manager Automation は、このランブックを開始するユーザーのアクセス許可を使用します。
   - MessageIds (必須)

     分析する Amazon Simple Email Service イベントのカンマ区切り Amazon Simple Email Service メッセージ IDs。
   - CloudWatchLogsGroup (オプション)

     Amazon Simple Email Service イベントを保存する Amazon CloudWatch Logs グループ。デフォルトのロググループ名は `/ses/sending_event_logs` です。デフォルトのロググループとは異なるロググループを使用する場合は、このフィールドにロググループ名を入力してください。"
   - QueryStartTime (オプション)

     イベント分析の時間範囲の開始時刻。有効な時間形式は ISO8601 (例: `yyyy-MM-ddTHH:mm:ss`、1970-01-01T00:00:00`) です。デフォルトの日時は 30 日前です。
   - QueryEndTime (オプション)

     イベントアナルヤーシスの時間範囲の終了時刻。有効な時間形式は ISO8601 (例: `yyyy-MM-ddTHH:mm:ss`、1970-01-01T00:00:00`) です。デフォルトの日時は現在の時刻です。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - **CheckConcurrency:**

     Amazon CloudWatch Logs グループをターゲットとするこのランブックの実行が 1 つだけであることを確認します。ランブックが同じロググループをターゲットとする別の実行を検出すると、エラーが返され、終了します。
   - **AnalyzeSesEvents:**

     オートメーションパラメータで指定された Amazon CloudWatch Logs グループに保存されている Amazon Simple Email Service イベントを分析します。
   - **OutputFailureReason:**

     ステップが失敗したときに実行AnalyzeSESMessageSendingStatusステップの失敗メッセージを出力します。
7. 完了したら、出力セクションで実行の詳細な結果を確認します。
   - バウンスによる未配信 E メールメッセージの分析の出力

     バウンスが原因で送信先メールボックスに到達しなかった E メールメッセージの自動化実行の出力。

リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

SageMaker AI

AWS Systems Manager Automation は、Amazon SageMaker AI 用の事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-DisableSageMakerNotebookRootAccess

AWS-DisableSageMakerNotebookRootAccess

説明

AWS-DisableSageMakerNotebookRootAccess ランブックは、Amazon SageMaker AI ノートブックインスタンスのルートアクセスを無効にします。自動化中、ノートブックインスタンスは停止

して必要な変更を加えます。SageMaker AI Studio ノートブックインスタンスはサポートされていません。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- NotebookInstanceName

  タイプ: 文字列

  説明: (必須) ルートアクセスを無効にする SageMaker AI ノートブックインスタンスの名前。
- StartInstanceAfterUpdate

  型: ブール値

  デフォルト: true

  説明: (オプション) ルートアクセスを無効にした後にノートブックインスタンスを起動するかどうかを決定します。このパラメータのデフォルト設定は ですtrue。に設定するとtrue、ルートアクセスが無効になった後にインスタンスが開始されます。に設定するとfalse、ルートアクセスが無効になった後、インスタンスは stopped状態のままになります。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- sagemaker:DescribeNotebookInstance
- sagemaker:StartNotebookInstance
- sagemaker:StopNotebookInstance
- sagemaker:UpdateNotebookInstance

ドキュメントステップ

- CheckNotebookInstanceStatus (aws:executeAwsApi): ノートブックインスタンスの現在のステータスを確認します。
- StopOrUpdateNotebookInstance (aws:branch): ノートブックインスタンスのステータスに基づいて分岐します。
- StopNotebookInstance (aws:executeAwsApi): ステータスが の場合、インスタンスを起動しますstopped。
- WaitForInstanceToStop (aws:waitForAwsResourceProperty): インスタンスが であることを確認しますstopped。
- UpdateNotebookInstance (aws:executeAwsApi): ノートブックインスタンスのルートアクセスを無効にします。
- WaitForNotebookUpdate (aws:waitForAwsResourceProperty): ルートアクセスが無効になっており、インスタンスstoppedのステータスが であることを確認します。
- ChooseInstanceStart (aws:branch): インスタンスを起動するかどうかに基づいて分岐します。
- StartNotebookInstance (aws:executeAwsApi): ノートブックインスタンスを起動します。
- VerifyNotebookInstanceStatus (aws:waitForAwsResourceProperty): ルートアクセスを無効にするavailable前にインスタンスが であるかどうかを確認します。
- VerifyNotebookInstanceRootAccess (aws:assertAwsResourceProperty): ノートブックインスタンスのルートアクセス設定が正常に無効になっていることを確認します。

Secrets Manager

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Secrets Manager。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-DeleteSecret
- AWSConfigRemediation-RotateSecret

AWSConfigRemediation-DeleteSecret

説明

AWSConfigRemediation-DeleteSecret ランブックは、シークレットと保存されているすべてのバージョンを削除します AWS Secrets Manager。必要に応じて、シークレットを復元できる復旧期間を指定できます。RecoveryWindowInDays パラメータに値を指定しない場合、オペレーションはデフォルトで 30 日になります。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- RecoveryWindowInDays

  タイプ: 整数

  有効な値: 7 ~ 30

  デフォルト: 30

  説明: (オプション) シークレットを復元できる日数。
- SecretId

  タイプ: 文字列

  説明: (必須) 削除するシークレットの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- secretsmanager:DeleteSecret
- secretsmanager:DescribeSecret

ドキュメントステップ

- aws:executeAwsApi - SecretId パラメータで指定したシークレットを削除します。
- aws:executeScript - シークレットが削除するようにスケジュールされていることを確認します。

AWSConfigRemediation-RotateSecret

説明

AWSConfigRemediation-RotateSecret ランブックは、 に保存されているシークレットをローテーションします AWS Secrets Manager。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- RotationInterval

  タイプ: 間隔

  有効な値: 1 ~ 365

  説明: (必須) シークレットのローテーション間隔の日数です。

- RotationLambdaArn

  タイプ: 文字列

  説明: (必須) シークレットをローテーションさせることができる AWS Lambda 関数の Amazon リソースネーム (ARN)。

- SecretId

  タイプ: 文字列

  説明: (必須) ローテーションするシークレットの Amazon リソースネーム (ARN)。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- lambda:InvokeFunction
- secretsmanager:DescribeSecret
- secretsmanager:RotateSecret

ドキュメントステップ

- aws:executeAwsApi - SecretId パラメータで指定したシークレットをローテーションします。
- aws:executeScript - シークレットでローテーションが有効になっていることを確認します。

Security Hub

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Security Hub。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-EnableSecurityHub

AWSConfigRemediation-EnableSecurityHub

説明

AWSConfigRemediation-EnableSecurityHub ランブックは、オートメーションを実行する AWS アカウント と AWS リージョン の (Security Hub) を有効にします AWS Security Hub 。Security Hub の詳細については、AWS Security Hub 「 ユーザーガイド」の「What is AWS Security Hub？」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- EnableDefaultStandards

  型: ブール値

  デフォルト: true

  説明: (必須) この値を `true` に設定すると、Security Hub で指定された、デフォルトのセキュリティ標準が有効になります。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

ドキュメントステップ

- `aws:executeAwsApi` - 現在のアカウントとリージョンで Security Hub を有効にします。

- `aws:executeAwsApi` - Security Hub が有効になっていることを確認します。

AWS Shield

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS Shield。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSPremiumSupport-DDoSResiliencyAssessment

AWSPremiumSupport-DDoSResiliencyAssessment

説明

`AWSPremiumSupport-DDoSResiliencyAssessment`， AWS Systems Manager automation ランブックは、 AWS Shield Advanced の保護に従って DDoS の脆弱性とリソースの設定を確認するのに役立ちます AWS アカウント。Distributed Denial of Service (DDoS) 攻撃に脆弱なリソースの構成設定レポートを提供します。これは、 AWS Shield Advanced Protection の推奨ベストプラクティスに従って、設定の Amazon Route 53、Amazon Load Balancer、Amazon CloudFront ディストリビューション、 AWS Global Accelerator および AWS Elastic IPsのリソースを収集、分析、評価するために使用されます。最終的な設定レポートは、選択した Amazon S3 バケットで HTML ファイルとして利用できます。

動作の仕組み

このランブックには、パブリックアクセスが有効になっているさまざまなタイプのリソースと、AWS DDoS ベストプラクティスホワイトペーパーの推奨事項に従って保護が設定されているかどうかに関する一連のチェックが含まれています。ランブックは、次の内容を実行します。

- のサブスクリプション AWS Shield Advanced が有効になっているかどうかを確認します。
- 有効にすると、Shield Advanced で保護されているリソースがあるかどうかが確認されます。
- AWS アカウント 内のすべてのグローバルリソースとリージョン別リソースを検索し、それらが Shield で保護されているかどうかを確認します。
- 評価には Resource Type パラメータ、Amazon S3 バケット名、Amazon S3 バケット AWS アカウント ID (S3BucketOwner) が必要です。
- 結果は、指定された Amazon S3 バケットに保存された HTML レポートとして返されます。

入力パラメータ AssessmentType によって、すべてのリソースのチェックを実行するかどうかが決まります。デフォルトでは、このランブックはすべてのタイプのリソースをチェックします。GlobalResources または RegionalResources パラメータのみを選択した場合、ランブックは選択したリソースタイプのみをチェックします。

> **Important**
>
> - AWSPremiumSupport-* ランブックにアクセスするには、エンタープライズサポートまたはビジネスサポートサブスクリプションが必要です。詳細については、「サポート プランの比較」を参照してください。
> - このランブックには ACTIVE AWS Shield Advanced サブスクリプションが必要です。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- AssessmentType

  タイプ: 文字列

説明: (オプション) DDoS レジリエンス評価の対象となるリソースのタイプを決定します。デフォルトでは、このランブックはグローバルリソースとリージョン別リソースの両方を評価します。リージョン別リソースについては、ランブックにはアプリケーション (ALB) とネットワーク (NLB) のすべてのロードバランサーのほか、 AWS アカウント/リージョンのすべての Auto Scaling グループが記載されています。

有効な値: `['Global Resources', 'Regional Resources', 'Global and Regional Resources']`

デフォルト: グローバルリソースとリージョン別リソース

- S3BucketName

  型: `AWS::S3::Bucket::Name`

  説明: (必須) レポートがアップロードされる Amazon S3 バケット名。

  許可されたパターン: `^[0-9a-z][a-z0-9\-\.]{3,63}$`

- S3BucketOwnerAccount

  タイプ: 文字列

  説明: (オプション) Amazon S3 バケットを所有 AWS アカウント する 。Amazon S3 バケットが別のバケットに属している場合は、このパラメータを指定してください。属していない場合は AWS アカウント、このパラメータを空のままにしておくことができます。

  許可されたパターン: `^$|^[0-9]{12,13}$`

- S3BucketOwnerRoleArn

  型: `AWS::IAM::Role::Arn`

  説明: (オプション) バケットが異なる にある場合、Amazon S3 バケットを記述し、パブリックアクセス設定を AWS アカウント ブロックするアクセス許可を持つ IAM ロールの ARN AWS アカウント。このパラメータが指定されていない場合、ランブックは `AutomationAssumeRole` またはこのランブックを起動する IAM ユーザーを使用します (`AutomationAssumeRole`が指定されていない場合)。ランブックの説明の「必要な権限」セクションを参照してください。

  許可されたパターン: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- S3BucketPrefix

タイプ: 文字列

説明: (オプション) 結果を保存するための Amazon S3 内のパスのプレフィックス。

許可されたパターン: ^[a-zA-Z0-9][-./a-zA-Z0-9]{0,255}$|^$

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

自動化引き受けロールの IAM ポリシーの例

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

指示

1. AWS Systems Manager コンソールの AWSPremiumSupport-DDoSResiliencyAssessment に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 次の入力パラメータを入力できます。
   - AutomationAssumeRole (オプション):

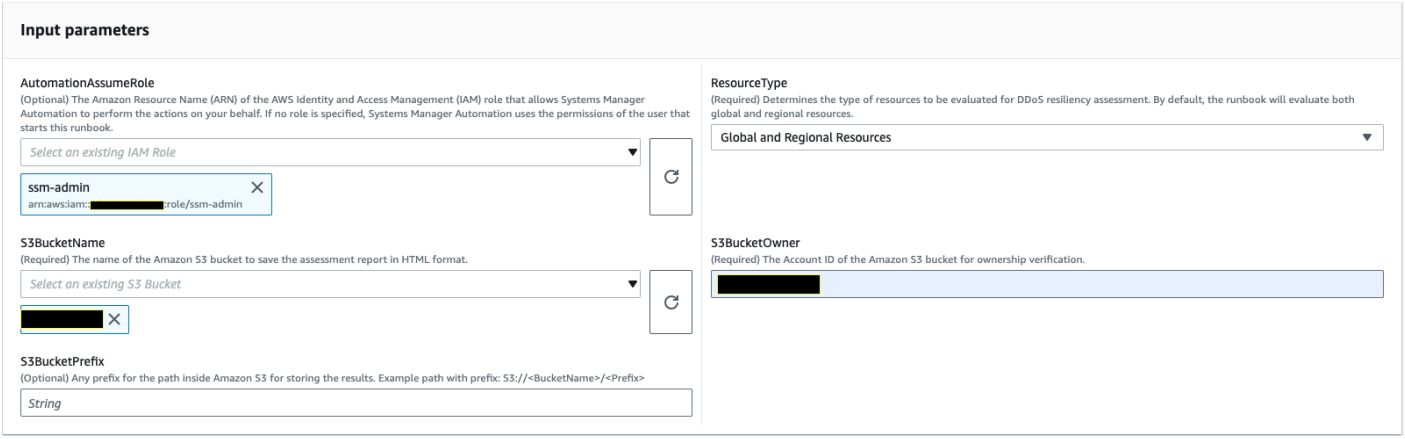
     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
   - 評価タイプ (オプション):

     DDoS レジリエンス評価の対象となるリソースのタイプを決定します。デフォルトでは、このランブックはグローバルリソースとリージョン別リソースの両方を評価します。
   - S3BucketName (必須):

     HTML 形式で評価レポートを保存する Amazon S3 バケットの名前。
   - S3BucketOwner (オプション):

     所有権検証用の Amazon S3 バケットの AWS アカウント ID。 AWS アカウント ID は、レポートがクロスアカウント Amazon S3 バケットに発行する必要がある場合に必須であり、Amazon S3 バケットがオートメーション開始 AWS アカウント と同じ にある場合はオプションです。
   - S3BucketPrefix (オプション):

     結果を保存するための Amazon S3 内のパスの任意のプレフィックス。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。

- CheckShieldAdvancedState:

  AWS アカウント が に AWS Shield Advanced サブスクライブされているかどうか、およびランブックが Amazon S3 バケットにアクセスできるかどうかを確認します。

- S3BucketSecurityChecks:

  「S3BucketName」で指定されている Amazon S3 バケットが匿名またはパブリックの読み取りまたは書き込みアクセス権限を許可しているかどうか、バケットで保存時の暗号化が有効になっているかどうか、「S3BucketOwner」で指定された AWS アカウント ID が Amazon S3 バケットの所有者であるかどうかを確認します。

- BranchOnShieldAdvancedStatus:

  分岐は、 AWS Shield Advanced サブスクリプションステータスや Amazon S3 バケット所有権ステータスに基づいてステップを文書化します。

- ShieldAdvancedConfigurationReview:

  Shield Advanced の設定を確認して、必要最小限の詳細が記載されていることを確認します。例: AWS Shield レスポンスチーム (SRT) チームの IAM アクセス、連絡先リストの詳細、SRT プロアクティブエンゲージメントステータス。

- ListShieldAdvancedProtections:

  Shield で保護されているリソースを一覧表示し、各サービスの保護リソースのグループを作成します。

- BranchOnResourceTypeAndCount:

  分岐は、リソースタイプパラメータの値と Shield で保護されているグローバルリソースの数に基づいてステップを文書化します。

- ReviewGlobalResources:

  Route 53 ホストゾーン、CloudFront ディストリビューション、グローバルアクセラレータなどの Shield Advanced で保護されたグローバルリソースについてレビューします。

- BranchOnResourceType:

リソースタイプの選択 (グローバル、リージョン別、または両方) に基づいてドキュメントステップを分岐します。

- ReviewRegionalResources:

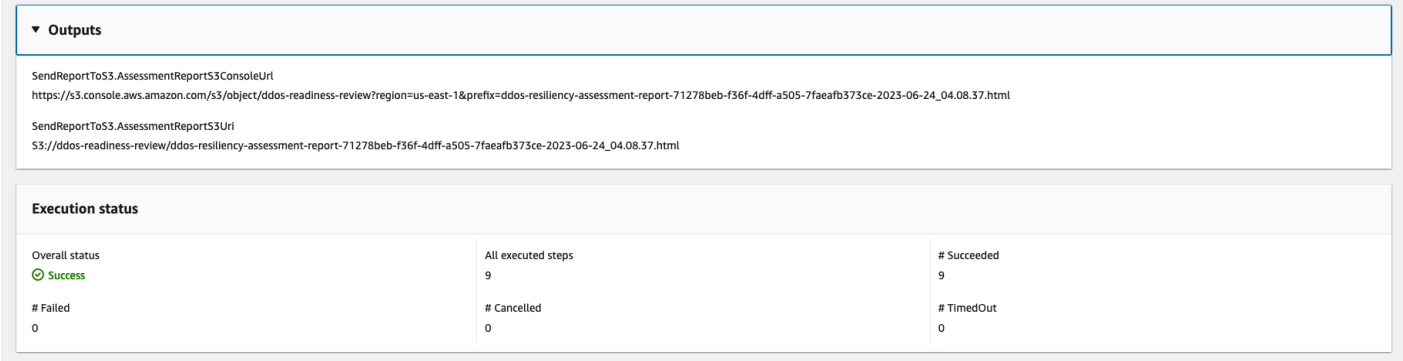
  Application Load Balancer、Network Load Balancer、Classic Load Balancer、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス (Elastic IP) などの Shield Advanced で保護されたリージョン別リソースをレビューします。

- SendReportToS3:

  Amazon S3 バケットに DDoS 評価レポートの詳細をアップロードします。

7. 完了すると、評価レポートの HTML ファイルの URI が Amazon S3 バケットに提供されます。

   ランブックが正常に実行された場合のレポートの S3 コンソールリンクと Amazon S3 URI



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスドキュメント

- AWS Shield Advanced

Amazon SNS

AWS Systems Manager Automation は、Amazon Simple Notification Service 用の事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-EnableSNSTopicDeliveryStatusLogging
- AWSConfigRemediation-EncryptSNSTopic
- AWS-PublishSNSNotification

AWS-EnableSNSTopicDeliveryStatusLogging

説明

AWS-EnableSNSTopicDeliveryStatusLogging ランブックは、、Amazon Data FirehoseHTTP、Lambda、、Platform applicationまたは Amazon Simple Queue Service (Amazon SQS) エンドポイントの配信ステータスのログ記録を設定します。これにより、Amazon SNS は失敗したアラートと成功したアラート通知のサンプルの割合を Amazon CloudWatch に記録することができます。トピックに配信ステータスのログ記録がすでに設定されている場合、ランブックは既存の設定を入力パラメータに指定した新しい値に置き換えます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- EndpointType

  タイプ: 文字列

  有効な値:

  - HTTP
  - Firehose
  - Lambda
  - アプリケーション
  - SQS

  説明: (必須) 配信ステータス通知メッセージをログに記録する Amazon SNS トピックエンドポイントのタイプ。

- TopicArn

  タイプ: 文字列

  説明: (必須) 配信ステータスのログ記録を設定する Amazon SNS トピックの ARN。

- SuccessFeedbackRoleArn

  タイプ: 文字列

  説明: (必須) Amazon SNS が CloudWatch への正常な通知メッセージのログの送信に使用する IAM ロールの ARN。 CloudWatch

- SuccessFeedbackSampleRate

  タイプ: 文字列

  有効な値: 0 ~ 100

  説明: (必須) 指定された Amazon SNS トピックのサンプリングに成功したメッセージの割合。

- FailureFeedbackRoleArn

  タイプ: 文字列

  説明: (必須) Amazon SNS が失敗通知メッセージのログを CloudWatch に送信するために使用する IAM ロールの ARN。 CloudWatch

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:PassRole
- sns:GetTopicAttributes
- sns:SetTopicAttributes

ドキュメントステップ

- aws:executeAwsApi - SuccessFeedbackRoleArnパラメータの値を Amazon SNS トピックに適用します。
- aws:executeAwsApi - SuccessFeedbackSampleRateパラメータの値を Amazon SNS トピックに適用します。
- aws:executeAwsApi - FailureFeedbackRoleArnパラメータの値を Amazon SNS トピックに適用します。
- aws:executeScript - Amazon SNS トピックで配信ステータスのログ記録が有効になっていることを確認します。

出力

VerifyDeliveryStatusLoggingEnabled.GetTopicAttributesResponse - GetTopicAttributes API オペレーションからのレスポンス。

VerifyDeliveryStatusLoggingEnabled.VerifyDeliveryStatusLoggingEnabled - 配信ステータスのログ記録の検証が成功したことを示すメッセージ。

AWSConfigRemediation-EncryptSNSTopic

説明

AWSConfigRemediation-EncryptSNSTopic ランブックは、 AWS Key Management Service () カスタマーマネージドキーを使用して指定した Amazon Simple Notification Service (Amazon SNS) トピックで暗号化を有効にします。AWS KMSこのランブックは、推奨される最小限セキュリティのベストプラクティスに従って Amazon SNS トピックが暗号化されるようにするための、ベースラインとしてのみ使用するようにします。複数のトピックは、それぞれ異なるカスタマーマネージドキーを使用して暗号化することをお勧めします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- KmsKeyArn

  タイプ: 文字列

  説明: (必須) Amazon SNS トピックの暗号化に使用する AWS KMS カスタマーマネージドキーの Amazon リソースネーム (ARN)。
- TopicArn

  タイプ: 文字列

説明: (必須) 暗号化する Amazon SNS トピックの ARN。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- sns:GetTopicAttributes
- sns:SetTopicAttributes

ドキュメントステップ

- aws:executeAwsApi - TopicArn パラメータで指定された Amazon SNS トピックを暗号化します。
- aws:assertAwsResourceProperty - Amazon SNS トピックで暗号化が有効になっていることを確認します。

AWS-PublishSNSNotification

説明

Amazon SNS に通知を発行します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- メッセージ

  タイプ: 文字列

  説明: (必須) SNS 通知に含めるメッセージ。
- TopicArn

  タイプ: 文字列

  説明: (必須) 通知の発行先の SNS トピックの ARN。

Amazon SQS

AWS Systems Manager Automation は、Amazon Simple Queue Service (Amazon SQS) 用の事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-EnableSQSEncryption

AWS-EnableSQSEncryption

説明

AWS-EnableSQSEncryption ランブックは、Amazon Simple Queue Service (Amazon SQS) キューの保管時の暗号化を有効にします。Amazon SQS キューは、Amazon SQS マネージドキー (SSE-SQS) または AWS Key Management Service （ AWS KMS) マネージドキー (SSE-KMS) で暗号

化できます。キューに割り当てるキーには、キューの使用が許可されているすべてのプリンシパルのアクセス許可を含むキーポリシーが必要です。暗号化を有効にするSendMessageと、匿名 および暗号化されたキューへのReceiveMessageリクエストは拒否されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- QueueUrl

  タイプ: 文字列

  説明: (必須) 暗号化を有効にする Amazon SQS キューの URL。
- KmsKeyId

  タイプ: 文字列

  説明: (オプション) 暗号化に使用する AWS KMS キー。この値は、グローバルに一意の識別子、エイリアスまたはキーへの ARN、または「alias/」というプレフィックスが付いたエイリアス名にすることができます。エイリアス aws/sqs を指定して、 AWS マネージドキーを使用することもできます。

- KmsDataKeyReusePeriodSeconds

  タイプ: 文字列

  有効な値: 60 ~ 86400

  デフォルト: 300

  説明: (オプション) Amazon SQS キューがデータキーを再利用して、 AWS KMS 再度 を呼び出す前にメッセージを暗号化または復号できる秒単位の時間。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- sqs:GetQueueAttributes
- sqs:SetQueueAttributes

ドキュメントステップ

- SelectKeyType (aws:branch): 指定されたキーに基づいて分岐します。
- PutAttributeSseKms (aws:executeAwsApi) - 暗号化に指定された AWS KMS キーを使用するように Amazon SQS キューを更新します。
- PutAttributeSseSqs (aws:executeAwsApi) - 暗号化にデフォルトキーを使用するように Amazon SQS キューを更新します。
- VerifySqsEncryptionKms (aws:assertAwsResourceProperty) - Amazon SQS キューで暗号化が有効になっていることを確認します。
- VerifySqsEncryptionDefault (aws:assertAwsResourceProperty) - Amazon SQS キューで暗号化が有効になっていることを確認します。

Step Functions

AWS Systems Manager Automation は、 AWS Step Functions (Step Functions) 用の事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-EnableStepFunctionsStateMachineLogging

AWS-EnableStepFunctionsStateMachineLogging

説明

AWS-EnableStepFunctionsStateMachineLogging ランブックは、指定した AWS Step Functions ステートマシンのログ記録を有効化または更新します。最小ログ記録レベルは、ALL、ERROR、または に設定する必要がありますFATAL。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- レベル

  タイプ: 文字列

  有効な値: ALL | ERROR | FATAL

  説明: (必須) 暗号化を有効にする Amazon SQS キューの URL。
- LogGroupArn

  タイプ: 文字列

  説明: (必須) ステートマシンログを送信する Amazon CloudWatch Logs ロググループの ARN。
- StateMachineArn

  タイプ: 文字列

  説明: (必須) ログ記録を有効にするステートマシンの ARN。
- IncludeExecutionData

  型: ブール値

  デフォルト: False

  説明: (オプション) 実行データをログに含めるかどうかを決定します。
- TracingConfiguration

  型: ブール値

  デフォルト: False

  説明: (オプション) AWS X-Ray トレースを有効にするかどうかを決定します。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- states:DescribeStateMachine

- `states:UpdateStateMachine`

ドキュメントステップ

- `EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)` - 指定されたステートマシンを、指定されたログ記録設定で更新します。
- `VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)` - 指定されたステートマシンでログ記録が有効になっていることを確認します。

出力

- EnableStepFunctionsStateMachineLogging.Response - UpdateStateMachine API コールからのレスポンス。

Systems Manager

AWS Systems Manager Automation は、Systems Manager 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- 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

説明

この AWS-BulkDeleteAssociation ランブックを使用すると、Systems Manager ステートマネージャーの関連付けを一度に 50 個まで削除できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- AssociationIds

  タイプ: StringList

  説明: (必須) 削除される関連付けの ID のカンマ区切りリスト。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:DeleteAssociation

ドキュメントステップ

- aws:executeScript - AssociationIds パラメータで指定した関連付けを削除します。

AWS-BulkEditOpsItems

説明

AWS-BulkEditOpsItems ランブックは、 AWS Systems Manager OpsItems のステータス、重要度、カテゴリ、または優先度を編集するのに役立ちます。この自動化では、一度に最大 50 個の OpsItems を編集できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム

(ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- カテゴリ

  タイプ: 文字列

  有効な値:

  - 可用性
  - コスト
  - 変更なし
  - パフォーマンス
  - 復旧
  - セキュリティ

  デフォルト: 変更なし

  説明: (オプション) 編集された OpsItems に指定する新しいカテゴリ。

- OpsItemIds

  タイプ: StringList

  説明: (必須) 編集する OpsItems ID をカンマで区切ったリスト (例: oi-XXXXXXXXXXXX、oi-XXXXXXXXXXXX)。

- 優先度

  タイプ: 文字列

  有効な値:

  - 変更なし
  - 1
  - 2
  - 3
  - 4
  - 5

  デフォルト: 変更なし

説明: (オプション) システム内の他の OpsItems と比較した編集済みの OpsItems の重大度。

- 緊急度

  タイプ: 文字列

  有効な値:

  - 変更なし
  - 1
  - 2
  - 3
  - 4

  デフォルト: 変更なし

  説明: (オプション) 編集された OpsItems の重大度。

- WaitTimeBetweenEditsInSecs

  タイプ: 文字列

  有効な値: 0.0 ~ 2.0

  デフォルト: 0.8

  説明: (オプション) `UpdateOpsItems` 操作を呼び出す間に自動化が待機する時間。

- ステータス

  タイプ: 文字列

  有効な値:

  - InProgress
  - 変更なし
  - を開きます。
  - Resolved (解決済み)

  デフォルト: 変更なし

  説明: (オプション) 編集された OpsItems の新しいステータス。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

ドキュメントステップ

- aws:executeScript - Category、Priority、SeverityおよびStatus パラメータに指定した値に基づいて、OpsItemIds パラメータで指定した OpsItems を編集します。

AWS-BulkResolveOpsItems

説明

AWS-BulkResolveOpsItems ランブックは、指定したフィルターに一致する AWS Systems Manager OpsItems を解決します。OpsInsightsId パラメータを使用して、解決済みの OpsItems に追加する OpsItemId を指定することもできます。S3BucketName パラメータの値を指定すると、結果の概要が Amazon Simple Storage Service (Amazon S3) バケットに送信されます。結果の概要が Amazon S3 バケットに送信された後に通知を受け取るには、SnsTopicArn パラメータの値を指定します。この自動化では、一度に最大 1,000 個の OpsItems を解決できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- フィルター

  タイプ: 文字列

  説明: (必須) 解決する OpsItems を返すフィルタのキーと値のペア。例えば、`[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]` です。OpsItems レスポンスのフィルタリングに使用できるオプションの詳細については、AWS Systems Manager API リファレンスの「OpsItemFilters」を参照してください。

- OpsInsightId

  タイプ: 文字列

  説明: (オプション) 解決された OpsItems に追加する関連リソース識別子。

- S3BucketName

  タイプ: 文字列

  説明: (オプション) 結果の概要を送信する Amazon S3 バケットの名前。

- SnsMessage

  タイプ: 文字列

  説明: (オプション) 自動化が完了したときに Amazon Simple Notification Service (Amazon SNS) に送信する通知。

- SnsTopicArn

  タイプ: 文字列

  説明: (オプション) 結果の概要が Amazon S3 に送信されたときに通知する Amazon SNS トピックの ARN。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- s3:GetBucketAcl
- s3:PutObject
- sns:Publish
- ssm:DescribeOpsItems
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

ドキュメントステップ

- aws:executeScript - 指定したフィルターに基づいて OpsItems を収集して解決します。OpsInsightId パラメータに値を指定した場合、その値は関連リソースとして追加されます。
- aws:executeScript - S3BucketName パラメータの値を指定すると、結果の概要が Amazon S3 バケットに送信されます。
- aws:executeScript - SnsTopicArn パラメータの値を指定した場合、結果の概要が Amazon S3 に送信された後に、指定されている場合は SnsMessage パラメータ値を含む通知が Amazon SNS トピックに送信されます。

AWS-ConfigureMaintenanceWindows

説明

AWS-ConfigureMaintenanceWindows ランブックを使用すると、複数の Systems Manager メンテナンスウィンドウを有効または無効にできます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- MaintenanceWindows

  タイプ: StringList

  説明: (必須) 有効または無効にするメンテナンスウィンドウの ID のカンマ区切りリスト。
- MaintenanceWindowsStatus

  タイプ: 文字列

  有効な値: "True" | "False"

  デフォルト: "False"

  説明: (必須) メンテナンスウィンドウを有効にするか無効にするかを決定します。「True」を指定してメンテナンスウィンドウを有効にし、「False」を指定してメンテナンスウィンドウを無効にします。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:GetMaintenanceWindow`

- ssm:UpdateMaintenanceWindow

ドキュメントステップ

- aws:executeScript - MaintenanceWindows パラメータで指定したメンテナンスウィンドウのステータスを収集し、メンテナンスウィンドウを有効または無効にします。

AWS-CreateManagedLinuxInstance

説明

Systems Manager に設定された Linux 用 EC2 インスタンスを作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

リナックス

パラメータ

- AmiId

  タイプ: 文字列

  説明: (必須) インスタンスの起動に使用する AMI ID。
- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- GroupName

  タイプ: 文字列

  デフォルト: SSMSecurityGroupForLinuxInstances

  説明: (必須) 作成するセキュリティグループの名前。

- HttpTokens

  タイプ: 文字列

  有効な値: オプション | 必須

  デフォルト: オプション

  説明: (オプション) IMDSv2 は、トークンバックセッションを使用します。HTTP トークンの使用を `optional` または `required` に設定して、IMDSv2がオプションか必須かを判断します。

- InstanceType

  タイプ: 文字列

  デフォルト: t2.medium

  説明: (必須) 起動するインスタンスのタイプ。デフォルトは t2.medium です。

- KeyPairName

  タイプ: 文字列

  説明: (必須) インスタンスの作成時に使用するキーのペア。

- RemoteAccessCidr

  タイプ: 文字列

  デフォルト: 0.0.0.0/0

  説明: (必須) CIDR で指定された IP (デフォルトは 0.0.0.0/0) に対して開いている SSH (ポート範囲は 22) のポートを持つセキュリティグループを作成します。セキュリティグループがすでに存在する場合は変更されず、ルールも変更されません。

- RoleName

  タイプ: 文字列

デフォルト: SSMManagedInstanceProfileRole

説明: (必須) 作成するロールの名前。

- StackName

  タイプ: 文字列

  デフォルト: CreateManagedInstanceStack{{automation:EXECUTION_ID}}

  説明: (オプション) このランブックで使用されるスタック名を指定します

- SubnetId

  タイプ: 文字列

  デフォルト: Default

  説明: (必須) 新しいインスタンスが指定されていない場合、新しいインスタンスはこのサブネットまたはデフォルトサブネットに展開されます。

- VpcId

  タイプ: 文字列

  デフォルト: Default

  説明: (必須) 新しいインスタンスは、この Amazon Virtual Private Cloud (Amazon VPC)、 または指定されていない場合はデフォルトの Amazon VPC にデプロイされます。

AWS-CreateManagedWindowsInstance

説明

Systems Manager に設定された Windows Server 用 EC2 インスタンスを作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Windows

パラメータ

パラメータ

- AmiId

  タイプ: 文字列

  デフォルト: {{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}

  説明: (必須) インスタンスの起動に使用する AMI ID。

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- GroupName

  タイプ: 文字列

  デフォルト: SSMSecurityGroupForLinuxInstances

  説明: (必須) 作成するセキュリティグループの名前。

- HttpTokens

  タイプ: 文字列

  有効な値: オプション | 必須

  デフォルト: オプション

説明: (オプション) IMDSv2 は、トークンバックセッションを使用します。HTTP トークンの使用を `optional` または `required` に設定して、IMDSv2がオプションか必須かを判断します。

- InstanceType

  タイプ: 文字列

  デフォルト: t2.medium

  説明: (必須) 起動するインスタンスのタイプ。デフォルトは t2.medium です。

- KeyPairName

  タイプ: 文字列

  説明: (必須) インスタンスの作成時に使用するキーのペア。

- RemoteAccessCidr

  タイプ: 文字列

  デフォルト: 0.0.0.0/0

  説明: (必須) CIDR で指定された IP (デフォルトは 0.0.0.0/0) に対して開いている RDP (ポート範囲が 3389) のポートを持つセキュリティグループを作成します。セキュリティグループがすでに存在する場合は変更されず、ルールも変更されません。

- RoleName

  タイプ: 文字列

  デフォルト: SSMManagedInstanceProfileRole

  説明: (必須) 作成するロールの名前。

- StackName

  タイプ: 文字列

  デフォルト: CreateManagedInstanceStack{{automation:EXECUTION_ID}}

  説明: (オプション) このランブックで使用されるスタック名を指定します

- SubnetId

  タイプ: 文字列

デフォルト: Default

説明: (必須) 新しいインスタンスが指定されていない場合、新しいインスタンスはこのサブネットまたはデフォルトサブネットに展開されます。

- VpcId

  タイプ: 文字列

  デフォルト: Default

  説明: (必須) 新しいインスタンスは、この Amazon Virtual Private Cloud (Amazon VPC)、 または指定されていない場合はデフォルトの Amazon VPC にデプロイされます。

AWSConfigRemediation-EnableCWLoggingForSessionManager

説明

AWSConfigRemediation-EnableCWLoggingForSessionManager ランブックにより、AWS Systems Manager Session Manager (Session Manager) セッションは出力ログを Amazon CloudWatch (CloudWatch) ロググループに保存できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- DestinationLogGroup

  タイプ: 文字列

  説明: (必須) CloudWatch ロググループの名前。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:UpdateDocument
- ssm:CreateDocument
- ssm:UpdateDefaultDocumentVersion
- ssm:DescribeDocument

ドキュメントステップ

- aws:executeScript - CloudWatch ロググループを受け入れ、Session Manager セッション出力ログの詳細設定を保存するドキュメントを更新するか、存在しない場合は作成します。

AWS-ExportOpsDataToS3

説明

このランブックは、 AWS Systems Manager Explorer で OpsData の概要のリストを取得し、指定された Amazon Simple Storage Service (Amazon S3) バケット内のオブジェクトにエクスポートします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- columnFields

  タイプ: StringList

  説明: (必須) 出力ファイルに書き込む列フィールド。
- フィルター

  タイプ: 文字列

  説明: (オプション) getOpsSummary リクエストのフィルターです。
- resultAttribute

  タイプ: 文字列

  説明: (オプション) getOpsSummary リクエストの結果属性です。
- s3BucketName

  タイプ: 文字列

  説明: (必須) 出力ファイルをダウンロードする S3 バケット。
- snsSuccessMessage

  タイプ: 文字列

説明: (オプション) ランブックの終了時に送信するメッセージ。

- snsTopicArn

  タイプ: 文字列

  説明: (必須) ダウンロードが完了したときに通知する Amazon Simple Notification Service (Amazon SNS) トピック ARN。

- syncName

  タイプ: 文字列

  説明: (オプション) リソースデータ同期の名前です。

ドキュメントステップ

getOpsSummaryStep – 最大 5,000 の ops サマリーを取得し、CSV ファイルにエクスポートします。

出力

OpsData オブジェクト – ランブックが正常に実行されると、ターゲット S3 バケット内で、エクスポートされた OpsData オブジェクトを確認できます。

AWS-ExportPatchReportToS3

説明

このランブックは、 AWS Systems Manager の Patch Manager のパッチ概要データとパッチの詳細リストを取得し、指定した Amazon Simple Storage Service (Amazon S3) バケットの .csv ファイルにエクスポートします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- assumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのドキュメントを実行するユーザーのアクセス許可を使用します。
- s3BucketName

  タイプ: 文字列

  説明: (必須) 出力ファイルをダウンロードする S3 バケット。
- snsTopicArn

  タイプ: 文字列

  説明: (オプション) ダウンロードが完了したときに通知する Amazon Simple Notification Service (Amazon SNS) トピック Amazon リソースネーム (ARN)。
- snsSuccessMessage

  タイプ: 文字列

  説明: (オプション) ランブックの終了時に送信するメッセージのテキスト。
- ターゲット

  タイプ: 文字列

  説明: (必須) 特定のインスタンスパッチデータをレポートするか、すべてのインスタンスのパッチデータをレポートするかを示すインスタンス ID またはワイルドカード文字 (*)。

ドキュメントステップ

ExportReportStep – このステップのアクションは、`targets` パラメータの値によって異なります。`targets` の形式が `instanceids=*` の場合、ステップはアカウント内のインスタンスについて最大 10,000 個のパッチ概要を取得し、データを .csv ファイルにエクスポートします。

targets の形式が instanceids=<instance-id> の場合、ステップはアカウント内の指定されたインスタンスのパッチ概要とすべてのパッチの両方を取得し、.csv ファイルにエクスポートします。

出力

PatchSummary/Patches オブジェクト – ランブックが正常に実行されると、エクスポートされたパッチレポートオブジェクトがターゲット S3 バケットにダウンロードされます。

AWS-SetupInventory

説明

1 つまたは複数のマネージドインスタンスに対して、Systems Manager Inventory の関連付けを作成します。システムは、関連づけのスケジュールに従ってメタデータを収集します。詳細については、「AWS Systems Manager インベントリ」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- アプリケーション

  タイプ: 文字列

  デフォルト: Enabled

  説明: (オプション) インストールされているアプリケーションに関するメタデータを収集します。
- AssociatedDocName

  タイプ: 文字列

デフォルト: AWS-GatherSoftwareInventory

説明: (オプション) マネージドインスタンスからインベントリを収集するために使用されるランブックの名前。

- AssociationName

  タイプ: 文字列

  説明: (オプション) インスタンスに割り当てられるインベントリの関連付けの名前。

- AssocWaitTime

  タイプ: 文字列

  デフォルト: PT5M

  説明: (オプション) インベントリの関連付けの開始時間になったときにインベントリ収集を一時停止する時間。時間は ISO 8601 形式を使用します。

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- AwsComponents

  タイプ: 文字列

  デフォルト: Enabled

  説明: (オプション) amazon-ssm-agent などの AWS コンポーネントのメタデータを収集します。

- CustomInventory

  タイプ: 文字列

  デフォルト: Enabled

  説明: (オプション) カスタムインベントリメタデータを収集します。

- ファイル

  タイプ: 文字列

  説明: (オプション) インスタンス上のファイルに関するメタデータを収集します。このタイプのインベントリデータを収集する方法の詳細については、「ファイルおよび Windows レジストリインベントリを使用する」を参照してください。SSMAgent バージョン 2.2.64.0 以降が必要です。Linux の例: `[{"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

  タイプ: 文字列

  デフォルト: Enabled

  説明: (オプション) CPU モデル、速度、コア数など、インスタンスに関する追加情報を収集します。

- InstanceIds

  タイプ: 文字列

  デフォルト: *

  説明: (必須) インベントリ対象の EC2 インスタンス。

- LambdaAssumeRole

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Lambda がユーザーに代わってアクションを実行できるようにするロールの ARN。指定されていない場合、Lambda 関数を実行するために一時的なロールが作成されます。

- NetworkConfig

  タイプ: 文字列

  デフォルト: Enabled

  説明: (オプション) ネットワーク設定に関するメタデータを収集します。

- OutputS3BucketName

  タイプ: 文字列

  説明: (オプション) Inventory ログデータを書き込む Amazon S3 バケットの名前。

- OutputS3KeyPrefix

  タイプ: 文字列

  説明: (オプション) Inventory ログデータを書き込む Amazon S3 キープレフィックス (サブフォルダ)。

- OutputS3Region

  タイプ: 文字列

  説明: (オプション) AWS リージョン Amazon S3 が存在する の名前。

- スケジュール

  タイプ: 文字列

  デフォルト: cron(0 */30 * * * ? *)

  説明: (オプション) インベントリ関連付けスケジュールの cron 式。デフォルト値は 30 分ごとです。

- サービス

  タイプ: 文字列

  デフォルト: Enabled

  説明: (オプション、Windows OS のみ、SSMAgent バージョン 2.2.64.0 以上が必要) サービス設定のデータを収集します。

- WindowsRegistry

  タイプ: 文字列

  説明: (オプション) Microsoft Windows レジストリキーに関するメタデータを収集します。このタイプのインベントリデータを収集する方法の詳細については、「ファイルおよび Windows レジストリインベントリを使用する」を参照してください。SSM エージェントバージョン 2.2.64.0 以降が必要です。例: [{"Path":"HKEY_CURRENT_CONFIG\System","Recursive":true},

{"Path":"HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\MachineImage", "ValueNames": ["AMIName"]}]

- WindowsRoles

  タイプ: 文字列

  デフォルト: Enabled

  説明: (オプション) インスタンス上の Windows ロールに関する情報を収集します。Windows オペレーティングシステムにのみ適用されます。SSMAgent バージョン 2.2.64.0 以降が必要です。

- WindowsUpdates

  タイプ: 文字列

  デフォルト: Enabled

  説明: (オプション) インスタンス上のすべての Windows Updates に関するデータを収集します。

AWS-SetupManagedInstance

説明

Systems Manager アクセス用の AWS Identity and Access Management (IAM) ロールを使用してインスタンスを設定します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) 設定する EC2 インスタンスの ID。

- LambdaAssumeRole

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Lambda がユーザーに代わってアクションを実行できるようにするロールの ARN。指定されていない場合、Lambda 関数を実行するために一時的なロールが作成されます。

- RoleName

  タイプ: 文字列

  デフォルト: SSMRoleForManagedInstance

  説明: (オプション) EC2 インスタンスの IAM ロールの名前。このロールが存在しない場合は、作成されます。この値を指定する場合は、ロールに [AmazonSSMManagedInstanceCore] 管理ポリシーが含まれていることを確認します。

AWS-SetupManagedRoleOnEC2Instance

説明

Systems Manager アクセスの SSMRoleForManagedInstance マネージド IAM ロールでインスタンスを設定します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

  タイプ: 文字列

  説明: (必須) 設定する EC2 インスタンスの ID。
- LambdaAssumeRole

  タイプ: 文字列

  説明: (オプション) 自動化によって作成された Lambda がユーザーに代わってアクションを実行できるようにするロールの ARN。指定されていない場合、Lambda 関数を実行するために一時的なロールが作成されます。
- RoleName

  タイプ: 文字列

  デフォルト: SSMRoleForManagedInstance

  説明: (オプション) EC2 インスタンスの IAM ロールの名前。このロールが存在しない場合は、作成されます。この値を指定する場合は、ロールに [AmazonSSMManagedInstanceCore] 管理ポリシーが含まれていることを確認します。

AWSSupport-TroubleshootManagedInstance

説明

AWSSupport-TroubleshootManagedInstance ランブックは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスが AWS Systems Managerによって管理対象として報告されない理由を判断するのに役立ちます。このランブックでは、セキュリティグループルール、VPC エンドポイント、ネットワークアクセスコントロールリスト (ACL) ルール、ルートテーブルなど、インスタンスの VPC 設定を確認します。また、必要なアクセス許可を含む AWS Identity and Access Management (IAM) インスタンスプロファイルがインスタンスにアタッチされていることを確認します。

> **Important**
>
> このオートメーションランブックは IPv6 ルールを評価しません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- InstanceId

タイプ: 文字列

説明: (必須) Systems Manager によって管理対象として報告されない Amazon EC2 インスタンスの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeScript- インスタンスの PingStatus を収集します。
- aws:branch - インスタンスが Systems Manager によって管理対象として既に報告されているかどうかに基づいて分岐させます。

- aws:executeAwsApi - VPC 設定を含むインスタンスの詳細を収集します。
- aws:executeScript - 該当する場合、Systems Manager で使用するためにデプロイされている VPC エンドポイントに関する追加情報を収集し、VPC エンドポイントにアタッチされているセキュリティグループが、インスタンスからの TCP ポート 443 でのインバウンドトラフィックを許可していることを確認します。
- aws:executeScript - ルートテーブルが VPC エンドポイントまたはパブリック Systems Manager エンドポイントへのトラフィックを許可しているかどうかを確認します。
- aws:executeScript - ネットワーク ACL ルールが VPC エンドポイントまたはパブリック Systems Manager エンドポイントへのトラフィックを許可しているかどうかを確認します。
- aws:executeScript - VPC エンドポイントまたはパブリック Systems Manager エンドポイントへのアウトバウンドトラフィックが、インスタンスに関連付けられたセキュリティグループによって許可されているかどうかを確認します。
- aws:executeScript - インスタンスにアタッチされたインスタンスプロファイルに、必要な権限を提供する管理ポリシーが含まれているかどうかを確認します。
- aws:branch - インスタンスのオペレーティングシステムに基づいて分岐させます。
- aws:executeScript - ssmagent-toolkit-linux シェルスクリプトへのリファレンスを提供します。
- aws:executeScript - ssmagent-toolkit-windows PowerShell スクリプトへのリファレンスを提供します。
- aws:executeScript - 自動化の最終出力を生成します。
- aws:executeScript - インスタンスの PingStatus が Online の場合、そのインスタンスはすでに Systems Manager によって管理されていることを返します。

AWSSupport-TroubleshootPatchManagerLinux

説明

AWSSupport-TroubleshootPatchManagerLinux ランブックは、 のツールである Patch Manager を使用して、Linux ベースのマネージドノードでパッチ障害を引き起こす可能性のある一般的な問題をトラブルシューティングします AWS Systems Manager。このランブックの主な目的は、パッチコマンドが失敗する根本原因を見きわめ、修復プランを提案することにあります。

動作の仕組み

AWSSupport-TroubleshootPatchManagerLinux ランブックは、トラブルシューティングのために提供された 2 つのインスタンス ID/コマンド ID を考慮します。コマンド ID が指定されていない

場合、指定されたインスタンスで過去 30 日以内に失敗した最新のパッチコマンドが選択されます。コマンドのステータス、前提条件のフルフィルメント、および OS ディストリビューションを確認した後、ランブックはログアナライザーパッケージをダウンロードして実行します。出力には、問題の根本原因と、問題を解決するために必要なアクションが含まれます。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

- Amazon Linux 2 および AL2023
- Red Hat Enterprise Linux 8.X および 9.X
- Centos 8.X および 9.X
- SUSE 15.X

パラメータ

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:SendCommand
- ssm:DescribeDocument
- ssm:GetCommandInvocation
- ssm:ListCommands
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ssm:GetDocument
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution

指示

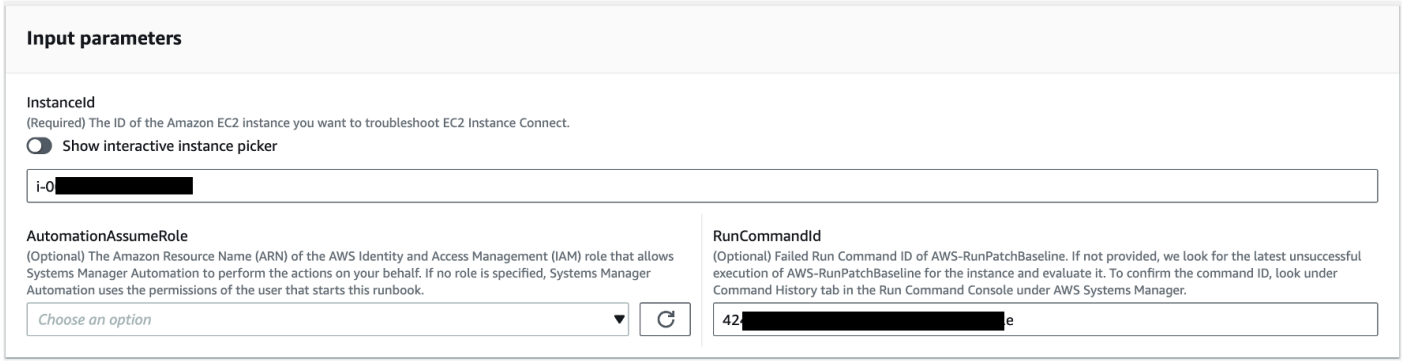
次の手順に従って自動化を設定します。

1. AWS Systems Manager コンソールAWSSupport-TroubleshootPatchManagerLinuxで に移動します。
2. [Execute automation] (オートメーションを実行) を選択します。
3. 入力パラメータには、次のように入力します。
   - InstanceId (必須):

     インタラクティブインスタンスピッカーを使用して、パッチコマンドが失敗した Linux ベースの SSM マネージドノード (Amazon Elastic Compute Cloud (Amazon EC2) または Hybrid Activated サーバー) の ID を選択するか、SSM マネージドインスタンスの ID を手動で入力します。
   - AutomationAssumeRole (オプション):

     オートメーションがユーザーに代わってアクションを実行できるようにする IAM ロールの ARN を入力します。ロールが指定されていない場合、オートメーションはこのランブックを開始するユーザーのアクセス許可を使用します。
   - RunCommandId (オプション):

     AWS-RunPatchBaseline ドキュメントの Failed Run Command ID を入力します。コマンド ID を指定しない場合、ランブックは選択したインスタンスで過去 30 日以内に失敗した最新のパッチコマンドを検索します。



4. [実行] を選択します。
5. 自動化が開始されます。
6. ドキュメントは以下のステップを実行します。
   - CheckConcurrency:

同じインスタンスをターゲットとするこのランブックの実行が 1 つだけであることを確認します。ランブックが同じインスタンスをターゲットとする別の実行を検出した場合、エラーが返され、終了します。

- ValidateCommandID:

  指定されたコマンド ID が入力パラメータとして SSM AWS-RunPatchBaseline ドキュメントに対して実行されたかどうかを検証します。コマンド ID が指定されていない場合、ランブックは選択したインスタンスでAWS-RunPatchBaseline過去 30 日以内に失敗した最新の の実行を考慮します。

- BranchOnCommandStatus:

  指定されたコマンドのステータスが失敗することを確認します。それ以外の場合、ランブックは実行を終了し、指定されたコマンドが正常に実行されたことを示すレポートを生成します。

- VerifyPrerequistes:

  上記の前提条件が満たされていることを確認します。

- GetPlatformDetails:

  オペレーティングシステム (OS) のディストリビューションとバージョンを取得します。

- GetDownloadURL:

  PatchManager Log Analyzer パッケージのダウンロード URL を取得します。

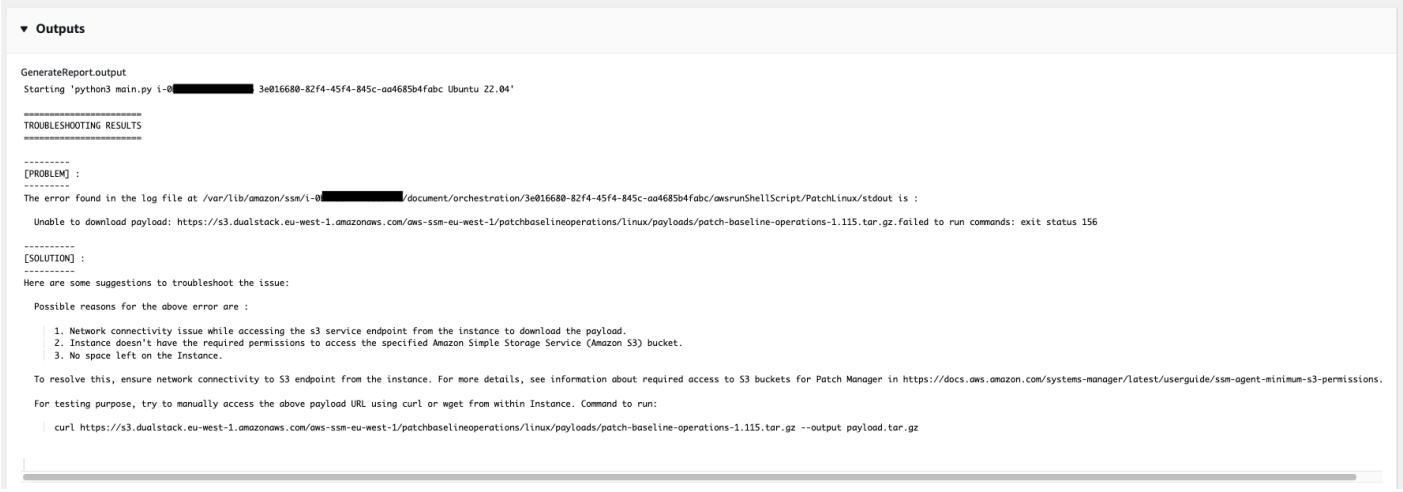
- EvaluatePatchManagerLogs:

  PatchManager Log Analyzer Python パッケージをインスタンスにダウンロードして実行し、ログファイルを評価します。

- GenerateReport:

  特定された問題と推奨される解決策を含むランブック実行の最終レポートを生成します。

7. 完了したら、出力セクションで実行の詳細な結果を確認します。



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWSSupport-TroubleshootSessionManager

説明

AWSSupport-TroubleshootSessionManager ランブックは、Session Manager を使用して管理対象の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに接続できない一般的な問題のトラブルシューティングに役立ちます。Session Manager は のツールです AWS Systems Manager。このランブックでは次の項目がチェックされます。

- インスタンスが実行中で、Systems Manager によって管理対象として報告されているかどうかを確認します。
- インスタンスが Systems Manager の管理対象として報告されない場合は、AWSSupport-TroubleshootManagedInstance ランブックを実行します。
- インスタンスにインストールされている SSM エージェントのバージョンを確認します。
- Session Manager の推奨 AWS Identity and Access Management (IAM) ポリシーを含むインスタンスプロファイルが Amazon EC2 インスタンスにアタッチされているかどうかを確認します。

- SSM エージェントログをインスタンスから収集します。
- Session Manager の設定を分析します。
- AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 ランブックを実行して、Session Manager、 AWS Key Management Service (AWS KMS)、Amazon Simple Storage Service (Amazon S3)、Amazon CloudWatch Logs (CloudWatch Logs) のエンドポイントへのインスタンスの接続を分析します。

考慮事項

- ハイブリッドマネージドノードはサポートされていません。
- このランブックは、推奨のマネージド IAM ポリシーがインスタンスプロファイルにアタッチされているかどうかのみをチェックします。インスタンスプロファイルに含まれる IAM や AWS KMS 権限は分析されません。

> **Important**
>
> AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 ランブックは VPC Reachability Analyzer を使用して、ソースとサービスエンドポイント間のネットワーク接続を分析します。ソースとターゲットの間で分析が実行されるたびに課金されます。詳細については、「Amazon VPC の料金」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- InstanceId

  タイプ: 文字列

  説明: (必須) Session Manager を使用して接続できない Amazon EC2 インスタンスの ID。

- SessionPreferenceDocument

  タイプ: 文字列

  デフォルト: SSM-SessionManagerRunShell

  説明: (オプション) セッション設定ドキュメントの名前。セッションの開始時にカスタムセッション設定ドキュメントを指定しない場合は、デフォルト値を使用してください。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

1. aws:waitForAwsResourceProperty: ターゲットインスタンスがステータスチェックに合格するまで最大 6 分間待機します。
2. aws:executeScript: セッション設定ドキュメントを解析します。
3. aws:executeAwsApi: インスタンスにアタッチされたインスタンスプロファイルの ARN を取得します。
4. aws:executeAwsApi: インスタンスが、Systems Manager によって管理対象として報告されているかどうかを確認します。
5. aws:branch: インスタンスが Systems Manager の管理どおりに実行され、レポートされているかどうかに基づいて分岐させます。

6. aws:executeScript: インスタンスにインストールされている SSM Agent が Session Manager をサポートしているかどうかを確認します。
7. aws:branch: インスタンスのプラットフォームに基づいて分岐させ、ssm-cli ログを収集します。
8. aws:runCommand: Linux または macOS インスタンスから ssm-cli の ログ出力を収集します。
9. aws:runCommand: Windows インスタンスの ssm-cli から ログ出力を収集します。
10. aws:executeScript:ssm-cli ログを解析します。
11. aws:executeScript: 推奨の IAM ポリシーがインスタンスプロファイルにアタッチされているかどうかをチェックします。
12. aws:branch: ssm-cli ログに基づいて ssmmessages エンドポイント接続を評価するかどうかを決定します。
13. aws:executeAutomation: インスタンスが ssmmessages エンドポイントに接続できるかどうかを評価します。
14. aws:branch: ssm-cli ログとセッション設定に基づいて Amazon S3 エンドポイント接続を評価するかどうかを決定します。
15. aws:executeAutomation: インスタンスが Amazon S3 エンドポイントに接続できるかどうかを評価します。
16. aws:branch: ssm-cliログとセッション設定に基づいて AWS KMS エンドポイントの接続を評価するかどうかを決定します。
17. aws:executeAutomation: インスタンスが AWS KMS エンドポイントに接続できるかどうかを評価します。
18. aws:branch: ssm-cli ログとセッション設定に基づいて CloudWatch Logs エンドポイント接続を評価するかどうかを決定します。
19. aws:executeAutomation: インスタンスが CloudWatch Logs エンドポイントに接続できるかどうかを評価します。
20. aws:executeAutomation: AWSSupport-TroubleshootManagedInstance ランブックを実行します。
21. aws:executeScript: 前のステップの出力をコンパイルし、レポートを出力します。

出力

- generateReport.EvalReport - ランブックが実行したチェックの結果をプレーンテキストで表示します。

Third-party

AWS Systems Manager Automation は、サードパーティーの製品やサービス用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-CreateJiraIssue
- AWS-CreateServiceNowIncident
- AWS-RunPacker

AWS-CreateJiraIssue

説明

Jira の問題を作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AssigneeName

  タイプ: 文字列

  説明: (オプション) 問題を割り当てる必要があるユーザーのユーザー名。
- DueDate

  タイプ: 文字列

説明: (オプション) 問題の期限、yyyy-mm-dd 形式。

- IssueDescription

  タイプ: 文字列

  説明: (必須) この問題に関する詳細な説明。

- IssueSummary

  タイプ: 文字列

  説明: (必須) この問題についての簡単な説明。

- IssueTypeName

  タイプ: 文字列

  説明: (必須) 作成する問題のタイプの名前 (タスク、サブタスク、バグなど)。

- JiraURL

  タイプ: 文字列

  説明: (必須) Jira インスタンスの url。

- JiraUsername

  タイプ: 文字列

  説明: (必須) 問題を作成したユーザーの名前。

- PriorityName

  タイプ: 文字列

  説明: (オプション) 問題の優先度の名前。

- ProjectKey

  タイプ: 文字列

  説明: (必須) 問題を作成する必要があるプロジェクトのキー。

- SSMParameterName

  タイプ: 文字列

説明: (必須) Jira ユーザーの API キーまたはパスワードを含む暗号化された SSM パラメータの名前。

ドキュメントステップ

aws:createStack - Lambda IAM ロールと関数を作成する CloudFormation スタックを作成します。

aws:invokeLambdaFunction - Jira 問題を作成する Lambda 関数を呼び出します

aws:deleteStack - CloudFormation スタックを削除します。

出力

IssueId: 新しく作成された Jira 問題 の ID

AWS-CreateServiceNowIncident

説明

ServiceNow インシデントテーブルにインシデントを作成します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- カテゴリ

  タイプ: 文字列

  説明: (オプション) インシデントのカテゴリです。

  有効な値: なし | 問い合わせ/ヘルプ | ソフトウェア | ハードウェア | ネットワーク | データベース

  デフォルト値: なし
- 説明

  タイプ: 文字列

  説明: (必須) インシデントの詳細な説明です。
- Impact

  タイプ: 文字列

  説明: (オプション) インシデントがビジネスに与える影響。

  有効な値: 高 | 中 | 低

  デフォルト値: 低
- ServiceNowInstanceUsername

  タイプ: 文字列

  説明: (必須) インシデントの作成に使用するユーザーの名前。
- ServiceNowInstancePassword

  タイプ: 文字列

  説明: (必須) ServiceNow ユーザーのパスワードを含む暗号化された SSM パラメータの名前。
- ServiceNowInstanceURL

  タイプ: 文字列

説明: （必須） ServiceNow インスタンスの URL

- ShortDescription

  タイプ: 文字列

  説明: （必須）インシデントの簡単な説明です。

- サブカテゴリ

  タイプ: 文字列

  説明: （オプション）インシデントのサブカテゴリです。

  有効な値: なし | ウイルス対策 | E メール | 内部アプリケーション | オペレーティングシステム | CPU | ディスク | ハードウェア | メモリ | モニター | マウス | DHCP | DNS | IP アドレス | VPN | ワイヤレス | DB2 | MS SQL Server | Oracle

  デフォルト値: なし

ドキュメントステップ

Push_incident – インシデント情報を ServiceNow にプッシュします。

出力

Push_incident.incidentID – 作成したインシデント ID です。

AWS-RunPacker

説明

このランブックは、マシンイメージの作成に使用される Packer テンプレートを検証、修正、またはビルドするために、HashiCorp Packer ツールを使用します。このランブックは、Packer v1.7.2 を使用します。

> **Note**
>
> vpc_id 値を指定する場合は、パブリックサブネット subnet_id の値も指定する必要があります。サブネットの IPv4 パブリックアドレス属性を変更しない限り、associate_public_ip_address も true に設定する必要があります。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- Force

  型: ブール値

  説明: 以前のビルドからのアーティファクトがビルドの実行を妨げた場合に、ビルダーを強制的に実行する Packer オプションです。

- モード

  タイプ: 文字列

  説明: テンプレートに対して検証するときに Packer を使用するモードまたはコマンドです。オプションには `Build`、`Validate`、および `Fix` があります。

- TemplateFileName

  タイプ: 文字列

  説明: S3 バケット内のテンプレートファイルの名前またはキー。

- TemplateS3BucketName

  タイプ: 文字列

  説明: Packer テンプレートを含む S3 バケットの名前です。

ドキュメントステップ

RunPackerProcessTemplate – Packer ツールを使用して、選択したモードをテンプレートに対して実行します。

出力

RunPackerProcessTemplate.output – Packer ツールからの stdout です。

RunPackerProcessTemplate.fixed_template_key –「修正」モードで実行されている場合にのみ使用する S3 バケットに保存されているテンプレートの名前です。

RunPackerProcessTemplate.s3_bucket –「修正」モードで実行されている場合にのみ使用する修正したテンプレートを含む S3 バケットの名前です。

Amazon VPC

AWS Systems Manager Automation は、Amazon Virtual Private Cloud 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- 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

説明

このランブックは、指定したセキュリティグループからすべてのイングレスルールとエグレスルールを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- SecurityGroupId

  タイプ: 文字列

  説明: (必須) 閉じるセキュリティグループの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

ドキュメントステップ

- `aws:executeScript` - `SecurityGroupId`パラメータで指定したセキュリティグループからすべての進入ルールと退出ルールを削除します。

AWSSupport-ConfigureDNSQueryLogging

説明

`AWSSupport-ConfigureDNSQueryLogging` ランブックは、仮想プライベートクラウド (VPC) または Amazon Route 53 ホストゾーンで発生する DNS クエリのロギングを設定します。Amazon

CloudWatch Logs、Amazon Simple Storage Service (Amazon S3)、または Amazon Data Firehose にクエリログを発行することを選択できます。クエリロギングとリゾルバークエリログの詳細については、「パブリック DNS クエリロギング」と「リゾルバークエリロギング」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- LogDestinationArn

  タイプ: 文字列

  説明: (オプション) クエリログを送信する CloudWatch Logs グループ、Amazon S3 バケット、または Firehose ストリームの ARN。Route 53 パブリック DNS クエリロギングは CloudWatch Logs グループのみをサポートしていることに注意してください。このパラメータに値を指定しない場合、自動化では `AWSSupport-ConfigureDNSQueryLogging-{automation:EXECUTION_ID}` という形式で CloudWatch Logs グループを作成し、クエリログを公開する IAM リソースポリシーを作成します。自動化によって作成された CloudWatch Logs グループの保持期間は 14 日間です。

- QueryLogType

タイプ: 文字列

説明: (オプション) 記録するクエリのタイプ。

有効な値: パブリック | リゾルバー/プライベート

デフォルト: パブリック

- ResourceId

  タイプ: 文字列

  説明: (必須) クエリを記録するリソースの ID。QueryLogType パラメータに Public を指定する場合、リソースは Route 53 プライベートホストゾーンの ID である必要があります。QueryLogType パラメータに Resolver/Private を指定する場合、リソースは VPC の ID である必要があります。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

ドキュメントステップ

- aws:executeScript - ResourceId パラメータに指定したリソースが存在することを確認し、リソースタイプが必須の QueryLogType オプションと一致するかどうかを確認します。
- aws:executeScript - LogDestinationArn パラメータに指定した値が必須の QueryLogType 値と一致することを確認します。
- aws:executeScript - Route 53 が CloudWatch Logs ロググループにログを発行するために必要な権限を確認し、必要な IAM リソースポリシーが存在しない場合はそれを作成します。

- aws:executeScript - 選択した宛先で DNS クエリのロギングを有効にします。

AWSSupport-ConfigureTrafficMirroring

説明

AWSSupport-ConfigureTrafficMirroring ランブックは、ロードバランサーと Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの間の接続の問題をトラブルシューティングできるようにトラフィックミラーリングを構成します。トラフィックミラーリングは、インスタンスにアタッチされているネットワークインターフェイスからインバウンドトラフィックとアウトバウンドトラフィックをコピーします。トラフィックミラーリングを設定するために、このランブックは必要なターゲット、フィルタ、およびセッションを作成します。デフォルトでは、ランブックは Amazon DNS を除くすべてのプロトコルのすべてのインバウンドトラフィックとアウトバウンドトラフィックのミラーリングを設定します。特定の送信元や送信先からのトラフィックをミラーリングする場合は、自動化が完了した後にインバウンドルールとアウトバウンドルールを変更できます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- SourceENI

  タイプ: 文字列

説明: (必須) トラフィックミラーリングを設定するエラスティックネットワークインターフェイス。

- Target

  タイプ: 文字列

  説明: (必須) ミラーリングされたトラフィックの宛先。ネットワークインターフェイス、Network Load Balancer、Gateway Load Balancer エンドポイントの ID を指定する必要があります。Network Load Balancer を指定する場合は、ポート 4789 に UDP リスナーが必要です。

- SessionNumber

  タイプ: 文字列

  有効な値: 1 ~ 32766

  説明: (必須) 使用するミラーセッションの数。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ec2:CreateTrafficMirrorTarget
- ec2:CreateTrafficMirrorFilter
- ec2:CreateTrafficMirrorFilterRule
- ec2:CreateTrafficMirrorSession
- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilter
- ec2:DeleteTrafficMirrorSession
- ec2:DeleteTrafficMirrorFilterRule
- iam:ListRoles
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution

ドキュメントステップ

- aws:executeScript - スクリプトを実行してターゲットを作成します。
- aws:executeAwsApi - フィルタールールを作成します。
- aws:executeAwsApi - すべてのインバウンドトラフィックのミラーフィルタールールを作成します。
- aws:executeAwsApi - すべてのアウトバウンドトラフィックのミラーフィルタールールを作成します。
- aws:executeAwsApi - トラフィックミラーセッションを作成します。
- aws:executeAwsApi - フィルターまたはセッションの作成に失敗した場合、フィルターを削除します。
- aws:executeAwsApi - フィルターまたはセッションの作成に失敗した場合、ターゲットを削除します。

出力

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget.TargetIDOutput

AWSSupport-ConnectivityTroubleshooter

説明

AWSSupport-ConnectivityTroubleshooter ランブックは、以下のリソース間の接続性の問題を診断します。

- AWS Amazon Virtual Private Cloud (Amazon VPC) 内の リソース
- AWS VPCsピアリングを使用して接続 AWS リージョン されている同じ 内の異なる Amazon VPC 内の リソース
- AWS インターネットゲートウェイを使用した Amazon VPC およびインターネットリソース内のリソース
- AWS ネットワークアドレス変換 (NAT) ゲートウェイを使用した Amazon VPC およびインターネットリソース内の リソース

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- DestinationIP

  タイプ: 文字列

  説明: (必須) 接続先のリソースの IPv4 アドレス。

- DestinationPort

  タイプ: 文字列

  デフォルト: true

  説明: (必須) 接続先リソース上で接続するポート番号。

- DestinationVpc

  タイプ: 文字列

  デフォルト: All

  説明: (オプション) テストする接続先の Amazon VPC の ID。

- SourceIP

  タイプ: 文字列

  説明: (必須) 接続をテストする Amazon VPC 内の AWS リソースのプライベート IPv4 アドレス。
- SourcePortRange

  タイプ: 文字列

  説明: (オプション) 接続をテストする Amazon VPC の AWS リソースで使用されるポート範囲。
- SourceVpc

  タイプ: 文字列

  デフォルト: All

  説明: (オプション) テストする接続元の Amazon VPC の ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcPeeringConnections

ドキュメントステップ

- aws:executeScript - SourceIPパラメータで指定した AWS リソースに関する詳細を収集します。
- aws:executeScript - 前のステップで収集したルートを使用して、 AWS リソースからのネットワークトラフィックの送信先を決定します。
- aws:branch - ネットワークトラフィックの宛先に基づいて分岐させます。

- aws:executeAwsApi - 宛先リソースの詳細を収集します。
- aws:executeScript - 宛先に対して返された ID が、DestinationVpc パラメータで指定された値 (存在する場合) Amazon VPC と一致することを確認します。
- aws:executeAwsApi - ソースリソースと宛先リソースのセキュリティグループルールを収集します。
- aws:executeScript - セキュリティグループルールでソースリソースと宛先リソース間の必要なトラフィックが許可されているかどうかを確認します。
- aws:executeAwsApi - 送信元および宛先リソースのサブネットに関連付けられたネットワークアクセス制御リスト (NACL) を収集します。
- aws:executeScript - NACL でソースリソースと宛先リソース間の必要なトラフィックが許可されているかどうかを確認します。
- aws:executeScript - ルートの宛先がインターネットゲートウェイの場合、リソースに関連付けられたパブリック IP アドレスがソースにあるかどうかを確認します。
- aws:executeAwsApi - ソースリソースのセキュリティグループルールを収集します。
- aws:executeScript - セキュリティグループルールでソースリソースから宛先リソースで必要なトラフィックが許可されているかどうかを確認します。
- aws:executeAwsApi - ソースリソースのサブネットに関連付けられた NACL を収集します。
- aws:executeScript - NACL でソースリソースから必要なトラフィックが許可されているかどうかを確認します。
- aws:executeAwsApi - NAT ゲートウェイの詳細を収集します。
- aws:executeAwsApi - NAT ゲートウェイのサブネットに関連付けられた NACL を収集します。
- aws:executeScript - NACL でNAT ゲートウェイのサブネットから必要なトラフィックが許可されているかどうかを確認します。
- aws:executeScript - NAT ゲートウェイのサブネットに関連付けられたルートを収集します。
- aws:executeScript - NAT ゲートウェイにインターネットゲートウェイへのルートがあるかどうかを確認します。
- aws:executeAwsApi - VPC ピアリング接続の詳細を収集します。
- aws:executeScript - 両方の VPC が同じリージョンにあり、宛先 VPC に対して返される ID が DestinationVpc パラメータで指定された値 (存在する場合) と一致することを確認します。
- aws:executeAwsApi - 宛先リソースのサブネットを返します。
- aws:executeScript - ピア接続された VPC のサブネットに関連付けられたルートを収集します。

- aws:executeScript - ピア接続された VPC にピア接続へのルートがあるかどうかを確認します。
- aws:executeScript - 宛先で自動化がサポートされていない場合、ソースリソースからのトラフィックが許可されているかどうかを確認します。

AWSSupport-TroubleshootVPN

説明

AWSSupport-TroubleshootVPN ランブックは、 AWS Site-to-Site VPN 接続のエラーをトレースして解決するのに役立ちます。自動化には、 AWS Site-to-Site VPN 接続トンネルに関連する IKEv1または IKEv2 エラーを追跡するように設計されたいくつかの自動チェックが含まれています。自動化は、一般的な問題のリストに含まれる特定のエラーとそれに対応する解決策を一致させようとします。

注: この自動化ではエラーは修正されません。指定された時間範囲で実行され、ロググループをスキャンして VPN CloudWatch ロググループにエラーがないか調べます。

動作の仕組み

ランブックはパラメータ検証を実行して、入力パラメータに含まれている Amazon CloudWatch ロググループが存在するかどうか、ロググループに VPN トンネルロギングに対応するログストリームがあるかどうか、VPN 接続 ID が存在するかどうか、トンネル IP アドレスが存在するかどうかを確認します。VPN ロギング用に設定された CloudWatch ロググループに対してログインサイト API コールを行います。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

タイプ: 文字列

説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- LogGroupName

  タイプ: 文字列

  説明: (必須) AWS Site-to-Site VPN 接続ログ用に設定された Amazon CloudWatch ロググループ名

  許可されたパターン: `^[\.\-_/#A-Za-z0-9]{1,512}`

- VpnConnectionId

  タイプ: 文字列

  説明: (必須) トラブルシューティングする AWS Site-to-Site VPN 接続 ID。

  許可されたパターン: `^vpn-[0-9a-f]{8,17}$`

- TunnelAIPAddress

  タイプ: 文字列

  説明: (必須) AWS Site-to-Site VPNに関連付けられているトンネル番号 1 の IPv4 アドレス。

  許可されたパターン: `^((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}$`

- TunnelBIPAddress

  タイプ: 文字列

  説明: (オプション) AWS Site-to-Site VPNに関連付けられているトンネル番号 2 の IPv4 アドレス。

  許可されたパターン: `^((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

  タイプ: 文字列

説明: (必須) 使用している IKE バージョンを選択します。許可された値: IKEv1、IKEv2

有効な値: `['IKEv1', 'IKEv2']`

- StartTimeinEpoch

  タイプ: 文字列

  説明: (オプション) ログ分析の開始時間。ログ分析には StartTimeinEpoch/EndTimeinEpoch または LookBackPeriod のどちらかを使用できます。

  許可されたパターン: `^\d{10}|^$`

- EndTimeinEpoch

  タイプ: 文字列

  説明: (オプション) ログ分析の終了時間。ログ分析には StartTimeinEpoch/EndTimeinEpoch または LookBackPeriod のどちらかを使用できます。StartTimeinEpoch/EndTimeinEpoch と LookBackPeriod の両方が与えられた場合、LookBackPeriod が優先されます。

  許可されたパターン: `^\d{10}|^$`

- LookBackPeriod

  タイプ: 文字列

  説明: (オプション) ログ分析のためにさかのぼる 2 桁の時間 (単位：時間)。有効な範囲: 01 ~ 99。StartTimeinEpoch と EndTime も与えられた場合、この値が優先されます。

  許可されたパターン: `^(\d?[1-9]|[1-9]0)|^$`

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`

- ec2:DescribeVpnConnections

指示

注: この自動化は、ロギングの出力形式が JSON の場合、VPN トンネルロギング用に設定された CloudWatch ロググループで機能します。

次の手順に従って自動化を設定します。

1. AWS Systems Manager コンソールで AWSSupport-TroubleshootVPN に移動します。
2. 次の入力パラメータを入力します。
   - AutomationAssumeRole (オプション):

     Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
   - LogGroupName (必須)

     検証先の Amazon CloudWatch ロググループ名。これは VPN がログの送信先となる CloudWatch ロググループである必要があります。
   - VpnConnectionId (必須):

     VPN エラーでロググループがトレースされる AWS Site-to-Site VPN 接続 ID。
   - TunnelAIPAddress (必須):

     トンネル AWS Site-to-Site VPN 接続に関連付けられた IP アドレス。
   - TunnelBIPAddress (オプション):

     AWS Site-to-Site VPN 接続に関連付けられているトンネル B の IP アドレス。
   - IKEVersion (必須):

     使用している IKEversion を選択します。許可された値: IKEv1、IKEv2。
   - StartTimeinEpoch (オプション):

     エラーを問い合わせる時間範囲の開始。範囲は包括的であるため、指定した開始時間がクエリに含まれます。1970 年 1 月 1 日 00:00:00 UTC からの秒数であるエポックタイムとして指定します。

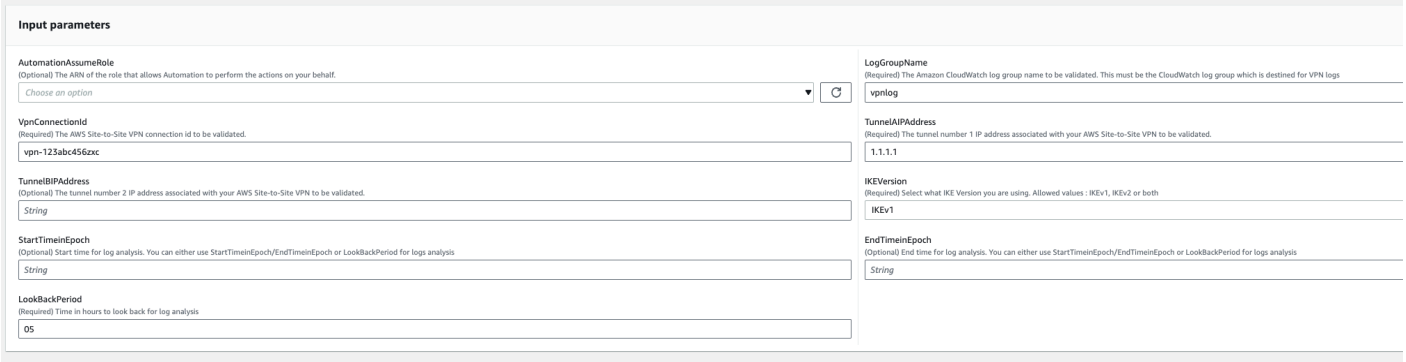
- EndTimeinEpoch (オプション):

  エラーを問い合わせる時間範囲の終了。範囲は包括的であるため、指定した終了時間がクエリに含まれます。1970 年 1 月 1 日 00:00:00 UTC からの秒数であるエポックタイムとして指定します。

- LookBackPeriod (必須):

  エラーを問い合わせる振り返りの時間 (単位：時間)。

注: ログ分析の時間範囲を固定するには、StartTimeinEpoch、EndTimeinEpoch、または LookBackPeriod を設定します。自動化開始時刻からの過去のエラーをチェックするための 2 桁の数字を時間単位で指定します。または、エラーが特定の時間範囲内の過去のものである場合は、LookBackPeriod の代わりに StartTimeinEpoch および EndTimeinEpoch を含めてください。



3. [実行] を選択します。
4. 自動化が開始されます。
5. 自動化ランブックは以下のステップを実行します。

- parameterValidation:

  自動化に含まれる入力パラメータに対して一連の検証を実行します。

- branchOnValidationOfLogGroup:

  パラメータで指定されたロググループが有効かどうかを確認します。無効な場合は、自動化ステップの以降の開始を停止します。

- branchOnValidationOfLogStream:

  含まれている CloudWatch ロググループにログストリームが存在するかどうかを確認します。無効な場合は、自動化ステップの以降の開始を停止します。

- branchOnValidationOfVpnConnectionId:

パラメータに含まれている VPN 接続 ID が有効かどうかを確認します。無効な場合は、自動化ステップの以降の開始を停止します。

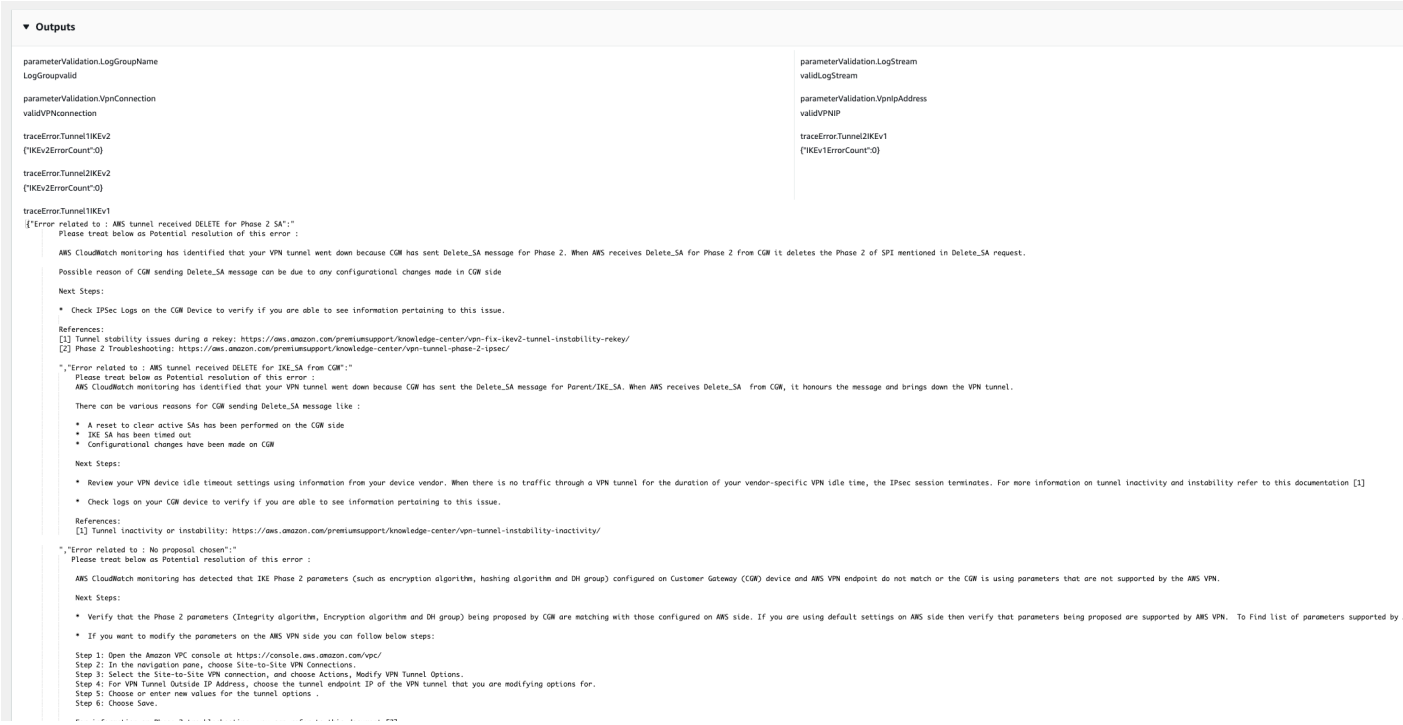
- branchOnValidationOfVpnIp:

  パラメータで指定されたトンネル IP アドレスが有効かどうかを確認します。無効な場合は、自動化ステップの以降の実行を停止します。

- traceError:

  含まれている CloudWatch ロググループでログインサイト API コールを行い、IKEv1/IKEv2 に関連するエラーと関連する推奨解決策を検索します。

6. 完了したら、出力セクションで詳細な実行結果を確認します。



リファレンス

Systems Manager Automation

- このオートメーションを実行する (コンソール)
- オートメーションを実行する
- オートメーションの設定
- 「自動化ワークフローをサポート」ランディングページ

AWS サービスドキュメント

- Site-to-Site VPN ログの内容

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

説明

AWSConfigRemediation-DeleteEgressOnlyInternetGateway ランブックは、指定された送出専用インターネットゲートウェイを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- EgressOnlyInternetGatewayId

  タイプ: 文字列

  説明: (必須) 削除される送出専用インターネットゲートウェイの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteEgressOnlyInternetGateway
- ec2:DescribeEgressOnlyInternetGateways

ドキュメントステップ

- aws:executeScript - EgressOnlyInternetGatewayId パラメータで指定された送出専用のインターネットゲートウェイを削除します。
- aws:executeScript - 送出専用インターネットゲートウェイが削除されたことを確認します。

AWSConfigRemediation-DeleteUnusedENI

説明

AWSConfigRemediation-DeleteUnusedENI ランブックは、アタッチに関するステータスが detached となっている Elastic Network Interface (ENI) を削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- NetworkInterfaceId

  タイプ: 文字列

  説明: (必須) 削除される ENI の ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces

ドキュメントステップ

- aws:executeAwsApi - NetworkInterfaceId パラメータで指定された ENI を削除します。
- aws:executeScript - ENI が削除されたことを確認します。

AWSConfigRemediation-DeleteUnusedSecurityGroup

説明

AWSConfigRemediation-DeleteUnusedSecurityGroup ランブックは、GroupId パラメーターで指定されたセキュリティグループを削除します。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに関連付けられている、または他のセキュリティグループから参照されているセキュリティグループを削除しようとすると、このオートメーションは失敗します。このオートメーションでは、デフォルトのセキュリティグループは削除されません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- GroupId

  タイプ: 文字列

  説明: (必須) 削除されるセキュリティグループの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

ドキュメントステップ

- `aws:executeAwsApi` - `GroupId` パラメータで指定された値を使用しながら、セキュリティグループ名を返します。
- `aws:branch` - グループ名が "デフォルト" でないことを確認します。

- aws:executeAwsApi - GroupId パラメータで指定されたセキュリティグループを削除します。
- aws:executeScript - セキュリティグループが削除されたことを確認します。

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

説明

AWSConfigRemediation-DeleteUnusedVPCNetworkACL ランブックは、サブネットに関連付けられていないネットワークアクセスコントロールリスト (ACL) を削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- NetworkAclId

  タイプ: 文字列

  説明: (必須) 削除されるネットワーク ACL の ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkAcl
- ec2:DescribeNetworkAcls

ドキュメントステップ

- aws:executeAwsApi - NetworkAclId パラメータで指定されたネットワーク ACL を削除します。
- aws:executeScript - NetworkAclId パラメータで指定されたネットワーク ACL が削除されたことを確認します。

AWSConfigRemediation-DeleteVPCFlowLog

説明

AWSConfigRemediation-DeleteVPCFlowLog ランブックは、指定する仮想プライベートクラウド (VPC) フローログを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- FlowLogId

  タイプ: 文字列

  説明: (必須) 削除されるフローログの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteFlowLogs
- ec2:DescribeFlowLogs

ドキュメントステップ

- aws:executeAwsApi - FlowLogId パラメータで指定されたフローログを削除します。
- aws:executeScript - フローログが削除されたことを確認します。

AWSConfigRemediation-DetachAndDeleteInternetGateway

説明

AWSConfigRemediation-DetachAndDeleteInternetGateway ランブックは、指定したインターネットゲートウェイをデタッチして削除します。仮想プライベートクラウド (VPC) の Amazon EC2 インスタンスに Elastic IP アドレスまたはパブリック IPv4 アドレスが関連付けられている場合、ランブックは失敗します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- InternetGatewayId

  タイプ: 文字列

  説明: (必須) 削除するインターネットゲートウェイの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

ドキュメントステップ

- `aws:waitForAwsResourceProperty` - 仮想プライベートゲートウェイの ID を受け入れ、仮想プライベートゲートウェイの状態プロパティが `available` に変わるかタイムアウトするまで待機します。
- `aws:executeAwsApi` - 指定された仮想プライベートゲートウェイ設定を取得します。

- aws:branch - VpcAttachments.state パラメータ値に基づいて分岐させます。

- aws:waitForAwsResourceProperty - 仮想プライベートゲートウェイの ID を受け入れ、仮想プライベートゲートウェイの VpcAttachments.state のプロパティが attached に変わるかタイムアウトするまで待機します。
- aws:executeAwsApi - 仮想プライベートゲートウェイの ID と Amazon VPC の ID を入力として受け入れ、Amazon VPC から仮想プライベートゲートウェイをデタッチします。
- aws:waitForAwsResourceProperty - 仮想プライベートゲートウェイの ID を受け入れ、仮想プライベートゲートウェイの VpcAttachments.state のプロパティが detached に変わるかタイムアウトするまで待機します。

- aws:executeAwsApi - 仮想プライベートゲートウェイの ID を入力として受け入れ、削除します。

- aws:waitForAwsResourceProperty - 仮想プライベートゲートウェイの ID を入力として受け入れ、削除を検証します。

  aws:executeAwsApi - インターネットゲートウェイ ID から VPC ID を収集します。
- aws:executeAwsApi - VPC からインターネットゲートウェイ ID をデタッチします。
- aws:executeAwsApi - インターネットゲートウェイを削除します。

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

説明

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway ランブックは、Amazon Virtual Private Cloud (Amazon VPC) で作成された仮想プライベートクラウド (VPC) にアタッチされた、特定の Amazon Elastic Compute Cloud (Amazon EC2) 仮想プライベートゲートウェイをデタッチおよび削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- VpnGatewayId

  タイプ: 文字列

  説明: (必須) 削除する仮想プライベートゲートウェイの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteVpnGateway`
- `ec2:DetachVpnGateway`
- `ec2:DescribeVpnGateways`

ドキュメントステップ

- `aws:waitForAwsResourceProperty` - 仮想プライベートゲートウェイの ID を受け入れ、仮想プライベートゲートウェイの状態プロパティが `available` に変わるかタイムアウトするまで待機します。
- `aws:executeAwsApi` - 指定された仮想プライベートゲートウェイ設定を取得します。

- aws:branch - VpcAttachments.state パラメータ値に基づいて分岐させます。

- aws:waitForAwsResourceProperty - 仮想プライベートゲートウェイの ID を受け入れ、仮想プライベートゲートウェイの VpcAttachments.state のプロパティが attached に変わるかタイムアウトするまで待機します。
- aws:executeAwsApi - 仮想プライベートゲートウェイの ID と Amazon VPC の ID を入力として受け入れ、Amazon VPC から仮想プライベートゲートウェイをデタッチします。
- aws:waitForAwsResourceProperty - 仮想プライベートゲートウェイの ID を受け入れ、仮想プライベートゲートウェイの VpcAttachments.state のプロパティが detached に変わるかタイムアウトするまで待機します。

- aws:executeAwsApi - 仮想プライベートゲートウェイの ID を入力として受け入れ、削除します。

- aws:waitForAwsResourceProperty - 仮想プライベートゲートウェイの ID を入力として受け入れ、削除を検証します。

AWS-DisableIncomingSSHOnPort22

説明

AWS-DisableIncomingSSHOnPort22 ランブックは、セキュリティグループの TCP ポート 22 で無制限の受信 SSH トラフィックを許可するルールを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- SecurityGroupIds

  タイプ: 文字列

  説明: (必須) SSH トラフィックを制限するセキュリティグループの IDs のカンマ区切りリスト。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ec2:DescribeSecurityGroups
- ec2:RevokeSecurityGroupIngress

ドキュメントステップ

- aws:executeAwsApi - TCP ポート 22 で受信 SSH トラフィックを許可するすべてのルールを、SecurityGroupIdsパラメータで指定したセキュリティグループから削除します。

出力

DisableIncomingSSHTemplate.RestrictedSecurityGroupIds - インバウンド SSH ルールが削除されたセキュリティグループの IDs のリスト。

AWS-DisablePublicAccessForSecurityGroup

説明

このランブックは、すべての IP アドレスに対して開かれている、デフォルトの SSH および RDP ポートを無効にします。

Important

このランブックは、以下に挙げる条件の両方を満たすセキュリティグループに対しては、"InvalidPermission.notFound" エラーで失敗します。1) セキュリティグループが非デフォルトの VPC に存在する、2) そのセキュリティグループのインバウンドルールで指定されている開かれたポートで、次の 4 つのパターンのいずれかが欠けている。

- `0.0.0.0/0`
- `::/0`
- `SSH or RDP port + 0.0.0.0/0`
- `SSH or RDP port + ::/0`

Note

このランブックは、中国国内 AWS リージョン にある では使用できません。

[このオートメーションを実行する (コンソール)]

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム

(ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- GroupId

  タイプ: 文字列

  説明: (必須) ポートを無効にする必要があるセキュリティグループの ID。

- IpAddressToBlock

  タイプ: 文字列

  説明: (オプション) アクセスをブロックする必要がある追加の IPv4 アドレス、形式は `1.2.3.4/32`。

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

説明

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP ランブックは、指定されたサブネットの IPv4 パブリックアドレッシング属性を無効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- SubnetId

  タイプ: 文字列

  説明: (必須) パブリック IPv4 アドレスの自動割り当て属性を無効にするサブネットの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

ドキュメントステップ

- `aws:executeAwsApi` - SubnetId パラメータで指定されたサブネットの自動割り当てパブリック IPv4 アドレス属性を無効にします。
- `aws:assertAwsResourceProperty` - 属性が無効になっていることを確認します。

AWSSupport-EnableVPCFlowLogs

説明

`AWSSupport-EnableVPCFlowLogs` ランブックは、 AWS アカウント内のサブネット、ネットワークインターフェイス、および VPC の Amazon Virtual Private Cloud (Amazon VPC) フローログを作成します。サブネットまたは VPC のフローログを作成する場合、そのサブネットまたは Amazon VPC 内の各エラスティックネットワークインターフェイスが監視されます。フローログデータは、Amazon CloudWatch Logs ロググループまたは指定した Amazon Simple Storage Service (Amazon S3) バケットに公開されます。詳細については、Amazon VPC ユーザーガイドのVPC フローログを参照してください。

> **Important**
>
> フローログを CloudWatch Logs または Amazon S3 に発行すると、提供されたログに対するデータの取り込み料金とアーカイブ料金が適用されます。詳細については、「フローログの料金」を参照してください。

このオートメーションを実行する (コンソール)

> **Note**
>
> ログの送信先s3として を選択するときは、バケットポリシーでログ配信サービスがバケットにアクセスできることを確認してください。詳細については、「フローログの Amazon S3 バケットのアクセス許可」を参照してください。

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- DeliverLogsPermissionArn

  タイプ: 文字列

説明: (オプション) Amazon Elastic Compute Cloud (Amazon EC2) がアカウントの CloudWatch Logs ロググループにフローログを発行することを許可する IAM ロールの ARN。LogDestinationType パラメータに s3 を指定する場合は、このパラメータの値を指定しないでください。詳細については、「Amazon VPC User Guide」の「フローログを CloudWatch Logs に発行する」を参照してください。

- LogDestinationARN

  タイプ: 文字列

  説明: (オプション) フローログデータが発行されたリソースの ARN。LogDestinationType パラメータに cloud-watch-logs が指定されている場合は、フローログデータの公開先となる CloudWatch Logs ロググループの ARN を指定します。または、代わりに LogGroupName を使用します。LogDestinationType パラメータに s3 を指定する場合は、このパラメータに、フローログデータの公開先となる Amazon S3 バケットの ARN を指定する必要があります。バケットにフォルダを指定することもできます。

  > **Important**
  >
  > s3 として を選択するLogDestinationTypeときは、選択したバケットが Amazon S3 バケットのセキュリティのベストプラクティスに従っていること、および組織と地域のデータプライバシー法に従っていることを確認する必要があります。

- LogDestinationType

  タイプ: 文字列

  有効な値: cloud-watch-logs | s3

  説明: (必須) フローログデータを公開する場所を決定します。LogDestinationType を s3 として指定した場合は、DeliverLogsPermissionArn または LogGroupName を指定しないでください。

- LogFormat

  タイプ: 文字列

  説明: フローログに含めるフィールド、およびレコードに表示される順番。使用可能なフィールドのリストについては、Amazon VPC ユーザーガイドの「フローログレコード」を参照してくださ

い。このパラメータに値を指定しない場合、フローログはデフォルトの形式で作成されます。このパラメータを指定する場合は、少なくとも 1 つのフィールドを指定する必要があります。

- LogGroupName

  タイプ: 文字列

  説明: (オプション) フローログデータの公開先となる CloudWatch Logs ロググループの名前。LogDestinationType パラメータに s3 を指定する場合は、このパラメータの値を指定しないでください。

- ResourceIds

  タイプ: StringList

  説明: (必須) フローログを作成するサブネット、エラスティックネットワークインターフェイス、または VPC の ID のカンマ区切りリスト。

- TrafficType

  タイプ: 文字列

  有効な値 :ACCEPT | REJECT | ALL

  説明: (必須) 記録するトラフィックのタイプ。リソースが受け入れたトラフィックまたは拒否したトラフィック、またはすべてのトラフィックを記録できます。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- 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

サンプルポリシー

```
       {
           "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}/*"
                    ]
                }
            ]
        }
```

ドキュメントステップ

- aws:branch - LogDestinationType パラメータで指定した値に基づいて分岐させます。
- aws:executeScript - ターゲット Amazon Simple Storage Service (Amazon S3) がオブジェクトへの読み取りまたは書き込みpublicアクセスを許可する可能性があるかどうかを確認します。
- aws:executeScript - LogDestinationARN パラメータに値が指定されておらず、LogDestinationType パラメータに cloud-watch-logs が指定されている場合は、ロググループを作成します。

- aws:executeScript - ランブックパラメータで指定された値に基づくフローログを作成します。

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

説明

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch ランブックは、Amazon Simple Storage Service (Amazon S3) にフローログデータを公開する既存の Amazon VPC フローログを、指定した Amazon CloudWatch Logs (CloudWatch Logs) ロググループにフローログデータを公開するフローログに置き換えます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DestinationLogGroup

  タイプ: 文字列

  説明: (必須) フローログデータの公開先となる CloudWatch Logs ロググループの名前。
- DeliverLogsPermissionArn

  タイプ: 文字列

説明: (必須) フローログデータを CloudWatch Logs に発行するために必要なアクセス許可を Amazon Elastic Compute Cloud (Amazon EC2) に提供する、使用する AWS Identity and Access Management (IAM) ロールの ARN。

- FlowLogId

  タイプ: 文字列

  説明: (必須) 置き換える Amazon S3 に公開するフローログの ID。

- MaxAggregationInterval

  タイプ: 整数

  有効な値: 60 | 600

  説明: (オプション) パケットのフローがキャプチャされ、フローログレコードに集約される最大時間間隔 (秒単位)。

- TrafficType

  タイプ: 文字列

  有効な値 :ACCEPT | REJECT | ALL

  説明: (必須) 記録および公開するフローログデータのタイプ。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

ドキュメントステップ

- aws:executeAwsApi - FlowLogId パラメータで指定した値から VPC の詳細を収集します。
- aws:executeAwsApi - ランブックパラメータに指定した値に基づいて、フローログを作成します。
- aws:assertAwsResourceProperty - 新しく作成されたフローログが CloudWatch Logs に公開されたことを確認します。
- aws:executeAwsApi - Amazon S3 に公開されたフローログを削除します。
- aws:executeScript - Amazon S3 に公開されたフローログが削除されたことを確認します。

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

説明

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket ランブックは、フローログデータを Amazon CloudWatch Logs (CloudWatch Logs) に公開する既存の Amazon VPC フローログを、指定した Amazon Simple Storage Service (Amazon S3) バケットにフローログデータを公開するフローログに置き換えます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DestinationS3BucketArn

タイプ: 文字列

説明: (必須) フローログデータの公開先となる Amazon S3 バケットの ARN。

- FlowLogId

  タイプ: 文字列

  説明: (必須) 置き換える CloudWatch Logs に公開するフローログの ID。

- MaxAggregationInterval

  タイプ: 整数

  有効な値: 60 | 600

  説明: (オプション) パケットのフローがキャプチャされ、フローログレコードに集約される最大時間間隔 (秒単位)。

- TrafficType

  タイプ: 文字列

  有効な値 :ACCEPT | REJECT | ALL

  説明: (必須) 記録および公開するフローログデータのタイプ。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

ドキュメントステップ

- `aws:executeAwsApi` - `FlowLogId` パラメータで指定した値から VPC の詳細を収集します。

- aws:executeAwsApi - ランブックパラメータに指定した値に基づいて、フローログを作成します。
- aws:assertAwsResourceProperty - 新しく作成されたフローログが Amazon S3 に公開されたことを確認します。
- aws:executeAwsApi - CloudWatch Logs に公開されたフローログを削除します。
- aws:executeScript - CloudWatch Logs に公開されたフローログが削除されたことを確認します。

AWS-ReleaseElasticIP

説明

割り当て ID を使用して、指定された Elastic IP アドレスをリリースします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- AllocationId

  タイプ: 文字列

説明: (必須) Elastic IP アドレスの割り当て ID。

AWS-RemoveNetworkACLUnrestrictedSSHRDP

説明

AWS-RemoveNetworkACLUnrestrictedSSHRDP ランブックは、すべてのソースアドレスからデフォルトの SSH および RDP ポートへの進入トラフィックを許可する、指定されたネットワーク ACL からすべてのネットワークアクセスコントロールリスト (ACL) ルールを削除します。デフォルトの SSH および RDP ポートと重複するポート範囲を含むルールは削除されません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- NetworkAclId

  タイプ: 文字列

  説明: (必須) すべての送信元アドレスからデフォルトの SSH および RDP ポートへの進入トラフィックを許可する無制限のルールを削除するネットワーク ACL の ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkAclEntry
- ec2:DescribeNetworkAcls

ドキュメントステップ

- aws:executeScript - SecurityGroupId パラメータで指定したセキュリティグループから、すべての送信元アドレスからのトラフィックを許可するすべての進入ルールを削除します。

出力

RemoveNaclEntriesAndVerify.VerificationMessage - 正常に削除されたネットワーク ACL ルールの検証メッセージ。

RemoveNaclEntriesAndVerify.RulesDeletedAndApiResponses - 削除されたネットワーク ACL ルールと DeleteNetworkAclEntry API オペレーションレスポンス。

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules

説明

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules ランブックは、すべての送信元アドレスからのトラフィックを許可する、指定したセキュリティグループからすべての進入ルールを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- SecurityGroupId

  タイプ: 文字列

  説明: (必須) すべての送信元アドレスからのトラフィックを許可する進入ルールを削除するセキュリティグループの ID。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

ドキュメントステップ

- `aws:executeScript` - SecurityGroupId パラメータで指定したセキュリティグループから、すべての送信元アドレスからのトラフィックを許可するすべての進入ルールを削除します。

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

説明

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules ランブックは、ユーザーにより指定された仮想プライベートクラウド (VPC) のデフォルトセキュリティグループから、すべてのルールを削除します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- GroupId

  タイプ: 文字列

  説明: (必須) すべてのルールが削除されるセキュリティグループの ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DescribeSecurityGroups

- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress

ドキュメントステップ

- aws:assertAwsResourceProperty - GroupId パラメータで指定されたセキュリティグループの名前が、default となっていることを確認します。
- aws:executeScript - GroupId パラメータで指定されたセキュリティグループから、すべてのルールを削除します。

AWSSupport-SetupIPMonitoringFromVPC

説明

AWSSupport-SetupIPMonitoringFromVPC は指定されたサブネットに Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを作成し、ping、MTR、traceroute および tracetcp テストを継続的に実行することによって、選択したターゲット IP (IPv4 または IPv6) を監視します。結果は Amazon CloudWatch Logs に保存され、メトリクスフィルターが適用され、CloudWatch ダッシュボードでレイテンシーとパケット損失の統計情報をすばやく視覚化できます。

追加情報

CloudWatch Logs データは、ネットワークのトラブルシューティングやパターン/傾向の分析に使用できます。さらに、パケット損失やレイテンシーがしきい値に達したときに、Amazon SNS 通知で CloudWatch アラームを設定できます。また、データを でケースを開くときに使用して AWS サポート、問題をすばやく分離し、ネットワークの問題を調査するときに解決までの時間を短縮することもできます。

> **Note**
>
> AWSSupport-SetupIPMonitoringFromVPC によって作成されたリソースをクリーンアップするには、ランブック AWSSupport-TerminateIPMonitoringFromVPC を使用できます。詳細については、「AWSSupport-TerminateIPMonitoringFromVPC」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- CloudWatchLogGroupNamePrefix

  タイプ: 文字列

  デフォルト: `/AWSSupport-SetupIPMonitoringFromVPC`

  説明: (オプション) テスト結果用に作成された各 CloudWatch ロググループに使用されるプレフィックス。
- CloudWatchLogGroupRetentionInDays

  タイプ: 文字列

  有効な値: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

  デフォルト: 7

  説明: (オプション) ネットワーク監視結果を保持する日数。
- InstanceType

  タイプ: 文字列

有効な値: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

デフォルト: t3.micro

説明: (オプション) EC2Rescue インスタンスの EC2 インスタンスタイプ。推奨サイズ: t3.micro。

- SubnetId

  タイプ: 文字列

  説明: (必須) インスタンスの監視に使用するサブネット ID。プライベートサブネットを指定する場合は、インスタンスの監視がテストをセットアップするためにインターネットアクセスが使用できることを確認する必要があります (つまり、CloudWatch Logs エージェントをインストールし、Systems Manager および CloudWatch と連携します)。

- TargetIPs

  タイプ: 文字列

  説明: (必須) 監視する IPv4 または IPv6 のカンマ区切り形式リスト。スペースは使用できません。最大サイズは 255 文字です。無効な IP を指定すると自動化は失敗し、テスト設定がロールバックされることに注意してください。

- TestInstanceSecurityGroupId

  タイプ: 文字列

  説明: (オプション) テストインスタンスのセキュリティグループ ID。指定しない場合、オートメーションはインスタンスの作成中に作成します。セキュリティグループがモニタリング IPs へのアウトバウンドアクセスを許可していることを確認します。

- TestInstanceProfileName

  タイプ: 文字列

  説明: (オプション) テストインスタンスの既存の IAM インスタンスプロファイルの名前。
  指定しない場合、オートメーションはインスタンスの作成中に作成します。ロールには、logs:CreateLogStream、、logs:DescribeLogGroupslogs:DescribeLogStreams、logs:よび AWS 管理ポリシー のアクセス許可が必要ですAmazonSSMManagedInstanceCore。

- TestInterval

タイプ: 文字列

説明: (オプション) テスト間隔間の分数。デフォルト値は 1分、最大値は 10分です。

- RetainDashboardAndLogsOnDeletion

  タイプ: 文字列

  説明: (オプション) AWS CloudFormation スタックFalseを削除するときに Amazon CloudWatch ダッシュボードと ログを削除するように を指定します。 Amazon CloudWatch AWS CloudFormation デフォルト値は True です。デフォルトでは、ダッシュボードと ログは保持され、不要になったら手動で削除する必要があります。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

> **Warning**
>
> ミュータブル IAM アクセス許可の誤用を防ぐために、TestInstanceProfileNameパラメータを渡すか、セキュリティガードレールが設定されていることを確認することをお勧めします。

オートメーションを実行するユーザーには [AmazonSSMAutomationRole] IAM 管理ポリシーがアタッチされていることが推奨されます。さらに、ユーザーは、ユーザーアカウント、グループ、またはロールに次のポリシーをアタッチする必要があります。

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

TestInstanceProfileName パラメータが指定されている場合、ランブックを実行するために次の IAM アクセス許可は必要ありません。

- iam:CreateRole
- iam:CreateInstanceProfile
- iam:DetachRolePolicy
- iam:AttachRolePolicy
- iam:AddRoleToInstanceProfile
- iam:RemoveRoleFromInstanceProfile
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:DeleteInstanceProfile

ドキュメントステップ

1. **aws:executeAwsApi** - 指定されたサブネットを説明します。
2. **aws:branch** - TargetIP の入力を評価します。

   (IPv6) TargetIP に IPv6 が含まれている場合:

   aws:assertAwsResourceProperty - 指定されたサブネットに IPv6 プールが関連付けられていることを確認します
3. **aws:executeScript** - 最新の Amazon Linux 2 AMI のインスタンスタイプとパブリックパラメータパスのアーキテクチャを取得します。
4. **aws:executeAwsApi** - Parameter Store から最新の Amazon Linux 2 AMI を取得します。
5. **aws:executeAwsApi** - サブネットの VPC でテスト用のセキュリティグループを作成します。

   (クリーンアップ) セキュリティグループの作成に失敗した場合:

   aws:executeAwsApi - 自動化によって作成されたセキュリティグループがあれば削除します。
6. **aws:executeAwsApi** - テストセキュリティグループ内のすべてのアウトバウンドトラフィックを許可します。

   (クリーンアップ) セキュリティグループ Egress ルールの作成に失敗した場合:

   aws:executeAwsApi - 自動化によって作成されたセキュリティグループがあれば削除します。
7. **aws:executeAwsApi** - テスト EC2 インスタンスの IAM ロールを作成します

   (クリーンアップ) ロールの作成に失敗した場合:

   a. **aws:executeAwsApi** - 自動化によって作成された IAM ロールがあれば削除します。

   b. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。
8. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーをアタッチします

   (クリーンアップ) ポリシーの添付が失敗した場合:

   a. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします (アタッチされている場合)。

   b. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

   c. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

9. **aws:executeAwsApi** - インラインポリシーを適用して、CloudWatch ロググループの保持設定を行い、CloudWatch ダッシュボードを作成できるようにします

   (クリーンアップ) インラインポリシーの添付に失敗した場合:

   a. **aws:executeAwsApi** - 作成された場合は、CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

   b. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

   c. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

   d. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

10. **aws:executeAwsApi** - IAM インスタンスプロファイルを作成します。

   (クリーンアップ) インスタンスプロファイルの作成に失敗した場合:

   a. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルがあれば削除します。

   b. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

   c. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールから削除します。

   d. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

   e. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

11. **aws:executeAwsApi** - IAM インスタンスプロファイルを IAM ロールに関連付けます。

   (クリーンアップ) インスタンスプロファイルとロールの関連づけに失敗した場合:

   a. **aws:executeAwsApi** - 関連付けられている場合は、IAM インスタンスプロファイルをロールから削除します。

   b. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

   c. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

   d. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

e. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

f. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

12**aws:sleep** - インスタンスプロファイルが利用可能になるのを待ちます。

13**aws:runInstances** - 指定されたサブネット内にテストインスタンスを作成し、以前に作成したインスタンスプロファイルを追加します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

14**aws:branch** - TargetIP の入力を評価します。

(IPv6) TargetIP に IPv6 が含まれている場合:

aws:executeAwsApi - IPv6 をテストインスタンスにアサインします。

15**aws:waitForAwsResourceProperty** - テストインスタンスがマネージドインスタンスになるのを待ちます。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

16**aws:runCommand** - インストールテストの前提条件:

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

17**aws:runCommand** - 提供された IP が構文的に正しい IPv4 または IPv6 アドレスあるいはその両方の検証:

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

18 **aws:runCommand** - 提供された各 IP の MTR テストを定義します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

19 **aws:runCommand** - 提供された各 IP の最初の ping テストを定義します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

20 **aws:runCommand** - 提供された各 IP の 2 番目の ping テストを定義します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

21 **aws:runCommand** - 提供された各 IP の tracepath テストを定義します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

22 **aws:runCommand** - 提供された各 IP の traceroute テストを定義します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

23 **aws:runCommand** - CloudWatch Logs を設定します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

24 **aws:runCommand** - 1 分ごとに各テストを実行するように cronjobs をスケジュールします。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

25**aws:sleep** - テストがデータを生成するのを待ちます。

26**aws:runCommand** - 目的の CloudWatch ロググループの保持を設定します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

27**aws:runCommand** - CloudWatch ロググループのメトリクスフィルターを設定します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:changeInstanceState** - テストインスタンスを終了します。

b. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。

c. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。

d. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。

e. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。

f. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。

g. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

28**aws:runCommand** - CloudWatch ダッシュボードを作成します。

(クリーンアップ) ステップが失敗した場合:

a. **aws:executeAwsApi** - CloudWatch ダッシュボードが存在する場合は削除します。

b. **aws:changeInstanceState** - テストインスタンスを終了します。

c. **aws:executeAwsApi** - IAM インスタンスプロファイルをロールから削除します。
d. **aws:executeAwsApi** - 自動化によって作成された IAM インスタンスプロファイルを削除します。
e. **aws:executeAwsApi** - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。
f. **aws:executeAwsApi** - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。
g. **aws:executeAwsApi** - 自動化によって作成された IAM ロールを削除します。
h. **aws:executeAwsApi** - 自動化によって作成されたセキュリティグループがあれば削除します。

出力

createCloudWatchDashboards.Output - CloudWatch ダッシュボードの URL です。

createManagedInstance.InstanceIds - テストインスタンス ID です。

AWSSupport-TerminateIPMonitoringFromVPC

説明

AWSSupport-TerminateIPMonitoringFromVPC は、過去に AWSSupport-SetupIPMonitoringFromVPC によって開始された IP モニタリングテストを終了します。指定されたテスト ID に関連するデータは削除されます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- AutomationExecutionId

  タイプ: 文字列

  説明: (必須) 以前に AWSSupport-SetupIPMonitoringFromVPC ランブックを実行したときの自動化実行 ID。この実行 ID に関連付けられているリソースはすべて削除されます。

- InstanceId

  タイプ: 文字列

  説明: (必須) インスタンスの監視に使用するインスタンス ID。

- SubnetId

  タイプ: 文字列

  説明: (必須) インスタンスの監視に使用するサブネット ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

オートメーションを実行するユーザーには [AmazonSSMAutomationRole] IAM 管理ポリシーがアタッチされていることが推奨されます。さらに、ユーザーは、ユーザー、グループ、またはロールに次のポリシーをアタッチする必要があります。

```
{
"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"
```

```
    ]
}
```

ドキュメントステップ

1. aws:assertAwsResourceProperty - AutomationExecutionId と InstanceId が同じテストに関連していることを確認します。
2. aws:assertAwsResourceProperty - SubnetId と InstanceId が同じテストに関連していることを確認します。
3. aws:executeAwsApi - セキュリティグループのテストを取得します。
4. aws:executeAwsApi - CloudWatch ダッシュボードを削除します。
5. aws:changeInstanceState - テストインスタンスを終了します。
6. aws:executeAwsApi - IAM インスタンスプロファイルをロールから削除します。
7. aws:executeAwsApi - 自動化によって作成された IAM インスタンスプロファイルを削除します。
8. aws:executeAwsApi - CloudWatch インラインポリシーをオートメーションによって作成されたロールから削除します。
9. aws:executeAwsApi - AmazonSSMManagedInstanceCore 管理ポリシーを自動化によって作成されたロールからデタッチします。
10. aws:executeAwsApi - 自動化によって作成された IAM ロールを削除します。
11. aws:executeAwsApi - 自動化によって作成されたセキュリティグループがあれば削除します。

出力

なし

AWS WAF

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS WAF。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl

- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

AWS-AddWAFRegionalRuleToRuleGroup

説明

AWS-AddWAFRegionalRuleToRuleGroup ランブックは、既存の AWS WAF リージョンルールを AWS WAF リージョンルールグループに追加します。 AWS WAF Classic リージョンルールグループのみがサポートされています。 AWS WAF Classic リージョンルールグループは、最大 10 個のルールを持つことができます。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- RuleGroupId

  タイプ: 文字列

説明: (必須) 更新するルールグループの ID。

- RulePriority

  タイプ: 整数

  説明: (必須) 新しいルールの優先度。ルールの優先度は、リージョングループ内のルールが評価される順序を決定します。値が低いルールは、値が高いルールよりも優先度が高くなります。値は一意の整数である必要があります。リージョンルールグループに複数のルールを追加する場合、値は連続している必要はありません。

- RuleId

  タイプ: 文字列

  説明: (必須) リージョンルールグループに追加するルールの ID。

- RuleAction

  タイプ: 文字列

  説明: (必須) ウェブリクエストがルールの条件に一致するときに が AWS WAF 実行するアクションを指定します。

  有効な値: 許可 | ブロック | カウント

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- waf-regional:GetChangeToken
- waf-regional:GetChangeTokenStatus
- waf-regional:ListActivatedRulesInRuleGroup
- waf-regional:UpdateRuleGroup

ドキュメントステップ

- GetWAFChangeToken (aws:executeAwsApi) - AWS WAF ランブックが競合するリクエストをサービスに送信しないように変更トークンを取得します。
- AddWAFRuleToWAFRegionalRuleGroup (aws:executeScript) - 指定されたルールを AWS WAF リージョンルールグループに追加します。
- VerifyChangeTokenPropagating (aws:waitForAwsResourceProperty) - 変更トークンのステータスが `PENDING`または `INSYNC`であることを確認します。
- VerifyRuleAddedToRuleGroup (aws:executeScript) - 指定された AWS WAF ルールがターゲットリージョンルールグループに追加されていることを確認します。

出力

- VerifyRuleAddedToRuleGroup.VerifyRuleAddedToRuleGroupResponse - 新しいルールがリージョンルールグループに追加されたことを確認するステップの出力。
- VerifyRuleAddedToRuleGroup.ListActivatedRulesInRuleGroupResponse - `ListActivatedRulesInRuleGroup` API オペレーションの出力。

AWS-AddWAFRegionalRuleToWebAcl

説明

`AWS-AddWAFRegionalRuleToWebAcl` ランブックは、既存の AWS WAF リージョンルール、ルールグループ、またはレートベースのルールを AWS WAF Classic リージョンウェブアクセスコントロールリスト (ACL) に追加します。このランブックは、 が管理する既存の AWS WAF Classic リージョンウェブ ACL を更新しません AWS Firewall Manager。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- WebACLId

  タイプ: 文字列

  説明: (必須) 更新するウェブ ACL の ID。

- ActivatedRulePriority

  タイプ: 整数

  説明: (必須) 新しいルールの優先度。ルールの優先度は、ウェブ ACL 内のルールが評価される順序を決定します。値が低いルールは、値が高いルールよりも優先度が高くなります。値は一意の整数である必要があります。リージョンウェブ ACL に複数のルールを追加する場合、値は連続している必要はありません。

- ActivatedRuleRuleId

  タイプ: 文字列

  説明: (必須) ウェブ ACL に追加する通常のルール、レートベースのルール、またはグループの ID。

- ActivatedRuleAction

  タイプ: 文字列

  有効な値: 許可 | ブロック | カウント

  説明: (オプション) ウェブリクエストがルールの条件に一致するときに が AWS WAF 実行するアクションを指定します。

- ActivatedRuleType

  タイプ: 文字列

  有効な値: REGULAR | RATE_BASED | GROUP

デフォルト: REGULAR

説明: (オプション) ウェブ ACL に追加するルールタイプ。このフィールドはオプションですが、タイプを設定せずにウェブ ACL にRATE_BASEDルールを追加しようとすると、リクエストのデフォルトはREGULARルールであるため、リクエストは失敗することに注意してください。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- waf-regional:GetChangeToken
- waf-regional:GetWebACL
- waf-regional:UpdateWebACL

ドキュメントステップ

- DetermineWebACLNotInFMSAndRulePriority (aws:executeScript) - AWS WAF ウェブ ACL が Firewall Manager セキュリティポリシーにあるかどうかを確認し、優先度 ID が既存の ACL と競合しないことを確認します。
- AddRuleOrRuleGroupToWebACL (aws:executeScript) - 指定されたルールを AWS WAF ウェブ ACL に追加します。
- VerifyRuleOrRuleGroupAddedToWebAcl (aws:executeScript) - 指定された AWS WAF ルールがターゲットウェブ ACL に追加されていることを確認します。

出力

- DetermineWebACLNotInFMSAndRulePriority.PrereqResponse: DetermineWebACLNotInFMSAndRulePriority ステップからの出力。
- VerifyRuleOrRuleGroupAddedToWebAcl.VerifyRuleOrRuleGroupAddedToWebACLResponse: AddRuleOrRuleGroupToWebACL ステップからの出力。
- VerifyRuleOrRuleGroupAddedToWebAcl.ListActivatedRulesOrRuleGroupsInWebACLResponse: VerifyRuleOrRuleGroupAddedToWebAcl ステップの出力。

AWSConfigRemediation-EnableWAFClassicLogging

説明

AWSConfigRemediation-EnableWAFClassicLogging ランブックは、指定した AWS WAF ウェブアクセスコントロールリスト (ウェブ ACL) の Amazon Data Firehose (Firehose) へのログ記録を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- DeliveryStreamName

  タイプ: 文字列

  説明: (必須) ログを送信する Firehose 配信ストリームの名前。
- WebACLId

  タイプ: 文字列

  説明: (必須) ログオンを有効にする AWS WAF ウェブ ACL の ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:CreateServiceLinkedRole
- waf:GetLoggingConfiguration
- waf:GetWebAcl
- waf:PutLoggingConfiguration

ドキュメントステップ

- aws:executeAwsApi - DeliveryStreamName で指定する配信ストリームが存在することを確認します。
- aws:executeAwsApi - WebACLIdパラメータで指定された AWS WAF ウェブ ACL の ARN を収集します。
- aws:executeAwsApi - ウェブ ACL のログ記録を有効にします。
- aws:assertAwsResourceProperty - AWS WAF ウェブ ACL でログ記録が有効になっていることを確認します。

AWSConfigRemediation-EnableWAFClassicRegionalLogging

説明

AWSConfigRemediation-EnableWAFClassicRegionalLogging ランブックは、指定した AWS WAF ウェブアクセスコントロールリスト (ACL) の Amazon Data Firehose (Firehose) へのログ記録を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- LogDestinationConfigs

  タイプ: 文字列

  説明: (必須) ログを送信する Firehose 配信ストリームの Amazon リソースネーム (ARN)。
- WebACLId

  タイプ: 文字列

  説明: (必須) ログオンを有効にする AWS WAF ウェブ ACL の ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- iam:CreateServiceLinkedRole
- waf-regional:GetLoggingConfiguration
- waf-regional:GetWebAcl
- waf-regional:PutLoggingConfiguration

ドキュメントステップ

- aws:executeAwsApi - WebACLIdパラメータで指定された AWS WAF ウェブ ACL の ARN を収集します。

- aws:executeAwsApi - ウェブ ACL のログ記録を有効にします。
- aws:assertAwsResourceProperty - AWS WAF ウェブ ACL でログ記録が有効になっていることを確認します。

AWSConfigRemediation-EnableWAFV2Logging

説明

AWSConfigRemediation-EnableWAFV2Logging ランブックは、指定された Amazon Data Firehose (Firehose) 配信ストリームを使用して AWS WAF （ AWS WAF V2) ウェブアクセスコントロールリスト (ウェブ ACL) のログ記録を有効にします。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。

- LogDestinationConfigs

  タイプ: 文字列

  説明: (必須) ウェブ ACL に関連付ける Firehose 配信ストリーム ARN。

> **Note**
>
> Firehose 配信ストリーム ARN はプレフィックス `aws-waf-logs-` で始まる必要があります。例えば、`aws-waf-logs-us-east-2-analytics` です。詳細については、「Amazon Data Firehose」を参照してください。

- WebAclArn

  タイプ: 文字列

  説明: (必須) ログ記録を有効にするウェブ ACL の ARN。

必要な IAM アクセス許可

`AutomationAssumeRole` パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

ドキュメントステップ

- `aws:executeScript` - AWS WAF V2 ウェブ ACL のログ記録を有効にし、ログ記録に指定された設定があることを確認します。

Amazon WorkSpaces

AWS Systems Manager Automation は、Amazon WorkSpaces 用に事前定義されたランブックを提供します。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWS-CreateWorkSpace
- AWSSupport-RecoverWorkSpace

AWS-CreateWorkSpace

説明

AWS-CreateWorkSpace ランブックは、入力パラメータに指定した値に基づいて、WorkSpace と呼ばれる新しい Amazon WorkSpaces 仮想デスクトップを作成します。WorkSpaces の詳細については、Amazon WorkSpaces 管理ガイドの「Amazon WorkSpaces とは?」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。
- BundleId

  タイプ: 文字列

  説明: (必須) WorkSpace に使用するバンドルの ID。

- ComputeTypeName

  タイプ: 文字列

  有効な値: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

  説明: (オプション) WorkSpace のコンピューティングタイプ。
- DirectoryId

  タイプ: 文字列

  説明: (必須) WorkSpace に追加するディレクトリの ID。
- RootVolumeEncryptionEnabled

  型: ブール値

  有効な値: true | false

  デフォルト: false

  説明: (オプション) WorkSpace のルートボリュームが暗号化されているかどうかを決定します。
- RootVolumeSizeGib

  タイプ: 整数

  説明: (必須) WorkSpace のルートボリュームのサイズ。
- RunningMode

  タイプ: 文字列

  有効な値: ALWAYS_ON | AUTO_STOP

  説明: (必須) WorkSpace の実行モード。
- RunningModeAutoStopTimeoutInMinutes

  タイプ: 整数

  説明: (オプション) ユーザーがログオフした後に WorkSpace が停止する時間。60 分間隔で値を指定します。
- [タグ]

タイプ: 文字列

説明: (オプション) WorkSpace に適用するタグ。

- ユーザーネーム

  タイプ: 文字列

  説明: (必須) WorkSpace に関連付けるユーザー名。

- UserVolumeEncryptionEnabled

  型: ブール値

  有効な値: true | false

  デフォルト: false

  説明: (オプション) WorkSpace のユーザーボリュームが暗号化されているかどうかを決定します。

- UserVolumeSizeGib

  タイプ: 整数

  説明: (必須) WorkSpace のユーザーボリュームのサイズ。

- VolumeEncryptionKey

  タイプ: 文字列

  説明: (オプション) WorkSpace に保存されているデータの暗号化に使用する対称 AWS Key Management Service キー。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- workspaces:CreateWorkspaces
- workspaces:DescribeWorkspaces

ドキュメントステップ

- aws:executeScript - 入力パラメータに指定した値に基づいて WorkSpace を作成します。
- aws:waitForAwsResourceProperty - WorkSpace の状態が AVAILABLE であることを確認します。

出力

CreateWorkspace.WorkspaceId

AWSSupport-RecoverWorkSpace

説明

AWSSupport-RecoverWorkSpace ランブックは、WorkSpace として知られる、指定した Amazon WorkSpaces 仮想デスクトップで復旧手順を実行します。ランブックは WorkSpace を再起動し、状態が UNHEALTHY のままな場合は、入力パラメータに指定した値に基づいて WorkSpace を復元または再構築します。このランブックを使用する前に、「Amazon WorkSpaces 管理ガイド」の「WorkSpaces の問題のトラブルシューティング」を確認することをお勧めします。

> **Important**
>
> WorkSpace の復元または再構築は、データが失われる可能性のある潜在的に破壊的なアクションです。これは、WorkSpace が最後に利用可能なスナップショットから復元され、スナップショットから復旧したデータは 12 時間前のものである可能性があるためです。復元オプションは、最新のスナップショットに基づいて、ルートボリュームとユーザーボリュームの両方を再作成します。再構築オプションは、最新のスナップショットからユーザーボリュームを再作成し、WorkSpace の作成元のバンドルに関連付けられたイメージから WorkSpace を再作成します。WorkSpace の作成後にインストールされたアプリケーション、または変更されたシステム設定は失われます。WorkSpaces の復元と再構築の詳細については、「Amazon WorkSpaces 管理ガイド」の「WorkSpace の復元」および「WorkSpace の再構築」を参照してください。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (オプション) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。ロールを指定しない場合、Systems Manager Automation はこのランブックを開始するユーザーのアクセス許可を使用します。

- 了解

  タイプ: 文字列

  有効な値: はい

  説明: (必須)「はい」と入力すると、復元および再構築アクションによって最新のスナップショットから WorkSpace の復旧が試行され、このようなスナップショットから復元されたデータは 12 時間前のものである可能性あることを理解していることを意味します。

- 再起動

  タイプ: 文字列

  有効な値: はい | いいえ

  デフォルト: Yes

  説明: (必須) WorkSpace を再起動するかどうかを決定します。

- 再構築

  タイプ: 文字列

  有効な値: はい | いいえ

  デフォルト: いいえ

説明: (必須) WorkSpace を再構築するかどうかを指定します。

- 復元

  タイプ: 文字列

  有効な値: はい | いいえ

  デフォルト: いいえ

  説明: (必須) WorkSpace を復元するかどうかを決定します。

- WorkspaceId

  タイプ: 文字列

  説明: (必須) 復旧する WorkSpace の ID。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- workspaces:DescribeWorkspaces
- workspaces:DescribeWorkspaceSnapshots
- workspaces:RebootWorkspaces
- workspaces:RebuildWorkspaces
- workspaces:RestoreWorkspace
- workspaces:StartWorkspaces

ドキュメントステップ

- aws:executeAwsApi - WorkspaceId パラメータで指定した WorkSpace の状態を収集します。
- aws:assertAwsResourceProperty - WorkSpace の状態が AVAILABLE、ERROR、IMPAIRED、STOPPED または UNHEALTHY であることを確認します。
- aws:branch - WorkSpace の状態に基づいて分岐させます。

- aws:executeAwsApi - WorkSpace を起動します。
- aws:branch - Action パラメータで指定した値に基づいて分岐させます。
- aws:waitForAwsResourceProperty - 起動後に WorkSpace の状態を待機します。
- aws:waitForAwsResourceProperty - 起動後に Workspace の状態が AVAILABLE、ERROR、IMPAIRED または UNHEALTHY に変更されるまで待機します。
- aws:executeAwsApi - 起動後の WorkSpace の状態を収集します。
- aws:branch - 起動後の WorkSpace の状態に基づいて分岐させます。
- aws:executeAwsApi - WorkSpace を復元または再構築するために利用可能なスナップショットを収集します。
- aws:branch - Reboot パラメータで指定した値に基づいて分岐させます。
- aws:executeAwsApi - WorkSpace を再起動します。
- aws:executeAwsApi - 起動後の WorkSpace の状態を収集します。
- aws:waitForAwsResourceProperty - WorkSpace の状態がREBOOTING に変わるまで待機します。
- aws:waitForAwsResourceProperty - 再起動後に WorkSpace の状態が AVAILABLE、ERROR、または UNHEALTHY に変わるまで待機します。
- aws:executeAwsApi - 再起動後の WorkSpace の状態を収集します。
- aws:branch - 再起動後の WorkSpace の状態に基づいて分岐させます。
- aws:branch - Restore パラメータで指定した値に基づいて分岐させます。
- aws:executeAwsApi - WorkSpace を復元します。復元が失敗すると、ランブックは WorkSpace の再構築を試みます。
- aws:waitForAwsResourceProperty - WorkSpace の状態がRESTORING に変わるまで待機します。
- aws:waitForAwsResourceProperty - 復元後に WorkSpace の状態が AVAILABLE、ERROR、または UNHEALTHY に変わるまで待機します。
- aws:executeAwsApi - 復元後の WorkSpace の状態を収集します。
- aws:branch - 復元後の WorkSpace の状態に基づいて分岐させます。
- aws:branch - Rebuild パラメータで指定した値に基づいて分岐させます。
- aws:executeAwsApi - WorkSpace を再構築します。
- aws:waitForAwsResourceProperty - WorkSpace の状態がREBUILDING に変わるまで待機します。

- aws:waitForAwsResourceProperty - 再構築後に WorkSpace の状態が AVAILABLE、ERROR、または UNHEALTHY に変わるまで待機します。
- aws:executeAwsApi - 再構築後の WorkSpace の状態を収集します。
- aws:assertAwsResourceProperty - WorkSpace の状態が AVAILABLE であることを確認します。

X-Ray

AWS Systems Manager 自動化には、事前定義されたランブックが用意されています AWS X-Ray。詳細については、「ランブックの使用」を参照してください。ランブックコンテンツを表示する方法については、ランブックの内容を表示する を参照してください。

トピック

- AWSConfigRemediation-UpdateXRayKMSKey

AWSConfigRemediation-UpdateXRayKMSKey

説明

AWSConfigRemediation-UpdateXRayKMSKey ランブックは、 AWS Key Management Service (AWS KMS) キーを使用して AWS X-Ray データの暗号化を有効にします。このランブックは、推奨される最小限のセキュリティのベストプラクティスに従って AWS X-Ray データが暗号化されるようにするためのベースラインとしてのみ使用してください。複数のデータセットは、それぞれ異なる KMS キーを使用して暗号化することを推奨します。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

[所有者]

Amazon

[Platforms] (プラットフォーム)

Linux、macOS、Windows

パラメータ

- AutomationAssumeRole

  タイプ: 文字列

  説明: (必須) Systems Manager Automation がユーザーに代わってアクションを実行できるようにする AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。
- KeyId

  タイプ: 文字列

  説明: (必須) データの暗号化 AWS X-Ray に使用する KMS キーの Amazon リソースネーム (ARN)、キー ID、またはキーエイリアス。

必要な IAM アクセス許可

AutomationAssumeRole パラメータでは、ランブックを正常に使用するために、次のアクションが必要です。

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- kms:DescribeKey
- xray:GetEncryptionConfig
- xray:PutEncryptionConfig

ドキュメントステップ

- aws:executeAwsApi - KeyId パラメータで指定した KMS キーを使用して X-Ray データの暗号化を有効にします。
- aws:waitForAwsResourceProperty - X-Ray の暗号化設定ステータスが ACTIVE になるまで待機します。
- aws:executeAwsApi - KeyId パラメータで指定したキーの ARN を収集します。
- aws:assertAwsResourceProperty - X-Ray で暗号化が有効化済みであることを確認します。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。