사용자 가이드

AWS Systems Manager 자동화 실행서 참조

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

AWS Systems Manager 자동화 실행서 참조: 사용자 가이드

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

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

Automation 실행서 참조 1
실행서 콘텐츠 보기 3
API 게이트웨이 4
AWSConfigRemediation-DeleteAPIGatewayStage 4
AWSConfigRemediation-EnableAPIGatewayTracing 5
AWSConfigRemediation-UpdateAPIGatewayMethodCaching 7
AWS Batch 8
AWSSupport-TroubleshootAWSBatchJob 8
AWS CloudFormation 14
AWS-DeleteCloudFormationStack 14
AWS-EnableCloudFormationSNSNotification 15
AWS-RunCfnLint 17
AWSSupport-TroubleshootCFNCustomResource 19
AWS-UpdateCloudFormationStack 21
CloudFront 22
AWSConfigRemediation-EnableCloudFrontDefaultRootObject 22
AWSConfigRemediation-EnableCloudFrontAccessLogs 24
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity 26
AWSConfigRemediation-EnableCloudFrontOriginFailover 27
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS 29
CloudTrail 30
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail 30
AWS-EnableCloudTrail 32
AWS-EnableCloudTrailCloudWatchLogs 33
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS 35
AWS-EnableCloudTrailKmsEncryption 36
AWSConfigRemediation-EnableCloudTrailLogFileValidation 38
AWS-EnableCloudTrailLogFileValidation 39
AWS-QueryCloudTrailLogs 40
CloudWatch 42
AWS-ConfigureCloudWatchOnEC2Instance 43
AWS-EnableCWAlarm 44
Amazon DocumentDB 46
AWS-EnableDocDbClusterBackupRetentionPeriod 47

CodeBuild 49
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK 49
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject 51
AWS CodeDeploy 52
AWSSupport-TroubleshootCodeDeploy 52
AWS Config 54
AWSSupport-SetupConfig 54
Amazon Connect 57
AWSSupport-AssociatePhoneNumbersToConnectContactFlows 57
AWSSupport-CollectAmazonConnectContactFlowLog 65
AWS Directory Service 70
AWS-CreateDSManagementInstance 70
AWSSupport-TroubleshootADConnectorConnectivity 75
AWSSupport-TroubleshootDirectoryTrust 78
AWS AppSync 81
AWS-EnableAppSyncGraphQLApiLogging 82
Amazon Athena 84
AWS-EnableAthenaWorkGroupEncryptionAtRest 84
DynamoDB 86
AWS-ChangeDDBRWCapacityMode 87
AWS-CreateDynamoDBBackup 89
AWS-DeleteDynamoDbBackup 90
AWSConfigRemediation-DeleteDynamoDbTable 91
AWS-DeleteDynamoDbTableBackups 92
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable 93
AWSConfigRemediation-EnablePITRForDynamoDbTable 95
AWS-EnableDynamoDbAutoscaling 96
AWS-RestoreDynamoDBTable 99
Amazon EBS 102
AWSSupport-AnalyzeEBSResourceUsage 102
AWS-ArchiveEBSSnapshots 108
AWS-AttachEBSVolume 111
AWSSupport-CalculateEBSPerformanceMetrics 112
AWS-CopySnapshot 118
AWS-CreateSnapshot 119
AWS-DeleteSnapshot 120

AWSConfigRemediation-DeleteUnusedEBSVolume 121
AWS-DeregisterAMIs 122
AWS-DetachEBSVolume 124
AWSConfigRemediation-EnableEbsEncryptionByDefault 125
AWS-ExtendEbsVolume 126
AWSSupport-ModifyEBSSnapshotPermission 129
AWSConfigRemediation-ModifyEBSVolumeType 131
Amazon EC2 132
AWS-ASGEnterStandby 134
AWS-ASGExitStandby 135
AWS-CreateImage 136
AWS-DeleteImage 138
AWS-PatchAsgInstance 139
AWS-PatchInstanceWithRollback 142
AWS-QuarantineEC2Instance 144
AWS-ResizeInstance 146
AWS-RestartEC2Instance 147
AWS-SetupJupyter 148
AWS-StartEC2Instance 151
AWS-StopEC2Instance 152
AWS-TerminateEC2Instance 153
AWS-UpdateLinuxAmi 154
AWS-UpdateWindowsAmi 157
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck 161
AWSConfigRemediation-EnforceEC2InstanceIMDSv2 162
AWSEC2-CloneInstanceAndUpgradeSQLServer 163
AWSEC2-CloneInstanceAndUpgradeWindows 167
AWSEC2-ConfigureSTIG 171
AWSEC2-PatchLoadBalancerInstance 201
AWSEC2-SQLServerDBRestore 202
AWSSupport-ActivateWindowsWithAmazonLicense 207
AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 210
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD 214
AWSSupport-CheckXenToNitroMigrationRequirements 220
AWSSupport-ConfigureEC2Metadata 223
AWSSupport-CopyEC2Instance 226

AWSSupport-EnableWindowsEC2SerialConsole 231
AWSSupport-ExecuteEC2Rescue 240
AWSSupport-ListEC2Resources 243
AWSSupport-ManageRDPSettings 245
AWSSupport-ManageWindowsService 247
AWSSupport-MigrateEC2ClassicToVPC 249
AWSSupport-MigrateXenToNitroLinux 255
AWSSupport-ResetAccess 267
AWSSupport-ResetLinuxUserPassword 270
AWSPremiumSupport-ResizeNitroInstance 276
AWSSupport-RestoreEC2InstanceFromSnapshot 282
AWSSupport-SendLogBundleToS3Bucket 287
AWSSupport-StartEC2RescueWorkflow 288
AWSPremiumSupport-TroubleshootEC2DiskUsage 299
AWSSupport-TroubleshootEC2InstanceConnect 303
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs 309
AWSSupport-TroubleshootRDP 312
AWSSupport-TroubleshootSSH 318
AWSSupport-TroubleshootSUSERegistration 321
AWSSupport-TroubleshootWindowsPerformance 323
AWSSupport-TroubleshootWindowsUpdate 331
AWSSupport-UpgradeWindowsAWSDrivers 337
Amazon ECS 341
AWSSupport-CollectECSInstanceLogs 341
AWS-InstallAmazonECSAgent 344
AWS-ECSRunTask 345
AWSSupport-TroubleshootECSContainerInstance 349
AWSSupport-TroubleshootECSTaskFailedToStart 351
AWS-UpdateAmazonECSAgent 354
Amazon EFS 356
AWSSupport-CheckAndMountEFS 356
Amazon EKS 360
AWSSupport-CollectEKSInstanceLogs 360
AWS-CreateEKSClusterWithFargateProfile 362
AWS-CreateEKSClusterWithNodegroup 366
AWS-DeleteEKSCluster 369

AWS-MigrateToNewEKSSelfManagedNodeGroup 372
AWSPremiumSupport-TroubleshootEKSCluster 378
AWSSupport-TroubleshootEKSWorkerNode 382
AWS-UpdateEKSCluster 384
AWS-UpdateEKSManagedNodeGroup 385
AWS-UpdateEKSSelfManagedLinuxNodeGroups 389
Elastic Beanstalk 393
AWSSupport-CollectElasticBeanstalkLogs 393
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming .. 396
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications 397
AWSSupport-TroubleshootElasticBeanstalk 399
Elastic Load Balancing 402
AWSConfigRemediation-DropInvalidHeadersForALB 402
AWS-EnableCLBAccessLogs 404
AWS-EnableCLBConnectionDraining 405
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing 407
AWSConfigRemediation-EnableELBDeletionProtection 408
AWSConfigRemediation-EnableLoggingForALBAndCLB 410
AWSSupport-TroubleshootCLBConnectivity 411
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing 415
AWS-UpdateALBDesyncMitigationMode 416
AWS-UpdateCLBDesyncMitigationMode 418
Amazon EMR 419
AWSSupport-AnalyzeEMRLogs 420
AWSSupport-DiagnoseEMRLogsWithAthena 426
Amazon OpenSearch Service 434
AWSConfigRemediation-DeleteOpenSearchDomain 434
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain 436
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups 437
AWSSupport-TroubleshootOpenSearchRedYellowCluster 439
AWSSupport-TroubleshootOpenSearchHighCPU 445
EventBridge 450
AWS-AddOpsItemDedupStringToEventBridgeRule 451
AWS-DisableEventBridgeRule 452
AWS Glue 454
AWSSupport-TroubleshootGlueConnection 454

Amazon FSx 464
AWSSupport-ValidateFSxWindowsADConfig 465
GuardDuty 478
AWSConfigRemediation-CreateGuardDutyDetector 479
IAM 480
AWS-AttachIAMToInstance 480
AWS-DeleteIAMInlinePolicy 483
AWSConfigRemediation-DeleteIAMRole 484
AWSConfigRemediation-DeleteIAMUser 485
AWSConfigRemediation-DeleteUnusedIAMGroup 488
AWSConfigRemediation-DeleteUnusedIAMPolicy 489
AWSConfigRemediation-DetachIAMPolicy 491
AWSConfigRemediation-EnableAccountAccessAnalyzer 492
AWSSupport-GrantPermissionsToIAMUser 493
AWSConfigRemediation-RemoveUserPolicies 498
AWSConfigRemediation-ReplaceIAMInlinePolicy 500
AWSConfigRemediation-RevokeUnusedIAMUserCredentials 502
AWSConfigRemediation-SetIAMPasswordPolicy 503
Amazon Kinesis Data Streams 506
AWS-EnableKinesisStreamEncryption 506
AWS KMS 508
AWSConfigRemediation-CancelKeyDeletion 508
AWSConfigRemediation-EnableKeyRotation 510
Lambda 511
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing 511
AWSConfigRemediation-DeleteLambdaFunction 513
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK 514
AWSConfigRemediation-MoveLambdaToVPC 515
AWSSupport-RemediateLambdaS3Event 517
AWSSupport-TroubleshootLambdaInternetAccess 520
AWSSupport-TroubleshootLambdaS3Event 523
Amazon Managed Workflows for Apache Airflow 525
AWSSupport-TroubleshootMWAAEnvironmentCreation 525
Neptune 531
AWS-EnableNeptuneDbAuditLogsToCloudWatch 531
AWS-EnableNeptuneDbBackupRetentionPeriod 533

AWS-EnableNeptuneClusterDeletionProtection 534
Amazon RDS 536
AWS-CreateEncryptedRdsSnapshot 537
AWS-CreateRdsSnapshot 540
AWSConfigRemediation-DeleteRDSCluster 541
AWSConfigRemediation-DeleteRDSClusterSnapshot 542
AWSConfigRemediation-DeleteRDSInstance 544
AWSConfigRemediation-DeleteRDSInstanceSnapshot 546
AWSConfigRemediation-DisablePublicAccessToRDSInstance 547
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster 548
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance 550
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance 552
AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS 553
AWSConfigRemediation-EnableMultiAZOnRDSInstance 555
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance 557
AWSConfigRemediation-EnableRDSClusterDeletionProtection 559
AWSConfigRemediation-EnableRDSInstanceBackup 560
AWSConfigRemediation-EnableRDSInstanceDeletionProtection 562
AWSConfigRemediation-ModifyRDSInstancePortNumber 564
AWSSupport-ModifyRDSSnapshotPermission 565
AWSPremiumSupport-PostgreSQLWorkloadReview 567
AWS-RebootRdsInstance 583
AWSSupport-ShareRDSSnapshot 584
AWS-StartRdsInstance 587
AWS-StartStopAuroraCluster 588
AWS-StopRdsInstance 590
AWSSupport-TroubleshootConnectivityToRDS 591
AWSSupport-TroubleshootRDSIAMAuthentication 593
AWSSupport-ValidateRdsNetworkConfiguration 601
Amazon Redshift 607
AWSConfigRemediation-DeleteRedshiftCluster 607
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster 609
AWSConfigRemediation-EnableRedshiftClusterAuditLogging 610
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot 612
AWSConfigRemediation-EnableRedshiftClusterEncryption 613
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting 615

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster 616
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings 617
AWSConfigRemediation-ModifyRedshiftClusterNodeType 619
Amazon S3 621
AWS-ArchiveS3BucketToIntelligentTiering 622
AWS-ConfigureS3BucketLogging 624
AWS-ConfigureS3BucketVersioning 626
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock 627
AWSConfigRemediation-ConfigureS3PublicAccessBlock 629
AWS-CreateS3PolicyToExpireMultipartUploads 631
AWS-DisableS3BucketPublicReadWrite 633
AWS-EnableS3BucketEncryption 634
AWS-EnableS3BucketKeys 635
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy 637
AWSConfigRemediation-RestrictBucketSSLRequestsOnly 638
AWSSupport-TroubleshootS3PublicRead 639
Amazon SES 645
AWSSupport-AnalyzeSESMessageSendingStatus 645
SageMaker 649
AWS-DisableSageMakerNotebookRootAccess 649
Secrets Manager 652
AWSConfigRemediation-DeleteSecret 652
AWSConfigRemediation-RotateSecret 653
Security Hub 655
AWSConfigRemediation-EnableSecurityHub 655
AWS Shield 656
AWSPremiumSupport-DDoSResiliencyAssessment 657
Amazon SNS 665
AWS-EnableSNSTopicDeliveryStatusLogging 665
AWSConfigRemediation-EncryptSNSTopic 668
AWS-PublishSNSNotification 669
Amazon SQS 670
AWS-EnableSQSEncryption 670
Step Functions 673
AWS-EnableStepFunctionsStateMachineLogging 673
Systems Manager 675

AWS-BulkDeleteAssociation 676
AWS-BulkEditOpsItems 677
AWS-BulkResolveOpsItems 680
AWS-ConfigureMaintenanceWindows 682
AWS-CreateManagedLinuxInstance 683
AWS-CreateManagedWindowsInstance 686
AWSConfigRemediation-EnableCWLoggingForSessionManager 689
AWS-ExportOpsDataToS3 690
AWS-ExportPatchReportToS3 692
AWS-SetupInventory 693
AWS-SetupManagedInstance 697
AWS-SetupManagedRoleOnEC2Instance 699
AWSSupport-TroubleshootManagedInstance 700
AWSSupport-TroubleshootPatchManagerLinux 703
AWSSupport-TroubleshootSessionManager 706
타사 712
AWS-CreateJiraIssue 712
AWS-CreateServiceNowIncident 714
AWS-RunPacker 716
Amazon VPC 718
AWS-CloseSecurityGroup 719
AWSSupport-ConfigureDNSQueryLogging 720
AWSSupport-ConfigureTrafficMirroring 723
AWSSupport-ConnectivityTroubleshooter 725
AWSSupport-TroubleshootVPN 729
AWSConfigRemediation-DeleteEgressOnlyInternetGateway 734
AWSConfigRemediation-DeleteUnusedENI 736
AWSConfigRemediation-DeleteUnusedSecurityGroup 737
AWSConfigRemediation-DeleteUnusedVPCNetworkACL 738
AWSConfigRemediation-DeleteVPCFlowLog 739
AWSConfigRemediation-DetachAndDeleteInternetGateway 741
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway 742
AWS-DisableIncomingSSHOnPort22 744
AWS-DisablePublicAccessForSecurityGroup 746
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP 747
AWSSupport-EnableVPCFlowLogs 748

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch 755
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket 757
AWS-ReleaseElasticIP 759
AWS-RemoveNetworkACLUnrestrictedSSHRDP 759
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules 761
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules 762
AWSSupport-SetupIPMonitoringFromVPC 763
AWSSupport-TerminateIPMonitoringFromVPC 775
AWS WAF 778
AWS-AddWAFRegionalRuleToRuleGroup 778
AWS-AddWAFRegionalRuleToWebAcl 781
AWSConfigRemediation-EnableWAFClassicLogging 783
AWSConfigRemediation-EnableWAFClassicRegionalLogging 785
AWSConfigRemediation-EnableWAFV2Logging 786
Amazon WorkSpaces 788
AWS-CreateWorkSpace 788
AWSSupport-RecoverWorkSpace 791
X-Ray 795
AWSConfigRemediation-UpdateXRayKMSKey 795
..... dccxcvii

Systems Manager Automation 실행서 참조

빠르게 시작할 수 있도록 는 사전 정의된 실행서를 AWS Systems Manager 제공합니다. 이러한 런북은 Amazon Web Services AWS Support, 및 에서 관리합니다 AWS Config. 실행서 참조에서는 Systems Manager AWS Support, 및 에서 제공하는 사전 정의된 각 실행서를 설명합니다 AWS Config.

> **Important**
>
> (IAM) 서비스 역할을 사용하여 다른 서비스를 호출하는 자동화 워크플로를 AWS Identity and Access Management 실행하는 경우 해당 서비스를 호출하려면 서비스 역할을 권한으로 구성해야 합니다. 이 요구 사항은 `AWS-ConfigureS3BucketLogging`, `AWS-CreateDynamoDBBackup`, `AWS-RestartEC2Instance` 실행서 등의 모든 AWS Automation 실행서(`AWS-*` 실행서)에 적용됩니다. 이 요구 사항은 다른 AWS 서비스를 호출하는 작업을 사용하여 다른 서비스를 호출하는 사용자 지정 Automation 런북에도 적용됩니다. 예를 들어, `aws:executeAwsApi`, `aws:createStack` 또는 `aws:copyImage` 작업을 사용하는 경우 이러한 서비스를 호출할 수 있는 권한을 포함하여 서비스 역할을 구성해야 합니다. 역할에 IAM 인라인 정책을 추가하여 다른 AWS 서비스에 대한 권한을 활성화할 수 있습니다. 자세한 내용은 자동화 인라인 정책 추가를 참조하여 다른 AWS 서비스를 호출합니다.

이 참조에는 AWS AWS Support, 및 에서 소유한 각 Systems Manager 런북을 설명하는 주제가 포함되어 있습니다 AWS Config. 런북은 관련 에 의해 구성됩니다 AWS 서비스. 각 페이지는 실행서를 사용할 때 지정할 수 있는 필수 및 선택 파라미터를 설명합니다. 각 페이지에는 실행서의 단계와 자동화 출력(있는 경우)도 나열되어 있습니다.

이 참조에는 `AWS-CreateManagedLinuxInstanceWithApproval` 또는 `AWS-StopEC2InstanceWithApproval` 실행서와 같이 승인이 필요한 실행서에 대한 별도의 페이지가 포함되어 있지 않습니다. `WithApproval`(을)를 포함하는 모든 실행서 이름은 실행서에 `aws:approve` 작업이 포함되어 있음을 의미합니다. 이 작업은 지정된 보안 주체가 작업을 승인 또는 거부할 때까지 자동화를 일시적으로 중지시킵니다. 필요한 승인 횟수에 도달하면 자동화가 다시 시작됩니다.

자동화 실행에 대한 자세한 내용은 단순 자동화 실행을 참조하세요. 여러 대상에서의 자동화 실행에 대한 자세한 내용은 대상 및 속도 제어를 사용하는 자동화 실행을 참조하세요.

주제

- 실행서 콘텐츠 보기
- API 게이트웨이

- AWS Batch
- AWS CloudFormation
- CloudFront
- CloudTrail
- CloudWatch
- Amazon DocumentDB
- CodeBuild
- AWS CodeDeploy
- AWS Config
- Amazon Connect
- AWS Directory Service
- AWS AppSync
- Amazon Athena
- DynamoDB
- Amazon EBS
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Elastic Beanstalk
- Elastic Load Balancing
- Amazon EMR
- Amazon OpenSearch Service
- EventBridge
- 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
- Secrets Manager
- Security Hub
- AWS Shield
- Amazon SNS
- Amazon SQS
- Step Functions
- Systems Manager
- 타사
- Amazon VPC
- AWS WAF
- Amazon WorkSpaces
- X-Ray

실행서 콘텐츠 보기

Systems Manager 콘솔에서 실행서에 대한 콘텐츠를 볼 수 있습니다.

실행서 콘텐츠를 보려면

1. 에서 AWS Systems Manager 콘솔을 엽니다https://console.aws.amazon.com/systems-manager/.
2. 탐색 창에서 Documents를 선택합니다.

   -또는-

AWS Systems Manager 홈 페이지가 먼저 열리면 메뉴 아이콘 (☰) 을 선택하여 탐색 창을 연 다음 탐색 창에서 문서를 선택합니다.

3. 범주 섹션에서 자동화 문서를 선택합니다.
4. 실행서를 선택한 후 세부 정보 보기를 선택합니다.
5. 콘텐츠 탭을 선택합니다.

API 게이트웨이

AWS Systems Manager 자동화는 Amazon API Gateway에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

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

AWSConfigRemediation-DeleteAPIGatewayStage

설명

`AWSConfigRemediation-DeleteAPIGatewayStage` 실행서는 Amazon API Gateway(API Gateway) 단계를 삭제합니다. 이 자동화를 실행하는 AWS 리전에서 AWS Config를 활성화해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- StageArn

  유형: 문자열

  설명: (필수) 삭제하려는 API Gateway 단계의 Amazon 리소스 이름(ARN) 입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `StageArn` 파라미터에 지정된 API Gateway 단계를 삭제합니다.

AWSConfigRemediation-EnableAPIGatewayTracing

설명

`AWSConfigRemediation-EnableAPIGatewayTracing` 실행서는 Amazon API Gateway(API Gateway) 단계에서 추적을 활성화합니다. 이 자동화를 실행하는 AWS 리전에서 AWS Config가 활성화되어야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- StageArn

  유형: 문자열

  설명: (필수) 추적을 활성화하려는 API Gateway 단계의 Amazon 리소스 이름(ARN)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `StageArn` 파라미터에 지정된 API Gateway 단계에서 추적을 활성화합니다.

AWSConfigRemediation-UpdateAPIGatewayMethodCaching

설명

AWSConfigRemediation-UpdateAPIGatewayMethodCaching 실행서는 Amazon API Gateway 단계 리소스의 캐시 메서드 설정을 업데이트합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- CachingAuthorizedMethods

  형식: StringList

  설명: (필수) 캐싱을 활성화하도록 승인된 메서드입니다. 목록은 DELETE, GET, HEAD, OPTIONS, PATCH, POST 및 PUT의 조합이어야 합니다. 캐싱은 선택한 메서드에 대해 활성화되고 선택되지 않은 메서드에 대해서는 비활성화됩니다. ANY을 선택하면 모든 메서드에 대해 캐싱이 활성화되고, NONE를 선택하면 모든 메서드에 대해 캐싱이 비활성화됩니다.
- StageArn

  유형: 문자열

  설명: (필수) REST API용 API Gateway 단계 ARN입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - 단계 리소스 ID를 입력으로 받아들이고, `UpdateStage` API 작업을 사용하여 API Gateway 단계의 캐시 메서드 설정을 업데이트하고, 업데이트를 확인합니다.

AWS Batch

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Batch. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-TroubleshootAWSBatchJob

AWSSupport-TroubleshootAWSBatchJob

설명

`AWSSupport-TroubleshootAWSBatchJob`런북은 AWS Batch 작업이 상태에서 상태로 진행되지 못하게 하는 문제를 해결하는 데 도움이 됩니다. `RUNNABLE` `STARTING`

어떻게 작동하나요?

이 런북은 다음 검사를 수행합니다.

- 컴퓨팅 환경이 `INVALID` or `DISABLED` 상태인 경우
- 컴퓨팅 환경의 `Max vCPU` 파라미터가 작업 큐의 작업 볼륨을 수용할 수 있을 만큼 충분히 큰 경우

- 작업에 컴퓨팅 환경의 인스턴스 유형이 제공할 수 있는 것보다 더 많은 vCPUs 메모리 리소스가 필요한 경우
- 작업이 GPU 기반 인스턴스에서 실행되어야 하는데 컴퓨팅 환경이 GPU 기반 인스턴스를 사용하도록 구성되지 않은 경우
- 컴퓨팅 환경의 Auto Scaling 그룹이 인스턴스를 시작하지 못한 경우
- 시작된 인스턴스가 기본 Amazon Elastic Container Service (AmazonECS) 클러스터에 조인할 수 있는 경우, 조인할 수 없는 경우 AWSSupport-T roubleshootECSContainer Instance 런북을 실행합니다.
- 권한 문제로 인해 작업을 실행하는 데 필요한 특정 작업이 차단되는 경우

> **Important**
>
> - 이 런북은 중단된 상태인 작업과 동일한 AWS 지역에서 시작해야 합니다. `RUNNABLE`
> - 이 런북은 Amazon 또는 Amazon Elastic Compute Cloud EC2 (AWS Fargate Amazon) 인스턴스에 예약된 AWS Batch 작업에 대해 시작할 수 있습니다. ECS Amazon Elastic Kubernetes Service EKS (Amazon) 에서 AWS Batch 작업에 대한 자동화가 시작되면 시작이 중지됩니다.
> - 작업을 실행할 수 있는 인스턴스가 있지만 Amazon ECS 클러스터를 등록하지 못하는 경우, 이 런북은 `AWSSupport-TroubleshootECSContainerInstance` 자동화 런북을 시작하여 이유를 확인합니다. 자세한 내용은 AWSSupport-T roubleshootECSContainer Instance 런북을 참조하십시오.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- JobId

  유형: 문자열

  설명: (필수) 중단된 `RUNNABLE` 상태인 AWS Batch Job의 ID입니다.

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

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

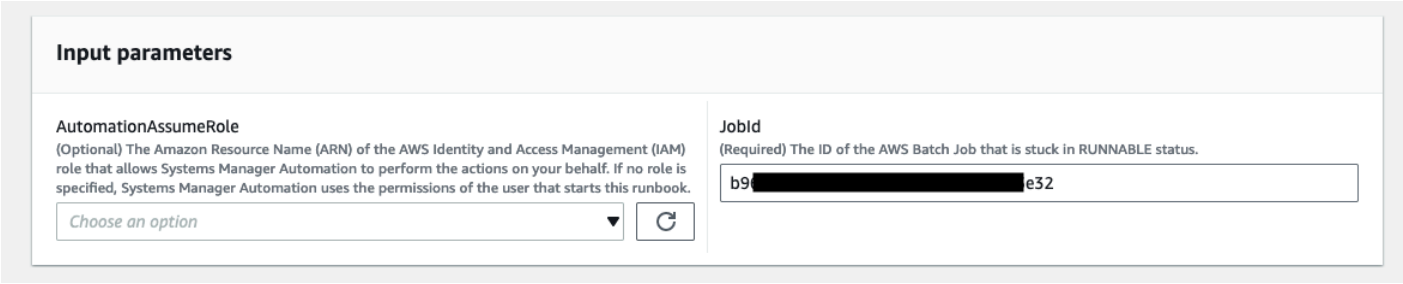
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetRequestHistory`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ecs:DescribeClusters`
- `ecs:DescribeContainerInstances`
- `ecs:ListContainerInstances`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListRoles`
- `iam:PassRole`
- `iam:SimulateCustomPolicy`
- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sts:GetCallerIdentity`

지침

1. AWS Systems Manager 콘솔에서 AWSSupport-T roubleshootAWSBatch Job으로 이동합니다.
2. 자동화 실행을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
   - AutomationAssumeRole(선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 () ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
   - JobId(필수):

현재 RUNNABLE 상태에 있는 AWS Batch Job의 ID입니다.



4. 실행을 선택합니다.
5. 자동화가 시작되는 것을 확인할 수 있습니다.
6. 문서는 다음 단계를 수행합니다.
   - PreflightPermissionChecks:

     시작한 사용자/역할에 대해 프리플라이트 IAM 권한 검사를 수행합니다. 누락된 권한이 있는 경우 이 단계는 글로벌 출력 섹션에서 누락된 API 작업을 제공합니다.
   - ProceedOnlyIfUserHasPermission:

     런북에 필요한 모든 작업에 대한 권한이 있는지 여부에 따라 분기합니다.
   - AWSBatchJobEvaluation:

     AWS Batch Job이 존재하고 RUNNABLE 상태인지 확인하는 검사를 수행합니다.
   - ProceedOnlyIfBatchJobExistsAndIsinRunnableState:

     작업이 존재하고 현재 RUNNABLE 상태인지 여부에 따라 분기합니다.
   - BatchComputeEnvironmentEvaluation:

     AWS Batch 컴퓨팅 환경을 대상으로 검사를 수행합니다.
   - ProceedOnlyIfComputeEnvironmentChecksAreOK:

     컴퓨팅 환경 검사 성공 여부에 따라 분기합니다.
   - UnderlyingInfraEvaluation:

     기본 Auto Scaling 그룹 또는 스팟 플릿 요청에 대해 검사를 수행합니다.
   - ProceedOnlyIfInstancesNotJoiningEcsCluster:

     Amazon ECS 클러스터에 가입하지 않는 인스턴스가 있는지 여부를 기준으로 분기합니다.
   - EcsAutomationRunner:

클러스터에 가입하지 않은 인스턴스에 대해 Amazon ECS 자동화를 실행합니다.

- ExecutionResults:

  이전 단계를 기반으로 출력을 생성합니다.

7. 작성이 완료되면 평가 보고서 URI HTML 파일용 파일이 제공됩니다.

   런북의 성공적인 실행에 대한 보고서를 URI 위한 S3 콘솔 링크 및 Amazon S3

▼ **Outputs**

ExecutionResults.message

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


✅[INFO]: Reviewing Compute Environment "ComputeEnvironment-eqMKnoNEEwNmt8eY":
⛔[ERROR]: Job "411[redacted]d606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-eqM[redacted]" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/updating-compute-environments.html
❗[WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-eqM[redacted]".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html
==============================================================
⛔[ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.



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

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

+++++++++++++++++++++++++++++
STEP:AWSBatchJobEvaluation
+++++++++++++++++++++++++++++
✅[INFO]: Job with ID "411[redacted]d606" exists and is in RUNNABLE status, proceeding further for next steps in execution.

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

✅[INFO]: Reviewing Compute Environment "ComputeEnvironment-eqMKnoNEEwNmt8eY":
⛔[ERROR]: Job "411[redacted]d606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-eqM[redacted]" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/updating-compute-environments.html
❗[WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-eqM[redacted]".
In general, we recommend the BEST_FIT strategy only when you want the lowest cost for your instance, and you are willing to trade cost for throughput and availability.
To favor availability, consider using BEST_FIT_PROGRESSIVE for on-demand and SPOT_CAPACITY_OPTIMIZED for spot. For more information see https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html
==============================================================
⛔[ERROR]: There is no Compute Environment attached to the Job's Queue that satisfies the conditions to run the Job.
Please double check above mentioned Compute Environments and errors.
```

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS CloudFormation

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS CloudFormation. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-DeleteCloudFormationStack
- AWS-EnableCloudFormationSNSNotification
- AWS-RunCfnLint
- AWSSupport-TroubleshootCFNCustomResource
- AWS-UpdateCloudFormationStack

AWS-DeleteCloudFormationStack

설명

AWS CloudFormation 스택을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니

다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- StackNameOrId

  유형: 문자열

  설명: (필수) 삭제할 CloudFormation 스택의 이름 또는 고유 ID입니다.

AWS-EnableCloudFormationSNSNotification

설명

`AWS-EnableCloudFormationSNSNotification`런북은 지정한 () 스택에 대한 Amazon 단순 알림 서비스 AWS CloudFormation (Amazon SNS AWS CloudFormation) 알림을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- StackArn

  타입: 문자열

설명: (필수) Amazon SNS 알림을 활성화하려는 AWS CloudFormation 스택의 ARN 또는 이름입니다.

- NotificationArn

  타입: 문자열

  설명: (필수) AWS CloudFormation 스택과 연결하려는 Amazon SNS 주제입니다. ARN

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- ssm: GetAutomationExecution
- ssm: StartAutomationExecution
- 클라우드 포메이션: DescribeStacks
- 클라우드 포메이션: UpdateStack
- kms:Decrypt
- kms: GenerateDataKey
- sns:Publish
- 예: GetQueueAttributes

문서 단계

- CheckCfnSnsLimits (`aws:executeScript`) - 지정한 AWS CloudFormation 스택과 아직 연결되지 않은 Amazon SNS 주제의 최대 개수를 확인합니다.
- EnableCfnSnsNotification (`aws:executeAwsApi`) - AWS CloudFormation 스택에 대한 Amazon SNS 알림을 활성화합니다.
- VerificationCfnSnsNotification (`aws:executeScript`) - AWS CloudFormation 스택에 Amazon SNS 알림이 활성화되었는지 확인합니다.

출력

CheckCfnSnsLimits. NotificationArnList - AWS CloudFormation 스택에 대한 Amazon SNS 알림을 수신하는 목록. ARNs

VerificationCfnSnsNotification. VerifySnsTopicsResponse - AWS CloudFormation 스택에 대해 Amazon SNS 알림이 활성화되었음을 확인하는 API 작업의 응답입니다.

AWS-RunCfnLint

설명

이 실행서에서는 AWS CloudFormation Linter(`cfn-python-lint`)를 사용하여 AWS CloudFormation 리소스 사양에 대해 YAML 및 JSON 템플릿의 유효성을 검사합니다. 이 `AWS-RunCfnLint` 실행서에서는 리소스 속성에 유효한 값이 입력되었는지 확인하는 등의 추가 검사를 수행합니다. 유효성 검사가 실패하면 `RunCfnLintAgainstTemplate` 단계가 실패하고 linter 도구의 출력이 오류 메시지에 제공됩니다. 이 실행서는 cfn-lint v0.24.4를 사용하고 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ConfigureRuleFlag

  유형: 문자열

  설명: (선택 사항) `--configure-rule` 파라미터에 전달할 규칙의 구성 옵션입니다.

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

- FormatFlag

  유형: 문자열

  설명: (선택 사항) 출력 형식을 지정하기 위해 `--format` 파라미터에 전달할 값입니다.

  유효한 값: Default | quiet | parseable | json

  기본값: Default

- IgnoreChecksFlag

  유형: 문자열

  설명: (선택 사항) --ignore-checks 파라미터에 전달할 규칙의 ID입니다. 이러한 규칙은 확인되지 않습니다.

  예: E1001,E1003,W7001

- IncludeChecksFlag

  유형: 문자열

  설명: (선택 사항) `--include-checks` 파라미터에 전달할 규칙의 ID입니다. 이러한 규칙이 확인이 됩니다.

  예: E1001,E1003,W7001

- InfoFlag

  유형: 문자열

  설명: `--info` (선택 사항) 파라미터에 대한 옵션입니다. 템플릿 처리에 대한 추가 로깅 정보를 사용하는 옵션을 포함합니다.

  기본값: false

- TemplateFileName

  유형: 문자열

  설명: S3 버킷에 있는 템플릿 파일의 이름 또는 키입니다.

- TemplateS3BucketName

유형: 문자열

설명: Packer 템플릿이 포함된 S3 버킷의 이름입니다.

- RegionsFlag

  유형: 문자열

  설명: (선택 사항) 지정된 AWS 리전에 대해 템플릿을 테스트하기 위해 `--regions` 파라미터에 전달할 값입니다.

  예: us-east-1,us-west-1

문서 단계

RunCfnLintAgainstTemplate - 지정된 AWS CloudFormation 템플릿에 대해 `cfn-python-lint` 도구를 실행합니다.

출력

RunCfnLintAgainstTemplate.output – `cfn-python-lint` 도구에서 나온 stdout입니다.

AWSSupport-TroubleshootCFNCustomResource

설명

`AWSSupport-TroubleshootCFNCustomResource` 실행서는 사용자 지정 리소스를 생성, 업데이트 또는 삭제할 때 AWS CloudFormation 스택이 실패한 이유를 진단하는 데 도움이 됩니다. 실행서는 사용자 지정 리소스에 사용된 서비스 토큰과 반환된 오류 메시지를 확인합니다. 사용자 지정 리소스의 세부 정보를 검토한 후, 실행서 출력본에는 스택 동작에 대한 설명과 사용자 지정 리소스의 문제 해결 단계가 제공됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- StackName

  유형: 문자열

  설명: (필수) 사용자 지정 리소스가 실패한 AWS CloudFormation 스택의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `validateCloudFormationStack` - AWS CloudFormation 스택이 동일한 AWS 계정 및 AWS 리전에 존재하는지 확인합니다.
- `checkCustomResource` - AWS CloudFormation 스택을 분석하고, 실패한 사용자 지정 리소스를 확인하고, 실패한 사용자 지정 리소스의 문제를 해결하는 방법에 대한 정보를 출력합니다.

AWS-UpdateCloudFormationStack

설명

Amazon S3 버킷에 저장된 AWS CloudFormation 템플릿을 사용하여 AWS CloudFormation 스택을 업데이트합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- LambdaAssumeRole

  유형: 문자열

  설명: (필수) ARN Lambda가 맡는 역할

- StackNameOrId

  유형: 문자열

  설명: (필수) 업데이트할 AWS CloudFormation 스택의 이름 또는 고유 ID
- TemplateUrl

  유형: 문자열

  설명: (필수) 업데이트된 CloudFormation 템플릿이 포함된 S3 버킷 위치 (예: `https://s3.amazonaws.com/amzn-s3-demo-bucket2/updated.template`)

CloudFront

AWS Systems Manager 자동화는 Amazon 에 사전 정의된 실행서를 제공합니다 CloudFront. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

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

AWSConfigRemediation-EnableCloudFrontDefaultRootObject

설명

`AWSConfigRemediation-EnableCloudFrontDefaultRootObject` 실행서는 사용자가 지정하는 Amazon CloudFront(CloudFront) 배포의 기본 루트 객체를 구성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- CloudFrontDistributionId

  유형: 문자열

  설명: (필수) 기본 루트 객체를 구성하려는 CloudFront 배포의 ID입니다.
- DefaultRootObject

  유형: 문자열

  설명: (필수) 뷰어 요청이 루트 URL을 가리킬 때 CloudFront에서 반환하려는 객체입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `CloudFrontDistributionId` 파라미터에 지정하는 CloudFront 배포의 기본 루트 객체를 구성합니다.

AWSConfigRemediation-EnableCloudFrontAccessLogs

설명

`AWSConfigRemediation-EnableCloudFrontAccessLogs`Runbook은 지정한 Amazon CloudFront (CloudFront) 배포에 대한 액세스 로깅을 가능하게 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- BucketName

  유형: 문자열

  설명: (필수) 액세스 로그를 저장할 Amazon Simple Storage Service(Amazon S3) 버킷의 이름입니다. af-south-1, ap-east-1, eu-south-1 및 me-south-1 AWS 리전의 버킷은 지원되지 않습니다.
- CloudFrontId

  유형: 문자열

  설명: (필수) 액세스 로깅을 활성화하려는 CloudFront 배포의 ID입니다.
- IncludeCookies

유형: 부울

유효한 값: true | false

설명: (필수) 액세스 로그에 `true` 쿠키를 포함하려면 이 매개 변수를 로 설정하십시오.

- 접두사

  유형: 문자열

  설명: (선택 사항) CloudFront 배포할 때 액세스 로그의 접두사로 `filenames` 사용할 선택적 문자열 (예:). `myprefix/`

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

> **Note**
>
> `s3:GetBucketLocation`API는 동일한 계정의 S3 버킷에만 사용할 수 있습니다. 계정 간 S3 버킷에는 사용할 수 없습니다.

문서 단계

- `aws:executeScript`- 파라미터에 지정한 CloudFront 배포에 대한 액세스 로깅을 활성화합니다`CloudFrontDistributionId`.

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity

설명

AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity 실행서는 지정하는 Amazon CloudFront(CloudFront) 배포에 대한 오리진 액세스 ID를 활성화합니다. 이 자동화는 지정하는 CloudFront 배포에 대한 오리진 액세스 ID 없이 Amazon Simple Storage Service(Amazon S3) 오리진 유형의 모든 오리진에 동일한 CloudFront 오리진 액세스 ID를 할당합니다. 이 자동화는 CloudFront가 Amazon S3 버킷의 객체에 액세스할 수 있도록 오리진 액세스 ID에 읽기 권한을 부여하지 않습니다. 액세스를 허용하려면 Amazon S3 버킷 권한을 업데이트해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- CloudFrontDistributionId

  유형: 문자열

  설명: (필수) 오리진 장애 조치를 활성화하려는 CloudFront 배포의 ID입니다.
- OriginAccessIdentityId

  유형: 문자열

설명: (필수) 오리진과 연결할 CloudFront 오리진 액세스 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `CloudFrontDistributionId` 파라미터에 지정하는 CloudFront 배포의 오리진 액세스 ID를 활성화하고, 오리진 액세스 ID가 할당되었는지 확인합니다.

AWSConfigRemediation-EnableCloudFrontOriginFailover

설명

`AWSConfigRemediation-EnableCloudFrontOriginFailover` 실행서는 사용자가 지정하는 Amazon CloudFront(CloudFront) 배포에 대한 오리진 장애 조치를 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

유형: 문자열

설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.

- CloudFrontDistributionId

  유형: 문자열

  설명: (필수) 오리진 장애 조치를 활성화하려는 CloudFront 배포의 ID입니다.

- OriginGroupId

  유형: 문자열

  설명: (필수) 오리진 그룹의 ID입니다.

- PrimaryOriginId

  유형: 문자열

  설명: (필수) 오리진 그룹의 기본 오리진 ID입니다.

- SecondaryOriginId

  유형: 문자열

  설명: (필수) 오리진 그룹의 보조 오리진 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `CloudFrontDistributionId` 파라미터에 지정한 CloudFront 배포에 대해 오리진 장애 조치를 활성화하고, 장애 조치가 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS

설명

AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS 실행서는 사용자가 지정하는 Amazon CloudFront(CloudFront) 배포에 대한 뷰어 프로토콜 정책을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- CloudFrontDistributionId

  유형: 문자열

  설명: (필수) 뷰어 프로토콜 정책을 활성화하려는 CloudFront 배포의 ID입니다.
- ViewerProtocolPolicy

  유형: 문자열

  유효한 값: https-only, redirect-to-https

  설명: (필수) 뷰어가 오리진에 있는 파일에 액세스하기 위해 사용할 수 있는 프로토콜입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `CloudFrontDistributionId` 파라미터에 지정한 CloudFront 배포에 대한 뷰어 프로토콜 정책을 활성화하고, 정책이 할당되었는지 확인합니다.

CloudTrail

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS CloudTrail. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

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

AWSConfigRemediation-CreateCloudTrailMultiRegionTrail

설명

`AWSConfigRemediation-CreateCloudTrailMultiRegionTrail` 실행서는 여러 개의 AWS 리전에서 선택한 Amazon Simple Storage Service(Amazon S3) 버킷으로 로그 파일을 전송하는 AWS CloudTrail(CloudTrail) 트레일을 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- BucketName

  유형: 문자열

  설명: (필수) 로그를 업로드하려는 Amazon S3 버킷의 이름입니다.
- KeyPrefix

  유형: 문자열

  설명: (선택 사항) 로그 파일 전송을 위해 지정한 버킷의 이름 다음에 오는 Amazon S3 키 접두사입니다.
- TrailName

  유형: 문자열

  설명: (필수) 생성할 CloudTrail 트레일의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeAwsApi` - 트레일 이름과 Amazon S3 버킷 이름을 입력으로 받아들이고 CloudTrail 트레일을 생성합니다.
- `aws:executeAwsApi` - 생성된 트레일에서 로깅을 활성화하고 지정한 Amazon S3 버킷으로 로그 전송을 시작합니다.
- `aws:assertAwsResourceProperty` - CloudTrail 트레일이 생성되었는지 확인합니다.

AWS-EnableCloudTrail

설명

AWS CloudTrail 트레일을 생성하고 S3 버킷에 대한 로깅을 구성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- S3BucketName

  유형: 문자열

  설명: (필수) 로그 파일을 게시하도록 지정된 S3 버킷의 이름입니다.

  > **Note**
  >
  > 이 S3 버킷이 존재해야 하며 버킷 정책이 쓰기 권한을 CloudTrail에 부여해야 합니다. 자세한 내용은 CloudTrail용 Amazon S3 버킷 정책을 참조하십시오.

- TrailName

  유형: 문자열

  설명: (필수) 새로운 트레일의 이름.

AWS-EnableCloudTrailCloudWatchLogs

설명

이 런북은 Amazon CloudWatch Logs 로그 그룹에 이벤트를 전송하기 위해 하나 이상의 AWS CloudTrail 트레일 구성을 업데이트합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- CloudWatchLogsLogGroupArn

  타입: 문자열

  설명: (필수) 로그가 전달될 CloudWatch 로그 로그 그룹의 ARN입니다. CloudTrail
- CloudWatchLogsRoleArn

  타입: 문자열

  설명: (필수) IAM 역할 CloudWatch 로그 로그의 ARN은 지정된 로그 그룹에 쓰는 것으로 가정합니다.
- TrailNames

  유형: StringList

  설명: (필수) Logs로 이벤트를 보내려는 CloudTrail CloudWatch 트레일의 이름을 쉼표로 구분한 목록입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript`- 지정된 CloudTrail 트레일을 업데이트하여 지정된 CloudWatch 로그 로그 그룹에 이벤트를 전송합니다.

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

설명

`AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS` 실행서는 지정하는 AWS Key Management Service(AWS KMS) 고객 관리형 키를 사용하여 AWS CloudTrail(CloudTrail) 트레일을 암호화합니다. 이 실행서는 CloudTrail 트레일이 최소 권장 보안 모범 사례에 따라 암호화되도록 하기 위한 기준으로만 사용해야 합니다. 서로 다른 KMS 키를 사용하여 여러 트레일을 암호화하는 것이 좋습니다. CloudTrail 다이제스트 파일은 암호화되지 않습니다. 이전에 트레일에 대해 `EnableLogFileValidation` 파라미터를 `true`로 설정한 경우, 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 예방적 보안 모범 사례 항목의 'AWS KMS 관리형 키를 사용한 서버 측 암호화 사용' 섹션을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.

- KMSKeyId

  유형: 문자열

  설명: (필수) `TrailName` 파라미터에 지정하는 트레일을 암호화하는 데 사용하려는 고객 관리형 키의 ARN, 키 ID 또는 키 별칭입니다.

- TrailName

  유형: 문자열

  설명: (필수) 암호화를 위해 업데이트하려는 트레일의 ARN 또는 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeAwsApi` - `TrailName` 파라미터에 지정하는 트레일에서 암호화를 활성화합니다.
- `aws:executeAwsApi` - `KMSKeyId` 파라미터에 지정하는 고객 관리형 키의 ARN을 수집합니다.
- `aws:assertAwsResourceProperty` - CloudTrail 트레일에서 암호화가 활성화되었는지 확인합니다.

AWS-EnableCloudTrailKmsEncryption

설명

이 런북은 AWS Key Management Service (AWS KMS) AWS CloudTrail 암호화를 사용하도록 하나 이상의 트레일 구성을 업데이트합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- KMS KeyId

  타입: 문자열

  설명: (필수) 파라미터에 지정한 트레일을 암호화하는 데 사용하려는 고객 관리 키의 키 ID입니다. `TrailName` 값은 “alias/”가 접두사로 붙은 별칭 이름, 별칭에 완전히 지정된 ARN 또는 키에 완전히 지정된 ARN일 수 있습니다.

- TrailNames

  유형: StringList

  설명: (필수) 암호화를 위해 업데이트하려는 트레일의 쉼표로 구분된 목록입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript`- 파라미터에 지정한 트레일의 AWS KMS 암호화를 활성화합니다. `TrailName`

AWSConfigRemediation-EnableCloudTrailLogFileValidation

설명

`AWSConfigRemediation-EnableCloudTrailLogFileValidation` 실행서는 AWS CloudTrail 트레일에 대한 로그 파일 검증을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- TrailName

유형: 문자열

설명: (필수) 로그 검증을 활성화하려는 트레일의 이름 또는 Amazon 리소스 이름(ARN)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeAwsApi` - `TrailName` 파라미터에 지정하는 AWS CloudTrail 트레일에 대한 로그 검증을 활성화합니다.
- `aws:assertAwsResourceProperty` - 트레일에 대한 로그 검증이 활성화되었는지 확인합니다.

AWS-EnableCloudTrailLogFileValidation

설명

`AWS-EnableCloudTrailLogFileValidation` 실행서는 지정한 AWS CloudTrail 추적에 대한 로그 파일 검증을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- TrailNames

  유형: StringList

  설명: (필수) 로그 검증을 활성화하려는 CloudTrail 추적 이름의 쉼표로 구분된 목록입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `TrailNames` 파라미터에서 지정한 AWS CloudTrail 추적에 대한 로그 검증을 활성화합니다.

AWS-QueryCloudTrailLogs

설명

`AWS-QueryCloudTrailLogs` 실행서는 선택한 Amazon Simple Storage Service(Amazon S3) 버킷에서 AWS CloudTrail (CloudTrail) 로그를 포함하는 Amazon Athena 테이블을 생성합니다. 테이블을 생성한 후, 자동화는 사용자가 지정하는 SQL 쿼리를 실행한 다음 테이블을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 쿼리

  유형: 문자열

  설명: (필수) 실행하려는 SQL 쿼리입니다.
- SourceBucketPath

  유형: 문자열

  설명: (필수) 쿼리하려는 CloudTrail 로그 파일이 포함된 Amazon S3 버킷의 이름입니다.
- TableName

  유형: 문자열

  설명: (선택 사항) 자동화로 생성된 Athena 테이블의 이름입니다.

  기본값: cloudtrail_logs

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeAwsApi` - Athena 테이블을 생성합니다.
- `aws:executeAwsApi` - `Query` 파라미터에 지정하는 쿼리 문자열을 실행합니다.
- `aws:executeScript` - 폴링하고 쿼리가 완료될 때까지 기다립니다.
- `aws:executeAwsApi` - 쿼리 결과를 가져옵니다.
- `aws:executeAwsApi` - 자동화로 생성된 테이블을 삭제합니다.

CloudWatch

AWS Systems Manager 자동화는 Amazon 에 사전 정의된 런북을 제공합니다 CloudWatch. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-ConfigureCloudWatchOnEC2Instance
- AWS-EnableCWAlarm

AWS-ConfigureCloudWatchOnEC2Instance

설명

관리형 인스턴스에 대한 Amazon CloudWatch 세부 모니터링을 활성화하거나 비활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) CloudWatch 모니터링을 활성화하려는 Amazon EC2 인스턴스의 ID입니다.
- 속성

유형: 문자열

설명: (선택 사항) 이 파라미터는 지원되지 않습니다. 이전 버전과의 호환성을 위해 여기에 나열되어 있습니다.

- 상태

  유효한 값: Enabled | Disabled

  설명: (선택 사항) CloudWatch를 활성화할지 또는 비활성화할지를 지정합니다.

  기본값: Enabled

문서 단계

configureCloudWatch - 지정된 상태로 Amazon EC2 인스턴스에서 CloudWatch를 구성합니다.

출력

이 자동화에는 출력이 없습니다.

AWS-EnableCWAlarm

설명

`AWS-EnableCWAlarm`Runbook은 사용자의 리소스 중 아직 AWS 계정 없는 AWS 리소스에 대해 Amazon CloudWatch (CloudWatch) 경보를 생성합니다. CloudWatch 경보는 다음 리소스에 대해 생성됩니다. AWS

- Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스
- Amazon Elastic Block Store(Amazon EBS) 볼륨
- Amazon Simple Storage Service(Amazon S3) 버킷
- 아마존 관계형 데이터베이스 서비스 (Amazon RDS) 클러스터

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ComparisonOperator

  타입: 문자열

  유효한 값: GreaterThanOrEqualToThreshold | | GreaterThanThreshold GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpper 임계값 | | LessThanLowerThreshold LessThanOrEqualToThreshold LessThanThreshold

  설명: (필수) 지정된 통계와 임계값을 비교할 때 사용할 산술 연산입니다.
- MetricName

  타입: 문자열

  설명: (필수) 경보와 관련된 지표의 이름입니다.
- 기간

  타입: 정수

  유효한 값: 10 | 30 | 60 | 60의 배수

  설명: (필수) 통계가 적용되는 기간 (초) 입니다.
- 리소스 ARN

  유형: StringList

설명: (필수) 경보를 생성할 리소스의 쉼표로 구분된 ARN 목록 CloudWatch

- 통계

  타입: 문자열

  유효한 값: 평균 | 최대값 | 최소값 | | 합계 SampleCount

  설명: (필수) 경보와 관련된 지표의 통계입니다.

- Threshold

  타입: 정수

  설명: (필수) 지정된 통계와 비교할 값입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `cloudwatch:PutMetricAlarm`

문서 단계

- `aws:executeScript`- 파라미터에 지정한 리소스에 대해 런북 파라미터에 지정된 값에 따라 CloudWatch 알람을 `ResourceARNs` 생성합니다.

출력

LCWalarm을 활성화합니다. FailedResources: CloudWatch 경보가 생성되지 않은 리소스 ARN과 실패 사유의 맵목록입니다.

CWalArm을 활성화합니다. SuccessfulResources: CloudWatch 경보가 성공적으로 생성된 리소스 ARN 목록입니다.

Amazon DocumentDB

AWS Systems Manager 자동화는 Amazon DocumentDB(MongoDB 호환성 포함)에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-EnableDocDbClusterBackupRetentionPeriod

AWS-EnableDocDbClusterBackupRetentionPeriod

설명

AWS-EnableDocDbClusterBackupRetentionPeriod런북은 지정한 Amazon DocumentDB 클러스터의 백업 보존 기간을 활성화합니다. 이 기능은 자동 백업이 보존되는 총 일수를 설정합니다. 클러스터를 수정하려면 클러스터가 엔진 유형이 인 가용 상태여야 합니다. docdb

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- DBClusterResourceId

  타입: 문자열

  설명: (필수) 백업 보존 기간을 활성화하려는 Amazon DocumentDB 클러스터의 리소스 ID입니다.
- BackupRetentionPeriod

유형: 정수

설명: (필수) 자동 백업이 유지되는 기간 (일). 7~35일 사이의 값이어야 합니다.

- PreferredBackupWindow

  타입: 문자열

  설명: (선택 사항) hh24:mm-hh24:mm 형식의 협정 세계시 (UTC) 로 표시된 일일 시간 범위 (예: 07:14-07:44). 값은 30분 이상이어야 하며 기본 유지 관리 기간과 충돌하지 않아야 합니다.

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

문서 단계

- GetDocDbClusterIdentifier (`aws:executeAwsApi`) - 제공된 리소스 ID를 사용하여 Amazon DocumentDB 클러스터 식별자를 반환합니다.
- VerifyDocDbEngine (`aws:assertAwsResourceProperty`) - Amazon DocumentDB 엔진 `docdb` 유형이 다른 Amazon 엔진 유형에 대한 의도치 않은 변경을 방지하기 위한 것인지 확인합니다. RDS
- VerifyDocDbStatus (`aws:waitAwsResourceProperty`) - Amazon DocumentDB 클러스터 상태가 다음과 같은지 확인합니다. `available`
- ModifyDocDbRetentionPeriod (`aws:executeAwsApi`) - 지정된 Amazon DocumentDB 클러스터에 제공된 값을 사용하여 보존 기간을 설정합니다.
- VerifyDocDbBackupsEnabled (`aws:executeScript`) - Amazon DocumentDB 클러스터의 보존 기간과 기본 백업 기간 (지정된 경우) 이 성공적으로 설정되었는지 확인합니다.

출력

ModifyDocDbRetentionPeriod. ModifyDbClusterResponse - `ModifyDBCluster` API 수술로 인한 응답.

VerifyDocDbBackupsEnabled. VerifyDbClusterBackupsEnabledResponse - Amazon DocumentDB 클러스터의 성공적인 수정을 확인하는 `VerifyDocDbBackupsEnabled` 단계의 출력입니다.

CodeBuild

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS CodeBuild. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK
- AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

`AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK`

설명

`AWSConfigRemediation-ConfigureCodeBuildProjectWithKMSCMK`Runbook은 지정한 AWS CodeBuild (CodeBuild) 고객 관리 키를 사용하여 () 프로젝트의 빌드 아티팩트를 암호화합니다. AWS Key Management Service AWS KMS AWS Config 이 자동화를 실행하는 AWS 리전 곳에서 활성화해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다.

- KMS KeyId

  타입: 문자열

  설명: (필수) 파라미터에 지정한 CodeBuild 프로젝트를 암호화하는 데 사용하려는 AWS KMS 고객 관리 키의 Amazon 리소스 이름 (ARN) 입니다. `ProjectId`

- ProjectId

  타입: 문자열

  설명: (필수) 암호화하려는 빌드 아티팩트가 있는 CodeBuild 프로젝트의 ID.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeAwsApi`- 프로젝트 ID에서 CodeBuild 프로젝트 이름을 수집합니다.
- `aws:executeAwsApi`- `ProjectId` 파라미터에 지정한 CodeBuild 프로젝트의 암호화를 활성화합니다.
- `aws:assertAwsResourceProperty`- CodeBuild 프로젝트에 암호화가 활성화되었는지 확인합니다.

출력

UpdateLambdaConfig. UpdateFunctionConfigurationResponse - `UpdateFunctionConfiguration` API 호출의 응답입니다.

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

설명

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject 실행서는 지정하는 AWS CodeBuild (CodeBuild) 프로젝트에서 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY 환경 변수를 삭제합니다. 이 자동화를 실행하는 AWS 리전에서 AWS Config가 활성화되어야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- ResourceId

  유형: 문자열

  설명: (필수) 삭제하려는 액세스 키 환경 변수가 있는 CodeBuild 프로젝트의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `ResourceId` 파라미터에 지정된 CodeBuild 프로젝트의 액세스 키 환경 변수를 삭제합니다.

AWS CodeDeploy

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS CodeDeploy. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-TroubleshootCodeDeploy

`AWSSupport-TroubleshootCodeDeploy`

설명

`AWSSupport-TroubleshootCodeDeploy` 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 AWS CodeDeploy 배포가 실패한 이유를 진단하는 데 도움이 됩니다. 실행서는 문제 해결이나 추가 문제 해결에 도움이 되는 단계를 출력합니다. 향후 유사한 문제를 방지하는 데 도움이 되는 CodeDeploy 모범 사례도 제공합니다.

이 실행서는 다음 문제를 해결하는 데 도움이 될 수 있습니다.

- CodeDeploy 에이전트가 Amazon EC2 인스턴스에 설치되어 있지 않거나 실행되고 있지 않습니다.
- Amazon EC2 인스턴스에는 연결된 AWS Identity and Access Management (IAM) 인스턴스 프로파일이 없습니다.
- Amazon EC2 인스턴스에 연결된 IAM 인스턴스 프로파일에는 필요한 Amazon Simple Storage Service(Amazon S3) 권한이 없습니다.

- Amazon S3에 저장된 수정 버전이 누락되었거나 사용된 Amazon S3 버킷이 Amazon EC2 인스턴스와 다른 AWS 리전에 있습니다.
- 애플리케이션 사양(AppSpec) 파일 문제
- “파일이 해당 위치에 이미 존재합니다” 오류
- CodeDeploy 관리형 수명 주기 이벤트 후크 실패
- 고객 관리형 수명 주기 이벤트 후크 실패
- 배포 중 이벤트 축소

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- DeploymentId

  유형: 문자열

  설명: (필수) 실패한 배포의 ID입니다.
- InstanceId

  유형: 문자열

설명: (필수) 배포가 실패한 Amazon EC2 인스턴스의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeAwsApi` - `DeploymentId` 및 `InstanceId` 파라미터에 제공된 값을 확인합니다.
- `aws:executeScript` - Amazon EC2 인스턴스에서 인스턴스 상태 및 IAM 인스턴스 프로파일 세부 정보와 같은 정보를 수집합니다.
- `aws:executeScript` - 지정된 배포를 검토하고 배포가 실패한 이유에 대한 분석을 반환합니다.

AWS Config

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Config. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-SetupConfig

AWSSupport-SetupConfig

설명

`AWSSupport-SetupConfig` 실행서는 AWS Identity and Access Management (IAM) 서비스 연결 역할, AWS Config 기반 구성 레코더, AWS Config가 구성 스냅샷과 구성 기록 파일을 전송하는 Amazon Simple Storage Service(Amazon S3) 버킷이 포함된 전송 채널을 생성합니다. `AggregatorAccountId` 및 `AggregatorAccountRegion` 파라미터의 값을 지정하면, 실행서는 또한 데이터 집계에 대한 권한을 생성하여 여러 개의 AWS 계정와 AWS 리전에서 AWS Config 구성 및

규정 준수 데이터를 수집합니다. 여러 계정 및 리전의 데이터를 집계하는 것에 대해 자세히 알아보려면 AWS Config 개발자 안내서의 다중 계정 다중 리전 데이터 집계를 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- AggregatorAccountId

  유형: 문자열

  설명: (선택 사항) 복수의 계정 및 AWS 리전으로부터 AWS Config 구성 및 규정 준수 데이터를 집계하기 위해 추가할 집계자 AWS 계정의 ID입니다. 이 계정은 집계자가 소스 계정을 승인하는 데도 사용됩니다.

- AggregatorAccountRegion

  유형: 문자열

  설명: (선택 사항) 복수의 계정 및 리전으로부터 AWS Config 구성 및 규정 준수 데이터를 집계하기 위해 추가할 집계자의 리전입니다.

- IncludeGlobalResourcesRegion

유형: 문자열

기본값: us-east-1

설명: (필수) 각 리전에 글로벌 리소스 데이터가 기록되지 않도록 하려면 글로벌 리소스 데이터를 기록할 리전 한 개를 지정하세요.

- 파티션

  유형: 문자열

  기본값: `aws`

  설명: (필수) AWS Config 구성 및 규정 준수 데이터를 수집하려는 파티션입니다.

- S3BucketName

  유형: 문자열

  기본값: `aws-config-delivery-channel`

  설명: (선택 사항) 전송 채널용으로 생성된 Amazon S3 버킷에 적용할 이름입니다. 이름 끝에 계정 ID가 추가됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeScript` - AWS Config에 대한 서비스 연결 IAM 역할이 아직 존재하지 않는 경우 생성합니다.
- `aws:executeScript` - 구성 레코더가 아직 존재하지 않는 경우 생성합니다.
- `aws:executeScript` - 전송 채널에서 사용할 Amazon S3 버킷이 아직 존재하지 않는 경우 생성합니다.
- `aws:executeScript` - 실행서에서 생성한 리소스를 사용하여 전송 채널을 생성합니다.
- `aws:executeAwsApi` - 구성 레코더를 시작합니다.
- `aws:executeScript` - `AggregatorAccountId` 및 `AggregatorAccountRegion` 파라미터 값을 지정한 경우 다중 계정 및 다중 리전 데이터 집계에 대한 승인이 구성됩니다.

Amazon Connect

AWS Systems Manager 자동화는 Amazon Connect용 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-AssociatePhoneNumbersToConnectContactFlows
- AWSSupport-CollectAmazonConnectContactFlowLog

`AWSSupport-AssociatePhoneNumbersToConnectContactFlows`

설명

전화번호를 Amazon Connect 인스턴스의 통화 흐름에 연결하는 `AWSSupport-AssociatePhoneNumbersToConnectContactFlows` 데 도움이 됩니다. 전화 번호와 통화 흐름의 매핑을 쉼표로 구분된 값 (CSV) 입력 파일에 제공함으로써 Runbook은 14.5분 내에 가능한 한 많은 전화 번호를 통화 흐름에 연결합니다. 런북은 제한 시간 내에 연결할 수 없었던 모든 전화 번호 및 통화 흐름 쌍의 CSV 파일을 생성하므로 다음 실행 시 입력할 수 있습니다.

어떻게 작동하나요?

런북을 AWSSupport-AssociatePhoneNumbersToConnectContactFlows 사용하면 Amazon Simple Storage Service (Amazon S3) 버킷에 저장된 매핑 데이터 CSV 파일을 사용하여 Amazon Connect 인스턴스의 통화 흐름에 전화번호를 연결할 수 있습니다. 입력 CSV 파일은 E.164 형식의 PhoneNumber 값을 포함하여 다음 형식에 맞아야 합니다.

입력 파일의 예 CSV

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

또한 자동화 런북은 DestinationFileBucket 및 DestinationFilePath 에 지정된 대상 위치에 다음 파일을 생성합니다.

- **automation:EXECUTION_ID/ResourceIdList.csv**: 에 필요한 PhoneNumberId 및 ContactFlowId 쌍이 들어 있는 임시 파일입니다. AssociatePhoneNumberContactFlow API
- **automation:EXECUTION_ID/ErrorResourceList.csv**: 의 형식과 같은 ResourceNotFoundException 오류로 인해 처리할 수 없는 전화 번호와 통화 흐름 쌍이 들어 있는 PhoneNumber,ContactFlowName,ErrorMessage 파일입니다.
- **automation:EXECUTION_ID/NonProcessedResourceList.csv**: 처리되지 않은 전화 번호와 통화 흐름 쌍이 포함된 파일입니다. 런북은 14.5분 (AWS Lambda 함수 타임아웃 15분 - 버퍼 30초) 내에 최대한 많은 전화번호와 통화 흐름을 처리하려고 합니다. 시간 제약으로 인해 처리할 수 없는 전화 번호/통화 흐름이 있는 경우 런북은 해당 번호를 CSV 파일에 포함시켜 다음 런북 실행을 위한 입력으로 사용합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems `AWSSupport-AssociatePhoneNumbersToConnectContactFlows`Manager의 문서 아래로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - AutomationAssumeRole (선택 사항)

Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.

- ConnectInstanceId (필수)

  아마존 커넥트 인스턴스의 ID.

- SourceFileBucket (필수)

  전화번호와 통화 흐름 쌍이 포함된 CSV 파일을 저장하는 Amazon S3 버킷입니다.

- SourceFilePath (필수)

  전화번호와 통화 흐름 쌍이 포함된 CSV 파일의 Amazon S3 객체 키. 예: `path/to/input.csv`.

- DestinationFileBucket (필수)

  자동화가 중간 파일 및 결과 보고서를 배치할 Amazon S3 버킷입니다.

- DestinationFilePath (선택 사항)

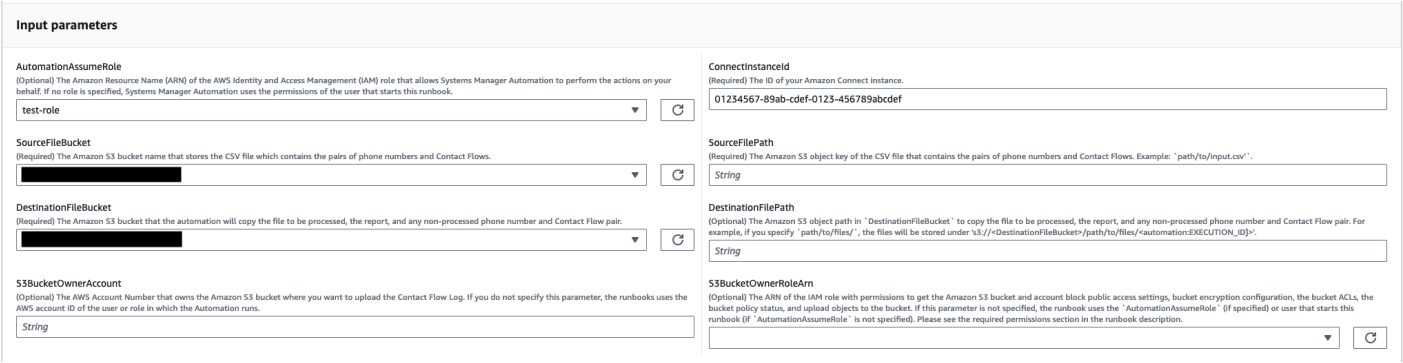
  중간 파일 및 결과 보고서가 저장되어야 하는 Amazon S3 객체 경로입니다. `DestinationFileBucket` 예를 들어`path/to/files/`, 지정하면 파일이 에 저장됩니다`s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/`.

- S3 BucketOwnerAccount (선택 사항)

  통화 흐름 로그를 업로드하려는 Amazon S3 버킷을 소유한 AWS 계정 번호입니다. 이 파라미터를 지정하지 않으면 Runbook은 자동화가 실행되는 사용자 또는 역할의 AWS 계정 ID를 사용합니다.

- S3 BucketOwnerRoleArn (선택 사항)

  Amazon S3 버킷 및 계정 블록 공개 액세스 설정, 버킷 암호화 구성, 버킷, 버킷 정책 상태를 가져오고 버킷에 객체를 업로드할 수 있는 권한이 있는 IAM 역할. ARN ACLs 이 파라미터가 지정되지 않은 경우, 런북은 이 런북을 시작하는 사용자 `AutomationAssumeRole` (지정된 경우) 또는 사용자 (지정되지 않은 경우`AutomationAssumeRole`) 를 사용합니다. 실행서 설명의 필수 권한 섹션을 참조하세요.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - CheckConnectInstanceExistance

     에서 제공한 Amazon Connect 인스턴스가 `ConnectInstanceId` 존재하는지 확인합니다.
   - 체크 S3 BucketPublicStatus

     에 지정된 Amazon S3 버킷이 `SourceFileBucket` 익명 또는 공개 읽기 또는 쓰기 액세스 권한을 `DestinationFileBucket` 허용하는지 확인합니다.
   - CheckSourceFileExistenceAndSize

     에서 지정한 소스 CSV 파일이 `SourceFilePath` 존재하는지, 파일 크기가 25MiB 제한을 초과하는지 확인합니다.
   - GenerateResourceIdMap

     및 ID `SourceFilePath` 및 각 리소스에 지정된 소스 CSV 파일을 다운로드합니다. `PhoneNumberId` `ContactFlowId` 작업이 완료되면,, 가 포함된 CSV `PhoneNumber` 파일을 에서 `DestinationFileBucket` 지정한 대상 Amazon S3 `ContactFlowId` 버킷에 업로드합니다. `PhoneNumberId` `ContactFlowName` 특정 개수로 `PhoneNumberId` 식별할 수 없는 경우 CSV 파일은 파일에서 비어 있게 됩니다.
   - AssociatePhoneNumbersToContactFlows

     AWS CloudFormation 스택을 사용하여 계정에 AWS Lambda 함수를 생성합니다. AWS Lambda 함수는 `SourceFileBucket` `SourceFilePath` 및 에 지정된 소스 CSV 파일에 나열된 통화 흐름에 각 번호를 연결하고 AWS CloudFormation 스택은 함수를 호출합니다. 이 AWS Lambda 함수는 제한 시간이 초과되기 전 (15분) 가능한 한 많은 전화 번호를 통화 흐름에 매핑합니다. 오류로 인해 처리하지 못한 전화번호 및 통화 흐름 목록이 업

로드됩니다`[automation:EXECUTION_ID]/ErrorResourceList.csv`. 한 번의 실행으로 처리할 수 있는 최대 전화번호 수를 초과하여 처리할 수 없었던 전화번호는 에 업로드됩니다`[automation:EXECUTION_ID]/NonProcessedResourceList.csv`. 이 단계가 실패하면 AWS CloudFormation 스택 이벤트에서 실패한 이유를 보여주는 `DescribeCloudFormationErrorFromStackEvents` 단계로 이동합니다.

- WaitForPhoneNumberContactFlowAssociationCompletion

  전화 번호를 통화 흐름에 매핑하는 AWS Lambda 함수가 생성되고 AWS CloudFormation 스택이 호출을 완료할 때까지 기다립니다.

- GenerateReport

  통화 흐름에 매핑된 전화 번호 수, 오류로 인해 처리할 수 없는 전화 번호 및 단일 실행으로 처리할 수 있는 최대 전화 번호 수를 초과하여 처리할 수 없는 전화 번호가 포함된 보고서를 생성합니다. 보고서에는 `[automation:EXECUTION_ID]/ErrorResourceList.csv` 또는 `[automation:EXECUTION_ID]/NonProcessedResourceList.csv` 해당하는 경우 위치 (Amazon S3 URI 및 Amazon S3 콘솔URL) 도 표시됩니다.

- **`DeleteCloudFormationStack`**

  매핑을 위한 Lambda 함수를 포함하여 AWS CloudFormation 스택을 삭제합니다.

- **`DescribeCloudFormationErrorFromStackEvent`**

  단계 AWS CloudFormation 스택의 오류를 설명합니다. `AssociatePhoneNumbersToContactFlows`

7. 완료 후 출력 섹션에서 실행의 세부 결과를 검토하십시오.

- GenerateReport.OutputPayload

  전화번호 및 통화 흐름 연결 출력. 이 보고서에는 다음 정보가 포함됩니다.

  - 입력 CSV 파일에 나열된 전화 번호 및 통화 흐름 쌍의 수
  - 입력 CSV 파일에 지정된 통화 흐름과 관련된 전화번호 수
  - 오류로 인해 통화 흐름에 연결할 수 없는 전화번호 수
  - 시간 제약으로 인해 통화 흐름과 연결되지 않은 전화번호 수
  - 오류로 인해 연결할 수 없는 전화 번호와 통화 흐름 쌍이 포함된 CSV 파일의 위치 (Amazon S3 URI 및 Amazon S3 콘솔URL)
  - 시간 제약으로 인해 연결되지 않은 전화 번호와 통화 흐름 쌍이 포함된 CSV 파일의 위치 (Amazon S3 URI 및 Amazon S3 콘솔URL)

- DescribeCloudFormationErrorFromStackEvents.이벤트

  `AssociatePhoneNumbersToContactFlows`단계가 실패할 경우 AWS CloudFormation 스택 이벤트를 표시하는 출력입니다.

적은 수의 전화번호와 통화 흐름을 사용한 실행 출력

```
▼ Outputs

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

GenerateReport.OutputPayload
{"Payload":"

==================================================
    Amazon Connect Phone Number Mapping Result
==================================================

* Phone number and Contact Flow pairs listed in the provided input: 7
* Phone numbers associated with Contact Flow processed: 7
* Phone numbers that could not be associated with Contact Flow due to an error: 0
* Phone numbers that weren't associated with Contact Flow due to the time constraint: 0


"}
```

오류나 시간 제약으로 인해 연결되지 않은 전화 번호, 통화 흐름 및 전화 번호가 많이 포함된 실행 결과

```
▼ Outputs

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

GenerateReport.OutputPayload
{"Payload":"

==================================================
    Amazon Connect Phone Number Mapping Result
==================================================

* Phone number and Contact Flow pairs listed in the provided input: 1634
* Phone numbers associated with Contact Flow processed: 1153
* Phone numbers that could not be associated with Contact Flow due to an error: 8
* Phone numbers that weren't associated with Contact Flow due to the time constraint: 473


==================================================
            Error list file location
==================================================

* S3 URI: s3://[redacted]/ErrorResourceList.csv
* S3 Console URL: https://s3.console.aws.amazon.com/s3/object/[redacted]ErrorResourceList.csv

INFO: The above file contains the list of phone numbers and Contact Flows that could not be associated due to an error.You can look into the error detail in order to address the issue.

==================================================
          Unprocessed list file location
==================================================

* S3 URI: s3://[redacted]/NonProcessedResourceList.csv
* S3 Console URL: https://s3.console.aws.amazon.com/s3/object/[redacted]/NonProcessedResourceList.csv

INFO: The above file contains the list of phone numbers and Contact Flows that weren't associated due to the time constraint (15 minutes).You can execute this runbook again by specifying the file as an input \"SourceFileLocation\" so that you can process them.

"}
```

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWSSupport-CollectAmazonConnectContactFlowLog

설명

`AWSSupport-CollectAmazonConnectContactFlowLog`자동화 런북은 특정 연락처 ID에 대한 Amazon Connect 통화 흐름 로그를 수집하는 데 사용됩니다. Amazon Connect 인스턴스 ID와 연락처 ID를 제공하면, 런북은 Amazon CloudWatch 로그 그룹에서 연락처 흐름 로그를 검색하여 요청 파라미터에 지정된 Amazon Simple Storage Service (Amazon S3) 버킷에 업로드합니다. 런북은 로그를 다운로드할 수 있는 Amazon S3 콘솔 URL 및 AWS CLI 명령을 제공하는 출력을 생성합니다.

어떻게 작동하나요?

`AWSSupport-CollectAmazonConnectContactFlowLog`자동화 런북은 구성된 CloudWatch 로그 그룹에 저장된 특정 연락처 ID에 대한 Amazon Connect 통화 흐름 로그를 수집하여 지정된 Amazon S3 버킷에 업로드하는 데 도움이 됩니다. Amazon Connect 통화 흐름에서 수집된 로그의 보안을 지원하기 위해 자동화는 Amazon S3 버킷 구성을 평가하여 해당 버킷이 퍼블릭 `read` 또는 `write` 액세스 권한을 부여하고 `S3BucketOwnerAccountId` 파라미터에 지정된 AWS 계정이 소유하는지 확인합니다. Amazon S3 버킷에서 AWS Key Management Service 키 (SSE-KMS) 를 사용한 서버 측 암호화를 사용하는 경우, 이 자동화를 실행하는 사용자 또는 AWS Identity and Access Management (IAM) 역할에 해당 키에 대한 `kms:GenerateDataKey` 권한이 있는지 확인하십시오. AWS KMS Amazon Connect 인스턴스에서 생성되는 로그에 대한 자세한 내용은 Amazon CloudWatch 로그 그룹에 저장된 흐름 로그를 참조하십시오.

> **Important**
>
> CloudWatch Logs Insights 쿼리에는 쿼리된 데이터 양에 따라 요금이 부과됩니다. 프리 티어 고객은 서비스 할당량을 초과하는 사용에 대해서만 요금이 부과됩니다. 자세한 내용은 Amazon CloudWatch 요금을 참조하십시오.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems AWSSupport-CollectAmazonConnectContactFlowLogManager의 문서 아래로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - ConnectInstanceId (필수):

     아마존 커넥트 인스턴스의 ID.
   - ContactId (필수):

     통화 흐름 로그를 수집하려는 연락처의 ID.
   - S3 BucketName (필수):

     통화 흐름 로그를 업로드하려는 계정의 Amazon S3 버킷 이름. 수집된 로그에 액세스할 필요가 없는 당사자에게 버킷 정책이 불필요한 읽기/쓰기 권한을 부여하지 않도록 하십시오.
   - S3 ObjectPrefix (선택 사항):

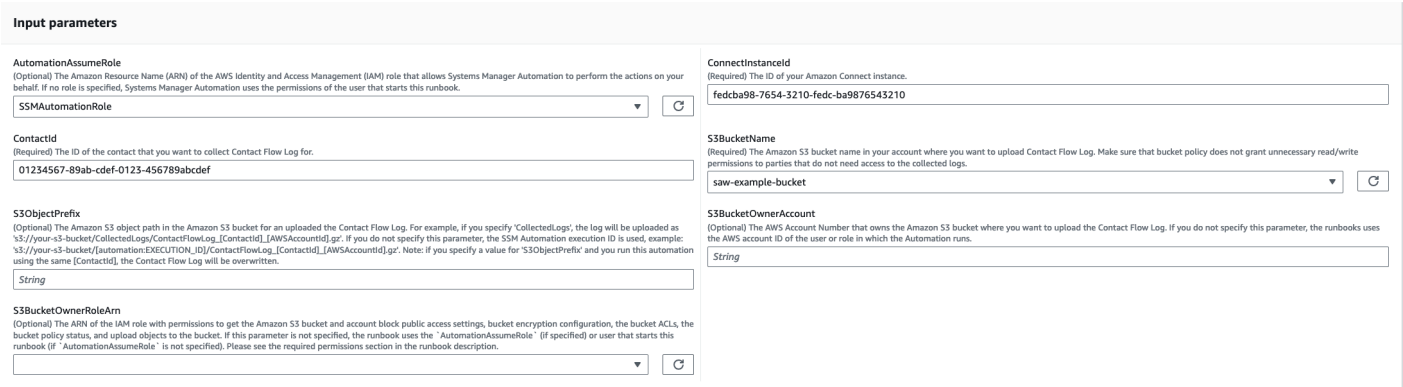
     업로드된 통화 흐름 로그의 Amazon S3 버킷의 Amazon S3 객체 경로입니다. 예를 들어`CollectedLogs`, 지정하면 로그가 다음과 같이 업로드됩니다`s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId][AWSAccountId].gz`. 이 매개변수를 지정하지 않으면 Systems Manager 자동화 실행 ID가 사용됩니다 (예:)`s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz`. 참고: 값을 지정하고 동일한 [ContactId] 를 사용하여 이 자동화를 실행하면 통화 흐름 로그를 덮어씁니다. `S3ObjectPrefix`

- S3 BucketOwnerAccount (선택 사항):

  통화 흐름 로그를 업로드하려는 Amazon S3 버킷을 소유한 AWS 계정 번호입니다. 이 파라미터를 지정하지 않으면 Runbook은 자동화가 실행되는 사용자 또는 역할의 AWS 계정 ID를 사용합니다.

- S3 BucketOwnerRoleArn (선택 사항):

  Amazon S3 버킷 및 계정 블록 공개 액세스 설정, 버킷 암호화 구성, 버킷, 버킷 정책 상태를 가져오고 ACLs 버킷에 객체를 업로드할 수 있는 권한이 있는 IAM 역할입니다. ARN 이 파라미터가 지정되지 않은 경우, 런북은 이 런북을 시작하는 사용자 `AutomationAssumeRole` (지정된 경우) 또는 사용자 (지정되지 않은 경우`AutomationAssumeRole`) 를 사용합니다. 런북 설명의 필수 권한 섹션을 참조하십시오.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.

   - CheckConnectInstanceExistance

     에 제공된 Amazon Connect 인스턴스가 맞는지 확인합니다`ACTIVE`. `ConnectInstanceId`

   - 체크 3 BucketPublicStatus

     에 지정된 Amazon S3 버킷이 익명 또는 공개 읽기 또는 쓰기 액세스 권한을 `S3BucketName` 허용하는지 확인합니다.

   - GenerateLogSearchTimeRange

     `EndTime`를 기반으로 `StartTime` 및 에서 `LastUpdateTimestamp` 반환한 `StartQuery` 단계를 생성하고 생성합니다 `DescribeContactAPI`. `InitiationTimestamp` `StartTime`한 시간 `InitiationTimestamp` 전이고 한 시간 후가 될 `EndTime` 것입니다`LastUpdateTimestamp`.

   - StartQuery

제공된 `ContactId` Amazon Connect 인스턴스와 관련된 로그 로그 그룹에 제공된 항목의 쿼리 CloudWatch 로그를 시작합니다`ConnectInstanceId`. 런타임 60분 후 쿼리 제한 시간이 초과되었습니다. 쿼리 제한 시간이 초과되면 검색되는 시간 범위를 줄이세요. CloudWatch 콘솔에서 현재 진행 중인 쿼리와 최근 쿼리 기록을 볼 수 있습니다. 자세한 내용은 실행 중인 쿼리 또는 쿼리 기록 보기를 참조하십시오.

- WaitForQueryCompletion

  제공된 CloudWatch `ContactId` 로그 쿼리 로그가 완료될 때까지 기다립니다. 런타임 60분 후 쿼리 제한 시간이 초과되는 것을 확인할 수 있습니다. 쿼리 제한 시간이 초과되면 검색되는 시간 범위를 줄이세요. Amazon Connect 콘솔에서 현재 진행 중인 쿼리와 최근 쿼리 기록을 볼 수 있습니다. 자세한 내용은 실행 중인 쿼리 또는 쿼리 기록 보기를 참조하십시오.

- UploadContactFlowLog

  쿼리 결과를 가져와 에서 `S3BucketName` 지정한 Amazon S3 버킷에 통화 흐름 로그를 업로드합니다.

- GenerateReport

  통화 흐름 URL 로그가 업로드된 Amazon S3 콘솔과 로그 파일을 다운로드하는 데 사용할 수 있는 예제 AWS CLI 명령을 반환합니다.

7. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토하십시오.

   - GenerateReport.OutputPayload

     런북이 지정된 연락처에 대한 통화 흐름 로그를 성공적으로 검색했음을 알려주는 출력입니다. 이 보고서에는 Amazon S3 URL 콘솔과 로그 파일을 다운로드할 수 있는 예제 AWS CLI 명령도 포함되어 있습니다.

```
▼ Outputs

GenerateReport.OutputPayload
{"Payload":"

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

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

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

- S3 Console URL for the Contact Flow Log file
https://s3.console.aws.amazon.com/s3/object/saw-example-bucket?region=us-west-2&prefix=01234567-89ab-cdef-0123-456789abcdef/ContactFlowLog_01234567-89ab-cdef-0123-456789abcdef_123456789012.gz


Alternatively, you can download the log file by using the AWS CLI command below:
```
aws s3 cp s3://saw-example-bucket/01234567-89ab-cdef-0123-456789abcdef/ContactFlowLog_01234567-89ab-cdef-0123-456789abcdef_123456789012.gz . --region us-west-2
```
```

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS Directory Service

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Directory Service. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

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

`AWS-CreateDSManagementInstance`

설명

`AWS-CreateDSManagementInstance` 실행서는 AWS Directory Service 디렉터리를 관리하는 데 사용할 수 있는 Amazon Elastic Compute Cloud(Amazon EC2) Windows 인스턴스를 생성합니다. 관리 인스턴스는 AD Connector 디렉터리를 관리하는 데 사용할 수 없습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- AmiID

  유형: 문자열

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

  설명: (필수) 관리 인스턴스를 시작하는 데 사용하려는 Amazon Machine Image(AMI)의 ID입니다.

- DirectoryId

  유형: 문자열

  설명: (필수) 관리하려는 AWS Directory Service 디렉터리의 ID입니다. 인스턴스는 지정하는 디렉터리에 연결됩니다.

- IamInstanceProfileName

  유형: 문자열

  설명: (필수) 지정하는 이름은 자동화로 생성되고, 관리 인스턴스에 연결되는 IAM 인스턴스 프로파일에 적용됩니다.

- InstanceType

  유형: 문자열

  기본값: t3.medium

  허용된 값:

  - 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

설명: (필수) 시작하려는 인스턴스 유형입니다.

- KeyPairName

  유형: 문자열

  설명: (선택 사항) 새 인스턴스를 생성할 때 사용할 키 페어입니다. 값을 지정하지 않으면 인스턴스는 키 페어를 연결하지 않습니다.

- RemoteAccessCidr

  유형: 문자열

  설명: (필수) RDP 트래픽(포트 3389)을 허용하려는 CIDR 블록입니다. 지정하는 CIDR 블록은 자동화로 생성된 보안 그룹에 추가된 인바운드 규칙에 적용됩니다.

- SecurityGroupName

  유형: 문자열

  설명: (필수) 지정하는 이름은 자동화로 생성되고 관리 인스턴스와 연결된 보안 그룹에 적용됩니다.

- 태그

  형식: MapList

설명: (선택 사항) 자동화로 생성된 리소스에 적용하려는 키-값 페어입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeAwsApi` - `DirectoryId` 파라미터에서 지정하는 디렉터리에 대한 세부 정보를 수집합니다.
- `aws:executeAwsApi` - 디렉터리가 시작된 Virtual Private Cloud(VPC)의 CIDR 블록을 가져옵니다.
- `aws:executeAwsApi` - `SecurityGroupName` 파라미터에서 지정하는 값을 사용하여 보안 그룹을 생성합니다.
- `aws:executeAwsApi` - `RemoteAccessCidr` 파라미터에서 지정하는 CIDR로부터 RDP 트래픽을 허용하는 새로 생성된 보안 그룹에 대한 인바운드 규칙을 생성합니다.
- `aws:executeAwsApi` - `IamInstanceProfileName` 파라미터에서 지정하는 값을 사용하여 IAM 역할 및 인스턴스 프로파일을 생성합니다.
- `aws:executeAwsApi` - 실행서 파라미터에서 지정하는 값을 기반으로 Amazon EC2 인스턴스를 시작합니다.
- `aws:executeAwsApi` - 새로 시작한 인스턴스를 디렉터리에 연결할 AWS Systems Manager 문서를 생성합니다.
- `aws:runCommand` - 새 인스턴스를 디렉터리에 연결합니다.

- `aws:runCommand` - 새 인스턴스에 원격 서버 관리 도구를 설치합니다.

`AWSSupport-TroubleshootADConnectorConnectivity`

설명

`AWSSupport-TroubleshootADConnectorConnectivity` 실행서는 AD Connector에 대한 다음 사전 요구 사항을 확인합니다.

- 필요한 트래픽이 AD Connector와 연결된 보안 그룹 및 네트워크 액세스 제어 목록 (ACL) 규칙에서 허용되는지 확인합니다.
- AWS Systems Manager, AWS Security Token Service, Amazon CloudWatch 인터페이스 VPC 엔드포인트가 AD Connector와 동일한 가상 사설 클라우드 (VPC) 에 있는지 확인합니다.

사전 요구 사항 검사가 성공적으로 완료되면 런북은 AD Connector와 동일한 서브넷에서 두 개의 Amazon Elastic Compute Cloud (AmazonEC2) Linux t2.micro 인스턴스를 시작합니다. 그런 다음, `netcat` 및 `nslookup` 유틸리티를 사용하여 네트워크 연결 테스트를 수행합니다.

이 자동화 실행(콘솔)

> **Important**
>
> 이 런북을 사용하면 자동화 중에 생성된 Amazon EC2 인스턴스, Amazon Elastic Block Store 볼륨 및 Amazon Machine Image (AMI) 에 AWS 계정 대해 추가 요금이 부과될 수 있습니다. 자세한 내용은 Amazon Elastic Compute Cloud 요금 및 Amazon Elastic Block Store 요금을 참조하세요.
>
> `aws:deletestack`단계가 실패할 경우 AWS CloudFormation 콘솔로 이동하여 스택을 수동으로 삭제하십시오. 이 실행서에서 만든 스택 이름은 `AWSSupport-TroubleshootADConnectorConnectivity`로 시작합니다. AWS CloudFormation 스택 삭제에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 스택 삭제를 참조하십시오.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- DirectoryId

  유형: 문자열

  설명: (필수) 연결 문제를 해결하려는 AD Connector 디렉터리의 ID입니다.
- Ec2 InstanceProfile

  유형: 문자열

  최대 문자 수: 128

  설명: (필수) 연결 테스트를 수행하기 위해 시작된 인스턴스에 할당하려는 인스턴스 프로파일의 이름입니다. 사용자가 지정하는 인스턴스 프로파일에는 `AmazonSSMManagedInstanceCore` 정책 또는 이에 상응하는 권한이 연결되어 있어야 합니다.

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:assertAwsResourceProperty` - `DirectoryId` 파라미터에 지정된 디렉터리가 AD Connector인지 확인합니다.
- `aws:executeAwsApi` - AD Connector에 대한 정보를 수집합니다.
- `aws:executeAwsApi` - AD Connector와 연결된 보안 그룹에 대한 정보를 수집합니다.
- `aws:executeAwsApi`- AD Connector의 서브넷과 연결된 네트워크 ACL 규칙에 대한 정보를 수집합니다.
- `aws:executeScript` - AD Connector 보안 그룹 규칙을 평가하여 필요한 아웃바운드 트래픽이 허용되는지 확인합니다.
- `aws:executeScript`- AD Connector 네트워크 ACL 규칙을 평가하여 필요한 아웃바운드 및 인바운드 네트워크 트래픽이 허용되는지 확인합니다.
- `aws:executeScript`- AWS Systems Manager,, Amazon CloudWatch 인터페이스 엔드포인트가 AD AWS Security Token Service Connector와 VPC 동일한 위치에 존재하는지 확인합니다.
- `aws:executeScript` - 이전 단계에서 수행한 검사의 출력을 컴파일합니다.

- `aws:branch` - 이전 단계의 출력에 따라 자동화를 분기합니다. 보안 그룹 및 네트워크에 필요한 아웃바운드 및 인바운드 규칙이 없는 경우 여기서 자동화가 중지됩니다. ACLs
- `aws:createStack`- Amazon EC2 인스턴스를 시작하여 연결 테스트를 수행하기 위한 AWS CloudFormation 스택을 생성합니다.
- `aws:executeAwsApi`- 새로 시작된 Amazon EC2 인스턴스를 수집합니다. IDs
- `aws:waitForAwsResourceProperty`- 새로 시작한 첫 번째 Amazon EC2 인스턴스가 관리 대상으로 보고될 때까지 기다립니다. AWS Systems Manager
- `aws:waitForAwsResourceProperty`- 새로 시작한 두 번째 Amazon EC2 인스턴스가 관리 대상으로 보고될 때까지 기다립니다. AWS Systems Manager
- `aws:runCommand`- 첫 번째 Amazon EC2 인스턴스의 온프레미스 DNS 서버 IP 주소에 대한 네트워크 연결 테스트를 수행합니다.
- `aws:runCommand`- 두 번째 Amazon EC2 인스턴스의 온프레미스 DNS 서버 IP 주소에 대한 네트워크 연결 테스트를 수행합니다.
- `aws:changeInstanceState`- 연결 테스트에 사용된 Amazon EC2 인스턴스를 중지합니다.
- `aws:deleteStack`- AWS CloudFormation 스택을 삭제합니다.
- `aws:executeScript`- 자동화가 스택 삭제에 실패할 경우 AWS CloudFormation 스택을 수동으로 삭제하는 방법에 대한 지침을 출력합니다.

`AWSSupport-TroubleshootDirectoryTrust`

설명

`AWSSupport-TroubleshootDirectoryTrust` 실행서는 AWS Managed Microsoft AD와 Microsoft Active Directory 간의 신뢰 생성 문제를 진단합니다. 자동화는 디렉터리 유형이 신뢰를 지원하는지 확인한 다음 연결된 보안 그룹 규칙, 네트워크 액세스 제어 목록(네트워크 ACL) 및 라우팅 테이블에서 잠재적인 연결 문제를 확인합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- DirectoryId

  유형: 문자열

  허용 패턴: ^d-[a-z0-9]{10}$

  설명: (필수) 문제를 해결할 AWS Managed Microsoft AD의 ID입니다.
- RemoteDomainCidrs

  형식: StringList

  허용 패턴: ^(([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]))$

  설명: (필수) 신뢰 관계를 설정하려는 원격 도메인의 CIDR입니다. 쉼표로 구분된 값을 사용하여 여러 CIDR을 추가할 수 있습니다. 예: 172.31.48.0/20, 192.168.1.10/32.
- RemoteDomainName

  유형: 문자열

  설명: (필수) 신뢰 관계를 설정할 원격 도메인의 정규화된 도메인 이름입니다.
- RequiredTrafficACL

  유형: 문자열

  설명: (필수) AWS Managed Microsoft AD에 대한 기본 포트 요구 사항입니다. 대부분의 경우 기본값을 수정하면 안 됩니다.

기본값: {"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

  유형: 문자열

  설명: (필수) AWS Managed Microsoft AD에 대한 기본 포트 요구 사항입니다. 대부분의 경우 기본값을 수정하면 안 됩니다.

  기본값: {"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

  유형: 문자열

  설명: (선택 사항) 문제를 해결할 신뢰 관계의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:assertAwsResourceProperty` - 디렉터리 유형이 AWS Managed Microsoft AD인지 확인합니다.
- AWS Managed Microsoft AD - `aws:executeAwsApi`에 대한 정보를 가져옵니다.

- `aws:branch` - `TrustId` 입력 파라미터에 값이 제공된 경우 자동화를 분기합니다.
- `aws:executeAwsApi` - 신뢰 관계에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - `RemoteDomainName`에 대한 조건부 전달자 DNS IP 주소를 가져옵니다.
- `aws:executeAwsApi` - AWS Managed Microsoft AD에 추가된 IP 라우팅에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - AWS Managed Microsoft AD 서브넷의 CIDR을 가져옵니다.
- `aws:executeAwsApi` - AWS Managed Microsoft AD와 연결된 보안 그룹에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - AWS Managed Microsoft AD와 연결된 네트워크 ACL에 대한 정보를 가져옵니다.
- `aws:executeScript` - `RemoteDomainCidrs` 값이 유효한지 확인합니다. `RemoteDomainCidrs`가 RFC 1918 IP 주소가 아닌 경우 AWS Managed Microsoft AD에 `RemoteDomainCidrs`에 대한 조건부 전달자가 있고, 필수 IP 라우팅이 AWS Managed Microsoft AD에 추가되었는지 확인합니다.
- `aws:executeScript` - 보안 그룹 규칙을 평가합니다.
- `aws:executeScript` - 네트워크 ACL을 평가합니다.

출력

evalDirectorySecurityGroup.output - AWS Managed Microsoft AD와 연결된 보안 그룹 규칙이 신뢰 생성에 필요한 트래픽을 허용하는지 평가한 결과입니다.

evalAclEntries.output - AWS Managed Microsoft AD와 연결된 네트워크 ACL이 신뢰 생성에 필요한 트래픽을 허용하는지 평가한 결과입니다.

evaluateRemoteDomainCidr.output - `RemoteDomainCidrs`가 유효한 값인지 평가한 결과입니다. `RemoteDomainCidrs`가 RFC 1918 IP 주소가 아닌 경우 AWS Managed Microsoft AD에 `RemoteDomainCidrs`에 대한 조건부 전달자가 있고, 필수 IP 라우팅이 AWS Managed Microsoft AD에 추가되었는지 확인합니다.

AWS AppSync

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS AppSync. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-EnableAppSyncGraphQLApiLogging

AWS-EnableAppSyncGraphQLApiLogging

설명

`AWS-EnableAppSyncGraphQLApiLogging`런북은 지정한 GraphQL API에 대한 필드 수준 로깅 및 요청 수준 로깅을 활성화합니다AWS AppSync. 런북은 로깅이 이미 활성화된 경우에도 지정된 GraphQL API에 변경 사항을 적용합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ApiId

  유형: 문자열

  설명: (필수) 로깅을 활성화하려는 API의 ID입니다.

- FieldLogLevel

  유형: 문자열

  유효한 값: 오류 | 모두

  설명: (필수) 필드 로깅 수준.
- CloudWatchLogsRoleArn

  유형: 문자열

  설명: (필수) Amazon Logs에 게시하는 AWS AppSync 것으로 가정하는 서비스 역할의 ARN입니다. CloudWatch
- ExcludeVerboseContent

  유형: 부울

  기본값: False

  설명: (선택 사항) 로깅 수준에 관계없이 헤더, 컨텍스트, 평가된 매핑 템플릿과 같은 정보를 `True` 제외하도록 설정합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- aws: executeAwsApi - 기본 인증 유형과 관련된 인증 유형 및 구성 정보를 수집합니다.
- aws:branch - 인증 유형을 기반으로 브랜치를 생성합니다.
- aws: executeAwsApi - 런북의 입력 매개변수에 지정된 값을 기반으로 GraphQL API의 로깅 구성을 업데이트합니다. AWS AppSync

출력

- `EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse`: 호출의 응답입니다. `UpdateGraphqlApi`
- `EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse`: `UpdateGraphqlApi` 전화 응답.
- `EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse`: `UpdateGraphqlApi` 전화 응답.
- `EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse`: `UpdateGraphqlApi` 전화 응답.

Amazon Athena

AWS Systems Manager 자동화는 Amazon Athena 에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-EnableAthenaWorkGroupEncryptionAtRest

AWS-EnableAthenaWorkGroupEncryptionAtRest

설명

`AWS-EnableAthenaWorkGroupEncryptionAtRest`런북은 지정한 Amazon Athena 워크그룹에 대해 저장 중 암호화를 지원합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- WorkGroup

  유형: 문자열

  설명: (필수) 저장 중 암호화를 활성화하려는 워크그룹입니다.

- EncryptionOption

  유형: 문자열

  유효한 값: SSE_S3 | SSE_KMS | CSE_KMS

  설명: (필수) 사용할 암호화 옵션을 지정합니다. Amazon S3 관리 키를 사용한 서버 측 암호화 (SSE_S3), 관리 키를 사용한 서버 측 암호화 (SSE_KMS) 또는 AWS KMS 관리 키를 사용한 클라이언트 측 암호화 (CSE_KMS) 를 선택할 수 있습니다. AWS KMS

- KmsKeyId

  유형: 문자열

  설명: (선택 사항) AWS KMS 암호화 옵션을 사용하는 경우 사용할 키의 키 ARN, 키 ID 또는 키 별칭을 지정합니다.

- EnableMinimumEncryptionConfiguration

  유형: 부울

  기본값: True

  설명: (선택 사항) Amazon S3에 기록된 쿼리 및 계산 결과에 대해 워크그룹에 최소 수준의 암호화를 적용합니다. 활성화된 경우 워크그룹 사용자는 관리자가 설정한 최소 수준 또는 쿼리를 제출할 때 그

이상 수준으로만 암호화를 설정할 수 있습니다. 이 설정은 Spark 지원 워크그룹에는 적용되지 않습니다.

- EnforceWorkGroupConfiguration

  유형: 부울

  기본값: True

  설명: (선택 사항) 로 설정하면 워크그룹 설정이 `True` 클라이언트측 설정보다 우선합니다. 로 설정하면 클라이언트측 설정이 `False` 사용됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- aws:branch - 파라미터에 지정된 암호화 옵션을 기반으로 브랜치합니다. `EncryptionOption`
- aws: executeAwsApi - 이 단계는 지정된 암호화 설정으로 Athena Work Group을 업데이트합니다.
- aws: executeAwsApi - 지정된 암호화 설정으로 Athena 작업 그룹을 업데이트합니다.
- aws: assertAwsResource 속성 - 워크그룹에 대한 암호화가 활성화되었는지 확인합니다.

DynamoDB

AWS Systems Manager 자동화는 Amazon DynamoDB용 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-ChangeDDBRWCapacityMode
- AWS-CreateDynamoDBBackup

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

AWS-ChangeDDBRWCapacityMode

설명

`AWS-ChangeDDBRWCapacityMode`런북은 하나 이상의 Amazon DynamoDB (DynamoDB) 테이블에 대한 읽기/쓰기 용량 모드를 온디맨드 모드 또는 프로비저닝 모드로 변경합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- CapacityMode

타입: 문자열

유효한 값: 프로비저닝됨 | PAY_PER_REQUEST

설명: (필수) 원하는 읽기/쓰기 용량 모드. on-demand (pay-per-request) 에서 프로비저닝된 용량으로 전환할 때는 초기 프로비저닝 용량 값을 설정해야 합니다. 초기 프로비저닝 용량 값은 지난 30분 동안 테이블과 글로벌 보조 인덱스의 사용된 읽기 및 쓰기 용량을 기반으로 추정됩니다.

- ReadCapacityUnits

  타입: 정수

  기본값: 0

  설명: (선택 사항) DynamoDB가 제한 예외를 반환하기 전에 소비되는 초당 매우 일관된 읽기의 최대 수입니다.

- TableNames

  타입: 문자열

  설명: (필수) 읽기/쓰기 용량 모드를 변경할 DynamoDB 테이블 이름을 쉼표로 구분한 목록입니다.

- WriteCapacityUnits

  타입: 정수

  기본값: 0

  설명: (선택 사항) DynamoDB가 제한 예외를 반환하기 전에 소비되는 초당 최대 쓰기 수입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript`- 파라미터에 지정된 DynamoDB 테이블의 읽기/쓰기 용량 모드를 변경합니다. `TableNames`

출력

DBRW를 CapacityMode 변경했습니다. SuccessesTables - 용량 모드가 성공적으로 변경된 DynamoDB 테이블 이름 목록

DBRW를 변경했습니다. CapacityMode FailedTables - 용량 모드 변경이 실패한 DynamoDB 테이블 이름 및 실패 원인 맵 목록입니다.

AWS-CreateDynamoDBBackup

설명

Amazon DynamoDB 테이블의 백업본을 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- BackupName

  유형: 문자열

설명: (필수) 생성할 백업의 이름입니다.

- LambdaAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 자동화에서 생성된 Lambda를 통해 작업을 수행할 수 있도록 허용하는 역할의 ARN입니다. 지정하지 않을 경우 Lambda 함수를 실행할 임시 역할이 생성됩니다.

- TableName

  유형: 문자열

  설명: (필수) DynamoDB 테이블의 이름입니다.

AWS-DeleteDynamoDbBackup

설명

Amazon DynamoDB 테이블의 백업을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니

다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- BackupArn

  유형: 문자열

  설명: (필수) 삭제할 DynamoDB 테이블 백업의 ARN입니다.

AWSConfigRemediation-DeleteDynamoDbTable

설명

`AWSConfigRemediation-DeleteDynamoDbTable` 실행서는 지정한 Amazon DynamoDB(DynamoDB) 테이블을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- TableName

  유형: 문자열

  설명: (필수) 삭제하려는 DynamoDB 테이블의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `TableName` 파라미터에 지정된 DynamoDB 테이블을 삭제합니다.
- `aws:executeScript` - DynamoDB 테이블이 삭제되었는지 확인합니다.

AWS-DeleteDynamoDbTableBackups

설명

보존 일수 또는 개수에 따라 DynamoDB 테이블 백업을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스

파라미터

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- LambdaAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 자동화에서 생성된 Lambda를 통해 작업을 수행할 수 있도록 허용하는 역할의 ARN입니다. 지정하지 않을 경우 Lambda 함수를 실행할 임시 역할이 생성됩니다.

- RetentionCount

  유형: 문자열

  기본값: 10

  설명: (선택 사항) 테이블에 대해 보존할 백업 수입니다. 지정한 개수보다 많은 백업이 존재하는 경우 해당 개수를 초과하면 가장 오래된 백업이 삭제됩니다. RetentionCount 또는 RetentionDays를 사용할 수 있지만, 둘 다 사용할 수는 없습니다.

- RetentionDays

  유형: 문자열

  설명: (선택 사항) 테이블의 백업을 보존할 일수입니다. 지정한 일수보다 오래된 백업은 삭제됩니다. RetentionCount 또는 RetentionDays를 사용할 수 있지만, 둘 다 사용할 수는 없습니다.

- TableName

  유형: 문자열

  설명: (필수) DynamoDB 테이블의 이름입니다.

AWSConfigRemediation-EnableEncryptionOnDynamoDbTable

설명

`AWSConfigRemediation-EnableEncryptionOnDynamoDbTable`런북은 파라미터에 지정한 () 고객 관리 키를 사용하여 AWS Key Management Service Amazon DynamoDB (DynamoDB) 테이블을 암호화합니다.AWS KMS`KMSKeyId`

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- KMS KeyId

  타입: 문자열

  설명: (필수) `TableName` 파라미터에 지정하는 DynamoDB 테이블을 암호화하는 데 사용할 고객 관리형 키에 대한 ARN입니다.
- TableName

  타입: 문자열

  설명: (필수) 암호화하려는 DynamoDB 테이블의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `dynamodb:UpdateTable`

문서 단계

- `aws:executeAwsApi` - `TableName` 파라미터에 지정한 DynamoDB 테이블을 암호화합니다.
- `aws:waitForAwsResourceProperty` - DynamoDB 테이블의 `SSESpecification`에 대한 `Enabled` 속성이 `true`로 설정되었는지 확인합니다.
- `aws:assertAwsResourceProperty` - DynamoDB 테이블이 `KMSKeyId` 파라미터에 지정된 고객 관리형 키로 암호화되었는지 확인합니다.

AWSConfigRemediation-EnablePITRForDynamoDbTable

설명

`AWSConfigRemediation-EnablePITRForDynamoDbTable` 실행서는 지정하는 Amazon DynamoDB 테이블에서 특정 시점으로 복구(PITR)를 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.

- TableName

  유형: 문자열

  설명: (필수) 특정 시점으로 복구를 활성화하기 위한 DynamoDB 테이블의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeAwsApi` - `TableName` 파라미터에 지정하는 DynamoDB 테이블에서 특정 시점으로 복구를 활성화합니다.
- `aws:assertAwsResourceProperty` - DynamoDB 테이블에서 특정 시점으로 복구가 활성화되었는지 확인합니다.

AWS-EnableDynamoDbAutoscaling

설명

`AWS-EnableDynamoDbAutoscaling`런북은 지정한 프로비저닝 용량 Amazon DynamoDB 테이블에 대해 Application Auto Scaling을 활성화합니다. Application Auto Scaling은 트래픽 패턴에 따라 프로비저닝된 처리 용량을 동적으로 조정합니다. 자세한 내용은 Amazon DynamoDB 개발자 안내서의 DynamoDB 자동 크기 조정을 통한 처리 용량 자동 관리를 참조하십시오.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- TableName

  타입: 문자열

  설명: (필수) Application Auto Scaling을 활성화하려는 DynamoDB 테이블의 이름입니다.
- MinReadCapacity

  유형: 정수

  설명: (필수) DynamoDB 테이블에 프로비저닝된 처리량 읽기 용량 단위의 최소 수입니다.
- MaxReadCapacity

  유형: 정수

  설명: (필수) DynamoDB 테이블에 프로비저닝된 처리량 읽기 용량 단위의 최대 수입니다.
- TargetReadCapacityUtilization

  유형: 정수

  설명: (필수) 원하는 목표 읽기 용량 사용률. 목표 사용률은 특정 시점에 사용된 프로비저닝된 처리량의 백분율입니다. Auto Scaling 목표 사용률 값을 20~ 90% 사이로 설정할 수 있습니다.
- ReadScaleOutCooldown

  유형: 정수

  설명: (필수) 이전 읽기 용량 확장 활동이 적용될 때까지 대기하는 시간 (초) 입니다.
- ReadScaleInCooldown

유형: 정수

설명: (필수) 읽기 용량 확장 활동이 완료된 후 다른 확장 활동을 시작할 수 있는 시간 (초) 입니다.

- MinWriteCapacity

  유형: 정수

  설명: (필수) DynamoDB 테이블에 프로비저닝된 처리량 쓰기 유닛의 최소 수입니다.

- MaxWriteCapacity

  유형: 정수

  설명: (필수) DynamoDB 테이블에 프로비저닝된 처리량 쓰기 유닛의 최대 수입니다.

- TargetWriteCapacityUtilization

  유형: 정수

  설명: (필수) 원하는 목표 쓰기 용량 사용률. 목표 사용률은 특정 시점에 사용된 프로비저닝된 처리량의 백분율입니다. Auto Scaling 목표 사용률 값을 20~ 90% 사이로 설정할 수 있습니다.

- WriteScaleOutCooldown

  유형: 정수

  설명: (필수) 이전 쓰기 용량 확장 작업이 적용될 때까지 기다리는 시간 (초) 입니다.

- WriteScaleInCooldown

  유형: 정수

  설명: (필수) 쓰기 용량 확장 작업이 완료된 후 다른 확장 작업을 시작할 수 있는 시간 (초) 입니다.

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `application-autoscaling:PutScalingPolicy`
- `application-autoscaling:RegisterScalableTarget`

- RegisterAppAutoscalingTargetWrite (`aws:executeAwsApi`) - 지정한 DynamoDB 테이블에서 Application Auto Scaling을 구성합니다.
- RegisterAppAutoscalingTargetWriteDelay (`aws:sleep`) - 스로틀링을 방지하기 위해 휴면 모드로 전환합니다. API
- PutScalingPolicyWrite (`aws:executeAwsApi`) - DynamoDB 테이블의 목표 쓰기 용량 사용률을 구성합니다.
- PutScalingPolicyWriteDelay (`aws:sleep`) - 스로틀링을 방지하기 위해 휴면 모드로 전환합니다. API
- RegisterAppAutoscalingTargetRead (`aws:executeAwsApi`) - DynamoDB 테이블의 최소 및 최대 읽기 용량 단위를 구성합니다.
- RegisterAppAutoscalingTargetReadDelay (`aws:sleep`) - 스로틀링을 방지하기 위해 휴면 모드로 전환합니다. API
- PutScalingPolicyRead (`aws:executeAwsApi`) - DynamoDB 테이블의 목표 읽기 용량 사용률을 구성합니다.
- VerifyDynamoDbAutoscalingEnabled (`aws:executeScript`) - 지정한 값에 따라 DynamoDB 테이블에 대해 Application Auto Scaling이 활성화되었는지 확인합니다.

출력

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

AWS-RestoreDynamoDBTable

설명

`AWS-RestoreDynamoDBTable` 실행서는 특정 시점으로 복구(PITR)를 사용하여 지정하는 Amazon DynamoDB 테이블을 복원합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- EnablePointInTimeRecoverAsNeeded

  유형: 부울

  기본값: true

  설명: (선택 사항) 테이블을 복원하는 데 필요한 경우 자동화를 통해 특정 시점으로 복구를 활성화할지 여부를 결정합니다.
- GlobalSecondaryIndexOverride

  유형: 문자열

  설명: (선택 사항) 새 테이블의 기존 보조 인덱스를 대체하는 새 글로벌 보조 인덱스입니다.
- LocalSecondaryIndexOverride

  유형: 문자열

  설명: (선택 사항) 새 테이블의 기존 보조 인덱스를 대체하는 새 로컬 보조 인덱스입니다.

- RestoreDateTime

  유형: 문자열

  설명: (필수) 최근 35일 중 테이블을 복원하려는 특정 시점으로의 복구입니다. `DD/MM/YYYY HH:MM:SS` 형식을 사용해 날짜와 시간을 지정합니다.
- SourceTableArn

  유형: 문자열

  설명: (필수) 복원하려는 테이블의 ARN입니다.
- SseSpecificationOverride

  유형: 문자열

  설명: (선택 사항) 새 테이블에 사용할 서버 측 암호화 설정입니다.
- TargetTableName

  유형: 문자열

  설명: (필수) 복원할 테이블의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - 특정 시점으로 복구를 사용하여 `TargetTableName` 파라미터에 지정하는 DynamoDB 테이블을 복원합니다.

Amazon EBS

AWS Systems Manager 자동화는 Amazon Elastic Block Store에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- 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`

설명

`AWSSupport-AnalyzeEBSResourceUsage`자동화 런북은 Amazon Elastic Block Store (AmazonEBS) 의 리소스 사용량을 분석하는 데 사용됩니다. 볼륨 사용량을 분석하고 특정 지역에서 중단된 볼륨, 이미지 및 스냅샷을 식별합니다. AWS

어떻게 작동하나요?

런북은 다음 네 가지 작업을 수행합니다.

1. Amazon Simple Storage 서비스 (Amazon S3) 버킷이 있는지 확인하거나 새 Amazon S3 버킷을 생성합니다.
2. 사용 가능한 상태의 모든 Amazon EBS 볼륨을 수집합니다.
3. 소스 볼륨이 삭제된 모든 Amazon EBS 스냅샷을 수집합니다.
4. 종료되지 않은 Amazon Elastic Compute Cloud (AmazonAMIs) 인스턴스에서 사용하지 않는 모든 Amazon 머신 이미지 () 를 수집합니다. EC2

Runbook은 CSV 보고서를 생성하여 사용자가 제공한 Amazon S3 버킷에 저장합니다. 제공된 버킷은 마지막에 설명된 AWS 보안 모범 사례에 따라 보호되어야 합니다. 사용자가 제공한 Amazon S3 버킷이 계정에 없는 경우, Runbook은 사용자 지정 AWS Key Management Service (AWS KMS) 키로 암호화하고`<User-provided-name>-awssupport-YYYY-MM-DD`, 객체 버전 관리를 활성화하고, 퍼블릭 액세스를 차단하고, 요청에서 /를 사용하도록 SSL 요구하는 이름 형식의 새 Amazon S3 버킷을 생성합니다. TLS

Amazon S3 버킷을 직접 지정하려면 다음 모범 사례에 따라 구성해야 합니다.

- 버킷에 대한 퍼블릭 액세스를 차단합니다 (`IsPublic`로 설정`False`).
- Amazon S3 액세스 로깅을 활성화합니다.
- 버킷에 SSL 대한 요청만 허용합니다.
- 객체 버전 관리를 활성화합니다.
- AWS Key Management Service (AWS KMS) 키를 사용하여 버킷을 암호화합니다.

> **Important**
>
> 이 런북을 사용하면 Amazon S3 버킷 및 객체 생성 시 계정에 추가 요금이 부과될 수 있습니다. 발생할 수 있는 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하십시오.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- S3 BucketName

  유형: `AWS::S3::Bucket::Name`

  설명: (필수) 보고서를 업로드할 계정의 Amazon S3 버킷입니다. 버킷 정책이 수집된 로그에 액세스할 필요가 없는 당사자에게 불필요한 읽기/쓰기 권한을 부여하지 않도록 하십시오. 지정된 버킷이 계정에 없는 경우 자동화를 통해 리전에 새 버킷이 생성되며, 이 리전에서 이름 형식으로 `<User-provided-name>-awssupport-YYYY-MM-DD` 자동화가 시작되고 사용자 지정 키로 암호화됩니다. AWS KMS

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

- CustomerManagedKmsKeyArn

  유형: 문자열

  설명: (선택 사항) 지정된 버킷이 계정에 없는 경우 생성되는 새 Amazon S3 버킷을 암호화하기 위한 사용자 지정 AWS KMS 키 Amazon 리소스 이름 (ARN) 입니다. 사용자 지정 AWS KMS 키를 ARN 지정하지 않고 버킷을 생성하려고 하면 자동화가 실패합니다.

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

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- 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

이 런북을 실행하는 데 필요한 최소 IAM 권한이 있는 예제 정책:

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

지침

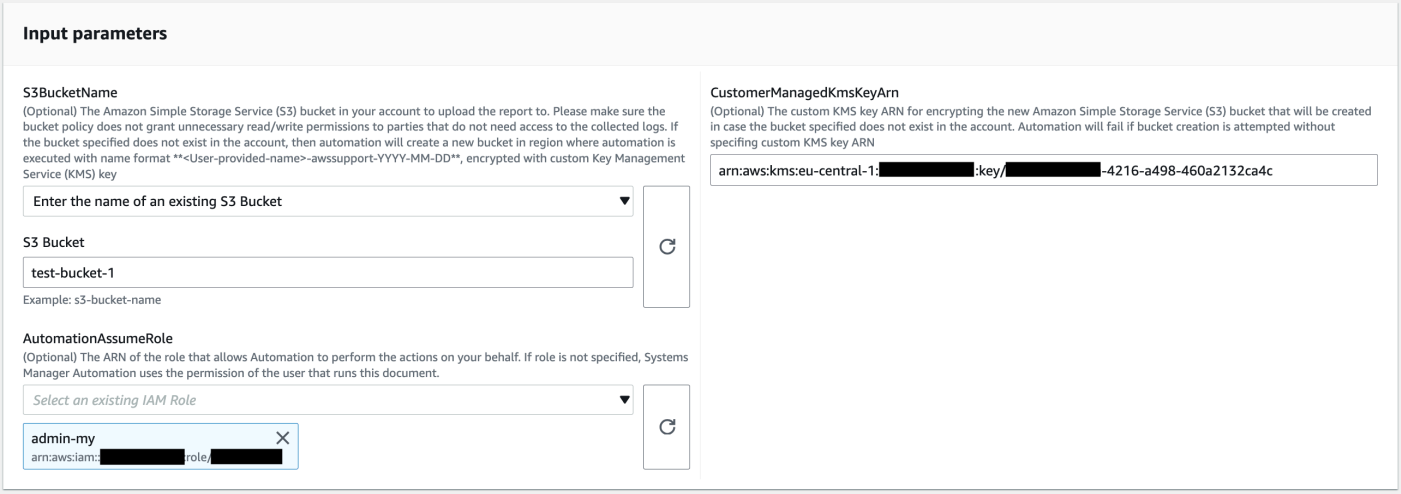
다음 단계에 따라 자동화를 구성합니다.

1. 콘솔에서 AWSSupport-A nalyzeEBSResource Usage로 이동합니다. AWS Systems Manager
2. 입력 파라미터의 경우, 다음 내용을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 () ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
   - S3 BucketName (필수):

     보고서를 업로드할 계정의 Amazon S3 버킷
   - CustomerManagedKmsKeyArn(선택 사항):

     새 Amazon S3 버킷을 암호화하기 위한 사용자 지정 AWS KMS 키 Amazon 리소스 이름 (ARN). 이 키는 지정된 버킷이 계정에 없는 경우 생성됩니다.



3. 실행을 선택합니다.
4. 자동화가 시작됩니다.
5. 자동화 실행서는 다음 단계를 수행합니다.
   - checkConcurrency:

     리전에서 이 런북을 한 번만 시작할 수 있도록 합니다. 런북에서 진행 중인 다른 실행을 발견하면 오류가 반환되고 종료됩니다.
   - verifyOrCreateS3버킷:

     Amazon S3 버킷이 존재하는지 확인합니다. 그렇지 않은 경우 사용자 지정 AWS KMS 키로 암호화된 이름 형식으로 `<User-provided-name>-awssupport-YYYY-MM-DD` 자동화가 시작되는 지역에 새 Amazon S3 버킷을 생성합니다.

- gatherAmiDetails:

  Amazon EC2 인스턴스에서 사용하지 않는 항목을 검색하여 이름 형식의 `<region>-images.csv` 보고서를 생성하여 Amazon S3 버킷에 업로드합니다. AMIs

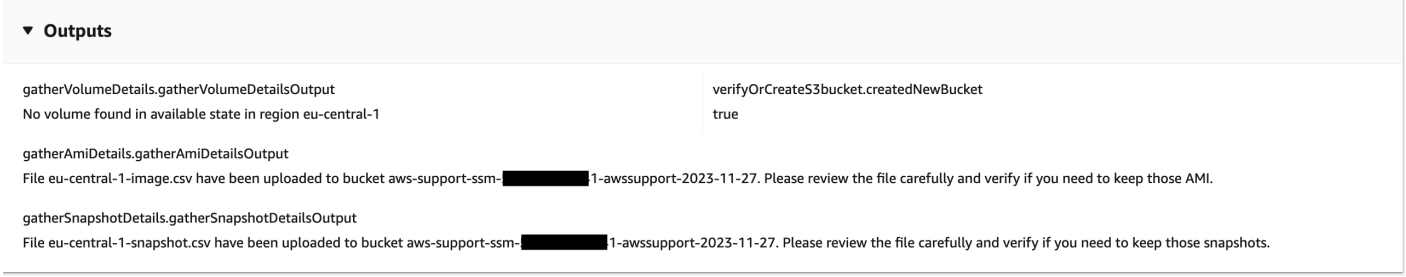
- gatherVolumeDetails:

  Amazon EBS 볼륨이 가용 상태인지 확인하고, 이름 형식으로 `<region>-volume.csv` 보고서를 생성하여 Amazon S3 버킷에 업로드합니다.

- gatherSnapshotDetails:

  이미 삭제된 Amazon EBS 볼륨의 Amazon EBS 스냅샷을 찾아 이름 형식으로 `<region>-snapshot.csv` 보고서를 생성하여 Amazon S3 버킷에 업로드합니다.

6. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.



참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS-ArchiveEBSSnapshots

설명

`AWS-ArchiveEBSSnapshots` 실행서는 스냅샷에 적용한 태그를 지정하여 Amazon Elastic Block Store(AmazonEBS) 볼륨에 대한 스냅샷을 아카이브하는 데 도움이 됩니다. 또는, 스냅샷에 태그가 지정되지 않은 경우 볼륨의 ID를 제공할 수도 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 설명

  유형: 문자열

  설명: (선택 사항) Amazon EBS 스냅샷에 대한 설명입니다.
- DryRun

  유형: 문자열

  유효한 값: Yes | No

  설명: (필수) 실제로 요청하지 않고도 작업을 위해 필요한 권한이 있는지 여부를 확인하고 오류 응답을 제공합니다.
- RetentionCount

  유형: 문자열

  설명: (선택 사항) 보관하려는 스냅샷의 개수입니다. `RetentionDays`에 대한 값을 지정하는 경우, 이 파라미터에 대한 값을 지정하지 마십시오.
- RetentionDays

유형: 문자열

설명: (선택 사항) 보관하려는 스냅샷의 이전 일 수입니다. `RetentionCount`에 대한 값을 지정하는 경우, 이 파라미터에 대한 값을 지정하지 마십시오.

- SnapshotWithTag

  유형: 문자열

  유효한 값: Yes | No

  설명: (필수) 보관하려는 스냅샷에 태그를 지정할지 여부를 지정합니다.

- TagKey

  유형: 문자열

  설명: (선택 사항) 보관하려는 스냅샷에 할당된 태그의 키입니다.

- TagValue

  유형: 문자열

  설명: (선택 사항) 보관하려는 스냅샷에 할당된 태그의 값입니다.

- VolumeId

  유형: 문자열

  설명: (선택 사항) 보관하려는 스냅샷이 있는 볼륨의 ID입니다. 스냅샷에 태그가 지정되지 않은 경우, 이 파라미터를 사용하십시오.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

`aws:executeScript` - `TagKey` 및 `TagValue` 파라미터 또는 `VolumeId` 파라미터를 사용하여 지정하는 태그를 사용하여 스냅샷을 보관합니다.

AWS-AttachEBSVolume

설명

Amazon Elastic Compute Cloud(Amazon EBS) 인스턴스에 Amazon Elastic Block Store(Amazon EC2) 볼륨을 연결합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 장치

  유형: 문자열

  설명: (필수) 디바이스 이름(예: /dev/sdh 또는 xvdh)입니다.
- InstanceId

  유형: 문자열

  설명: (필수) 볼륨을 연결할 인스턴스의 ID입니다.
- VolumeId

유형: 문자열

설명: (필수) Amazon EBS 볼륨의 ID입니다. 볼륨 및 인스턴스는 동일 가용 영역에 위치해야 합니다.

AWSSupport-CalculateEBSPerformanceMetrics

설명

AWSSupport-CalculateEBSPerformanceMetrics런북은 EBS 성능 지표를 계산하고 CloudWatch 대시보드에 게시하여 Amazon 성능 문제를 진단하는 데 도움이 됩니다. 대시보드에는 대상 Amazon EBS 볼륨 또는 대상 Amazon Elastic Compute Cloud (AmazonEC2) 인스턴스에 연결된 모든 볼륨의 예상 평균 IOPS 및 처리량이 표시됩니다. Amazon EC2 인스턴스의 경우 인스턴스의 평균 IOPS 및 처리량도 표시됩니다. Runbook은 관련 계산된 CloudWatch 지표를 표시하는 새로 만든 CloudWatch 대시보드로 연결되는 링크를 출력합니다. CloudWatch 대시보드는 계정에 다음과 AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID> 같은 이름으로 생성됩니다.

어떻게 작동하나요?

런북은 다음 단계를 수행합니다.

- 지정된 타임스탬프가 유효한지 확인합니다.
- 리소스 ID (Amazon EBS 볼륨 또는 Amazon EC2 인스턴스) 가 유효한지 검증합니다.
- Amazon을 EC2 ResourceID로 제공하면 해당 Amazon 인스턴스의 실제 IOPS 총계 /처리량과 Amazon 인스턴스에 연결된 EBS 모든 EC2 Amazon 볼륨의 IOPS 예상 평균 /처리량 그래프가 포함된 대시보드가 생성됩니다 CloudWatch . EC2
- Amazon EBS 볼륨을 ResourceID로 제공하면 해당 볼륨의 예상 IOPS 평균/처리량 CloudWatch 그래프가 포함된 대시보드가 생성됩니다.
- CloudWatch 대시보드가 생성된 후 예상 평균 IOPS 또는 예상 평균 처리량이 각각 최대 IOPS 또는 최대 처리량보다 크면 Amazon EC2 인스턴스에 연결된 볼륨에 대해 마이크로버스팅이 가능합니다.

> **Note**
>
> 버스트 가능한 볼륨 (gp2, sc2, st1) 의 경우 버스트 밸런스를 확보할 때까지 최대 IOPS /처리량을 고려해야 합니다. 버스트 밸런스가 완전히 활용된 후 (즉, 0이 된 경우) 기준 /처리량 지표를 고려해 보십시오. IOPS

> **Important**
>
> CloudWatch 대시보드를 만들면 계정에 추가 요금이 부과될 수 있습니다. 자세한 내용은 Amazon CloudWatch 가격 책정 가이드를 참조하십시오.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

샘플 정책

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

지침

다음 단계에 따라 자동화를 구성합니다.

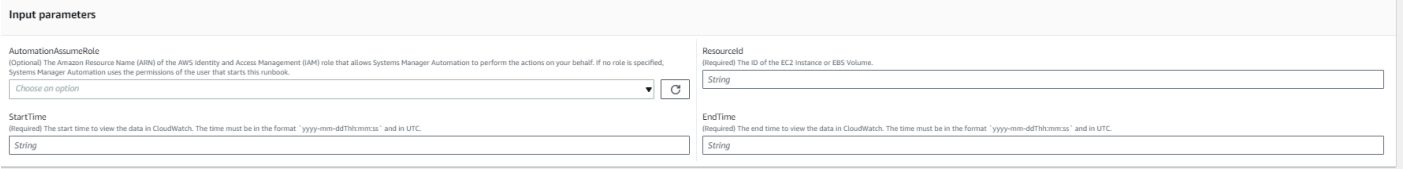
1. Systems AWSSupport-CalculateEBSPerformanceMetricsManager의 문서 아래로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 () ARN 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - 리소스 ID (필수):

     아마존 EC2 인스턴스 또는 아마존 EBS 볼륨의 ID.
   - 시작 시간 (필수):

     데이터를 볼 수 있는 시작 시간입니다 CloudWatch. 시간은 `yyyy-mm-ddThh:mm:ss` 형식과 단위여야 UTC 합니다.
   - 종료 시간 (필수):

데이터를 볼 수 있는 종료 시간 CloudWatch. 시간은 `yyyy-mm-ddThh:mm:ss` 형식과 단위여야 UTC 합니다.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - CheckResourceIdAndTimeStamps:

     종료 시간이 시작 시간보다 1분 이상 큰지, 제공된 리소스가 존재하는지 확인합니다.
   - CreateCloudWatchDashboard:

     Amazon EBS 성능을 계산하고 리소스 ID를 기반으로 그래프를 표시합니다. 매개 변수 리소스 ID에 Amazon EBS 볼륨 ID를 제공하는 경우 이 런북은 Amazon EBS 볼륨의 예상 평균 IOPS 및 예상 평균 처리량을 포함하는 CloudWatch 대시보드를 생성합니다. 매개 변수 리소스 ID에 Amazon EC2 인스턴스 ID를 제공하는 경우 이 런북은 Amazon 인스턴스의 평균 총 처리량 IOPS 및 평균 총 처리량과 Amazon EC2 인스턴스에 연결된 모든 Amazon EBS 볼륨의 예상 평균 IOPS 및 예상 평균 처리량이 포함된 CloudWatch 대시보드를 생성합니다. EC2
7. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토하십시오.

Amazon EC2 인스턴스로서의 리소스 ID에 대한 예제 CloudWatch 대시보드

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]

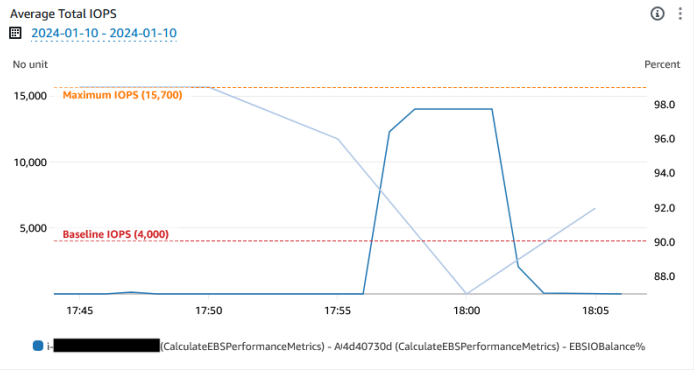
- Instance Type: t3.large
- EBS Optimized: True

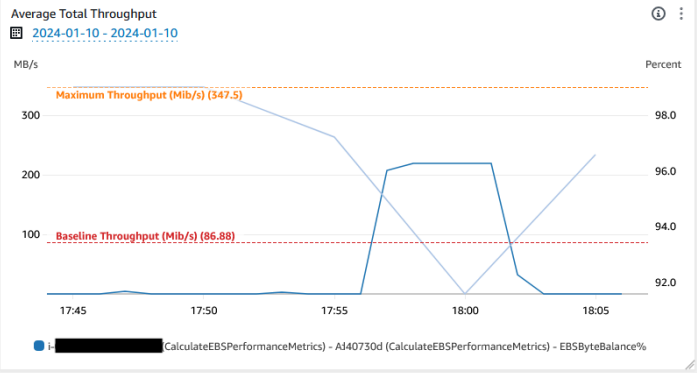
More details on EBS Optimized instances | More details on EBS Volume Types

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.





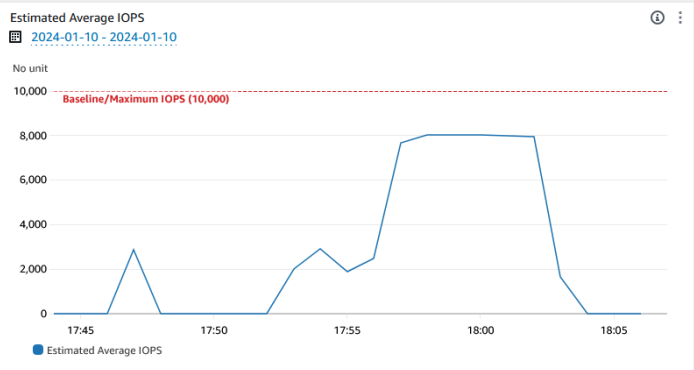
EBS Volume(s) Metrics

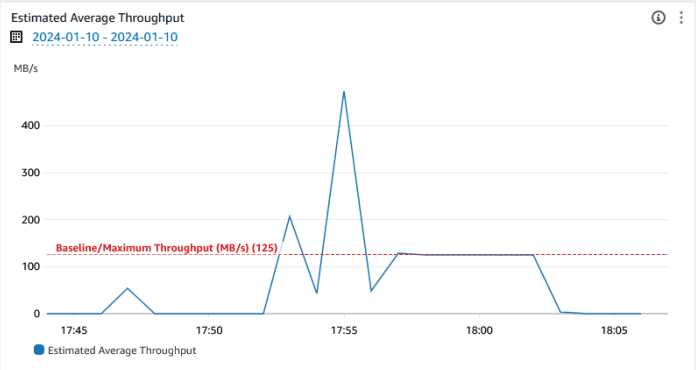
Calculated Metric	Mathematical Expression	Unit
Estimated Average IOPS	(SUM(VolumeReadOps) + SUM(VolumeWriteOps)) / (Period - SUM(VolumeIdleTime))	IOPS
Estimated Average Throughput	(SUM(VolumeReadBytes) + SUM(VolumeWriteBytes)) / (Period - SUM(VolumeIdleTime)) / 1024 / 1024	MiB/s

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.

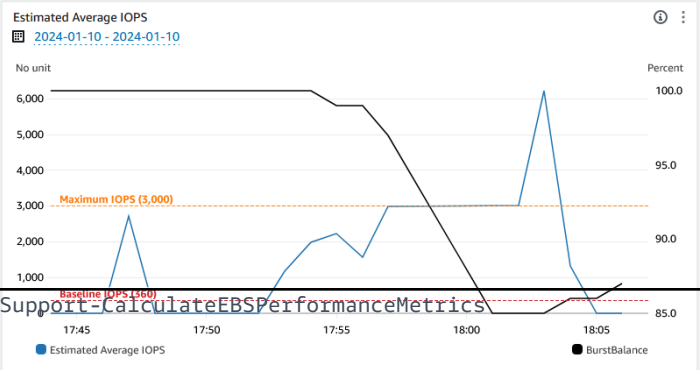
For more information, please review - How can I identify if my Amazon EBS volume is micro-bursting and then prevent this from happening?

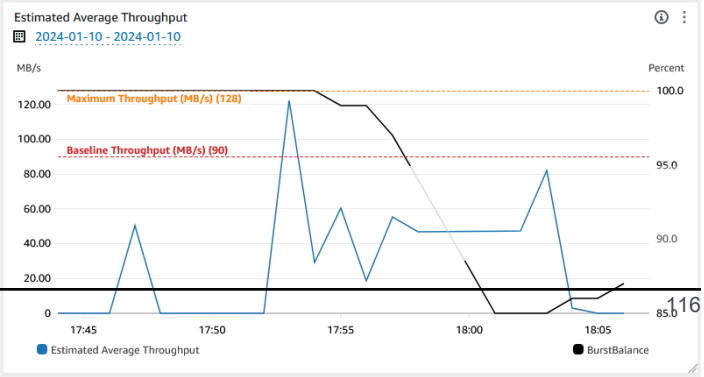
Volume: vol[redacted] Type: gp3





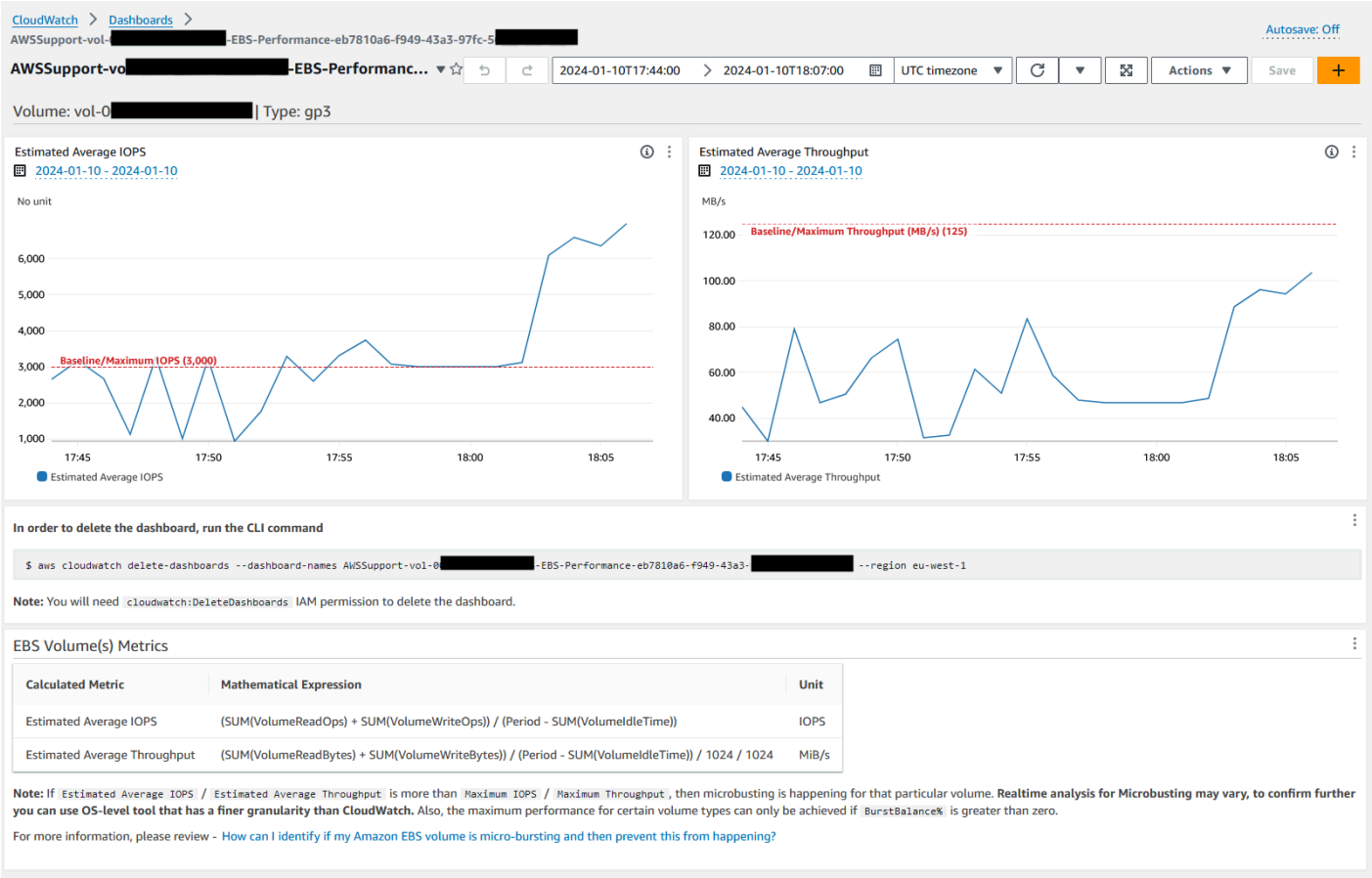
Volume: vol[redacted] | Type: gp2





Volume: vol[redacted] | Type: gp3

리소스 ID를 Amazon EBS 볼륨 ID로 사용하는 CloudWatch 대시보드 예시



참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 설명서

- Amazon EBS 볼륨이 마이크로 버스팅되고 있는지 식별하여 이러한 일이 발생하지 않도록 하려면 어떻게 해야 합니까?
- EC2인스턴스의 Amazon EBS 성능 지표 집계를 CloudWatch 보려면 어떻게 해야 합니까?

AWS-CopySnapshot

설명

Amazon Elastic Block Store(AmazonEBS) 볼륨의 스냅샷을 복사합니다 point-in-time. 동일한 내에서 AWS 리전 또는 한 리전에서 다른 리전으로 스냅샷을 복사할 수 있습니다. 암호화된 Amazon EBS 스냅샷의 사본은 암호화된 상태로 유지됩니다. 암호화되지 않은 스냅샷의 복사본은 암호화되지 않은 상태로 유지됩니다. 다른 계정에서 공유된 암호화된 스냅샷을 복사하려면 스냅샷을 암호화하는 데 사용되는 KMS 키에 대한 권한이 있어야 합니다. 다른 스냅샷을 복사하여 생성된 스냅샷에는 어떠한 용도에도 사용되지 않는 임의 볼륨 ID가 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 설명

  유형: 문자열

  설명: (선택 사항) Amazon EBS 스냅샷에 대한 설명입니다.
- SnapshotId

유형: 문자열

설명: (필수) 복사할 Amazon EBS 스냅샷의 ID입니다.

- SourceRegion

  유형: 문자열

  설명: (필수) 현재 소스 스냅샷이 존재하는 리전입니다.

문서 단계

copySnapshot - Amazon EBS 볼륨의 스냅샷을 복사합니다.

출력

copySnapshot.SnapshotId - 새 스냅샷의 ID입니다.

AWS-CreateSnapshot

설명

Amazon EBS 볼륨의 스냅샷을 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 설명

  유형: 문자열

  설명: (선택 사항) 스냅샷에 대한 설명입니다.

- VolumeId

  유형: 문자열

  설명: (필수) 볼륨의 ID입니다.

AWS-DeleteSnapshot

설명

Amazon EBS 볼륨의 스냅샷을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- SnapshotId

  유형: 문자열

  설명: (필수) EBS 스냅샷의 ID입니다.

AWSConfigRemediation-DeleteUnusedEBSVolume

설명

`AWSConfigRemediation-DeleteUnusedEBSVolume` 실행서는 사용되지 않은 Amazon Elastic Block Store(Amazon EBS) 볼륨을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- CreateSnapshot

타입: 부울

설명: (선택 사항) `true` 로 설정하면 자동화가 삭제되기 전에 Amazon EBS 볼륨의 스냅샷을 생성합니다.

- VolumeId

  유형: 문자열

  설명: (필수) 삭제하려는 Amazon EBS 볼륨의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `VolumeId` 파라미터에 지정한 Amazon EBS 볼륨이 사용되지 않는지 확인하고 `CreateSnapshot` 파라미터에 대해 선택한 값에 따라 스냅샷을 생성합니다.
- `aws:branch` - `CreateSnapshot` 파라미터에 대해 선택한 값을 기반으로 분기합니다.
- `aws:waitForAwsResourceProperty` - 스냅샷이 완료될 때까지 기다립니다.
- `aws:executeAwsApi` - 스냅샷 생성에 실패한 경우 스냅샷을 삭제합니다.
- `aws:executeAwsApi` - `VolumeId` 파라미터에서 지정한 Amazon EBS 볼륨을 삭제합니다.
- `aws:executeScript` - Amazon EBS 볼륨이 삭제되었는지 확인합니다.

AWS-DeregisterAMIs

설명

`AWS-DeregisterAMIs` 실행서는 등록 취소에 도움이 됩니다.Amazon Machine Images (AMIs)에 적용한 태그를 지정하여 AMIs.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- DryRun

  유형: 문자열

  유효한 값: Yes | No

  설명: (필수) 실제로 요청하지 않고도 작업을 위해 필요한 권한이 있는지 여부를 확인하고 오류 응답을 제공합니다.

- RetainNumber

  유형: 문자열

  설명: (선택 사항) 의 수 AMIs 보존하려는 입니다. `Age`에 대한 값을 지정하는 경우, 이 파라미터에 대한 값을 지정하지 마십시오.

- 나이

  유형: 문자열

  설명: (선택 사항) 이전 일 수 AMIs 보존하려는 입니다. `RetainNumber`에 대한 값을 지정하는 경우, 이 파라미터에 대한 값을 지정하지 마십시오.
- TagKey

  유형: 문자열

  설명: (필수) 에 할당된 태그의 키입니다.AMIs 등록을 취소하려는 입니다.
- TagValue

  유형: 문자열

  설명: (필수) 에 할당된 태그의 값입니다.AMIs 등록을 취소하려는 입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeAwsApi` - 실행서 입력 파라미터에 대해 지정하는 값의 유효성을 검사합니다.
- `aws:executeAwsApi` - 등록 취소 AMIs `TagKey` 및 `TagValue` 파라미터를 사용하여 지정하는 태그를 사용합니다.

AWS-DetachEBSVolume

설명

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 Amazon EBS 볼륨을 분리합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- LambdaAssumeRole

  유형: 문자열

  설명: (선택 사항) Lambda가 맡은 역할ARN의 입니다.
- VolumeId

  유형: 문자열

  설명: (필수) EBS 볼륨의 ID입니다. 볼륨과 인스턴스는 동일 가용 영역 내에 있어야 합니다.

AWSConfigRemediation-EnableEbsEncryptionByDefault

설명

`AWSConfigRemediation-EnableEbsEncryptionByDefault` 실행서는 자동화를 AWS 리전 실행하는 AWS 계정 및 의 모든 새 Amazon Elastic Block Store(Amazon EBS) 볼륨에서 암호화를 활성화합니다. 자동화를 실행하기 전에 생성된 볼륨은 암호화되지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeAwsApi` - 현재 계정 및 리전에서 기본 Amazon EBS 암호화 설정을 활성화합니다.
- `aws:assertAwsResourceProperty` - 기본 Amazon EBS 암호화 설정이 활성화되었는지 확인합니다.

AWS-ExtendEbsVolume

설명

`AWS-ExtendEbsVolume` 실행서는 Amazon EBS 볼륨의 크기를 늘리고 파일 시스템을 확장합니다. 이 자동화는 `xfs` 및 `ext4` 파일 시스템을 지원합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- DriveLetter

  유형: 문자열

  설명: (선택 사항) 확장하려는 파일 시스템이 있는 드라이브의 문자입니다. 이 파라미터는 에 필요합니다.Windows 인스턴스.
- InstanceId

  유형: 문자열

  설명: (선택 사항) 확장하려는 Amazon EBS 볼륨이 연결된 Amazon EC2 인스턴스의 ID입니다.
- KeepSnapshot

  타입: 부울

  기본값: true

설명: (선택 사항) Amazon EBS 볼륨 크기를 늘리기 전에 생성된 스냅샷을 유지할지 여부를 결정합니다.

- MountPoint

  유형: 문자열

  설명: (선택 사항) 확장하려는 파일 시스템이 있는 드라이브의 탑재 지점입니다. 이 파라미터는 Linux 인스턴스에 대해 필요합니다.

- SizeGib

  유형: 문자열

  설명: (필수) Amazon EBS 볼륨을 수정할 GiB의 크기입니다.

- VolumeId

  유형: 문자열

  설명: (필수) 확장하려는 EBS 볼륨의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - 볼륨 크기를 `VolumeId` 파라미터에서 지정한 값으로 늘리고 파일 시스템을 확장합니다.

AWSSupport-ModifyEBSSnapshotPermission

설명

AWSSupport-ModifyEBSSnapshotPermission 실행서는 여러 Amazon Elastic Block Store(AmazonEBS) 스냅샷에 대한 권한을 수정하는 데 도움이 됩니다. 이 실행서를 사용하여 Public 또는 Private 스냅샷을 만들거나 다른 AWS 계정와 공유할 수 있습니다. 기본 KMS 키로 암호화된 스냅샷은 이 런북을 사용하여 다른 계정과 공유할 수 없습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- AccountIds

  유형: StringList

  기본값: 없음

  설명: (선택 사항) 스냅샷을 공유하려는 계정IDs의 입니다. Private 파라미터의 값에 대해 No(을)를 입력하는 경우 이 파라미터는 필수입니다.
- AccountPermissionOperation

유형: 문자열

유효한 값: add | remove

기본값: 없음

설명: (선택 사항) 수행할 작업의 유형입니다.

- 프라이빗

  유형: 문자열

  유효한 값: Yes | No

  설명: (필수) 스냅샷을 특정 계정과 공유하려는 경우 해당 값에 대해 No(을)를 입력합니다.

- SnapshotIds

  유형: StringList

  설명: (필수) 권한을 수정하려는 Amazon EBS 스냅샷IDs의 입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

1. `aws:executeScript` - `SnapshotIds` 파라미터에 제공된 스냅샷IDs의 를 확인합니다. 를 확인한 후 스크립트IDs는 암호화된 스냅샷을 확인하고 검색된 경우 목록을 출력합니다.
2. `aws:branch` - `Private` 파라미터에 대해 입력하는 값을 기반으로 자동화를 분기합니다.
3. `aws:executeScript` - 지정된 스냅샷의 권한을 수정하여 지정된 계정과 해당 내용을 공유합니다.
4. `aws:executeScript` - 스냅샷의 권한을 수정하여 해당 내용을 `Public`에서 `Private`(으)로 변경합니다.

출력

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.결과

MakePrivate.결과

MakePrivate.명령

AWSConfigRemediation-ModifyEBSVolumeType

설명

`AWSConfigRemediation-ModifyEBSVolumeType` 실행서는 Amazon Elastic Block Store(Amazon EBS) 볼륨의 볼륨 유형을 수정합니다. 볼륨 유형이 수정된 후, 볼륨은 `optimizing` 상태로 들어갑니다. 볼륨 수정 진행 상황 모니터링에 대한 자세한 내용은 Amazon EC2 사용 설명서의 볼륨 수정 진행 상황 모니터링을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- EbsVolumeId

유형: 문자열

설명: (필수) 수정하려는 Amazon EBS 볼륨의 ID입니다.

- EbsVolumeType

  유형: 문자열

  유효한 값: standard | io1 | io2 | gp2 | gp3 | sc1 | st1

  설명: Amazon 볼륨을 변경하려는 EBS 볼륨 유형입니다. Amazon EBS 볼륨 유형에 대한 자세한 내용은 Amazon 사용 설명서의 Amazon EBS 볼륨 유형을 참조하세요. EC2

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:waitForAwsResourceProperty` - 볼륨 상태가 `available` 또는 `in-use`인지 확인합니다.
- `aws:executeAwsApi` - `EbsVolumeId` 파라미터에서 지정한 Amazon EBS 볼륨을 수정합니다.
- `aws:waitForAwsResourceProperty` - 볼륨 유형이 `EbsVolumeType` 파라미터에서 지정한 값으로 변경되었는지 확인합니다.

Amazon EC2

AWS Systems Manager 자동화는 Amazon Elastic Compute Cloud에 사전 정의된 런북을 제공합니다. Amazon Elastic Block Store용 실행서는 실행서 참조의 Amazon EBS 섹션에 위치하고 있습니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- 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-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

설명

Auto Scaling 그룹에서 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 대기 상태를 변경합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) Auto Scaling 그룹 내에서 대기 상태를 변경하려는 Amazon EC2 인스턴스의 ID입니다.
- LambdaRoleArn

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 자동화에서 생성된 Lambda를 통해 작업을 수행할 수 있도록 허용하는 역할의 ARN입니다. 지정하지 않을 경우 Lambda 함수를 실행할 임시 역할이 생성됩니다.

AWS-ASGExitStandby

설명

Auto Scaling 그룹에서 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 대기 상태를 변경합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) Auto Scaling 그룹 내에서 대기 상태를 변경하려는 EC2 인스턴스의 ID입니다.
- LambdaRoleArn

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 자동화에서 생성된 Lambda를 통해 작업을 수행할 수 있도록 허용하는 역할의 ARN입니다. 지정하지 않을 경우 Lambda 함수를 실행할 임시 역할이 생성됩니다.

AWS-CreateImage

설명

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 새로운 Amazon Machine Image(AMI)을(를) 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) EC2 인스턴스의 ID입니다.
- NoReboot

  유형: 부울

  설명: (선택 사항) 이미지를 생성하기 전에 인스턴스를 재부팅하지 마십시오.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

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

AWS-DeleteImage

설명

Amazon Machine Image(AMI) 및 모든 관련 스냅샷을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ImageId

  유형: 문자열

  설명: (필수) AMI의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

```
{
    "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

설명

Auto Scaling 그룹에서 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 패치를 적용합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) 패치를 적용할 인스턴스의 ID입니다. 유지 관리 기간 동안 실행하도록 구성된 인스턴스 ID는 지정하지 마십시오.
- LambdaRoleArn

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 자동화에서 생성된 Lambda를 통해 작업을 수행할 수 있도록 허용하는 역할의 ARN입니다. 지정하지 않을 경우, Lambda 함수를 실행할 임시 역할이 생성됩니다.
- WaitForInstance

  유형: 문자열

  기본 값: PT2M

  설명: (선택 사항) 인스턴스가 다시 활동 상태로 전환되도록 허용하기 위해 자동화가 대기 상태로 유지되어야 하는 기간입니다.
- WaitForReboot

  유형: 문자열

기본 값: PT5M

설명: (선택 사항) 패치가 적용된 인스턴스가 재부팅되도록 허용하기 위해 자동화가 대기 상태로 유지되어야 하는 기간입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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

설명

EC2 인스턴스가 해당 패치 기준선을 준수하도록 합니다. 실패 시 루트 볼륨을 롤백합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  유형: 문자열

  설명: (필수) 패치 기준선이 적용되는 EC2 InstanceId.

- LambdaAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 자동화에서 생성된 Lambda를 통해 작업을 수행할 수 있도록 허용하는 역할의 ARN입니다. 지정하지 않을 경우 Lambda 함수를 실행할 임시 역할이 생성됩니다.

- ReportS3Bucket

  유형: 문자열

  설명: (선택 사항) 프로세스 도중 생성되는 규정 준수 보고서의 Amazon S3 버킷 대상입니다.

문서 단계

단계 번호	단계 이름	자동화 작업
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`

출력

IdentifyRootVolume.Payload

PrePatchSnapshot.Output

SaveComplianceReportToS3.Payload

RestoreFromSnapshot.Payload

CheckCompliance.Payload

AWS-QuarantineEC2Instance

설명

`AWS-QuarantineEC2Instance` 실행서를 사용하면, 인바운드 또는 아웃바운드 트래픽을 허용하지 않는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 보안 그룹을 할당할 수 있습니다.

> **Important**
> 이 실행서를 실행하기 전에 RDP 설정에 대한 변경 내용을 신중히 검토해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

유형: 문자열

설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  유형: 문자열

  설명: (필수) RDP 설정을 관리할 관리형 인스턴스의 ID입니다.

- IsolationSecurityGroup

  유형: 문자열

  설명: (필수) 인바운드 또는 아웃바운드 트래픽을 방지하기 위해 인스턴스에 할당하려는 보안 그룹의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeAwsApi` - 인스턴스에 대한 세부 정보를 수집합니다.

- `aws:executeScript` - 인스턴스가 Auto Scaling 그룹의 일부가 아닌지 확인합니다.
- `aws:executeAwsApi` - 인스턴스에 연결된 루트 볼륨의 스냅샷을 생성합니다.
- `aws:waitForAwsResourceProperty` - 스냅샷 상태가 `completed`가 될 때까지 기다립니다.
- `aws:executeAwsApi` - `IsolationSecurityGroup` 파라미터에 지정된 보안 그룹을 인스턴스에 할당합니다.

출력

`GetEC2InstanceResources.RevokedSecurityGroupsIds`

`GetEC2InstanceResources.RevokedSecurityGroupsNames`

`createSnapshot.SnapId`

AWS-ResizeInstance

설명

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 인스턴스 유형을 변경합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  유형: 문자열

  설명: (필수) 인스턴스의 ID입니다.

- InstanceType

  유형: 문자열

  설명: (필수) 인스턴스 유형입니다.

- LambdaAssumeRole

  유형: 문자열

  설명: (선택 사항) Lambda에서 수임하는 역할의 ARN입니다.

AWS-RestartEC2Instance

설명

하나 이상의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 다시 시작합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  형식: StringList

  설명: (필수) 다시 시작할 Amazon EC2 인스턴스의 ID입니다.

`AWS-SetupJupyter`

설명

`AWS-SetupJupyter` 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 Jupyter Notebook을 설정하는 데 도움이 됩니다. 기존 인스턴스를 지정하거나 자동화에 사용할 Amazon Machine Image(AMI) ID를 제공하여 새 인스턴스를 시작하고 설정할 수 있습니다. 시작하기 전에, Parameter Store에서 Jupyter Notebook의 암호로 사용할 `SecureString` 파라미터를 생성해야 합니다. Parameter Store는 AWS Systems Manager의 기능입니다. 파라미터를 생성하는 것에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 파라미터 생성을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- AmiId

  유형: 문자열

  설명: (선택 사항) 새 인스턴스를 시작하고 Jupyter Notebook을 설정하는 데 사용하려는 AMI의 ID입니다.

- InstanceId

  유형: 문자열

  설명: (필수) Jupyter Notebook을 설정하려는 인스턴스의 ID입니다.

- InstanceType

  유형: 문자열

  기본값: t3.medium

  설명: (선택 사항) 새 인스턴스를 시작하여 Jupyter Notebook을 설정하는 경우, 사용하려는 인스턴스 유형을 지정하세요.

- JupyterPasswordSSMKey

  유형: 문자열

  설명: (필수) Jupyter Notebook의 암호로 사용하려는 Parameter Store의 `SecureString` 파라미터 이름입니다.

- KeyPairName

  유형: 문자열

  설명: (선택 사항) 새로 시작한 인스턴스와 연결하려는 키 페어입니다.

- RemoteAccessCidr

  유형: 문자열

  기본값: 0.0.0.0/0

  설명: (선택 사항) SSH 트래픽을 허용하려는 CIDR 범위입니다.
- RoleName

  유형: 문자열

  기본값: SSMManagedInstanceProfileRole

  설명: (선택 사항) 새로 시작한 인스턴스용 인스턴스 프로파일의 이름입니다.
- StackName

  유형: 문자열

  기본값: CreateManagedInstanceStack{{automation:EXECUTION_ID}}

  설명: (선택 사항) 자동화에서 사용할 AWS CloudFormation 스택 이름입니다.
- SubnetId

  유형: 문자열

  기본값: Default

  설명: (선택 사항) 사용할 새 인스턴스를 시작하려는 서브넷입니다.
- VpcId

  유형: 문자열

  기본값: Default

  설명: (선택 사항) 새 인스턴스를 시작하려는 Virtual Private Cloud(VPC)의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeScript` - 사용자가 실행서 입력 파라미터에 대해 지정하는 값을 사용하여, 사용자가 지정하는 인스턴스 또는 새로 시작된 인스턴스에 Jupyter Notebook을 설정합니다.

AWS-StartEC2Instance

설명

하나 이상의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 시작합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  형식: StringList

  설명: (필수) 시작할 EC2 인스턴스입니다.

AWS-StopEC2Instance

설명

하나 이상의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 중지합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  형식: StringList

  설명: (필수) 중지할 EC2 인스턴스입니다.

AWS-TerminateEC2Instance

설명

하나 이상의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 종료합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  형식: StringList

  설명: (필수) 종료할 하나 이상의 EC2 인스턴스의 ID입니다.

AWS-UpdateLinuxAmi

설명

Amazon Machine Image(AMI)를 Linux 배포 패키지 및 Amazon 소프트웨어로 업데이트합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ExcludePackages

  타입: 문자열

  기본값: 없음

  설명: (선택 사항) 어떤 조건에서나 업데이트를 보류할 패키지의 이름입니다. 기본적으로("none"), 어떤 패키지도 제외되지 않습니다.

- IamInstanceProfileName

  타입: 문자열

  기본값: ManagedInstanceProfile

  설명: (필수) Systems Manager에서 인스턴스를 관리할 수 있는 인스턴스 프로파일입니다.

- IncludePackages

  타입: 문자열

  기본값: all

  설명: (선택 사항) 이름 지정된 패키지만 업데이트합니다. 기본적으로("all"), 사용 가능한 업데이트는 모두 적용합니다.

- InstanceType

  타입: 문자열

  기본값: t2.micro

  설명: (선택 사항) 작업 영역의 호스트로 시작할 인스턴스의 유형입니다. 인스턴스 유형은 리전마다 다릅니다.

- MetadataOptions

유형: StringMap

기본값: {" HttpEndpoint ": "활성화", "HttpTokens": "선택 사항"}

설명: (선택 사항) 인스턴스에 대한 메타데이터 옵션입니다. 자세한 내용은 을 참조하십시오 InstanceMetadataOptionsRequest.

- PostUpdateScript

  타입: 문자열

  기본값: 없음

  설명: (선택 사항) 패키지 업데이트가 적용된 후에 실행할 스크립트의 URL입니다. 기본값("none")은 스크립트를 실행하지 않는 것입니다.

- PreUpdateScript

  타입: 문자열

  기본값: 없음

  설명: (선택 사항) 업데이트가 적용되기 전에 실행할 스크립트의 URL입니다. 기본값("none")은 스크립트를 실행하지 않는 것입니다.

- SecurityGroupIds

  타입: 문자열

  설명: (필수) 적용하려는 보안 그룹 ID를 쉼표로 구분한 AMI 목록입니다.

- SourceAmiId

  타입: 문자열

  설명: (필수) 소스 Amazon 머신 이미지 ID입니다.

- SubnetId

  타입: 문자열

  설명: (선택 사항) 인스턴스를 시작하려는 서브넷의 ID입니다. 기본 VPC를 삭제한 경우, 이 파라미터는 필수입니다.

- TargetAmiName

타입: 문자열

기본값: UpdateLinuxAmi _from_ {{SourceAmiId}} _on_ {{글로벌:날짜_시간}}

설명: (선택 사항) 생성될 새 AMI의 이름입니다. 기본값은 소스 AMI ID 및 생성 날짜/시간을 포함하는 시스템 생성 문자열입니다.

AWS-UpdateWindowsAmi

설명

Microsoft Windows Amazon Machine Image(AMI)를 업데이트하세요. 기본적으로, 이 실행서는 모든 Windows 업데이트, Amazon 소프트웨어 및 Amazon 드라이버를 설치합니다. 그런 다음 새 AMI를 생성하는 Sysprep을 실행합니다. Windows Server 2008 R2 이상을 지원합니다.

> **Important**
>
> VPC 엔드포인트를 AWS Systems Manager 사용하여 인스턴스를 연결하는 경우 us-east-1 지역에서 사용하지 않는 한 이 런북은 실패합니다. 이 실행서를 사용하려면 인스턴스에 TLS 1.2가 활성화되어 있어야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 카테고리

  타입: 문자열

  설명: (선택 사항)하나 이상의 업데이트 범주를 지정합니다. 쉼표로 분리된 값을 사용하여 범주를 필터링할 수 있습니다. 옵션: 응용 프로그램, 커넥터 CriticalUpdates DefinitionUpdates, DeveloperKits,, 드라이버FeaturePacks, 지침, Microsoft, SecurityUpdates ServicePacks,, 도구 UpdateRollups, 업데이트. 유효한 형식에는 단일 항목이 포함됩니다 (예:CriticalUpdates. 또는 쉼표로 구분된 목록 (CriticalUpdates,SecurityUpdates) 을 지정할 수 있습니다. 참고: 쉼표 앞/뒤에 공백이 없어야 합니다.

- ExcludeKbs

  타입: 문자열

  설명: (선택 사항) 제외할 하나 이상의 Microsoft Knowledge Base(KB) 문서 ID를 지정합니다. 쉼표로 분리된 값을 사용하여 여러 ID를 제외할 수 있습니다. 유효한 형식: KB9876543 또는 9876543.

- IamInstanceProfileName

  타입: 문자열

  기본값: ManagedInstanceProfile

  설명: (필수) Systems Manager에서 인스턴스를 관리할 수 있는 역할의 이름입니다.

- IncludeKbs

  타입: 문자열

  설명: (선택 사항) 포함할 하나 이상의 Microsoft Knowledge Base(KB) 문서 ID를 지정합니다. 쉼표로 분리된 값을 사용하여 여러 ID를 설치할 수 있습니다. 유효한 형식: KB9876543 또는 9876543.

- InstanceType

  타입: 문자열

  기본값: t2.medium

설명: (선택 사항) 작업 영역의 호스트로 시작할 인스턴스의 유형입니다. 인스턴스 유형은 리전마다 다릅니다. 기본값은 t2.medium입니다.

- MetadataOptions

  유형: StringMap

  기본값: {" HttpEndpoint ": "활성화", "HttpTokens": "선택 사항"}

  설명: (선택 사항) 인스턴스에 대한 메타데이터 옵션입니다. 자세한 내용은 을 참조하십시오 InstanceMetadataOptionsRequest.

- PostUpdateScript

  타입: 문자열

  설명: (선택 사항) 문자열로 제공된 스크립트입니다. OS 업데이트 설치 후에 실행합니다.

- PreUpdateScript

  타입: 문자열

  설명: (선택 사항) 문자열로 제공된 스크립트입니다. OS 업데이트 설치 전에 실행합니다.

- PublishedDateAfter

  타입: 문자열

  설명: (선택 사항) 업데이트 게시 이전 날짜를 지정합니다. 예를 들어 01/01/2017을 지정할 경우 01/01/2017 또는 그 이후에 게시되어 Windows 업데이트 검색 중에 발견된 모든 업데이트가 반환됩니다.

- PublishedDateBefore

  타입: 문자열

  설명: (선택 사항) 업데이트 게시 이후 날짜를 지정합니다. 예를 들어 01/01/2017을 지정할 경우 01/01/2017 또는 그 이전에 게시되어 Windows 업데이트 검색 중에 발견된 모든 업데이트가 반환됩니다.

- PublishedDaysOld

  타입: 문자열

설명: (선택 사항) 업데이트가 게시된 날짜로부터 경과되어야 할 일수를 지정합니다. 예를 들어 10을 지정할 경우 최소 10일 전에 게시되어 Windows 업데이트 검색 중에 발견된 모든 업데이트가 반환됩니다.

- SecurityGroupIds

  타입: 문자열

  설명: (필수) 적용하려는 보안 그룹 ID를 쉼표로 구분한 AMI 목록입니다.

- SeverityLevels

  타입: 문자열

  설명: (선택 사항) 업데이트와 연결되는 하나 이상의 MSRC 심각도를 지정합니다. 쉼표로 분리된 값을 사용하여 심각도를 필터링할 수 있습니다. 기본적으로 모든 보안 수준에 대한 패치가 선택됩니다. 값을 지정한 경우 업데이트 목록이 이러한 값으로 필터링됩니다. 옵션: 심각, 중요, 낮음, 보통 또는 비지정. 유효한 형식에는 심각 등 단일 입력이 포함됩니다. 또는 심각,중요,낮음처럼 쉼표로 구분된 목록을 지정할 수 있습니다.

- SourceAmiId

  타입: 문자열

  설명: (필수) 소스 AMI ID.

- SubnetId

  타입: 문자열

  설명: (선택 사항) 인스턴스를 시작하려는 서브넷의 ID입니다. 기본 VPC를 삭제한 경우, 이 파라미터는 필수입니다.

- TargetAmiName

  타입: 문자열

  기본값: UpdateWindowsAmi _from_ {{SourceAmiId}} _on_ {{글로벌:날짜_시간}}

  설명: (선택 사항) 생성될 새 AMI의 이름입니다. 기본값은 소스 AMI ID 및 생성 날짜/시간을 포함하는 시스템 생성 문자열입니다.

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck

설명

AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck 실행서는 사용자가 지정하는 Amazon EC2 Auto Scaling(Auto Scaling) 그룹의 상태 점검을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.
- AutoScalingGroupARN

  유형: 문자열

  설명: (필수) 상태 점검을 활성화하려는 Auto Scaling 그룹의 Amazon 리소스 이름(ARN)입니다.
- HealthCheckGracePeriod

  유형: 정수

  기본값: 300

  설명: (선택 사항) 서비스를 시작한 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 상태를 점검하기 전에 Auto Scaling이 대기하는 시간(초)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `AutoScalingGroupARN` 파라미터에 지정한 Auto Scaling 그룹의 상태 점검을 활성화합니다.

AWSConfigRemediation-EnforceEC2InstanceIMDSv2

설명

`AWSConfigRemediation-EnforceEC2InstanceIMDSv2` 실행서에서는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용하려면 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 필요합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- InstanceId

  타입: 문자열

설명: (필수) IMDSv2를 사용하는 데 필요한 Amazon EC2 인스턴스의 ID입니다.

- AutomationAssumeRole

  타입: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다.

- HttpPutResponseHopLimit

  타입: 정수

  설명: (선택 사항) IMDS 서비스에서 요청자에게 보내는 홉 응답 한도입니다. 컨테이너를 호스팅하는 EC2 인스턴스의 경우 2 이상으로 설정합니다. 변경하지 않으려면 0으로 설정합니다 (기본값).

  허용 패턴: `^([1-5]?\d|6[0-4])$`

  기본값: 0

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - `InstanceId` 파라미터에 지정하는 Amazon EC2 인스턴스에서 `HttpTokens` 옵션을 `required`으로 설정합니다.
- `aws:assertAwsResourceProperty` - Amazon EC2 인스턴스에서 IMDS2가 필요한지 확인합니다.

AWSEC2-CloneInstanceAndUpgradeSQLServer

설명

SQLServer 2008 Windows Server 이상을 AMI 실행하기 위한 AMI EC2 인스턴스에서 인스턴스를 만든 다음 최신 버전의 SQL Server로 업그레이드하십시오. 영문 버전의 SQL Server만 지원됩니다.

다음 업그레이드 경로가 지원됩니다.

- SQL서버 2008에서 SQL 서버 2017, 2016 또는 2014로
- SQL서버 2008 R2에서 2017, 2016 또는 2014 SQL 서버로
- SQL서버 2012에서 SQL 서버 2019, 2017, 2016 또는 2014로
- SQL서버 2014에서 SQL 서버 2019, 2017 또는 2016으로
- SQL서버 2016에서 SQL 서버 2019 또는 2017으로

Server 2019와 호환되지 않는 이전 버전의 Windows Server를 사용하는 경우, 자동화 문서를 통해 Windows SQL Server 버전을 2016으로 업그레이드해야 합니다.

이 업그레이드는 완료하는 데 2시간이 걸릴 수 있는 다단계 프로세스입니다. 자동화는 인스턴스에서 인스턴스를 만든 다음 지정된 `SubnetID` 새 AMI 인스턴스에서 임시 인스턴스를 시작합니다. AMI 원래 인스턴스와 연결된 보안 그룹이 임시 인스턴스에 적용됩니다. 이제 자동화는 임시 인스턴스에서 `TargetSQLVersion`에 대한 현재 위치 업그레이드를 수행합니다. 업그레이드 후, 이 자동화는 임시 인스턴스에서 새 AMI을 생성한 다음 임시 인스턴스를 종료합니다.

AMI에서 새 애플리케이션을 실행하여 애플리케이션 기능을 테스트할 수 있습니다VPC. 테스트를 완료하고 나서나 다른 업그레이드를 수행하기 전에는 업그레이드된 인스턴스로 완전히 전환하기에 앞서 애플리케이션 중단 시간을 예약하십시오.

> **Note**
>
> 새 EC2 AMI 인스턴스에서 시작된 인스턴스의 컴퓨터 이름을 수정하려면 서버의 독립 실행형 인스턴스를 호스팅하는 컴퓨터 이름 바꾸기를 참조하십시오. SQL

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

Parameters

사전 조건

- TLS버전 1.2.
- 영어 버전의 SQL 서버만 지원됩니다.
- EC2인스턴스는 Windows Server 2008 R2 (이상) 및 SQL 서버 2008 (또는 이후) 버전을 사용해야 합니다. Windows Server
- 인스턴스에 SSM 에이전트가 설치되어 있는지 확인하십시오. 자세한 내용은 Windows Server용 EC2 인스턴스에 SSM 에이전트 설치 및 구성을 참조하십시오.
- AWS Identity and Access Management (IAM) 인스턴스 프로필 역할을 사용하도록 인스턴스를 구성합니다. 자세한 내용은 Systems Manager의 IAM 인스턴스 프로파일 생성을 참조하십시오.
- 인스턴스 부트 디스크에 20GB의 사용 가능한 디스크 공간이 있는지 확인합니다.
- Bring Your Own License (BYOL) SQL 서버 버전을 사용하는 인스턴스의 경우 다음과 같은 추가 사전 요구 사항이 적용됩니다.
  - 대상 SQL 서버 설치 미디어가 포함된 EBS 스냅샷 ID를 제공하십시오. 방법:
    1. EC2인스턴스가 Windows Server 2008 R2 이상을 실행하고 있는지 확인하십시오.
    2. 인스턴스가 실행되는 동일한 가용 영역에 6GB EBS 볼륨을 생성합니다. 볼륨을 인스턴스에 연결합니다. 예를 들면 드라이브 D에 탑재합니다.
    3. 를 ISO 마우스 오른쪽 버튼으로 클릭하고 인스턴스 (예: 드라이브 E) 에 마운트합니다.
    4. E:\ ISO 드라이브의 내용을 D:\ 드라이브로 복사합니다.
    5. 2단계에서 만든 6GB 볼륨의 EBS 스냅샷을 생성합니다.

제한 사항

- Windows 인증을 사용하는 SQL 서버에서만 업그레이드를 수행할 수 있습니다.
- 인스턴스에서 대기 중인 보안 패치 업데이트가 없는지 확인합니다. 제어판을 열고 나서 업데이트 확인을 선택합니다.
- SQLHA 및 미러링 모드의 서버 배포는 지원되지 않습니다.

Parameters

- IamInstanceProfile

  타입: 문자열

  설명: (필수) IAM 인스턴스 프로파일입니다.
- InstanceId

  타입: 문자열

  설명: (필수) Windows Server 2008 R2 (이상) 및 SQL 서버 2008 (이상) 을 실행하는 인스턴스입니다.
- KeepPreUpgradeImageBackUp

  타입: 문자열

  설명: (선택 사항) 로 `true` 설정하면 자동화가 업그레이드 전에 인스턴스에서 AMI 만든 인스턴스를 삭제하지 않습니다. 로 `true` 설정된 경우 를 삭제해야 합니다AMI. 기본적으로 AMI 은 삭제됩니다.
- SubnetId

  타입: 문자열

  설명: (필수) 업그레이드 프로세스에 대한 서브넷을 제공합니다. 서브넷이 AWS 서비스, Amazon S3 및 Microsoft (패치 다운로드) 에 대한 아웃바운드 연결을 갖추고 있는지 확인합니다.
- SQLServerSnapshotId

  타입: 문자열

  설명: (조건부) 대상 SQL 서버 설치 미디어의 스냅샷 ID. 이 매개변수는 BYOL SQL 서버 버전을 사용하는 인스턴스에 필요합니다. 이 파라미터는 SQL 서버 라이선스가 포함된 인스턴스 (Microsoft SQL Server가 설치된 Windows Server용 제공된 AWS Amazon 머신 이미지를 사용하여 시작된 인스턴스) 의 경우 선택 사항입니다.
- RebootInstanceBeforeTakingImage

  타입: 문자열

  설명: (선택 사항) 로 설정하면 사전 `true` 업그레이드를 생성하기 전에 자동화가 인스턴스를 재부팅합니다. AMI 기본적으로, 이 자동화는 업그레이드 전에 재부팅되지 않습니다.
- T argetSQLVersion

타입: 문자열

설명: (선택 사항) 대상 SQL 서버 버전을 선택합니다.

가능한 대상:

- SQL서버 2019
- SQL서버 2017
- SQL서버 2016
- SQL서버 2014

기본 대상: SQL 서버 2016

출력

AMIId: 이후 버전의 SQL Server로 업그레이드된 인스턴스에서 AMI 만든 ID입니다.

AWSEC2-CloneInstanceAndUpgradeWindows

설명

Windows Server2008 R2, 2012 R2, 2016 또는 2019년 인스턴스에서 Amazon Machine Image (AMI)를 생성한 다음 이를 2016, 2019 또는 AMI 2022년으로 Windows Server 업그레이드하십시오. 지원되는 업그레이드 경로는 다음과 같습니다.

- Windows Server2008 R2에서 2016년까지 Windows Server
- Windows Server 2012 R2에서 Windows Server 2016으로
- Windows Server 2012 R2에서 Windows Server 2019로
- Windows Server 2012 R2에서 Windows Server 2022로
- Windows Server 2016에서 Windows Server 2019로
- Windows Server 2016에서 Windows Server 2022로
- Windows Server 2019에서 Windows Server 2022로

업그레이드 작업은 완료하는 데 2시간이 걸릴 수 있는 다단계 프로세스입니다. 2개 이상의 vCPU와 4GB 이상의 RAM을 이용하는 인스턴스에서 운영 체제 업그레이드를 수행하는 것이 좋습니다. 자동화는 인스턴스에서 AMI를 생성한 다음, 지정한 `SubnetId`의 새로 생성된 AMI에서 임시 인스턴스를 시작합니다. 원래 인스턴스와 연결된 보안 그룹이 임시 인스턴스에 적용됩니다. 이제 자동화는 임시 인스턴

스에서 `TargetWindowsVersion`에 대한 현재 위치 업그레이드를 수행합니다. Windows Server 2008 R2 인스턴스를 Windows Server 2016, 2019 또는 2022로 업그레이드하려면 Windows Server 2008 R2를 Windows Server 2016, 2019 또는 2022로 직접 업그레이드하는 것이 지원되지 않으므로 현재 위치 업그레이드가 두 번 수행됩니다. 이 자동화는 또한 임시 인스턴스에 필요한 AWS 드라이버를 업데이트하거나 설치합니다. 업그레이드 후 이 자동화는 임시 인스턴스에서 새 AMI를 생성한 다음 임시 인스턴스를 종료합니다.

Amazon Virtual Private Cloud(Amazon VPC)의 업그레이드된 AMI에서 테스트 인스턴스를 시작하여 애플리케이션 기능을 테스트할 수 있습니다. 테스트를 완료하고 난 후나 다른 업그레이드를 수행하기 전에는 업그레이드된 AMI로 완전히 전환하기에 앞서 애플리케이션 중단 시간을 예약하십시오.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows Server 2008 R2, 2012 R2, 2016 또는 2019 Standard 및 Datacenter Edition

사전 조건

- TLS 버전 1.2.
- 인스턴스에 SSM Agent가 설치되었는지 확인합니다. 자세한 내용은 Windows Server용 EC2 인스턴스에 SSM Agent 설치 및 구성을 참조하세요.
- 인스턴스에 Windows PowerShell 3.0 이상이 설치되어 있어야 합니다.
- Microsoft Active Directory 도메인에 조인된 인스턴스의 경우, 호스트 이름 충돌을 피하기 위해 도메인 컨트롤러에 연결되지 않은 `SubnetId`를 지정하는 것이 좋습니다.
- 인스턴스 서브넷에는 Amazon S3와 AWS 서비스 같은 액세스와 Microsoft의 패치 다운로드 액세스를 제공하는 인터넷에 대한 아웃바운드 연결이 있어야 합니다. 서브넷이 퍼블릭 서브넷이고 인스턴스에 퍼블릭 IP 주소가 있거나, 서브넷이 퍼블릭 NAT 디바이스에 인터넷 트래픽을 전송하는 경로가 있는 프라이빗 서브넷인 경우에 이 요구 사항이 충족됩니다.
- 이 자동화는 Windows Server 2008 R2, 2012 R2, 2016 및 2019 인스턴스에서만 작동합니다.

- Systems Windows Server Manager에 필요한 권한을 제공하는 AWS Identity and Access Management (IAM) 인스턴스 프로필로 인스턴스를 구성합니다. 자세한 내용은 Systems Manager용 IAM 인스턴스 프로파일 생성을 참조하세요.
- 인스턴스의 부트 디스크에 20GB의 사용 가능한 디스크 공간이 있는지 확인합니다.
- 인스턴스가 AWS 제공한 Windows 라이선스를 사용하지 않는 경우 Windows Server 2012 R2 설치 미디어가 포함된 Amazon EBS 스냅샷 ID를 지정하십시오. 방법:
  - EC2 인스턴스가 Windows Server 2012 이상을 실행 중인지 확인합니다.
  - 인스턴스가 실행 중인 동일 가용 영역에서 6GB EBS 볼륨을 생성합니다. 볼륨을 인스턴스에 연결합니다. 예를 들면 드라이브 D에 탑재합니다.
  - ISO를 마우스 오른쪽 버튼으로 클릭하고 인스턴스(예를 들면 드라이브 E)에 탑재합니다.
  - 드라이브 E:\에서 드라이브 D:\로 ISO의 내용을 복사합니다.
  - 위의 2단계에서 생성한 6GB 볼륨의 EBS 스냅샷을 생성합니다.

제한 사항

이 자동화는 Windows 도메인 컨트롤러, 클러스터 또는 Windows 데스크톱 운영 체제 업그레이드를 지원하지 않습니다. Automation은 다음 역할이 설치된 Windows Server용 EC2 인스턴스를 지원하지 않습니다.

- 원격 데스크톱 세션 호스트(RDSH)
- 원격 데스크톱 연결 브로커(RDCB)
- 원격 데스크톱 가상화 호스트(RDVH)
- 원격 데스크톱 웹 액세스(RDWA)

Parameters

- AlternativeKeyPairName

  타입: 문자열

  설명: (선택 사항) 업그레이드 프로세스 중에 사용할 대체 키 페어의 이름입니다. 이는 기존 인스턴스에 할당된 키 페어를 사용할 수 없는 경우에 유용합니다. 기존 인스턴스에 키 페어가 할당되지 않은 경우 이 파라미터의 값을 지정해야 합니다.
- BYOL WindowsMediaSnapshotId

  타입: 문자열

설명: (선택 사항) 복사할 Amazon EBS 스냅샷(Windows Server 2012R2 설치 미디어 포함)의 ID입니다. BYOL 인스턴스를 업그레이드하려는 경우에만 필수입니다.

- IamInstanceProfile

  타입: 문자열

  설명: (필수) Systems Manager에서 인스턴스를 관리할 수 있는 IAM 인스턴스 프로파일의 이름입니다.

- InstanceId

  타입: 문자열

  설명: (필수) Windows Server 2008 R2, 2012 R2, 2016 또는 2019를 실행하는 EC2 인스턴스입니다.

- KeepPreUpgradeImageBackUp

  타입: 문자열

  설명: (선택 사항) True로 설정된 경우 이 자동화는 업그레이드 전에 EC2 인스턴스에서 생성된 AMI를 삭제하지 않습니다. True로 설정된 경우 AMI를 삭제해야 합니다. 기본적으로 AMI가 삭제됩니다.

- SubnetId

  타입: 문자열

  설명: (필수) 업그레이드 프로세스를 위한 서브넷으로, 소스 EC2 인스턴스가 상주합니다. 서브넷이 AWS 서비스, Amazon S3 및 Microsoft (패치 다운로드) 에 대한 아웃바운드 연결이 있는지 확인합니다.

- TargetWindowsVersion

  타입: 문자열

  설명: (필수) 대상 Windows 버전을 선택합니다.

  기본값: 2022

- RebootInstanceBeforeTakingImage

  타입: 문자열

  설명: (선택 사항) True로 설정된 경우 이 자동화는 업그레이드 이전 AMI를 생성하기 전에 인스턴스를 재부팅합니다. 기본적으로 이 자동화는 업그레이드 전에 재부팅하지 않습니다.

AWSEC2-ConfigureSTIG

보안 기술 구현 가이드 (STIGs) 는 정보 시스템 및 소프트웨어를 보호하기 위해 국방 정보 시스템국 (DISA) 에서 만든 구성 강화 표준입니다. 시스템이 STIG 표준을 준수하도록 하려면 다양한 보안 설정을 설치, 구성 및 테스트해야 합니다.

EC2Amazon은 인스턴스에 STIG 설정을 적용하는 데 사용할 수 있는 Systems Manager 런북을 제공합니다. AWSEC2-ConfigureSTIG 이 문서는 표준을 준수하는 이미지를 신속하게 구축하는 데 도움이 됩니다. STIG STIGSystems Manager 문서는 잘못된 구성을 검사하고 수정 스크립트를 실행합니다. 또한 국방부 (DoD) InstallRoot 에서 AMIs Windows에 설치하여 DoD 인증서를 설치 및 업데이트하고 규정 준수를 유지하기 위해 불필요한 인증서를 제거합니다. STIG STIGSystems Manager 문서 사용에 따른 추가 요금은 없습니다.

> **Important**
>
> Systems Manager 문서에서 다운로드하는 구성 요소를 STIG 강화해도 타사 패키지는 설치되지 않는 몇 가지 예외가 있습니다. 타사 패키지가 이미 인스턴스에 설치되어 있고 Amazon에서 해당 패키지에 STIGs EC2 지원하는 관련 패키지가 있는 경우 해당 STIGs 패키지가 적용됩니다.

이 페이지에는 STIG 강화 구성 요소가 EC2 인스턴스에 적용되는 Amazon이 STIGs EC2 지원하는 모든 내용이 나열되어 있습니다.

적용할 STIG 규정 준수 범주를 선택할 수 있습니다.

규정 준수 수준

- 높음(카테고리 I)

  가장 심각한 위험. 기밀성, 가용성 또는 무결성의 손실을 초래할 수 있는 모든 취약성을 포함합니다.
- 보통(카테고리 II)

  기밀성, 가용성 또는 무결성의 손실을 초래할 수 있지만 위험을 완화할 수 있는 모든 취약성을 포함합니다.
- 낮음 (카테고리III)

  기밀성, 가용성 또는 무결성의 손실을 방지하기 위해 조치를 저하시키는 모든 취약성을 포함합니다.

주제

- STIG구성 요소 다운로드 강화
- 윈도우 설정 STIG
- 윈도우 버전 기록 STIG
- 리눅스 STIG 설정
- 리눅스 STIG 버전 기록

STIG구성 요소 다운로드 강화

Amazon은 STIG 강화 구성 요소를 각 릴리스의 운영 체제 관련 번들로 그룹화합니다. 번들은 다운로드 및 실행되는 대상 운영 체제에 적합한 아카이브 파일입니다. Linux 구성 요소 번들은 TAR 파일 (.tgz 파일 확장자) 로 저장됩니다. Windows 구성 요소 번들은 ZIP 파일 (.zip 파일 확장자) 로 저장됩니다.

Amazon은 구성 요소 번들을 각각 AWS 리전의 Image Builder S3 `STIG` 버킷에 저장합니다. SSL/를 사용하여 리소스와 TLS AWS 통신할 수 있습니다. TLS1.2가 필요하고 TLS 1.3을 권장합니다.

구성 요소 스토리지 경로와 번들 파일 이름의 패턴 및 예는 다음과 같습니다.

구성 요소 스토리지 경로

`s3://aws-windows-downloads-<region>/STIG/<bundle file name>`

구성 요소 경로 변수

region

AWS 리전 (각 지역에는 자체 구성 요소 버킷이 있습니다.)

bundle file name

형식은 다음과 같습니다.*<os bundle name>*_*<YYYY>*_Q*<quarter>*[_*<release>*].*<file extension>*. 이름에는 마침표가 아니라 노드 사이에 밑줄이 있다는 점에 유의하세요.

os bundle name

운영 체제 번들의 표준 이름 접두사는 `LinuxAWSConfigureSTIG` 또는 `AWSConfigureSTIG`입니다. 이전 버전과의 호환성을 유지하기 위해 Windows용 다운로드에는 플랫폼 접두사가 포함되지 않습니다.

YYYY

릴리스 연도는 4자리 숫자입니다.

quarter

해당 연도의 분기를 1, 2, 3 또는 4로 식별합니다.

release

1부터 시작하여 새 릴리스마다 1씩 증가하는 증분 번호입니다. 릴리스는 분기 내 첫 번째 릴리스에는 포함되지 않으며 후속 릴리스에만 추가됩니다.

file extension

압축 파일 형식 `tgz`(Linux) 또는 `zip`(Windows)입니다.

번들 파일 이름 예시

- `LinuxAWSConfigureSTIG_2023_Q1_2.tgz`
- `AWSConfigureSTIG_2022_Q4.zip`

윈도우 설정 STIG

Amazon EC2 Windows STIG AMIs 및 강화 구성 요소는 독립형 서버용으로 설계되었으며 로컬 그룹 정책을 적용합니다. STIG-DoD 인증서를 다운로드, 설치 및 AMIs 업데이트하려면 Windows 국방부(DoD) InstallRoot 에서 호환 구성 요소를 설치합니다. 또한 규정 준수를 유지하기 위해 불필요한 인증서를 제거합니다. STIG 현재 아마존은 2012 R2, 2016, 2019, 2022와 같은 윈도우 서버 버전에 대한 STIG 베이스라인을 EC2 지원합니다.

이 섹션에는 Amazon이 Windows 인프라에 EC2 지원하는 현재 STIG 설정과 버전 기록 로그가 나열되어 있습니다.

낮음, 중간 또는 높음 STIG 설정을 적용할 수 있습니다.

윈도우 STIG 로우 (카테고리III)

다음 목록에는 Amazon이 인프라에 EC2 지원하는 STIG 설정이 포함되어 있습니다. 지원되는 설정이 인프라에 적용되지 않는 경우 Amazon은 해당 설정을 EC2 건너뛰고 계속 진행합니다. 예를 들어 일부 STIG 강화 설정은 독립형 서버에는 적용되지 않을 수 있습니다. 조직별 정책도 적용되는 설정 종류(예: 관리자가 문서 설정을 검토하기 위한 요구 사항)에 영향을 미칠 수 있습니다.

전체 Windows 목록은 STIGs문서 STIGs 라이브러리를 참조하십시오. 전체 목록을 보는 방법에 대한 자세한 내용은 STIG보기 도구를 참조하십시오.

- 윈도우 서버 2022 STIG 버전 1 릴리스 1

V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 및 V-254481

- 윈도우 서버 2019 STIG 버전 2 릴리스 5

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871, 및 V-205923

- 윈도우 서버 2016 STIG 버전 2 릴리스 5

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 및 V-225060

- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 5

  V-225537, V-225536, V-225526, V-225525, V-225514, V-225511, V-225490, V-225489, V-225488, V-225487, V-225485, V-225484, V-225483, V-225482, V-225481, V-225480, V-225479, V-225476, V-225473, V-225468, V-225462, V-225460, V-225459, V-225412, V-225394, V-225392, V-225376, V-225363, V-225362, V-225360, V-225359, V-225358, V-225357, V-225355, V-225343, V-225342, V-225336, V-225335, V-225334, V-225333, V-225332, V-225331, V-225330, V-225328, V-225327, V-225324, V-225319, V-225318 및 V-225250

- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 2

  Microsoft에는 STIG 설정이 적용되지 않습니다. NET카테고리 III 취약성에 대한 프레임워크.

- 윈도우 방화벽 STIG 버전 2 릴리스 1

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 및 V-242008

- 인터넷 익스플로러 11 STIG 버전 2 릴리스 3

  V-46477, V-46629 및 V-97527

- 마이크로소프트 엣지 STIG 버전 1 릴리스 6 (윈도우 서버 2022만 해당)

  V-235727, V-235731, V-235751, V-235752 및 V-235765

윈도우 STIG 미디엄 (카테고리 II)

다음 목록에는 Amazon이 인프라에 EC2 지원하는 STIG 설정이 포함되어 있습니다. 지원되는 설정이 인프라에 적용되지 않는 경우 Amazon은 해당 설정을 EC2 건너뛰고 계속 진행합니다. 예를 들어 일부 STIG 강화 설정은 독립형 서버에는 적용되지 않을 수 있습니다. 조직별 정책도 적용되는 설정 종류(예: 관리자가 문서 설정을 검토하기 위한 요구 사항)에 영향을 미칠 수 있습니다.

전체 Windows 목록은 STIGs문서 STIGs 라이브러리를 참조하십시오. 전체 목록을 보는 방법에 대한 자세한 내용은 STIG보기 도구를 참조하십시오.

> **Note**
>
> Windows STIG Medium 카테고리에는 Amazon에서 카테고리 II 취약성에 대해 EC2 지원하는 STIG 강화 설정 외에도 Windows STIG 로우 (카테고리III) 에 적용되는 나열된 모든 STIG 강화 설정이 포함됩니다.

- 윈도우 서버 2022 STIG 버전 1 릴리스 1

  Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  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-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-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 및 V-254512

- 윈도우 서버 2019 STIG 버전 2 릴리스 5

  Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

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-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 및 V-236001

- 윈도우 서버 2016 STIG 버전 2 릴리스 5

  Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  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-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 및 V-236000

- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 5

  Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  V-225574, V-225573, V-225572, V-225571, V-225570, V-225569, V-225568, V-225567, V-225566, V-225565, V-225564, V-225563, V-225562, V-225561, V-225560, V-225559, V-225558, V-225557, V-225555, V-225554, V-225553, V-225551, V-225550, V-225549, V-225548, V-225546, V-225545, V-225544, V-225543, V-225542, V-225541, V-225540, V-225539, V-225538, V-225535, V-225534, V-225533, V-225532, V-225531, V-225530, V-225529, V-225528, V-225527, V-225524, V-225523, V-225522, V-225521, V-225520, V-225519, V-225518, V-225517, V-225516, V-225515, V-225513, V-225510, V-225509, V-225508, V-225506, V-225504, V-225503, V-225502, V-225501, V-225500, V-225494, V-225486, V-225478, V-225477, V-225475, V-225474, V-225472, V-225471, V-225470, V-225469, V-225464, V-225463, V-225461, V-225458, V-225457, V-225456, V-225455, V-225454, V-225453, V-225452, V-225448, V-225443, V-225442, V-225441, V-225415, V-225414, V-225413, V-225411, V-225410, V-225409, V-225408, V-225407, V-225406, V-225405, V-225404, V-225402, V-225401, V-225400, V-225398, V-225397, V-225395, V-225393, V-225391, V-225389, V-225386, V-225385, V-225384, V-225383, V-225382, V-225381, V-225380, V-225379, V-225378, V-225377, V-225375, V-225374, V-225373, V-225372, V-225371, V-225370, V-225369, V-225368, V-225367, V-225356, V-225353, V-225352, V-225351, V-225350, V-225349, V-225348, V-225347, V-225346, V-225345, V-225344, V-225341, V-225340, V-225339, V-225338, V-225337, V-225329, V-225326, V-225325, V-225317, V-225316, V-225315, V-225314, V-225305, V-225304, V-225303, V-225302, V-225301, V-225300, V-225299, V-225298, V-225297, V-225296, V-225295, V-225294, V-225293, V-225292, V-225291, V-225290, V-225289, V-225288, V-225287, V-225286, V-225285, V-225284, V-225283, V-225282, V-225281, V-225280, V-225279, V-225278, V-225277, V-225276, V-225275, V-225273, V-225272, V-225271, V-225270, V-225269, V-225268, V-225267, V-225266, V-225265, V-225264, V-225263, V-225261, V-225260, V-225259 및 V-225239

- 마이크로소프트. NET프레임워크 STIG 4.0 버전 2 릴리스 2

  Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  V-225238

- 윈도우 방화벽 STIG 버전 2 릴리스 1

Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

V-241989, V-241990, V-241991, V-241993, V-241998 및 V-242003

- 인터넷 익스플로러 11 STIG 버전 2 릴리스 3

  Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  V-46473, V-46475, V-46481, V-46483, V-46501, V-46507, V-46509, V-46511, V-46513, V-46515, V-46517, V-46521, V-46523, V-46525, V-46543, V-46545, V-46547, V-46549, V-46553, V-46555, V-46573, V-46575, V-46577, V-46579, V-46581, V-46583, V-46587, V-46589, V-46591, V-46593, V-46597, V-46599, V-46601, V-46603, V-46605, V-46607, V-46609, V-46615, V-46617, V-46619, V-46621, V-46625, V-46633, V-46635, V-46637, V-46639, V-46641, V-46643, V-46645, V-46647, V-46649, V-46653, V-46663, V-46665, V-46669, V-46681, V-46685, V-46689, V-46691, V-46693, V-46695, V-46701, V-46705, V-46709, V-46711, V-46713, V-46715, V-46717, V-46719, V-46721, V-46723, V-46725, V-46727, V-46729, V-46731, V-46733, V-46779, V-46781, V-46787, V-46789, V-46791, V-46797, V-46799, V-46801, V-46807, V-46811, V-46815, V-46819, V-46829, V-46841, V-46847, V-46849, V-46853, V-46857, V-46859, V-46861, V-46865, V-46869, V-46879, V-46883, V-46885, V-46889, V-46893, V-46895, V-46897, V-46903, V-46907, V-46921, V-46927, V-46939, V-46975, V-46981, V-46987, V-46995, V-46997, V-46999, V-47003, V-47005, V-47009, V-64711, V-64713, V-64715, V-64717, V-64719, V-64721, V-64723, V-64725, V-64729, V-72757, V-72759, V-72761, V-72763, V-75169 및 V-75171

- 마이크로소프트 엣지 STIG 버전 1 릴리스 6 (윈도우 서버 2022만 해당)

  V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774 및 V-246736

- 디펜더 STIG 버전 2 릴리스 4 (윈도우 서버 2022만 해당)

  V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465 및 V-213466

윈도우 STIG 하이 (카테고리 I)

다음 목록에는 Amazon이 인프라에 EC2 지원하는 STIG 설정이 포함되어 있습니다. 지원되는 설정이 인프라에 적용되지 않는 경우 Amazon은 해당 설정을 EC2 건너뛰고 계속 진행합니다. 예를 들어 일부 STIG 강화 설정은 독립형 서버에는 적용되지 않을 수 있습니다. 조직별 정책도 적용되는 설정 종류(예: 관리자가 문서 설정을 검토하기 위한 요구 사항)에 영향을 미칠 수 있습니다.

전체 Windows 목록은 STIGs문서 STIGs 라이브러리를 참조하십시오. 전체 목록을 보는 방법에 대한 자세한 내용은 STIG보기 도구를 참조하십시오.

> **Note**
>
> Windows STIG 높음 카테고리에는 Amazon에서 카테고리 I 취약성에 대해 EC2 지원하는 STIG 강화 설정 외에도 Windows STIG 중간 및 낮음 카테고리에 적용되는 나열된 모든 STIG 강화 설정이 포함됩니다.

- 윈도우 서버 2022 STIG 버전 1 릴리스 1

  V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475 및 V-254500
- 윈도우 서버 2019 STIG 버전 2 릴리스 5

  Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914 및 V-205919
- 윈도우 서버 2016 STIG 버전 2 릴리스 5

  Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054 및 V-225079
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 5

  Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

V-225556, V-225552, V-225547, V-225507, V-225505, V-225498, V-225497, V-225496, V-225493, V-225492, V-225491, V-225449, V-225444, V-225399, V-225396, V-225390, V-225366, V-225365, V-225364, V-225354 및 V-225274

- 마이크로소프트. NET프레임워크 STIG 4.0 버전 2 릴리스 2

  Microsoft의 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 Amazon이 EC2 지원하는 모든 STIG 강화 설정이 포함되어 있습니다. NET프레임워크. 카테고리 I 취약성에는 추가 STIG 설정이 적용되지 않습니다.

- 윈도우 방화벽 STIG 버전 2 릴리스 1

  Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  V-241992, V-241997 및 V-242002

- 인터넷 익스플로러 11 STIG 버전 2 릴리스 3

  Internet Explorer 11의 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 Amazon이 EC2 지원하는 모든 STIG 강화 설정이 포함되어 있습니다. 카테고리 I 취약성에는 추가 STIG 설정이 적용되지 않습니다.

- 마이크로소프트 엣지 STIG 버전 1 릴리스 6 (윈도우 서버 2022만 해당)

  Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  V-235758 및 V-235759

- 디펜더 STIG 버전 2 릴리스 4 (윈도우 서버 2022만 해당)

  Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

  V-213426, V-213452 및 V-213453

윈도우 버전 기록 STIG

이 섹션에서는 분기별 STIG 업데이트의 Windows 구성 요소 버전 기록을 기록합니다. 한 분기의 변경 사항과 게시된 버전을 보려면 제목을 선택하여 정보를 확장하세요.

2024년 2분기 변경 - 2024년 5월 10일 (변경 없음):

2024년 2분기 릴리스의 Windows 구성 STIGS 요소에는 변경 사항이 없습니다.

2024년 1분기 변경 사항 - 2024년 2월 23일 (변경 없음):

2024년 1분기 릴리스의 Windows 구성 STIGS 요소에는 변경 사항이 없습니다.

2023년 4분기 변경 - 2023년 7월 12일 (변경 없음):

2023년 4분기 릴리스의 윈도우 구성 STIGS 요소에는 변경 사항이 없습니다.

2023년 3분기 변경 사항 - 2023년 10월 4일(변경 없음):

2023년 3분기 릴리스의 Windows 구성 STIGS 요소에는 변경 사항이 없습니다.

2023년 2분기 변경 사항 - 2023년 5월 3일(변경 없음):

2023년 2분기 릴리스의 Windows 구성 STIGS 요소에는 변경 사항이 없습니다.

2023년 1분기 변경 사항 - 2023년 3월 27일(변경 없음):

2023년 1분기 릴리스의 Windows 구성 STIGS 요소에는 변경 사항이 없습니다.

2022년 4분기 변경 사항 - 2023년 2월 1일:

다음과 같이 STIG 버전이 업데이트되어 2022년 4분기 STIGS 릴리스에 적용되었습니다.

STIG-빌드-윈도우-로우 버전 2022.4.0

- 윈도우 서버 2022 버전 1 릴리스 1 STIG
- 윈도우 서버 2019 STIG 버전 2 릴리스 5
- 윈도우 서버 2016 STIG 버전 2 릴리스 5
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 5
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 2
- 윈도우 방화벽 STIG 버전 2 릴리스 1
- 인터넷 익스플로러 11 STIG 버전 2 릴리스 3
- 마이크로소프트 엣지 STIG 버전 1 릴리스 6 (윈도우 서버 2022만 해당)

STIG- 빌드-윈도우-미디엄 버전 2022.4.0

- 윈도우 서버 2022 버전 1 릴리스 1 STIG

- 윈도우 서버 2019 STIG 버전 2 릴리스 5
- 윈도우 서버 2016 STIG 버전 2 릴리스 5
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 5
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 2
- 윈도우 방화벽 STIG 버전 2 릴리스 1
- 인터넷 익스플로러 11 STIG 버전 2 릴리스 3
- 마이크로소프트 엣지 STIG 버전 1 릴리스 6 (윈도우 서버 2022만 해당)
- 디펜더 STIG 버전 2 릴리스 4 (윈도우 서버 2022만 해당)

STIG- 빌드 - 윈도우 하이 버전 2022.4.0

- 윈도우 서버 2022 버전 1 릴리스 1 STIG
- 윈도우 서버 2019 STIG 버전 2 릴리스 5
- 윈도우 서버 2016 STIG 버전 2 릴리스 5
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 5
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 2
- 윈도우 방화벽 STIG 버전 2 릴리스 1
- 인터넷 익스플로러 11 STIG 버전 2 릴리스 3
- 마이크로소프트 엣지 STIG 버전 1 릴리스 6 (윈도우 서버 2022만 해당)
- 디펜더 STIG 버전 2 릴리스 4 (윈도우 서버 2022만 해당)

2022년 3분기 변경 사항 - 2022년 9월 30일(변경 없음):

2022년 3분기 릴리스의 Windows 구성 STIGS 요소에는 변경 사항이 없습니다.

2022년 2분기 변경 사항 - 2022년 8월 2일:

STIG버전이 업데이트되어 2022년 2분기 STIGS 릴리스에 적용되었습니다.

STIG-빌드-윈도우-로우 버전 1.5.0

- 윈도우 서버 2019 버전 2 릴리스 4 STIG
- 윈도우 서버 2016 STIG 버전 2 릴리스 4
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 3

- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 1
- 윈도우 방화벽 STIG 버전 2 릴리스 1
- 인터넷 익스플로러 11 STIG 버전 1 릴리스 19

STIG-빌드-윈도우-미디엄 버전 1.5.0

- 윈도우 서버 2019 버전 2 릴리스 4 STIG
- 윈도우 서버 2016 STIG 버전 2 릴리스 4
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 3
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 1
- 윈도우 방화벽 STIG 버전 2 릴리스 1
- 인터넷 익스플로러 11 STIG 버전 1 릴리스 19

STIG-빌드-윈도우-하이 버전 1.5.0

- 윈도우 서버 2019 버전 2 릴리스 4 STIG
- 윈도우 서버 2016 STIG 버전 2 릴리스 4
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 3
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 1
- 윈도우 방화벽 STIG 버전 2 릴리스 1
- 인터넷 익스플로러 11 STIG 버전 1 릴리스 19

2022년 1분기 변경 사항 - 2022년 8월 2일(변경 없음):

2022년 1분기 릴리스의 Windows 구성 STIGS 요소에는 변경 사항이 없습니다.

2021년 4분기 변경 사항 - 2021년 12월 20일:

STIG버전이 업데이트되어 2021년 4분기 STIGS 릴리스에 적용되었습니다.

STIG-빌드-윈도우-로우 버전 1.5.0

- 윈도우 서버 2019 버전 2 릴리스 3 STIG
- 윈도우 서버 2016 STIG 버전 2 릴리스 3
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 3

- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 1
- 윈도우 방화벽 STIG 버전 2 릴리스 1
- 인터넷 익스플로러 11 STIG 버전 1 릴리스 19

STIG-빌드-윈도우-미디엄 버전 1.5.0

- 윈도우 서버 2019 버전 2 릴리스 3 STIG
- 윈도우 서버 2016 STIG 버전 2 릴리스 3
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 3
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 1
- 윈도우 방화벽 STIG 버전 2 릴리스 1
- 인터넷 익스플로러 11 STIG 버전 1 릴리스 19

STIG-빌드-윈도우-하이 버전 1.5.0

- 윈도우 서버 2019 버전 2 릴리스 3 STIG
- 윈도우 서버 2016 STIG 버전 2 릴리스 3
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 3
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 1
- 윈도우 방화벽 STIG 버전 2 릴리스 1
- 인터넷 익스플로러 11 STIG 버전 1 릴리스 19

2021년 3분기 변경 사항 - 2021년 9월 30일:

STIG버전이 업데이트되었으며 2021년 3분기 STIGS 릴리스에 적용되었습니다.

STIG-빌드-윈도우-로우 버전 1.4.0

- 윈도우 서버 2019 버전 2 릴리스 2 STIG
- 윈도우 서버 2016 STIG 버전 2 릴리스 2
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 2
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 1
- 윈도우 방화벽 STIG 버전 1 릴리스 7
- 인터넷 익스플로러 11 STIG 버전 1 릴리스 19

STIG-빌드-윈도우-미디엄 버전 1.4.0

- 윈도우 서버 2019 버전 2 릴리스 2 STIG
- 윈도우 서버 2016 STIG 버전 2 릴리스 2
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 2
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 1
- 윈도우 방화벽 STIG 버전 1 릴리스 7
- 인터넷 익스플로러 11 STIG 버전 1 릴리스 19

STIG-빌드-윈도우-하이 버전 1.4.0

- 윈도우 서버 2019 버전 2 릴리스 2 STIG
- 윈도우 서버 2016 STIG 버전 2 릴리스 2
- 윈도우 서버 2012 R2 MS STIG 버전 3 릴리스 2
- 마이크로소프트. NET프레임워크 4.0 STIG 버전 2 릴리스 1
- 윈도우 방화벽 STIG 버전 1 릴리스 7
- 인터넷 익스플로러 11 STIG 버전 1 릴리스 19

리눅스 STIG 설정

이 섹션에는 Amazon이 EC2 지원하는 Linux STIG 강화 설정에 대한 정보와 버전 기록 로그가 포함되어 있습니다. Linux 배포판에 자체 STIG 강화 설정이 없는 경우 EC2 Amazon은 RHEL 설정을 사용합니다. 지원되는 STIG 강화 설정은 Amazon EC2 Linux AMIs 및 Linux 배포를 기반으로 하는 구성 요소에 다음과 같이 적용됩니다.

- 레드햇 엔터프라이즈 리눅스 (RHEL) 7 설정 STIG
  - RHEL7
  - CentOS 7
  - 아마존 리눅스 2 (AL2)
- RHEL8가지 STIG 설정
  - RHEL8
  - CentOS 8
  - Amazon Linux 2023(AL 2023)

- RHEL9가지 STIG 설정
  - RHEL9
  - CentOS Stream 9

리눅스 STIG 로우 (카테고리III)

다음 목록에는 Amazon이 인프라에 EC2 지원하는 STIG 설정이 포함되어 있습니다. 지원되는 설정이 인프라에 적용되지 않는 경우 Amazon은 해당 설정을 EC2 건너뛰고 계속 진행합니다. 예를 들어 일부 STIG 강화 설정은 독립형 서버에는 적용되지 않을 수 있습니다. 조직별 정책도 적용되는 설정 종류(예: 관리자가 문서 설정을 검토하기 위한 요구 사항)에 영향을 미칠 수 있습니다.

전체 목록은 STIGs문서 라이브러리를 참조하십시오. 전체 목록을 보는 방법에 대한 자세한 내용은 STIG보기 도구를 참조하십시오.

RHEL7 STIG 버전 3 릴리스 14

- RHEL7/센토스 7/ AL2

  V-204452, V-204576 및 V-204605

RHEL8 STIG 버전 1 릴리스 14

- RHEL8/센토스 8/AL 2023

  V-230241, V-244527, V-230269, V-230270, V-230285, V-230253, V-230346 V-230381 V-230395 V-230468 V-230469 V-230491 V-230485 V-230486, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499, V-230281

RHEL9 버전 1 릴리스 3 STIG

- RHEL9/센토스 스트림 9

  V-257782, V-257795, V-257796, V-257824, V-257880, V-257946, V-257947 V-258037 V-258067 V-258069 V-258076 V-258173

우분투 18.04 STIG 버전 2 릴리스 14

V-219172, V-219173, V-219174, V-219175, V-219210, V-219164, V-219165 V-219178 V-219180 V-219301 V-219163 V-219332 V-219327 V-219333

우분투 20.04 STIG 버전 1 릴리스 12

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 V-238308

우분투 22.04 STIG 버전 1 릴리스 1

V-260472, V-260476, V-260479, V-260480, V-260481, V-260520, V-260521 V-260549 V-260550 V-260551 V-260552 V-260581 V-260596

리눅스 STIG 미디엄 (카테고리 II)

다음 목록에는 Amazon이 인프라에 EC2 지원하는 STIG 설정이 포함되어 있습니다. 지원되는 설정이 인프라에 적용되지 않는 경우 Amazon은 해당 설정을 EC2 건너뛰고 계속 진행합니다. 예를 들어 일부 STIG 강화 설정은 독립형 서버에는 적용되지 않을 수 있습니다. 조직별 정책도 적용되는 설정 종류(예: 관리자가 문서 설정을 검토하기 위한 요구 사항)에 영향을 미칠 수 있습니다.

전체 목록은 STIGs문서 라이브러리를 참조하십시오. 전체 목록을 보는 방법에 대한 자세한 내용은 STIG보기 도구를 참조하십시오.

> **Note**
>
> Linux STIG Medium 카테고리에는 Amazon이 카테고리 II 취약성에 대해 EC2 지원하는 STIG 강화 설정 외에도 Linux STIG Low (카테고리III) 에 적용되는 나열된 모든 STIG 강화 설정이 포함됩니다.

RHEL7 STIG 버전 3 릴리스 14

Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

- RHEL7/센토스 7/ AL2

  V-204585, V-204490, V-204491, V-255928, V-204405, V-204406, V-204407, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204422, V-204423, V-204427, V-204416, V-204418, V-204426, V-204431, V-204457, V-204466, V-204417, V-204434, V-204435, V-204587, V-204588, V-204589, V-204591, V-204592, V-204596, V-204597, V-204596, V-204597, V-204596, V-204597, V-204596 98, V-204599, V-204600, V-204601, V-204602, V-204622, V-233307, V-255925, V-204578, V-204595, V-204437, V-204503, V-204507, V-204508, V-204511, V-204512, V-204514,

V-204512, V-204514, V-204512, V-204514, V-204512, V-204514, V-204512 4515, 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-204584, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204625, V-204630, V-255927, V-237634, V-237635, V-251703, V-204449, V-204451, V-204619, V-20451, V-204619, V-20451 79,V-204631, V-204633, V-256970

RHEL8 STIG 버전 1 릴리스 14

Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

- RHEL8/센토스 8/AL 2023

V-230257, V-230258, V-230259, V-230550, V-230248, V-230249, V-230250, V-230245, V-230246, V-230247, V-230397, V-230399, V-230400, V-230401, V-230228, V-230298, V-230387, V-230231, V-230233, V-230324, V-230365, V-230370, V-230378, V-230383, V-230236, V-230314, V-230315, V-244523, V-230267, V-230268, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, V-230280, 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-230543, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544, V-230544 30546, 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-230369, V-230375, V-230375, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230376, V-230377, V-244524, V-244533, V-251713, V-251717, V-251714, V-251715, V-251716, V-230332, V-230334, V-230336, V-230338, V-230340, V-230344, V-230333, V-230333, V-230333, V-230333, V-230333, V-230333, V-230333, V-230333, V-230335, V-230333, V-230333, V-230333, V-230335, V-230333, V-230333, V-230335, V-230333, 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-230399 2, 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-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-230439, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, V-230444, 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-230473, V-230473, V-230473, V-230473, V-230473, V-230473, V-230474, V-230473, V-230473, V-230474, V-230473, V-230473, V-230474, V-230473, V-230473, V-230473, V-230474, V-230473, V-230473, V-230480, V-230483, V-244542, V-230503, V-230244, V-230286, V-230287, V-230288, V-230290, V-230291,V-230296, V-230330, V-230382, V-230526, V-230527, V-230555, V-230556 V-244526 V-244528 V-237642 V-237643 V-251711 V-230238 V-230239 V-230273 V-230275, V-230478, V-230488, V-230489, V-230559, V-230560, V-230561, V-237640, V-256974

RHEL9 STIG 버전 1 릴리스 3

Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

- RHEL9/센토스 스트림 9

  V-257780, V-257781, V-257783, V-257786, V-257788, V-257790, V-257791, V-257792, V-257793, V-257794, V-257797, V-257798, V-257799, V-257801, V-257802, V-257803, V-257803, V-257804, V-257803, V-257804, V-257803, V-257804, V-257803, V-257804, V-257803, V-257804, V-257803, V-257804, V-257803, V-257804, 257805, V-257806, V-257807, V-257808, V-257809, V-257810, V-257811, V-257812, V-257813, V-257814, V-257815, V-257816, V-257817, V-257825, V-257827, V-257828, V-257829, V-257829, V-257829, V-257829, 257830, V-257831, V-257832, V-257833, V-257834, V-257836, V-257838, V-257839, V-257840, V-257841, V-257842, V-257849, V-257882, V-257883, V-257884, V-257886, V-257886, V-257887, 257888, 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-257906, V-257907, V-257907, V-257907, V-257907 7909, V-257910, V-257911, V-257912, V-257913, V-257914, V-257915, V-257916, V-257917, V-257918, V-257919, V-257920, V-257921, V-257922, V-257924, V-257925, V-257926, V-257927, V-257927, 257928, V-257929, V-257930, V-257931, V-257933, V-257934, V-257935, V-257936, V-257939, V-257940, V-257942, V-257943, V-257944, V-257949, V-257951, V-257952, V-257953, V-257954, V-257957, 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-257976, V-257977, V-257978, V-257979, V-257980, V-257982, V-257985, V-257987, V-257988, V-257989, V-257991, V-257992, V-257993, V-257994, V-257996, V-257998, V-257999, V-258000, 258001, V-258002, V-258003, V-258004, V-258005, V-258006, V-258007, V-258008, V-258009, V-258010, V-258011, V-258028, V-258034, V-258035, V-258036, V-258038, V-258040, V-258041, V-258043, V-258043, 258049, V-258052,V-258054, V-258055, V-258056, V-258057, V-258060, V-258063, V-258064, V-258065, V-258066, V-258068, V-258070, V-258071, V-258072, V-258073, V-258077, V-258079, V-258080, V-258081, V-258082, V-258083, V-258084, V-258085, V-258088, V-258089, V-258090, V-258091, V-258092, V-258093, V-258095, V-258097, V-258098, V-258099, V-258100, V-258101, V-258102, V-258103, V-258104, V-258105, V-258107, V-258108, V-258109, V-258110, V-258111, V-258112, V-258113, V-258114, V-258115, V-258116, V-258117, V-258118, V-258119, V-258122, V-258123, V-258124,V-258125, V-258126, V-258128, V-258129, V-258130, V-258133, V-258134, V-258137, V-258140, V-258141, V-258144, V-258144, V-258147, V-258147, V-258147, V-258147, V-258147, V-258147, V-258147, V-258147, V-258147, V-258147, V-258148 150, V-258151, 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-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258166, V-258167, V-258168, V-258169, V-258170, V-258171, V-258172, V-258175, 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-258218, V-258219, V-258220, V-258221, V-258221, V-258221, V-258221, V-258221, V-258221, V-258221, V-258221, V-258221, V-258221, V-258221, V-258221, V-258221, V-258221 2, V-258223, V-258224, V-258225, V-258226, V-258227, V-258228, V-258229, V-258232, V-258234, V-258237, V-258239 및 V-258240

우분투 18.04 STIG 버전 2 릴리스 14

V-219188, V-219190, V-219191, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219208, V-219209, V-219303, V-219303, V-219303, 219326, V-219328, V-219330, V-219342, V-219189, V-219192, V-219193, V-219194, V-219315, V-219195, V-219196, V-219197, V-219213, V-219214, V-219215, V-219215, V-219216, V-219217, V-219218, V-219219, V-219220, V-219221, V-219222, V-219223, V-219224, V-219227, V-219228, V-219229, V-219230, V-219231, V-219232, V-219233, V-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-219309, V-219309, V-219309, V-219309, V-219310, V-219309, V-219309, V-219310, V-219309, V-2193010, V-219309, V-2193010, V-219309, V-2193010, V-219309, V-2193010, V-219309, V-219310, -219311, V-219312, V-233779, V-233780, V-255906, V-219336, V-219338, V-219344, V-219181, V-219184, V-219186, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-219156, V-V-219149, V-219166, V-219176, V-2193939, V-219331, V-219337, V-219335

우분투 20.04 STIG 버전 1 릴리스 12

V-238205, V-238207, V-238329, V-238337, V-238339, V-238340, V-238344, V-238345, V-238346, V-238347, V-238349, V-238351, V-238352, V-238376, V-238377, V-238378, V-238209, V-238325, V-238330, V-238333, V-238369, V-238338, V-238341, V-238342, V-238343, V-238353, V-238228, V-238227, V-238299, V-238238, V-238239, V-238240, V-238241, V-238242, V-238244, V-238245, V-238246, V-238247, V-238249, V-238249, V-238252, V-238252, V-238253, V-238253, 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-238302, V-238310, V-238315, V-238316, V-238317, V-238317, V-238318, V-238319, V-238320, V-251505, V-238360, V-238211, V-238212, V-238213, V-238216, V-238220, V-255912, V-238355, V-238236, V-238303, V-238303, V-238303, V-238303 358, V-238356, V-238359, V-238370 및 V-238334

우분투 22.04 STIG 버전 1 릴리스 1

Amazon이 카테고리 III (낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

V-260471, V-260473, V-260474, V-260475, V-260477, V-260478, V-260485, V-260486, V-260487, V-260488, V-260489, V-260491, V-260492, V-260493, V-260494, V-260495, V-260496, V-260497, V-260498, V-260499, V-260500, V-260505, V-260506, V-260507, V-260508, V-260509, V-260510, V-260511, V-260512, V-260513, V-260514, V-260516, V-260522, V-260527, V-260528, V-260530, V-260531, V-260532, V-260533, V-260534, V-260542, V-260543, V-260545, V-260546, V-260547, V-260553, V-260553, V-260553, V-260553, V-260553 4, V-260555, V-260556, V-260557, V-260560, V-260561, V-260562, V-260563, V-260564, V-260565,V-260566, V-260567, V-260568, V-260572, V-260573, V-260574, V-260576, V-260582, V-260584, V-260584, V-260589, V-260590, V-260591, V-260594, V-260597, V-260598, V-260599, V-260600, V-260601, V-260602, V-2603, V-2604, V-260605, V-260606, V-260607, 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-260627, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, V-260628, 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

리눅스 STIG 하이 (카테고리 I)

다음 목록에는 Amazon이 인프라에 EC2 지원하는 STIG 설정이 포함되어 있습니다. 지원되는 설정이 인프라에 적용되지 않는 경우 Amazon은 해당 설정을 EC2 건너뛰고 계속 진행합니다. 예를 들어 일부 STIG 강화 설정은 독립형 서버에는 적용되지 않을 수 있습니다. 조직별 정책도 적용되는 설정 종류(예: 관리자가 문서 설정을 검토하기 위한 요구 사항)에 영향을 미칠 수 있습니다.

전체 목록은 STIGs문서 라이브러리를 참조하십시오. 전체 목록을 보는 방법에 대한 자세한 내용은 STIG보기 도구를 참조하십시오.

> **Note**
>
> Linux STIG High 카테고리에는 Amazon이 카테고리 I 취약성에 대해 EC2 지원하는 STIG 강화 설정 외에도 Linux STIG Medium 및 Low 카테고리에 적용되는 나열된 모든 STIG 강화 설정이 포함됩니다.

RHEL7 STIG 버전 3 릴리스 14

Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

- RHEL7/센토스 7/ AL2

  V-204425, V-204594, V-204455, V-204424, V-204442, V-204443, V-204447 V-204448 V-204502 V-204620 V-204621

RHEL8 STIG 버전 1 릴리스 14

Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

- RHEL8/센토스 8/AL 2023

V-230265, V-230529, V-230531, V-230264, V-230487, V-230492, V-230533, V-230558

RHEL9 STIG 버전 1 릴리스 3

Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

- RHEL9/센토스 스트림 9

  V-257784, V-257785, V-257820, V-257821, V-257826, V-257835, V-257955 V-257956 V-257984 V-257986 V-258059 V-258078 V-258094 V-258235

우분투 18.04 STIG 버전 2 릴리스 14

V-219157, V-219158, V-219177, V-219212 V-219308, V-219314, V-219316, V-251507

우분투 20.04 STIG 버전 1 릴리스 12

V-238218, V-238219, V-238201, V-238326, V-238327, V-238380 및 V-251504

우분투 STIG 22.04버전 1 릴리스 1

Amazon이 카테고리 II 및 III (중간 및 낮음) 취약성에 대해 EC2 지원하는 모든 STIG 강화 설정과 함께 다음이 포함됩니다.

V-260469, V-260482, V-260483, V-260523, V-260524, V-260526, V-260529 V-260570 V-260571 V-260579

리눅스 STIG 버전 기록

이 섹션에서는 분기별 STIG 업데이트의 Linux 구성 요소 버전 기록을 기록합니다. 한 분기의 변경 사항과 게시된 버전을 보려면 제목을 선택하여 정보를 확장하세요.

2024년 2분기 변경 사항 - 2024년 5월 10일:

STIG버전이 업데이트되어 2024년 2분기 릴리스에 STIGS 적용되었습니다. 또한 다음과 같이 RHEL 9, CentOS 스트림 9 및 우분투 22.04에 대한 지원이 추가되었습니다.

STIG-빌드-리눅스-로우 버전 2024.2.x

- RHEL7 STIG 버전 3 릴리스 14

- RHEL8 STIG 버전 1 릴리즈 14
- RHEL9 STIG 버전 1 릴리즈 3
- 우분투 18.04 STIG 버전 2 릴리스 14
- 우분투 20.04 버전 1 릴리스 12 STIG
- 우분투 22.04버전 1 릴리즈 1 STIG

STIG-빌드-리눅스-미디엄 버전 2024.2.x

- RHEL7 STIG 버전 3 릴리스 14
- RHEL8 STIG 버전 1 릴리즈 14
- RHEL9 STIG 버전 1 릴리즈 3
- 우분투 18.04 STIG 버전 2 릴리스 14
- 우분투 20.04 버전 1 릴리스 12 STIG
- 우분투 22.04버전 1 릴리즈 1 STIG

STIG-빌드-리눅스 하이 버전 2024.2.x

- RHEL7 STIG 버전 3 릴리스 14
- RHEL8 STIG 버전 1 릴리즈 14
- RHEL9 STIG 버전 1 릴리즈 3
- 우분투 18.04 STIG 버전 2 릴리스 14
- 우분투 20.04 버전 1 릴리스 12 STIG
- 우분투 22.04버전 1 릴리즈 1 STIG

2024년 1분기 변경 사항 - 2024년 2월 6일:

다음과 같이 STIG 버전이 업데이트되어 2024년 1분기 STIGS 릴리스에 적용되었습니다.

STIG-빌드-리눅스-로우 버전 2024.1.x

- RHEL7 STIG 버전 3 릴리스 14
- RHEL8 STIG 버전 1 릴리즈 13
- 우분투 18.04 STIG 버전 2 릴리스 13
- 우분투 20.04 버전 1 릴리스 11 STIG

STIG-빌드-리눅스-미디엄 버전 2024.1.x

- RHEL7 STIG 버전 3 릴리스 14
- RHEL8 STIG 버전 1 릴리즈 13
- 우분투 18.04 STIG 버전 2 릴리스 13
- 우분투 20.04 버전 1 릴리스 11 STIG

STIG-빌드-리눅스 하이 버전 2024.1.x

- RHEL7 STIG 버전 3 릴리스 14
- RHEL8 STIG 버전 1 릴리즈 13
- 우분투 18.04 STIG 버전 2 릴리스 13
- 우분투 20.04 버전 1 릴리스 11 STIG

2023년 4분기 변경 사항 - 2023년 7월 12일:

다음과 같이 STIG 버전이 업데이트되어 2023년 4분기 STIGS 릴리스에 적용되었습니다.

STIG-빌드-리눅스-로우 버전 2023.4.x

- RHEL7 STIG 버전 3 릴리스 13
- RHEL8 STIG 버전 1 릴리즈 12
- 우분투 18.04 STIG 버전 2 릴리즈 12
- 우분투 20.04 버전 1 릴리즈 10 STIG

STIG-빌드-리눅스-미디엄 버전 2023.4.x

- RHEL7 STIG 버전 3 릴리스 13
- RHEL8 STIG 버전 1 릴리즈 12
- 우분투 18.04 STIG 버전 2 릴리즈 12
- 우분투 20.04 버전 1 릴리즈 10 STIG

STIG-빌드-리눅스 하이 버전 2023.4.x

- RHEL7 STIG 버전 3 릴리스 13

- RHEL8 STIG 버전 1 릴리즈 12
- 우분투 18.04 STIG 버전 2 릴리즈 12
- 우분투 20.04 버전 1 릴리즈 10 STIG

2023년 3분기 변경 사항 - 2023년 10월 4일:

다음과 같이 STIG 버전이 업데이트되어 2023년 3분기 STIGS 릴리스에 적용되었습니다.

리눅스 STIG 로우 (카테고리III)

- RHEL7 STIG 버전 3 릴리스 12
- RHEL8 STIG 버전 1 릴리즈 11
- 우분투 18.04 STIG 버전 2 릴리스 11
- 우분투 20.04 버전 1 릴리스 9 STIG

리눅스 STIG 미디엄 (카테고리 II)

- RHEL7 STIG 버전 3 릴리스 12
- RHEL8 STIG 버전 1 릴리즈 11
- 우분투 18.04 STIG 버전 2 릴리스 11
- 우분투 20.04 버전 1 릴리스 9 STIG

리눅스 STIG 하이 (카테고리 I)

- RHEL7 STIG 버전 3 릴리스 12
- RHEL8 STIG 버전 1 릴리즈 11
- 우분투 18.04 STIG 버전 2 릴리스 11
- 우분투 20.04 버전 1 릴리스 9 STIG

2023년 2분기 변경 사항 - 2023년 5월 3일:

다음과 같이 STIG 버전이 업데이트되어 2023년 2분기 STIGS 릴리스에 적용되었습니다.

리눅스 STIG 로우 (카테고리III)

- RHEL7 STIG 버전 3 릴리스 11

- RHEL8 STIG 버전 1 릴리즈 10
- 우분투 18.04 STIG 버전 2 릴리스 11
- 우분투 20.04 버전 1 릴리스 8 STIG

리눅스 STIG 미디엄 (카테고리 II)

- RHEL7 STIG 버전 3 릴리스 11
- RHEL8 STIG 버전 1 릴리즈 10
- 우분투 18.04 STIG 버전 2 릴리스 11
- 우분투 20.04 버전 1 릴리스 8 STIG

리눅스 STIG 하이 (카테고리 I)

- RHEL7 STIG 버전 3 릴리스 11
- RHEL8 STIG 버전 1 릴리즈 10
- 우분투 18.04 STIG 버전 2 릴리스 11
- 우분투 20.04 버전 1 릴리스 8 STIG

2023년 1분기 변경 사항 - 2023년 3월 27일:

다음과 같이 STIG 버전이 업데이트되고 2023년 1분기 STIGS 릴리스에 적용되었습니다.

리눅스 STIG 로우 (카테고리III)

- RHEL7 STIG 버전 3 릴리스 10
- RHEL8 STIG 버전 1 릴리즈 9
- 우분투 18.04 STIG 버전 2 릴리즈 10
- 우분투 20.04 버전 1 릴리스 7 STIG

리눅스 STIG 미디엄 (카테고리 II)

- RHEL7 STIG 버전 3 릴리스 10
- RHEL8 STIG 버전 1 릴리즈 9
- 우분투 18.04 STIG 버전 2 릴리즈 10
- 우분투 20.04 버전 1 릴리스 7 STIG

리눅스 STIG 하이 (카테고리 I)

- RHEL7 STIG 버전 3 릴리스 10
- RHEL8 STIG 버전 1 릴리즈 9
- 우분투 18.04 STIG 버전 2 릴리즈 10
- 우분투 20.04 버전 1 릴리스 7 STIG

2022년 4분기 변경 사항 - 2023년 2월 1일:

다음과 같이 STIG 버전이 업데이트되고 2022년 4분기 STIGS 릴리스에 적용되었습니다.

리눅스 STIG 로우 (카테고리III)

- RHEL7 STIG 버전 3 릴리스 9
- RHEL8 STIG 버전 1 릴리즈 8
- 우분투 18.04 STIG 버전 2 릴리스 9
- 우분투 20.04 버전 1 릴리스 6 STIG

리눅스 STIG 미디엄 (카테고리 II)

- RHEL7 STIG 버전 3 릴리스 9
- RHEL8 STIG 버전 1 릴리즈 8
- 우분투 18.04 STIG 버전 2 릴리스 9
- 우분투 20.04 버전 1 릴리스 6 STIG

리눅스 STIG 하이 (카테고리 I)

- RHEL7 STIG 버전 3 릴리스 9
- RHEL8 STIG 버전 1 릴리즈 8
- 우분투 18.04 STIG 버전 2 릴리스 9
- 우분투 20.04 버전 1 릴리스 6 STIG

2022년 3분기 변경 사항 - 2022년 9월 30일(변경 없음):

2022년 3분기 릴리스의 Linux 구성 STIGS 요소에는 변경 사항이 없습니다.

2022년 2분기 변경 사항 - 2022년 8월 2일:

다음과 같이 Ubuntu 지원을 도입하고 STIG 버전을 업데이트하고 2022년 2분기 STIGS 릴리스에 적용했습니다.

리눅스 STIG 로우 (카테고리) III

- RHEL7 STIG 버전 3 릴리스 7
- RHEL8 STIG 버전 1 릴리즈 6
- 우분투 18.04 STIG 버전 2 릴리스 6 (신규)
- 우분투 20.04 STIG 버전 1 릴리스 4 (신규)

리눅스 STIG 미디엄 (카테고리 II)

- RHEL7 STIG 버전 3 릴리스 7
- RHEL8 STIG 버전 1 릴리즈 6
- 우분투 18.04 STIG 버전 2 릴리스 6 (신규)
- 우분투 20.04 STIG 버전 1 릴리스 4 (신규)

리눅스 STIG 하이 (카테고리 I)

- RHEL7 STIG 버전 3 릴리스 7
- RHEL8 STIG 버전 1 릴리즈 6
- 우분투 18.04 STIG 버전 2 릴리스 6 (신규)
- 우분투 20.04 STIG 버전 1 릴리스 4 (신규)

2022년 1분기 변경 사항 - 2022년 4월 26일:

리팩터링하여 컨테이너에 대해 더 나은 지원을 포함했습니다. 이전 AL2 스크립트를 7과 결합했습니다. RHEL 다음과 같이 STIG 버전이 업데이트되어 2022년 1분기 STIGS 릴리스에 적용되었습니다.

리눅스 STIG 로우 (카테고리III)

- RHEL7 STIG 버전 3 릴리스 6
- RHEL8 STIG 버전 1 릴리즈 5

리눅스 STIG 미디엄 (카테고리 II)

- RHEL7 STIG 버전 3 릴리스 6
- RHEL8 STIG 버전 1 릴리즈 5

리눅스 STIG 하이 (카테고리 I)

- RHEL7 STIG 버전 3 릴리스 6
- RHEL8 STIG 버전 1 릴리즈 5

2021년 4분기 변경 사항 - 2021년 12월 20일:

다음과 같이 STIG 버전이 업데이트되고 2021년 4분기 STIGS 릴리스에 적용되었습니다.

리눅스 STIG 로우 (카테고리III)

- RHEL7 STIG 버전 3 릴리스 5
- RHEL8 STIG 버전 1 릴리즈 4

리눅스 STIG 미디엄 (카테고리 II)

- RHEL7 STIG 버전 3 릴리스 5
- RHEL8 STIG 버전 1 릴리즈 4

리눅스 STIG 하이 (카테고리 I)

- RHEL7 STIG 버전 3 릴리스 5
- RHEL8 STIG 버전 1 릴리즈 4

2021년 3분기 변경 사항 - 2021년 9월 30일:

다음과 같이 STIG 버전이 업데이트되고 2021년 3분기 STIGS 릴리스에 적용되었습니다.

리눅스 STIG 로우 (카테고리III)

- RHEL7 STIG 버전 3 릴리스 4
- RHEL8 STIG 버전 1 릴리즈 3

리눅스 STIG 미디엄 (카테고리 II)

- RHEL7 STIG 버전 3 릴리스 4
- RHEL8 STIG 버전 1 릴리즈 3

리눅스 STIG 하이 (카테고리 I)

- RHEL7 STIG 버전 3 릴리스 4
- RHEL8 STIG 버전 1 릴리즈 3

AWSEC2-PatchLoadBalancerInstance

설명

로드 밸런서(클래식, ALB 또는 NLB)에 연결된 Amazon EC2 인스턴스(Windows 또는 Linux)의 마이너 버전을 업그레이드하고 패치를 적용합니다. 기본 Connection Draining 시간은 인스턴스에 패치가 적용되기 전에 적용됩니다. ConnectionDrainTime 파라미터에 대해 사용자 지정 드레이닝 시간을 분(1-59) 단위로 입력하여 대기 시간을 무시할 수 있습니다.

자동화 워크플로는 다음과 같습니다.

1. 인스턴스가 연결된 로드 밸런서 또는 대상 그룹이 결정되고, 인스턴스가 정상으로 확인됩니다.
2. 로드 밸런서 또는 대상 그룹에서 인스턴스가 제거됩니다.
3. 자동화는 Connection Draining 시간을 위해 지정된 시간 동안 대기합니다.
4. AWS-RunPatchBaseline 자동화가 호출되어 인스턴스에 패치를 적용합니다.
5. 인스턴스가 로드 밸런서 또는 대상 그룹에 다시 연결됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

사전 조건

- 인스턴스에 SSM Agent가 설치되었는지 확인합니다. 자세한 내용은 Windows Server용 EC2 인스턴스에서 SSM Agent 사용을 참조하세요.

파라미터

- InstanceId

  유형: 문자열

  설명: (필수) 로드 밸런서(클래식, ALB 또는 NLB)에 연결된 패치를 적용할 인스턴스의 ID입니다.
- ConnectionDrainTime

  유형: 문자열

  설명: (선택 사항) 로드 밸런서의 Connection Draining 시간(분) (1-59)입니다.

AWSEC2-SQLServerDBRestore

설명

`AWSEC2-SQLServerDBRestore` 실행서는 Amazon S3에 저장된 Microsoft SQL Server 데이터베이스 백업을 Amazon Elastic Compute Cloud(EC2) Linux 인스턴스에서 실행되는 SQL Server 2017로 복원합니다. SQL Server 2017 Linux를 실행하는 자체 EC2 인스턴스를 제공할 수 있습니다. EC2 인스턴스를 제공하지 않을 경우, 자동화가 새 Ubuntu 16.04 EC2 인스턴스를 시작하고 SQL Server 2017을 사용하여 구성합니다. 자동화는 전체, 차등 및 트랜잭션 로그 백업을 지원합니다. 이 자동화는 복수의 데이터베이스 백업 파일을 수락하고 제공된 파일에서 각 데이터베이스의 유효한 가장 최근 백업을 자동으로 복원합니다.

SQL Server 2017 Linux를 실행하는 EC2 인스턴스로의 온프레미스 SQL Server 데이터베이스 백업 및 복원을 모두 자동화하려면 AWS 서명 PowerShell 스크립트 `MigrateSQLServerToEC2Linux`를 사용하면 됩니다.

> **Important**
>
> 이 실행서는 자동화가 실행될 때마다 SQL Server 서버 관리자(SA) 사용자 암호를 재설정합니다. 자동화가 완료된 후, SQL Server 인스턴스에 연결하기 전에 자체 SA 사용자 암호를 다시 설정해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

필수 조건

이 자동화를 실행하려면, 다음 필수 조건을 충족해야 합니다.

- 이 자동화를 실행하는 IAM 사용자 또는 역할에는 필수 IAM 권한에 개략적으로 설명된 권한과 연결된 인라인 정책이 있어야 합니다.
- 자체 EC2 인스턴스를 제공하는 경우:
  - 제공하는 EC2 인스턴스는 Microsoft SQL Server 2017을 실행하는 Linux 인스턴스여야 합니다.
  - 제공하는 EC2 인스턴스는 `AmazonSSMManagedInstanceCore` 관리형 정책이 연결된 AWS Identity and Access Management (IAM) 인스턴스 프로파일로 구성되어야 합니다. 자세한 내용은 Systems Manager용 IAM 인스턴스 프로파일 생성을 참조하세요.
  - SSM Agent가 EC2 인스턴스에 설치되어야 합니다. 자세한 내용은 Linux용 EC2 인스턴스에 SSM Agent 설치 및 구성을 참조하세요.
  - EC2 인스턴스에 SQL Server 백업을 다운로드하고 복원할 충분한 여유 디스크 공간이 있어야 합니다.

제한 사항

이 자동화는 Windows Server용 EC2 인스턴스에서 실행되는 SQL Server에 대한 복원을 지원하지 않습니다. 이 자동화는 SQL Server Linux 2017과 호환되는 데이터베이스 백업만 복원합니다. 자세한 내용은 Linux의 SQL Server 2017에서 버전 및 지원하는 기능을 참조하십시오.

파라미터

이 자동화에는 다음과 같은 파라미터가 있습니다.

- DatabaseNames

  유형: 문자열

  설명: (선택 사항) 복원할 데이터베이스의 이름의 쉼표로 구분된 목록입니다.

- DataDirectorySize

  유형: 문자열

  설명: (선택 사항) 새 EC2 인스턴스에 사용할 SQL Server Data 디렉터리의 원하는 볼륨 크기(GiB)입니다.

  기본값: 100

- KeyPair

  유형: 문자열

  설명: (선택 사항) 새 EC2 인스턴스를 생성할 때 사용할 키 페어입니다.

- IamInstanceProfileName

  유형: 문자열

  설명: (선택 사항) 새 EC2 인스턴스에 연결할 IAM 인스턴스 프로파일입니다. IAM 인스턴스 프로파일은 `AmazonSSMManagedInstanceCore` 관리형 정책이 연결되어 있어야 합니다.

- InstanceId

  유형: 문자열

  설명: (선택 사항) Linux의 SQL Server 2017을 실행하는 인스턴스입니다. 제공된 InstanceId가 없을 경우 Automation은 제공된 InstanceType 및 SQLServerEdition을 사용하여 새 EC2 인스턴스를 시작합니다.

- InstanceType

  유형: 문자열

  설명: (선택 사항) 시작할 EC2 인스턴스의 인스턴스 유형입니다.

- IsS3PresignedUrl

  유형: 문자열

설명: (선택 사항) S3Input이 미리 서명된 S3 URL일 경우 yes을 표시합니다.

기본값: no

유효한 값: yes | no

- LogDirectorySize

  유형: 문자열

  설명: (선택 사항) 새 EC2 인스턴스에 사용할 SQL Server Log 디렉터리의 원하는 볼륨 크기(GiB)입니다.

  기본값: 100

- S3Input

  유형: 문자열

  설명: (필수) 복원할 SQL 백업 파일을 포함하는 S3 버킷 이름, S3 객체 키의 쉼표로 분리된 목록 또는 미리 서명된 S3 URL의 쉼표로 구분된 목록입니다.

- SQLServerEdition

  유형: 문자열

  설명: (선택 사항) 새로 생성된 EC2 인스턴스에 설치할 SQL Server 2017의 버전입니다.

  유효한 값: Standard | Enterprise | Web | Express

- SubnetId

  유형: 문자열

  설명: (선택 사항) 새 EC2 인스턴스를 시작할 서브넷입니다. 이 서브넷은 AWS 서비스에 대한 아웃바운드 연결이 있어야 합니다. SubnetId 값을 제공하지 않을 경우 자동화가 기본 서브넷을 사용합니다.

- TempDbDirectorySize

  유형: 문자열

  설명: (선택 사항) 새 EC2 인스턴스에 사용할 SQL Server TempDB 디렉터리의 원하는 볼륨 크기(GiB)입니다.

기본값: 100

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

이 자동화를 사용하려면, 다음과 같이 인스턴스 유형에 해당하는 단계를 따르세요.

새 EC2 인스턴스의 경우:

1. `aws:executeAwsApi` - Ubuntu 16.04에서 SQL Server 2017의 AMI ID를 검색합니다.

2. `aws:runInstances` - Linux용 새 EC2 인스턴스를 시작합니다.
3. `aws:waitForAwsResourceProperty` - 새로 만든 EC2 인스턴스가 준비될 때까지 기다립니다.
4. `aws:executeAwsApi` - 인스턴스가 준비되지 않은 경우 인스턴스를 재부팅합니다.
5. `aws:assertAwsResourceProperty` - SSM Agent가 설치되었는지 확인합니다.
6. `aws:runCommand` - PowerShell에서 SQL Server 복원 스크립트를 실행합니다.

기존 EC2 인스턴스의 경우:

1. `aws:waitForAwsResourceProperty` - EC2 인스턴스가 준비되었는지 확인합니다.
2. `aws:executeAwsApi` - 인스턴스가 준비되지 않은 경우 인스턴스를 재부팅합니다.
3. `aws:assertAwsResourceProperty` - SSM Agent가 설치되었는지 확인합니다.
4. `aws:runCommand` - PowerShell에서 SQL Server 복원 스크립트를 실행합니다.

출력

getInstance.InstanceId

restoreToNewInstance.Output

restoreToExistingInstance.Output

AWSSupport-ActivateWindowsWithAmazonLicense

설명

`AWSSupport-ActivateWindowsWithAmazonLicense` 실행서는 Amazon에서 제공하는 라이선스를 사용하여 Windows Server에 대한 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 활성화합니다. 자동화는 필수 키 관리 서비스 운영 체제 설정을 확인 및 구성하고 활성화를 시도합니다. 여기에는 Amazon의 키 관리 서버로 라우팅되는 운영 체제 경로와 키 관리 서비스 운영 체제 설정이 포함됩니다. `AllowOffline` 파라미터를 `true`로 설정하면 자동화가 AWS Systems Manager에서 관리하지 않지만 인스턴스를 중지했다가 시작해야 하는 인스턴스를 대상으로 지정할 수 있습니다.

> **Note**
>
> 이 실행서는 기존 보유 라이선스 사용(BYOL) 모델 Windows Server 인스턴스에서 사용할 수 없습니다. 본인 소유의 라이선스 사용에 대한 자세한 내용은 AWS에서의 Microsoft 라이선스를 참조하시오.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

- AllowOffline

  유형: 문자열

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) 온라인 문제 해결에 실패하거나 제공된 인스턴스가 관리형 인스턴스가 아닌 경우 오프라인으로 Windows 정품 인증을 수정할 수 있도록 하려면 `true`로 설정합니다.

  > **Important**
  > 오프라인 방법을 사용하려면 제공된 EC2 인스턴스를 중지했다가 다시 시작해야 합니다. 인스턴스 스토어 볼륨에 저장되어 있는 데이터가 손실됩니다. 탄력적 IP를 사용하지 않는 경우 퍼블릭 IP 주소가 변경됩니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ForceActivation

유형: 문자열

유효한 값: true | false

기본값: false

설명: (선택 사항) Windows가 이미 정품 인증되었더라도 계속 진행하려면 `true`로 설정합니다.

- InstanceId

  유형: 문자열

  설명: (필수) Windows Server에 대한 관리형 EC2 인스턴스의 ID입니다.

- SubnetId

  유형: 문자열

  기본값: CreateNewVPC

  설명: (선택 사항) 오프라인 전용 - 오프라인 문제 해결을 수행하는 데 사용하는 EC2Rescue 인스턴스용 서브넷 ID. 인스턴스와 동일한 서브넷을 사용하려면 `SelectedInstanceSubnet`을 사용하고, 새 VPC를 생성하려면 `CreateNewVPC`를 사용합니다. 중요: 서브넷이 InstanceId와 동일한 가용 영역이어야 하며 SSM 엔드포인트와의 통신을 허용해야 합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

이 명령을 수신하는 EC2 인스턴스에 AmazonSSMManagedInstanceCore Amazon 관리형 정책이 연결된 IAM 역할이 있는 것이 좋습니다. 자동화를 실행하고 인스턴스로 명령을 전송하려면 적어도 ssm:StartAutomationExecution 및 ssm:SendCommand가 있어야 하며, 추가로 자동화 출력을 읽을 수 있으려면 ssm:GetAutomationExecution도 있어야 합니다. 오프라인 수정에 대해서는 `AWSSupport-StartEC2RescueWorkflow`에서 필요한 권한을 참조하십시오.

문서 단계

1. `aws:assertAwsResourceProperty` - 제공된 인스턴스의 플랫폼이 Windows인지 확인합니다.
2. `aws:assertAwsResourceProperty` - 제공된 인스턴스가 관리형 인스턴스인지 확인합니다.
   a. (온라인 정품 인증 수정) 입력 인스턴스가 관리형 인스턴스인 경우 `aws:runCommand`을 실행하여 Windows 정품 인증을 수정하는 PowerShell 스크립트를 실행합니다.

b. (오프라인 정품 인증 수정) 입력 인스턴스가 관리형 인스턴스가 아닌 경우:

   i. `aws:assertAwsResourceProperty` - `AllowOffline` 플래그가 `true`으로 설정되었는지 확인합니다. 만일 그렇다면 오프라인 수정이 시작되며, 그렇지 않은 경우 자동화가 종료됩니다.

   ii. `aws:executeAutomation` - Windows 정품 인증 오프라인 수정 스크립트를 사용하여 `AWSSupport-StartEC2RescueWorkflow`를 호출합니다. 이 스크립트는 OS 버전에 따라 EC2Config 또는 EC2Launch 중 하나를 사용합니다.

   iii. `aws:executeAwsApi` - `AWSSupport-StartEC2RescueWorkflow`에서 결과를 읽습니다.

출력

activateWindows.Output

getActivateWindowsOfflineResult.Output

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2

설명

`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 탄력적 네트워크 인스턴스에서 AWS 서비스 엔드포인트로의 연결을 분석합니다. IPv6은 지원되지 않습니다. 실행서는 `ServiceEndpoint` 파라미터에 대해 지정하는 값을 사용하여 엔드포인트에 대한 연결을 분석합니다. VPC에서 AWS PrivateLink 엔드포인트를 찾을 수 없는 경우, 실행서는 현재 AWS 리전의 서비스에 대한 퍼블릭 IP 주소를 사용합니다. 이 자동화는 Amazon Virtual Private Cloud의 Reachability Analyzer를 사용합니다. 자세한 내용은 Reachability Analyzer의 Reachability Analyzer가 무엇인가요?를 참조하세요.

이 자동화는 다음 사항을 확인합니다.

- Virtual Private Cloud(VPC)가 Amazon에서 제공한 DNS 서버를 사용하도록 구성되어 있는지 여부를 확인합니다.
- 지정한 AWS PrivateLink 엔드포인트가 VPC에 존재하는지 확인합니다. AWS 서비스 엔드포인트가 발견되면, 자동화가 `privateDns` 속성이 켜져 있는지 확인합니다.
- 엔드포인트가 기본 AWS PrivateLink 엔드포인트 정책을 사용하고 있는지 확인합니다.

고려 사항

- 소스와 대상 간의 분석 실행당 요금이 부과됩니다. 자세한 내용은 Amazon VPC 요금을 참조하세요.

- 자동화 중에, 네트워크 인사이트 경로와 네트워크 인사이트 분석이 생성됩니다. 자동화가 성공적으로 완료되면, 실행서가 이러한 리소스를 삭제합니다. 정리 단계가 실패하는 경우, 네트워크 인사이트 경로가 실행서에 의해 삭제되지 않으므로 수동으로 이 내용을 삭제해야 합니다. 네트워크 인사이트 경로를 수동으로 삭제하지 않으면 AWS 계정의 할당량에 해당 내용이 계속 포함됩니다. Reachability Analyzer의 할당량에 대한 자세한 내용은 Reachability Analyzer의 Reachability Analyzer의 할당량을 참조하세요.
- 프록시, 로컬 DNS 해석기 또는 호스트 파일 사용과 같은 운영 체제 수준 구성은 Reachability Analyzer가 `PASS`을 반환하더라도 연결에 영향을 줄 수 있습니다.
- Reachability Analyzer에서 수행한 모든 검사의 평가를 검토하세요. 검사 중 하나라도 `FAIL` 상태로 반환되면, 전체 접근성 검사에서 `PASS` 상태로 반환되더라도 연결에 영향을 미칠 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 소스

  타입: 문자열

  설명: (필수) 접근성을 분석하려는 Amazon EC2 인스턴스 또는 네트워크 인터페이스의 ID입니다.

- ServiceEndpoint

  타입: 문자열

  설명: (필수) 접근성을 분석하려는 서비스 엔드포인트의 호스트 이름입니다.
- RetainVpcReachabilityAnalysis

  타입: 문자열

  기본값: false

  설명: (선택 사항) 생성된 네트워크 인사이트 경로 및 관련 분석을 유지할지 여부를 결정합니다. 기본적으로 접근성 분석에 사용된 리소스는 분석에 성공한 후에 삭제됩니다. 분석을 보존하기로 선택한 경우, 실행서는 분석을 삭제하지 않으며 Amazon VPC 콘솔에서 분석을 시각화할 수 있습니다. 콘솔 링크는 자동화 출력본을 통해 사용할 수 있습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

1. `aws:executeScript`: 호스트 이름 확인을 시도하여 서비스 엔드포인트를 검증합니다.
2. `aws:executeScript`: VPC 및 서브넷에 대한 세부 정보를 수집합니다.
3. `aws:executeScript`: VPC의 DNS 구성을 평가합니다.
4. `aws:executeScript`: VPC 엔드포인트 검사를 평가합니다.
5. `aws:executeScript`: 퍼블릭 서비스 엔드포인트에 연결할 인터넷 게이트웨이를 찾습니다.
6. `aws:executeScript`: 접근성 분석에 사용할 대상을 결정합니다.
7. `aws:executeScript`: Reachability Analyzer를 사용하여 소스에서 엔드포인트까지의 접근성을 분석하고, 분석에 성공하면 리소스를 정리합니다.
8. `aws:executeScript`: 접근성 평가 보고서를 생성합니다.
9. `aws:executeScript`: JSON의 출력본을 생성합니다.

출력

- `generateReport.EvalReport` - 자동화를 통해 수행된 검사 결과를 텍스트 형식으로 표시합니다.
- `generateJsonOutput.Output` - JSON 형식의 최소 결과 버전입니다.

AWSPremiumSupport-ChangeInstanceTypeIntelToAMD

설명

`AWSPremiumSupport-ChangeInstanceTypeIntelToAMD` 실행서는 Intel 기반 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 동등한 AMD 기반 인스턴스 유형으로의 마이그레이션을 자동화합니다. 이 실행서는 Nitro 시스템에 구축된 범용(M), 버스트 가능 범용(T), 컴퓨팅 최적화(C) 및 메모리 최적화(R) 인스턴스를 지원합니다. 이 실행서는 Systems Manager에서 관리되지 않는 인스턴스에서 사용할 수 있습니다.

데이터 손실 및 가동 중지 시간의 잠재적 위험을 줄이기 위해, 실행서는 인스턴스의 중지 동작, 인스턴스가 Amazon EC2 Auto Scaling 그룹에 속하는지 여부, 인스턴스 상태, 동등한 AMD 구동 인스턴

스 유형을 동일한 가용 영역에서 사용할 수 있는지 여부를 확인합니다. 기본적으로, 이 실행서는 인스턴스 스토어 볼륨이 연결되어 있거나 인스턴스가 AWS CloudFormation 스택의 일부인 경우, 인스턴스 유형을 변경하지 않습니다. 이 동작을 변경하려면 `AllowInstanceStoreInstances` 및 `AllowCloudFormationInstances` 파라미터 중 하나에 대해 `yes`을 지정하세요.

> **Important**
>
> `AWSPremiumSupport-*` 실행서에 액세스하려면 Enterprise 또는 Business Support Subscription이 필요합니다. 자세한 내용은 AWS Support 플랜 비교를 참조하세요.

고려 사항

- 이 실행서를 사용하기 전에 인스턴스를 백업해 두는 것이 좋습니다.
- 인스턴스 유형을 변경하려면 실행서에서 인스턴스를 중지해야 합니다. 인스턴스가 중지되면, RAM 또는 인스턴스 스토어 볼륨에 저장된 모든 데이터가 손실되고 자동 퍼블릭 IPv4 주소가 해제됩니다. 자세한 내용은 인스턴스 중지 및 시작을 참조하세요.
- 사용자가 `TargetInstanceType` 파라미터에 대한 값을 지정하지 않으면, 실행서는 동일한 인스턴스 패밀리 내의 가상 CPU 및 메모리 측면에서 동등한 AMD 인스턴스를 식별하려고 시도합니다. 동등한 AMD 인스턴스 유형을 식별할 수 없는 경우, 실행서가 종료됩니다.
- `DryRun` 옵션을 사용하면, 인스턴스 유형을 실제로 변경하지 않고도 동등한 AMD 인스턴스 유형을 캡처하고 요구 사항을 검증할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 확인

  유형: 문자열

  설명: (필수) `yes`을 입력하여 대상 인스턴스가 실행 중인 경우 중지될 것임을 확인합니다.

- InstanceId

  유형: 문자열

  설명: (필수) 유형을 변경하려는 Amazon EC2 인스턴스의 ID입니다.

- TargetInstanceType

  유형: 문자열

  기본값: automatic

  설명: (선택 사항) 인스턴스를 변경하려는 AMD 인스턴스 유형입니다. 기본 `automatic` 값은 가상 CPU 및 메모리 측면에서 동등한 인스턴스 유형을 사용합니다. 예를 들어, m5.large는 m5a.large로 변경됩니다.

- AllowInstanceStoreInstances

  유형: 문자열

  유효한 값: no | yes

  기본값: 아니요

  설명: (선택 사항) 사용자가 `yes`을 지정하는 경우, 실행서는 인스턴스 스토어 볼륨이 연결된 인스턴스에서 실행됩니다.

- AllowCloudFormationInstances

  유형: 문자열

유효한 값: no | yes

기본값: 아니요

설명: (선택 사항) `yes`로 설정하면 AWS CloudFormation 스택의 일부인 인스턴스에서 실행서가 실행됩니다.

- AllowCrossGeneration

  유형: 문자열

  유효한 값: no | yes

  기본값: 아니요

  설명: (선택 사항) `yes`로 설정하면 실행서는 동일한 인스턴스 패밀리 내에서 동등한 최신 AMD 인스턴스 유형을 찾으려고 시도합니다.

- DryRun

  유형: 문자열

  유효한 값: no | yes

  기본값: 아니요

  설명: (선택 사항) `yes`로 설정하면 실행서는 동등한 AMD 인스턴스 유형을 반환하고 인스턴스 유형을 변경하지 않고도 마이그레이션 요구 사항을 검증합니다.

- SleepWait

  유형: 문자열

  기본값: PT3S

  설명: (선택 사항) 새 자동화를 시작하기 전에 실행서가 대기해야 하는 시간입니다. 이 파라미터에 제공하는 값은 ISO 8601 표준과 일치해야 합니다. ISO 8601 문자열 생성에 대한 자세한 내용은 Systems Manager의 날짜 및 시간 문자열 형식 지정을 참조하세요.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- 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

문서 단계

1. aws:assertAwsResourceProperty: 대상 Amazon EC2 인스턴스의 상태가running, pending, stopped 또는 stopping인지 확인합니다. 그렇지 않으면, 자동화가 종료됩니다.
2. aws:executeAwsApi: 대상 Amazon EC2 인스턴스에서 속성을 수집합니다.
3. aws:branch: Amazon EC2 인스턴스의 상태를 기반으로 자동화를 분기합니다.
   a. stopped 또는 stopping인 경우, Amazon EC2 인스턴스가 완전히 중지될 때까지 자동화가 aws:waitForAwsResourceProperty을 실행합니다.
   b. running 또는 pending인 경우, Amazon EC2 인스턴스가 상태 검사를 통과할 때까지 자동화가 aws:waitForAwsResourceProperty을 실행합니다.
4. aws:assertAwsResourceProperty: aws:autoscaling:groupName 태그가 적용되었는지 확인하여 Amazon EC2 인스턴스가 Auto Scaling 그룹의 일부가 아닌지 확인합니다.
5. aws:executeAwsApi: 현재 인스턴스 유형 속성을 수집하여 동등한 AMD 인스턴스 유형을 찾습니다.
6. aws:assertAwsResourceProperty: AWS Marketplace 제품 코드가 Amazon EC2 인스턴스와 연결되어 있지 않음을 확인합니다. 일부 제품은 일부 인스턴스 유형에서는 사용할 수 없습니다.
7. aws:branch: 자동화를 통해 Amazon EC2 인스턴스가 AWS CloudFormation 스택의 일부인지 확인하려는지 여부에 따라 자동화를 분기합니다.

   a. `aws:cloudformation:stack-name` 태그를 인스턴스에 적용하면 자동화가 `aws:assertAwsResourceProperty`를 실행하여 인스턴스가 AWS CloudFormation 스택의 일부가 아님을 확인합니다.

8. `aws:branch`: 인스턴스 루트 볼륨 유형이 Amazon Elastic Block Store(Amazon EBS)인지 여부에 따라 자동화를 분기합니다.

9. `aws:assertAwsResourceProperty`: 인스턴스 종료 동작이 `terminate`이 아닌 `stop`인지 확인합니다.

10. `aws:executeScript`: 현재 인스턴스를 대상으로 하는 이 실행서의 자동화가 하나만 존재한다는 점을 확인합니다. 동일한 인스턴스를 대상으로 하는 다른 자동화가 이미 진행 중인 경우 오류를 반환하고 종료합니다.

11. `aws:executeAwsApi`: 메모리 및 vCPU 용량이 같은 AMD 인스턴스 유형 목록을 반환합니다.

12. `aws:executeScript`: 현재 인스턴스 유형이 지원되는지 확인하고 동등한 AMD 인스턴스 유형을 반환합니다. 동등한 항목이 없는 경우 자동화를 종료합니다.

13. `aws:executeScript`: AMD 인스턴스 유형이 동일한 가용 영역에서 사용 가능한지 확인하고, 제공된 IAM 권한을 확인합니다.

14. `aws:branch`: `DryRun` 파라미터 값이 `yes`인지 여부에 따라 자동화를 분기합니다.

15. `aws:branch`: 원본 인스턴스 유형과 대상 인스턴스 유형이 동일한 내용인지 확인합니다. 동일하면, 자동화가 종료됩니다.

16. `aws:executeAwsApi`: 현재 인스턴스 상태를 가져옵니다.

17. `aws:changeInstanceState`: Amazon EC2 인스턴스를 중지합니다.

18. `aws:changeInstanceState`: 중지 상태에서 멈춘 경우, 인스턴스를 강제로 중지합니다.

19. `aws:executeAwsApi`: 인스턴스 유형을 대상 AMD 인스턴스 유형으로 변경합니다.

20. `aws:sleep`: 최종 일관성을 위해 인스턴스 유형을 변경한 후 3초 동안 기다립니다.

21. `aws:branch`: 이전 인스턴스 상태를 기반으로 자동화를 분기합니다. 해당 내용이 `running`이었을 경우, 인스턴스가 시작됩니다.

    a. `aws:changeInstanceState`: 인스턴스 유형을 변경하기 전에 Amazon EC2 인스턴스가 실행 중이었다면, 해당 인스턴스를 시작합니다.

    b. `aws:waitForAwsResourceProperty`: Amazon EC2 인스턴스가 상태 검사를 통과할 때까지 기다립니다. 인스턴스가 상태 확인을 통과하지 못하면, 원래 인스턴스 유형으로 다시 변경됩니다.

       i. `aws:changeInstanceState`: 원래 인스턴스 유형으로 변경하기 전에 Amazon EC2 인스턴스를 중단합니다.

ii. `aws:changeInstanceState`: 중지 상태에서 멈출 경우를 대비하여 해당 내용을 원래 인스턴스 유형으로 변경하기 전에 Amazon EC2 인스턴스를 강제로 중지합니다.

iii. `aws:executeAwsApi`: Amazon EC2 인스턴스를 해당하는 원래 유형으로 변경합니다.

iv. `aws:sleep`: 최종 일관성을 위해 인스턴스 유형을 변경한 후 3초 동안 기다립니다.

v. `aws:changeInstanceState`: 인스턴스 유형을 변경하기 전에 Amazon EC2 인스턴스가 실행 중이었다면, 해당 인스턴스를 시작합니다.

vi. `aws:waitForAwsResourceProperty`: Amazon EC2 인스턴스가 상태 검사를 통과할 때까지 기다립니다.

22.`aws:sleep`: 실행서를 종료하기 전에 기다립니다.

AWSSupport-CheckXenToNitroMigrationRequirements

설명

`AWSSupport-CheckXenToNitroMigrationRequirements` 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 인스턴스 유형을 Xen 유형 인스턴스에서 Nitro 기반 인스턴스 유형으로 성공적으로 변경하기 위한 필수 조건을 충족하는지 확인합니다. 이 자동화는 다음 사항을 확인합니다.

- 루트 디바이스는 Amazon Elastic Block Store(Amazon EBS) 볼륨입니다.
- `enaSupport` 속성이 활성화되어 있습니다.
- ENA 모듈이 인스턴스에 설치되어 있습니다.
- NVMe 모듈이 인스턴스에 설치되어 있습니다. 예일 경우, 모듈이 설치되고, 스크립트에서 모듈이 `initramfs` 이미지에 로드되어 있는지 확인합니다.
- `/etc/fstab`을 분석하고 디바이스 이름을 사용하여 마운트되는 블록 디바이스를 찾습니다.
- 운영 체제(OS)가 예측 가능한 네트워크 인터페이스 이름을 기본으로 사용하는지 여부를 결정합니다.

이 실행서는 다음 운영 체제를 지원합니다.

- Red Hat Enterprise Linux
- CentOS
- Amazon Linux 2
- Amazon Linux

- Debian 서버
- Ubuntu 서버
- SUSE Linux Enterprise Server 15 SP2
- SUSE Linux Enterprise Server 12 SP5

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  유형: 문자열

  기본값: false

  설명: (필수) Nitro 기반 인스턴스 유형으로 마이그레이션하기 전에 필수 조건을 확인하려는 Amazon EC2 인스턴스의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeAwsApi` - 인스턴스에 대한 세부 정보를 수집합니다.
- `aws:executeAwsApi` - 인스턴스의 하이퍼바이저에 대한 정보를 수집합니다.
- `aws:branch` - 대상 인스턴스가 이미 Nitro 기반 인스턴스 유형을 실행하고 있는지 여부를 기반으로 분기합니다.
- `aws:branch` - 인스턴스의 OS가 Nitro 기반 인스턴스에서 지원되는지 확인합니다.
- `aws:assertAwsResourceProperty` - 지정한 인스턴스가 Systems Manager에서 관리되고 있으며 상태가 `Online`인지 확인합니다.
- `aws:branch` - 인스턴스의 루트 디바이스가 Amazon EBS 볼륨인지 여부를 기반으로 분기합니다.
- `aws:branch` - 인스턴스에 대해 ENA 속성이 활성화되어 있는지 여부를 기반으로 분기합니다.
- `aws:runCommand` - 인스턴스의 ENA 드라이버를 확인합니다.

- `aws:runCommand` - 인스턴스의 NVMe 드라이버를 확인합니다.
- `aws:runCommand` - `fstab` 파일에 인식할 수 없는 형식이 있는지 확인합니다.
- `aws:runCommand` - 인스턴스에서 예측 가능한 인터페이스 이름 구성을 확인합니다.
- `aws:executeScript` - 이전 단계를 기반으로 출력을 생성합니다.

출력

finalOutput.output - 자동화를 통해 수행된 검사의 결과입니다.

AWSSupport-ConfigureEC2Metadata

설명

이 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대한 인스턴스 메타데이터 서비스(IMDS) 옵션을 구성하는 데 도움이 됩니다. 이 실행서를 사용하면, 다음과 같은 방법으로 구성 가능합니다.

- 인스턴스 메타데이터에 대해 IMDSv2 사용을 강제 시행합니다.
- `HttpPutResponseHopLimit` 값을 구성합니다.
- 인스턴스 메타데이터 액세스를 허용하거나 거부합니다.

인스턴스 메타데이터에 대한 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 메타데이터 서비스 구성을 참조하십시오.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- EnforceIMDSv2

  타입: 문자열

  유효한 값: required | optional

  기본값: optional

  설명: (선택 사항) IMDSv2를 강제 시행합니다. `required`을 선택하는 경우, Amazon EC2 인스턴스는 IMDSv2만 사용하게 됩니다. `optional`을 선택하는 경우, 메타데이터 액세스를 위해 IMDSv1과 IMDSv2 중에서 선택할 수 있습니다.

  > **Important**
  >
  > IMDSv2를 강제 시행할 경우, IMDSv1을 사용하는 애플리케이션이 제대로 작동하지 않을 수 있습니다. IMDSv2를 강제 시행하기 전에, IMDS를 사용하는 애플리케이션이 IMDSv2를 지원하는 버전으로 업그레이드되어 있어야 합니다. 인스턴스 메타데이터 서비스 버전 2 (IMDSv2) 에 대한 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 메타데이터 서비스 구성을 참조하십시오.

- HttpPutResponseHop한도

  유형: 정수

  유효한 값: 0~64

  기본값: 0

  설명: (선택 사항) 인스턴스 메타데이터 요청에 대해 원하는 HTTP PUT 응답 홉 제한 값(1~64)입니다. 이 값은 PUT 응답이 탐색할 수 있는 홉 수를 제어합니다. 응답이 인스턴스 외부로 이동하는 것을 방지하려면 파라미터 값에 1을 지정하세요.

- InstanceId

타입: 문자열

설명: (필수) 구성하려는 메타데이터 설정이 있는 Amazon EC2 인스턴스의 ID입니다.

- MetadataAccess

  타입: 문자열

  유효한 값: enabled | disabled

  기본값: enabled

  설명: (선택 사항) Amazon EC2 인스턴스에서 인스턴스 메타데이터 액세스를 허용하거나 거부합니다. `disabled`을 지정하는 경우, 다른 모든 파라미터가 무시되고 인스턴스에 대한 메타데이터 액세스가 거부됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

1. branch OnMetadataAccess - `MetadataAccess` 매개변수 값을 기반으로 하는 브랜치 자동화.
2. disableMetadataAccess - ModifyInstanceMetadataOptions API 작업을 호출하여 메타데이터 엔드포인트 액세스를 비활성화합니다.
3. branch OnHttpPutResponseHopLimit - `HttpPutResponseHopLimit` 파라미터 값에 따른 브랜치 자동화.
4. 유지 HopLimitAndConfigureImdsVersion - `HttpPutResponseHopLimit` 0인 경우, 현재 홉 제한을 유지하고 다른 메타데이터 옵션을 변경합니다.
5. BeforeAssertingIMDSv2 상태 대기 - IMDSv2 상태를 확인하기 전에 30초 동안 기다립니다.
6. set HopLimitAndConfigureImdsVersion - `HttpPutResponseHopLimit` 이 0보다 큰 경우, 지정된 입력 파라미터를 사용하여 메타데이터 옵션을 구성합니다.

7. wait BeforeAssertingHopLimit - 메타데이터 옵션을 설정하기 전에 30초 동안 기다립니다.
8. assertHopLimit - `HttpPutResponseHopLimit` 속성이 지정한 값으로 설정되어 있는지 확인합니다.
9. 브랜치 VerificationOn IMDSv2옵션 - 파라미터 값을 기반으로 브랜치를 검증합니다. `EnforceIMDSv2`
10. ImDSv2 어설션 - 설정된 값을 지정합니다. IsOptional `HttpTokens optional`
11. ImDSv2 어설션 IsEnforced - 값을 로 설정합니다. `HttpTokens required`
12. wait BeforeAssertingMetadataState - 메타데이터 상태가 비활성화되었음을 확인하기 전에 30초 동안 기다립니다.
13. assert - 메타데이터가 다음과 같음을 확인합니다. MetadataIsDisabled `disabled`
14. describeMetadataOptions - 지정한 변경 내용이 적용된 후 메타데이터 옵션을 가져옵니다.

출력

MetadataOptions.State를 설명하세요

설명해 주세요MetadataOptions. MetadataAccess

MetadataOptions.imdsv2를 설명하세요

MetadataOptions설명해 주세요. HttpPutResponseHop한도

AWSSupport-CopyEC2Instance

설명

`AWSSupport-CopyEC2Instance` 실행서는 Knowledge Center 항목 EC2 인스턴스를 다른 서브넷, 가용 영역 또는 VPC로 이동하려면 어떻게 합니까?에 개략적으로 설명된 절차에 대한 자동화된 솔루션을 제공합니다. 자동화는 `Region` 및 `SubnetId` 파라미터에 대해 사용자가 지정하는 값에 따라 분기됩니다.

`SubnetId` 파라미터의 값을 지정하지만 `Region` 파라미터의 값을 지정하지 않는 경우, 자동화가 대상 인스턴스의 Amazon Machine Image(AMI)을 생성하고 지정한 서브넷의 AMI에서 새 인스턴스를 시작합니다.

`SubnetId` 파라미터 및 `Region` 파라미터의 값을 지정하는 경우, 자동화가 대상 인스턴스의 AMI을 생성하고, AMI를 지정한 인스턴스 AWS 리전에 복사한 다음 ,지정한 서브넷의 AMI에서 새 인스턴스를 시작합니다.

`SubnetId` 파라미터의 값을 지정하지만 `Region` 파라미터의 값을 지정하지 않는 경우, 자동화가 대상 인스턴스의 AMI을 생성하고, 지정한 리전에 AMI를 복사한 다음, 대상 리전에 있는 Virtual Private Cloud(VPC)의 기본 서브넷에 있는 AMI에서 새 인스턴스를 시작합니다.

`Region` 또는 `SubnetId` 파라미터 중 어느 하나에도 값을 지정하지 않는 경우, 자동화가 대상 인스턴스의 AMI을 생성하고, VPC의 기본 서브넷에 있는 AMI에서 새 인스턴스를 시작합니다.

AMI을 다른 리전으로 복사하려면, `AutomationAssumeRole` 파라미터의 값을 제공해야 합니다. `waitForAvailableDestinationAmi`단계 중에 자동화 제한 시간이 초과되어도 AMI는 여전히 복사 중일 수 있습니다. 이 경우 복사가 완료될 때까지 기다렸다가 인스턴스를 수동으로 시작할 수 있습니다.

이 자동화를 실행하기 전에 다음 사항에 유의하세요.

- AMI들은 Amazon Elastic Block Store(Amazon EBS) 스냅샷을 기반으로 합니다. 이전 스냅샷이 없는 대형 파일 시스템의 경우, AMI 생성에 몇 시간이 걸릴 수 있습니다. AMI 생성 시간을 줄이려면 AMI를 생성하기 전에 Amazon EBS 스냅샷을 생성하세요.
- AMI을 생성해도 인스턴스 스토어 볼륨의 스냅샷은 인스턴스에 생성되지 않습니다. Amazon EBS에 인스턴스 스토어 볼륨을 백업하는 방법에 대한 자세한 내용은 Amazon EC2 인스턴스의 인스턴스 스토어 볼륨을 Amazon EBS에 백업하려면 어떻게 해야 하나요?를 참조하세요.
- 새 Amazon EC2 인스턴스는 서로 다른 프라이빗 IPv4 또는 퍼블릭 IPv6 IP 주소를 가지고 있습니다. 이전 IP 주소에 대한 모든 참조(예: DNS 항목)를 새 인스턴스에 할당된 새 IP 주소로 업데이트해야 합니다. 소스 인스턴스에서 탄력적 IP 주소를 사용할 경우, 이 주소를 새 인스턴스에 연결해야 합니다.
- 도메인 보안 식별자(SID) 충돌 문제는 사본이 시작되어 도메인에 접속하려고 할 때 발생할 수 있습니다. AMI를 캡처하기 전에 Sysprep을 사용하거나 도메인에서 도메인 연결 인스턴스를 제거하여 충돌 문제를 방지하세요. 자세한 내용은 Sysprep을 사용하여 재사용 가능한 사용자 지정 Windows AMI를 생성하고 설치하려면 어떻게 해야 하나요?를 참조하세요.

이 자동화 실행(콘솔)

> **Important**
>
> Microsoft Active Directory Domain Controller 인스턴스를 복사할 때는 이 실행서를 사용하지 않는 것이 좋습니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  유형: 문자열

  설명: (필수) 복사할 인스턴스의 ID입니다.

- KeyPair

  유형: 문자열

  설명: (선택 사항) 복사된 새 인스턴스와 연결하려는 키 페어입니다. 인스턴스를 다른 리전에 복사하는 경우, 키 페어가 지정된 리전에 존재하는지 확인하세요.

- 리전

  유형: 문자열

  설명: (선택 사항) 인스턴스를 복사하려는 리전입니다. 이 파라미터의 값을 지정하지만 `SubnetId` 및 `SecurityGroupIds` 파라미터의 값을 지정하지 않는 경우, 자동화는 기본 보안 그룹이 있는 기본 VPC에서 인스턴스를 시작하려고 시도합니다. 대상 리전에서 EC2-Classic이 활성화된 경우, 시작이 되지 않습니다.

- SubnetId

유형: 문자열

설명: (선택 사항) 인스턴스를 복사하려는 서브넷의 ID입니다. 대상 리전에서 EC2-Classic이 활성화된 경우, 이 파라미터의 값을 제공해야 합니다.

- InstanceType

  유형: 문자열

  설명: (선택 사항) 복사된 인스턴스가 시작되어야 하는 인스턴스 유형입니다. 이 파라미터에 대한 값을 지정하지 않으면, 소스 인스턴스 유형이 사용됩니다. 인스턴스가 복사되는 리전에서 소스 인스턴스 유형이 지원되지 않는 경우, 자동화가 실패합니다.

- SecurityGroupIds

  유형: 문자열

  설명: (선택 사항) 복사된 인스턴스와 연결하려는 보안 그룹 ID의 쉼표로 구분된 목록입니다. 이 파라미터의 값을 지정하지 않고 인스턴스가 다른 리전으로 복사되지 않는 경우, 소스 인스턴스와 연결된 보안 그룹이 사용됩니다. 인스턴스를 다른 리전에 복사하는 경우, 대상 리전의 기본 VPC에 대한 기본 보안 그룹이 사용됩니다.

- KeepImageSourceRegion

  유형: 부울

  유효한 값: true | false

  기본값: true

  설명: (선택 사항) 이 파라미터에 `true`을 지정하는 경우, 자동화는 소스 인스턴스의 AMI를 삭제하지 않습니다. 이 파라미터에 `false`을 지정하는 경우, 자동화가 AMI의 등록을 취소하고 관련 스냅샷을 삭제합니다.

- KeepImageDestinationRegion

  유형: 부울

  유효한 값: true | false

  기본값: true

설명: (선택 사항) 이 파라미터에 `true`을 지정하는 경우, 자동화가 지정한 리전에 복사된 AMI를 삭제하지 않습니다. 이 파라미터에 `false`을 지정하는 경우, 자동화가 AMI의 등록을 취소하고 관련 스냅샷을 삭제합니다.

- NoRebootInstanceBeforeTakingImage

  유형: 부울

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) 이 파라미터에 `true`을 지정하는 경우, AMI를 생성하기 전에 소스 인스턴스가 다시 시작되지 않습니다. 이 옵션을 사용하는 경우 생성된 이미지의 파일 시스템 무결성을 보장할 수 없습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ec2:CreateImage`
- `ec2:DeleteSnapshot`
- `ec2:DeregisterImage`
- `ec2:DescribeInstances`
- `ec2:DescribeImages`
- `ec2:RunInstances`

인스턴스를 다른 리전으로 복사할 경우, 다음 권한도 필요합니다.

- `ec2:CopyImage`

문서 단계

- describeOriginalInstanceDetails - 복사할 인스턴스에서 세부 정보를 수집합니다.
- assertRootVolumeIsEbs - 루트 볼륨 디바이스 유형이 `ebs`인지 확인하고, 그렇지 않으면, 자동화가 종료됩니다.
- evalInputParameters - 입력 파라미터에 제공된 값을 평가합니다.

- createLocalAmi - 소스 인스턴스의 AMI을 생성합니다.
- tagLocalAmi - 이전 단계에서 생성한 AMI에 태그를 지정합니다.
- branchAssertRegionIsSame - 인스턴스가 동일한 리전 내에서 복사되고 있는지 아니면 다른 리전으로 복사되고 있는지 여부를 기반으로 분기합니다.
- branchAssertSameRegionWithKeyPair - 동일한 리전 내에서 복사되고 있는 인스턴스의 `KeyPair` 파라미터에 값이 제공되었는지 여부를 기반으로 분기합니다.
- sameRegionLaunchInstanceWithKeyPair - 동일한 서브넷 또는 지정한 키 페어를 사용하여 지정한 서브넷에 있는 소스 인스턴스의 AMI에서 Amazon EC2 인스턴스를 시작합니다.
- sameRegionLaunchInstanceWithoutKeyPair - 동일한 서브넷 또는 키 페어가 없는 지정한 서브넷에 있는 소스 인스턴스의 AMI에서 Amazon EC2 인스턴스를 시작합니다.
- copyAmiToRegion - AMI을 대상 리전으로 복사합니다.
- waitForAvailableDestinationAmi - 복사한 AMI 상태가 `available`가 될 때까지 기다립니다.
- destinationRegionLaunchInstance - 복사한 AMI을 사용하여 Amazon EC2 인스턴스를 시작합니다.
- branchAssertDestinationAmiToDelete - `KeepImageDestinationRegion` 파라미터에 제공한 값을 기반으로 분기합니다.
- deregisterDestinationAmiAndDeleteSnapshots - 복사한 AMI의 등록을 취소하고 관련 스냅샷을 삭제합니다.
- branchAssertSourceAmiTodelete - `KeepImageSourceRegion` 파라미터에 제공한 값을 기반으로 분기합니다.
- deregisterSourceAmiAndDeleteSnapshots - 소스 인스턴스에서 생성된 AMI의 등록을 취소하고 관련 스냅샷을 삭제합니다.
- sleep - 자동화를 2초 동안 대기 상태로 유지합니다. 이것은 종료 단계입니다.

출력

sameRegionLaunchInstanceWithKeyPair.InstanceIds

sameRegionLaunchInstanceWithoutKeyPair.InstanceIds

destinationRegionLaunchInstance.DestinationInstanceId

`AWSSupport-EnableWindowsEC2SerialConsole`

설명

런북은 Amazon EC2 Windows 인스턴스에서 Amazon EC2 직렬 콘솔, 특수 관리 콘솔 (SAC) 및 부팅 메뉴를 활성화하는 `AWSSupport-EnableWindowsEC2SerialConsole` 데 도움이 됩니다. Amazon Elastic Compute Cloud (AmazonEC2) 직렬 콘솔 기능을 사용하면 Amazon EC2 인스턴스의 직렬 포트에 액세스하여 부팅, 네트워크 구성 및 기타 문제를 해결할 수 있습니다. Runbook은 실행 중이고 관리 중인 인스턴스뿐 아니라 중지 상태이거나 관리되지 않는 인스턴스에서도 기능을 활성화하는 데 필요한 단계를 자동화합니다. AWS Systems Manager AWS Systems Manager

어떻게 작동하나요?

`AWSSupport-EnableWindowsEC2SerialConsole`자동화 런북은 Microsoft Windows Server를 실행하는 Amazon EC2 인스턴스에서 메뉴를 SAC 활성화하고 부팅하는 데 도움이 됩니다. 실행 중이고 에서 관리하는 인스턴스의 경우 AWS Systems Manager, 런북은 AWS Systems Manager Run Command PowerShell 스크립트를 실행하여 메뉴를 SAC 활성화하고 부팅합니다. 중지된 상태이거나 관리되지 않는 인스턴스의 경우 AWS Systems Manager, Runbook은 AWSSupportEC2RescueWorkflow-Start를 사용하여 필요한 변경을 오프라인으로 수행할 임시 Amazon EC2 인스턴스를 생성합니다.

자세한 내용은 Windows용 Amazon EC2 직렬 콘솔 인스턴스를 참조하십시오.

> **Important**
>
> - 인스턴스에서 SAC 활성화하면 암호 검색에 의존하는 Amazon EC2 서비스가 Amazon EC2 콘솔에서 작동하지 않습니다. 자세한 내용은 Windows 인스턴스 문제 SAC 해결에 사용을 참조하십시오.
> - 직렬 콘솔에 대한 액세스를 구성하려면 계정 수준에서 직렬 콘솔 액세스 권한을 부여한 다음 사용자에게 액세스 권한을 부여하도록 configure AWS Identity and Access Management (IAM) 정책을 구성해야 합니다. 또한 사용자가 직렬 콘솔을 사용하여 문제를 해결할 수 있도록 모든 인스턴스에서 암호 기반 사용자를 구성해야 합니다. 자세한 내용은 Amazon EC2 직렬 콘솔에 대한 액세스 구성을 참조하십시오.
> - 계정에서 직렬 콘솔이 활성화되었는지 확인하려면 직렬 콘솔에 대한 계정 액세스 상태 보기를 참조하십시오.
> - 직렬 콘솔 액세스는 Nitro System에 구축된 가상화된 인스턴스에서만 지원됩니다.

자세한 내용은 Amazon EC2 직렬 콘솔 사전 요구 사항을 참조하십시오.

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

Parameters

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

```
{
    "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"
                    ]
```

```
                        }
                    }
                }
            ]
        }
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. `AWSSupport-EnableWindowsEC2SerialConsole` AWS Systems Manager 콘솔에서 로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - InstanceId: (필수)

     Amazon EC2 직렬 콘솔, (SAC) 및 부팅 메뉴를 활성화하려는 Amazon EC2 인스턴스의 ID.
   - AutomationAssumeRole: (선택 사항)

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 IAM 역할의 Amazon 리소스 이름 (ARN) 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - HelperInstanceType: (조건부)

     오프라인 EC2 인스턴스용 Amazon EC2 직렬 콘솔을 구성하기 위해 Runbook이 프로비저닝하는 Amazon 인스턴스 유형입니다.
   - HelperInstanceProfileName: (조건부)

     헬퍼 IAM 인스턴스의 기존 인스턴스 프로필 이름. 중지 상태이거나 관리되지 않는 인스턴스에서 부팅 메뉴를 SAC 활성화하는 AWS Systems Manager경우 이 설정은 필수입니다. IAM인스턴스 프로필이 지정되지 않은 경우 자동화가 사용자 대신 프로필을 생성합니다.
   - SubnetId: (조건부)

     헬퍼 인스턴스의 서브넷 ID. 기본적으로 제공된 인스턴스가 있는 곳과 동일한 서브넷을 사용합니다.

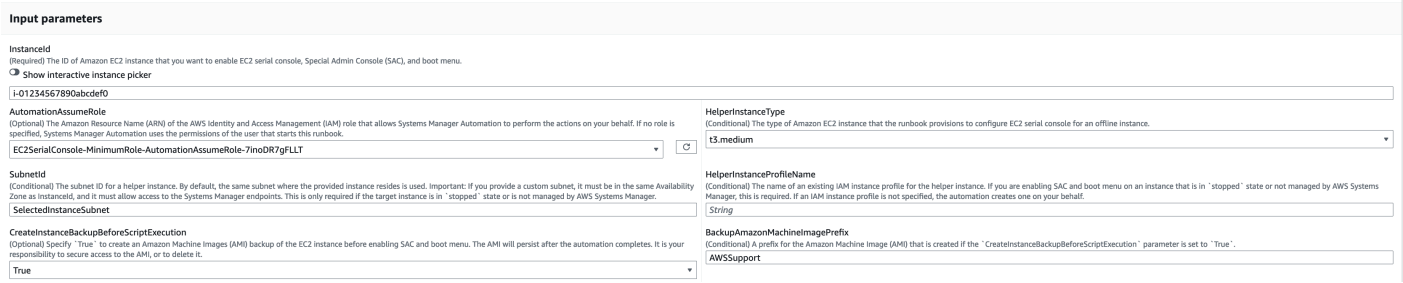
> **Important**
>
> 사용자 지정 서브넷을 제공하는 경우 해당 서브넷은 동일한 가용 영역에 있어야 하며 Systems Manager 엔드포인트에 대한 액세스를 허용해야 합니다. InstanceId 이는 대상 인스턴스가 중지 상태이거나 에서 관리되지 않는 경우에만 필요합니다. AWS Systems Manager

- CreateInstanceBackupBeforeScriptExecution: (선택 사항)

  활성화 SAC 및 부팅 메뉴를 활성화하기 전에 Amazon EC2 인스턴스의 Amazon 머신 이미지 (AMI) 백업을 생성하려면 True를 지정하십시오. 자동화가 완료된 후에도 AMI 지속됩니다. 에 대한 액세스를 AMI 보호하거나 삭제하는 것은 사용자의 책임입니다.

- BackupAmazonMachineImagePrefix: (조건부)

  `CreateInstanceBackupBeforeScriptExecution`파라미터가 로 설정된 경우 생성되는 Amazon 머신 이미지 (AMI) 의 접두사입니다. `True`



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - CheckIfEc2: SerialConsoleAccessEnabled

     Amazon EC2 직렬 콘솔 액세스가 계정 수준에서 활성화되어 있는지 확인합니다. 참고: 직렬 콘솔에 대한 액세스는 기본적으로 사용할 수 없습니다. 자세한 내용은 Amazon EC2 직렬 콘솔에 대한 액세스 구성을 참조하십시오.

   - CheckIfEc2InstanceIsWindows:

     대상 인스턴스 플랫폼이 Windows인지 확인합니다.

   - GetInstanceType:

     대상 인스턴스의 인스턴스 유형을 검색합니다.

- CheckIfInstanceTypeIsNitro:

  인스턴스 유형 하이퍼바이저가 Nitro 기반인지 확인합니다. 직렬 콘솔 액세스는 Nitro 시스템에 구축된 가상화된 인스턴스에서만 지원됩니다.

- CheckIfInstanceIsInAutoScalingGroup:

  를 호출하여 아마존 EC2 인스턴스가 아마존 EC2 Auto Scaling 그룹에 속해 있는지 확인합니다 `DescribeAutoScalingInstances`API. 인스턴스가 Amazon EC2 Auto Scaling 그룹의 일부인 경우 포팅 어시스턴트가 해당 그룹에 속하는지 확인합니다. NET인스턴스가 대기 수명 주기 상태에 있습니다.

- WaitForEc2InstanceStateStablized:

  인스턴스가 실행 중 또는 중지 상태가 될 때까지 기다립니다.

- GetEc2: InstanceState

  인스턴스의 현재 상태를 가져옵니다.

- BranchOnEc2InstanceState:

  이전 단계에서 검색한 인스턴스 상태를 기반으로 분기합니다. 해당 인스턴스 상태가 실행 중이면 `CheckIfEc2InstanceIsManagedBySSM` 단계로 이동하고 그렇지 않으면 `CheckIfHelperInstanceProfileIsProvided` 단계로 이동합니다.

- CheckIfEc2 InstanceIsManagedBySSM:

  인스턴스가 에서 관리되는지 확인합니다 AWS Systems Manager. 관리되는 경우 런북은 PowerShell Run Command를 사용하여 부팅 메뉴를 SAC 활성화합니다.

- BranchOnPreEC2RescueBackup:

  `CreateInstanceBackupBeforeScriptExecution`입력 파라미터를 기반으로 분기합니다.

- CreateAmazonMachineImageBackup:

  인스턴스의 AMI 백업을 생성합니다.

- E nableSACAndBootMenu:

  PowerShell Run Command 스크립트를 실행하여 메뉴를 SAC 활성화하고 부팅합니다.

- RebootInstance:

  Amazon EC2 인스턴스를 재부팅하여 구성을 적용합니다. 이 단계는 인스턴스가 온라인 상태이고 에서 관리하는 AWS Systems Manager경우의 마지막 단계입니다.

- CheckIfHelperInstanceProfileIsProvided:

  임시 Amazon EC2 인스턴스를 사용하여 메뉴를 SAC 활성화하고 오프라인으로 부팅하기 전에 `HelperInstanceProfileName` 지정된 항목이 존재하는지 확인합니다.

- RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu:

  인스턴스가 중지된 `AWSSupport-StartEC2RescueWorkflow` 상태이거나 에서 관리하지 않는 경우 활성화 SAC 및 부팅 메뉴를 실행합니다 AWS Systems Manager.

- GetExecutionDetails:

  백업 및 오프라인 스크립트 출력의 이미지 ID를 검색합니다.

7. 완료 후 출력 섹션에서 실행의 세부 결과를 검토하십시오.

- E nableSACAndBootMenu. 출력:

  `EnableSACAndBootMenu`단계의 명령 실행 출력입니다.

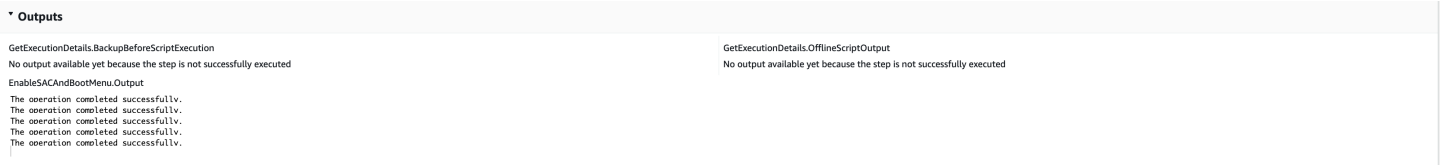
- GetExecutionDetails.OfflineScriptOutput:

  `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu`단계에서 실행된 오프라인 스크립트의 출력입니다.

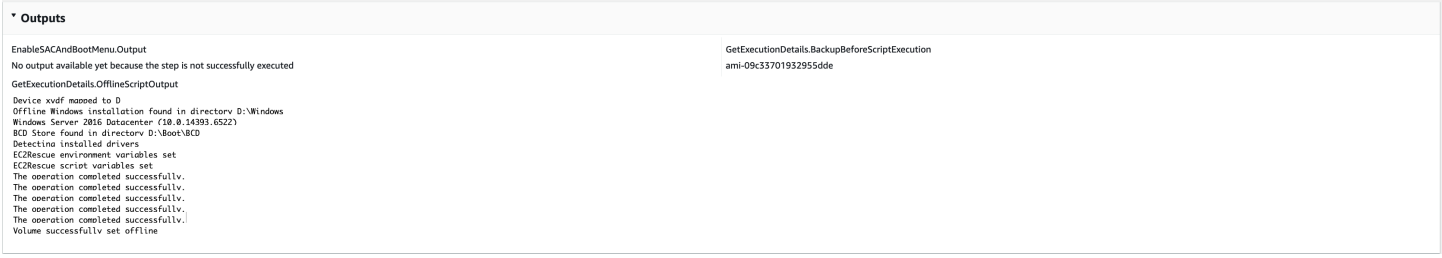
- GetExecutionDetails.BackupBeforeScriptExecution:

  `CreateInstanceBackupBeforeScriptExecution`입력 매개변수가 True인 경우 생성된 AMI 백업의 이미지 ID입니다.

에서 실행 및 관리하는 인스턴스에서의 실행 출력 AWS Systems Manager



에서 중지하거나 관리하지 않는 인스턴스에서의 실행 출력 AWS Systems Manager



참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWSSupport-ExecuteEC2Rescue

설명

이 실행서는 EC2Rescue 도구를 사용하여 문제를 해결하고 가능한 경우 Linux용 또는 Windows Server에 지정된 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 관련된 일반적인 연결 문제를 해결합니다. 루트 볼륨이 암호화된 인스턴스는 지원되지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- EC2RescueInstanceType

  유형: 문자열

  유효한 값: t2.small | t2.medium | t2.large

  기본값: t2.small

  설명: (필수) EC2Rescue 인스턴스의 EC2 인스턴스 유형입니다. 권장 크기: `t2.small`

- LogDestination

  유형: 문자열

  설명: (선택 사항) 문제 해결 로그를 업로드할 계정의 Amazon S3 버킷 이름입니다. 버킷 정책에서 수집된 로그에 액세스할 필요가 없는 당사자에 대해 불필요한 읽기/쓰기 권한을 부여하지 않도록 해야 합니다.

- SubnetId

  유형: 문자열

  기본값: CreateNewVPC

  설명: (선택 사항) EC2Rescue 인스턴스의 서브넷 ID입니다. 기본적으로 AWS Systems ManagerAutomation은 새 VPC를 생성합니다. 또는 `SelectedInstanceSubnet`을 사용하여 인스턴스와 동일한 서브넷을 사용하거나 사용자 지정 서브넷 ID를 지정합니다.

  > **Important**
  >
  > 서브넷은 `UnreachableInstanceId`과 동일한 가용 영역이어야 하며 SSM 엔드포인트와의 통신을 허용해야 합니다.

- UnreachableInstanceId

  유형: 문자열

  설명: (필수) 연결할 수 없는 EC2 인스턴스의 ID입니다.

> **Important**
>
> Systems Manager Automation은 이 인스턴스를 중지하고, 작업을 시도하기 전에 AMI를 생성합니다. 인스턴스 스토어 볼륨에 저장되어 있는 데이터가 손실됩니다. 탄력적 IP를 사용하지 않는 경우 퍼블릭 IP 주소가 변경됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

자동화 출력본을 읽을 수 있으려면 적어도 `ssm:StartAutomationExecution`과 `ssm:GetAutomationExecution`가 있어야 합니다. 필요한 권한에 대한 자세한 내용은 `AWSSupport-StartEC2RescueWorkflow`(을)를 참조하십시오.

문서 단계

1. `aws:assertAwsResourceProperty` - 제공된 인스턴스가 Windows Server인 경우를 단정합니다.
   a. (Windows Server용 EC2Rescue) 제공된 인스턴스가 Windows Server 인스턴스인 경우:
      i. `aws:executeAutomation` - Windows Server용 EC2Rescue 오프라인 스크립트를 사용하여 `AWSSupport-StartEC2RescueWorkflow`를 호출합니다.
      ii. `aws:executeAwsApi` - 중첩된 자동화에서 백업 AMI ID를 검색합니다.
      iii. `aws:executeAwsApi` - 중첩된 자동화에서 EC2Rescue 요약을 검색합니다.
   b. (Linux용 EC2Rescue) 제공된 인스턴스가 Linux 인스턴스인 경우:
      i. `aws:executeAutomation` - Linux용 EC2Rescue 오프라인 스크립트를 사용하여 `AWSSupport-StartEC2RescueWorkflow`를 호출합니다.
      ii. `aws:executeAwsApi` - 중첩된 자동화에서 백업 AMI ID를 검색합니다.
      iii. `aws:executeAwsApi` - 중첩된 자동화에서 EC2Rescue 요약을 검색합니다.

출력

`getEC2RescueForWindowsResult.Output`

`getWindowsBackupAmi.ImageId`

`getEC2RescueForLinuxResult.Output`

`getLinuxBackupAmi.ImageId`

AWSSupport-ListEC2Resources

설명

`AWSSupport-ListEC2Resources` 실행서는 Amazon EC2 인스턴스 및 사용자가 지정하는 AWS 리전에서 Amazon Elastic Block Store(Amazon EBS) 볼륨, 탄력적 IP 주소 및 Amazon EC2 Auto Scaling 그룹과 같은 관련 리소스에 대한 정보를 반환합니다. 기본적으로, 정보는 모든 리전에서 수집되며 자동화 출력본에 표시됩니다. 선택적으로, 쉼표로 구분된 값(.csv) 파일로 업로드되어야 하는 정보에 대해 Amazon Simple Storage Service(Amazon S3) 버킷을 지정할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 버킷

  유형: 문자열

  설명: (선택 사항) 수집된 정보가 업로드되는 S3 버킷의 이름입니다.

- DisplayResourceDeletionDocumentation

  유형: 문자열

  기본값: true

  설명: (선택 사항) `true`로 설정하면, 자동화가 출력에 리소스 삭제와 관련된 문서에 대한 링크를 생성합니다.

- RegionsToQuery

  유형: 문자열

  기본값: All

  설명: (선택 사항) Amazon EC2 관련 정보를 수집하려는 리전입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `autoscaling:DescribeAutoScalingGroups`
- `ec2:DescribeAddresses`
- `ec2:DescribeImages`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRegions`
- `ec2:DescribeVolumes`
- `ec2:DescribeSnapshots`
- `elasticloadbalancing:DescribeLoadBalancers`

또한, 지정하는 S3 버킷에 수집된 정보를 성공적으로 업로드하려면 `AutomationAssumeRole`에 다음 작업이 필요합니다.

- `s3:GetBucketAcl`
- `s3:GetBucketPolicyStatus`
- `s3:PutObject`

문서 단계

- `aws:executeAwsApi` - 계정에 대해 활성화된 리전을 수집합니다.
- `aws:executeScript` - 계정에 대해 활성화된 리전이 `RegionsToQuery` 파라미터에 지정된 리전을 지원하는지 확인합니다.
- `aws:branch` - 계정에 대해 활성화된 리전이 없는 경우, 자동화가 종료됩니다.
- `aws:executeScript` - 지정하는 계정 및 리전의 모든 EC2 인스턴스를 나열합니다.
- `aws:executeScript` - 지정하는 계정 및 리전의 모든 Amazon Machine Images(AMI)를 나열합니다.
- `aws:executeScript` - 지정하는 계정 및 리전의 모든 EBS 볼륨을 나열합니다.
- `aws:executeScript` - 지정하는 계정 및 리전의 모든 탄력적 IP 주소를 나열합니다.
- `aws:executeScript` - 지정하는 계정 및 리전의 모든 탄력적 네트워크 인터페이스를 나열합니다.
- `aws:executeScript` - 지정하는 계정 및 리전의 모든 Auto Scaling 그룹을 나열합니다.
- `aws:executeScript` - 지정하는 계정 및 리전의 모든 로드 밸런서를 나열합니다.
- `aws:executeScript` - `Bucket` 파라미터 값을 제공할 경우, 지정한 S3 버킷에 수집된 정보를 업로드합니다.

AWSSupport-ManageRDPSettings

설명

`AWSSupport-ManageRDPSettings` 실행서를 사용하면 사용자가 RDP 포트 및 네트워크 계층 인증(NLA)과 같은 일반적인 원격 데스크톱 프로토콜(RDP) 설정을 관리할 수 있습니다. 기본적으로, 이 실행서는 설정 값을 읽고 출력합니다.

> **Important**
>
> 이 실행서를 실행하기 전에 RDP 설정에 대한 변경 내용을 신중히 검토해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  유형: 문자열

  설명: (필수) RDP 설정을 관리할 관리형 인스턴스의 ID입니다.

- NLASettingAction

  유형: 문자열

  유효한 값: Check | Enable | Disable

  기본값: Check

  설명: (필수) NLA 설정에 대해 수행할 작업(Check, Enable, Disable)입니다.

- RDPPort

  유형: 문자열

  기본값: 3389

  설명: (선택 사항) 새 RDP 포트를 지정합니다. 작업을 Modify로 설정한 경우에만 사용됩니다. 포트 번호는 1025-65535입니다. 참고: 포트를 변경한 후 RDP 서비스가 다시 시작됩니다.

- RDPPortAction

  유형: 문자열

유효한 값: Check | Modify

기본값: Check

설명: (필수) RDP 포트에 적용할 작업입니다.

- RemoteConnections

  유형: 문자열

  유효한 값: Check | Enable | Disable

  기본값: Check

  설명: (필수) fDenyTSConnections 설정에 대해 수행할 작업입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

이 명령을 수신하는 EC2 인스턴스에는 AmazonSSMManagedInstanceCore Amazon 관리형 정책이 연결된 IAM 역할이 있어야 합니다. 명령을 인스턴스로 전송하려면 사용자에게 적어도 ssm:SendCommand가 있어야 하며, 추가로 명령 출력을 읽을 수 있으려면 ssm:GetCommandInvocation이 있어야 합니다.

문서 단계

`aws:runCommand` - 대상 인스턴스에서 RDP 설정을 변경하거나 확인하는 PowerShell 스크립트를 실행합니다.

출력

manageRDPSettings.Output

AWSSupport-ManageWindowsService

설명

`AWSSupport-ManageWindowsService` 실행서를 통해 대상 인스턴스의 모든 Windows 서비스를 중지, 시작, 재시작, 일시 중지 또는 비활성화할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) 서비스를 관리할 관리형 인스턴스의 ID입니다.
- ServiceAction

  유형: 문자열

  유효한 값: Check | Restart | Force-Restart | Start | Stop | Force-Stop | Pause

  기본값: Check

  설명: (필수) Windows 서비스에 적용할 작업입니다. `Force-Restart` 및 `Force-Stop`를 사용하여 종속 서비스가 있는 서비스를 다시 시작 및 중지할 수 있다는 점에 유의하세요.
- StartupType

  유형: 문자열

  유효한 값: Check | Auto | Demand | Disabled | DelayedAutoStart

기본값: Check

설명: (필수) Windows 서비스에 적용할 시작 유형입니다.

- WindowsServiceName

  유형: 문자열

  설명: (필수) 유효한 Windows 서비스 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

이 명령을 수신하는 EC2 인스턴스에 AmazonSSMManagedInstanceCore Amazon 관리형 정책이 연결된 IAM 역할을 지정하는 것이 좋습니다. 자동화를 실행하고 인스턴스로 명령을 전송하려면 사용자에게 적어도 ssm:StartAutomationExecution 및 ssm:SendCommand가 있어야 하며, 추가로 자동화 출력을 읽을 수 있으려면 ssm:GetAutomationExecution도 있어야 합니다.

문서 단계

`aws:runCommand` - 대상 인스턴스의 Windows 서비스에 원하는 구성을 적용하는 PowerShell 스크립트를 실행합니다.

출력

manageWindowsService.Output

AWSSupport-MigrateEC2ClassicToVPC

설명

`AWSSupport-MigrateEC2ClassicToVPC` 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 EC2-Classic에서 Virtual Private Cloud(VPC)로 마이그레이션합니다. 이 실행서는 Amazon Elastic Block Store(Amazon EBS) 루트 볼륨을 통해 하드웨어 가상 머신(HVM) 가상화 유형의 Amazon EC2 인스턴스 마이그레이션을 지원합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다.

- ApproverIAM

  형식: StringList

  설명: (선택 사항) 작업을 승인하거나 거부할 수 있는 IAM 사용자의 Amazon 리소스 이름(ARN)입니다. 이 파라미터는 `MigrationType` 파라미터에 대해 `CutOver` 값을 지정하는 경우에만 적용됩니다.

- DestinationSecurityGroupId

  형식: StringList

  설명: (선택 사항) VPC에서 시작되는 Amazon EC2 인스턴스와 연결하려는 보안 그룹의 ID입니다. 이 파라미터에 대한 값을 지정하지 않으면, 자동화가 VPC에 보안 그룹을 생성하고 EC2-Classic의 보안 그룹에서 규칙을 복사합니다. 규칙이 새 보안 그룹으로 복사되지 않는 경우, VPC의 기본 보안 그룹이 Amazon EC2 인스턴스와 연결됩니다.

- DestinationSubnetId

  유형: 문자열

  설명: (선택 사항) Amazon EC2 인스턴스를 마이그레이션하려는 서브넷의 ID입니다. 이 파라미터에 대한 값을 지정하지 않으면, 자동화가 VPC에서 서브넷을 무작위로 선택합니다.

- InstanceId

  유형: 문자열

설명: (필수) 마이그레이션하려는 Amazon EC2 인스턴스의 ID입니다.

- MigrationType

  유형: 문자열

  유효한 값: CutOver | Test

  설명: (필수) 수행하려는 마이그레이션 유형입니다.

  EC2-Classic에서 실행 중인 Amazon EC2 인스턴스를 중지하려면 이 `CutOver` 옵션에 대한 승인이 필요합니다. 이 작업이 승인되면 Amazon EC2 인스턴스가 중지되고 자동화가 Amazon Machine Image(AMI)을 생성합니다. AMI 상태가 `available`이면 VPC에서 지정하는 `DestinationSubnetId`의 이 AMI에서 새 Amazon EC2 인스턴스가 시작됩니다. EC2-Classic에서 실행 중인 Amazon EC2 인스턴스에 탄력적 IP 주소가 연결된 경우, 인스턴스는 VPC에서 새로 생성된 Amazon EC2 인스턴스로 이동합니다. VPC에서 시작한 Amazon EC2 인스턴스가 어떤 이유로든 생성되지 않는 경우, 인스턴스가 종료되며 EC2-Classic에서 Amazon EC2 인스턴스를 시작할 수 있도록 승인을 요청합니다.

  이 `Test` 옵션은 재부팅 없이 EC2-Classic에서 실행 중인 Amazon EC2 인스턴스의 AMI를 생성합니다. Amazon EC2 인스턴스는 재부팅되지 않으므로, 생성된 이미지의 파일 시스템 무결성을 보장할 수 없습니다. AMI 상태가 `available`이면 VPC에서 지정하는 `DestinationSubnetId`의 이 AMI에서 새 Amazon EC2 인스턴스가 시작됩니다. EC2-Classic에서 실행 중인 Amazon EC2 인스턴스에 탄력적 IP 주소가 연결된 경우, 자동화를 통해 지정하는 `DestinationSubnetId`이 퍼블릭인지 확인합니다. VPC에서 시작한 Amazon EC2 인스턴스가 어떤 이유로든 생성되지 않는 경우, 인스턴스가 종료되며 자동화가 종료됩니다.

- SNSNotificationARNforApproval

  유형: 문자열

  설명: (선택 사항) 승인 요청을 보내려는 Amazon Simple Notification Service(SNS) 주제의 ARN입니다. 이 파라미터는 `MigrationType` 파라미터에 대해 `CutOver` 값을 지정하는 경우에만 적용됩니다.

- TargetInstanceType

  유형: 문자열

  기본값: t2.2xlarge

설명: (선택 사항) VPC에서 시작하려는 Amazon EC2 인스턴스의 유형입니다. T2, M4 또는 C4와 같은 Xen 기반 인스턴스 유형만 지원됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeAwsApi` - `InstanceId` 파라미터에서 사용자가 지정하는 Amazon EC2 인스턴스에 대한 세부 정보를 수집합니다.
- `aws:assertAwsResourceProperty` - `TargetInstanceType` 파라미터에서 사용자가 지정하는 인스턴스 유형이 Xen 기반인지 확인합니다.
- `aws:assertAwsResourceProperty` - `InstanceId` 파라미터에서 사용자가 지정하는 Amazon EC2 인스턴스가 HVM 가상화 유형인지 확인합니다.
- `aws:assertAwsResourceProperty` - `InstanceId` 파라미터에서 사용자가 지정하는 Amazon EC2 인스턴스에 Amazon EBS 루트 볼륨이 있는지 확인합니다.
- `aws:executeScript` - `DestinationSecurityGroupId` 파라미터에서 사용자가 지정하는 값에 따라 필요한 경우 보안 그룹을 생성합니다.
- `aws:branch` - `DestinationSubnetId` 파라미터에서 사용자가 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - 이 자동화를 실행하는 AWS 리전의 기본 VPC를 식별합니다.
- `aws:executeAwsApi` - 기본 VPC에 위치한 서브넷의 ID를 무작위로 선택합니다.
- `aws:createImage` - Amazon EC2 인스턴스를 재부팅하지 않은 상태로 AMI를 생성합니다.
- `aws:branch`- `MigrationType` 파라미터에 대해 사용자가 지정하는 값을 기반으로 분기합니다.
- `aws:branch`- `DestinationSubnetId` 파라미터에 대해 사용자가 지정하는 값을 기반으로 분기합니다.
- `aws:runInstances` - EC2-Classic에서 Amazon EC2 인스턴스를 재부팅하지 않은 상태로 생성된 AMI에서 새 인스턴스를 시작합니다.
- `aws:changeInstanceState` - 어떤 이유로든 이전 단계가 실패할 경우 새로 시작한 Amazon EC2 인스턴스를 종료합니다.
- `aws:runInstances` - 제공된 경우, `DestinationSubnetId`의 EC2-Classic에서 Amazon EC2 인스턴스를 재부팅하지 않은 상태로 생성된 AMI에서 새 인스턴스를 시작합니다.

- `aws:changeInstanceState` - 어떤 이유로든 이전 단계가 실패할 경우 새로 시작한 Amazon EC2 인스턴스를 종료합니다.
- `aws:assertAwsResourceProperty` - EC2-Classic에서 실행 중인 Amazon EC2 인스턴스의 중지 동작을 확인합니다.
- `aws:approve` - Amazon EC2 인스턴스 중지 승인을 기다립니다.
- `aws:changeInstanceState` - EC2-Classic에서 실행 중인 Amazon EC2 인스턴스를 중지합니다.
- `aws:changeInstanceState` - 필요한 경우 EC2-Classic에서 실행 중인 Amazon EC2 인스턴스를 강제 중지합니다.
- `aws:createImage` - 해당 내용을 중지한 후에 Amazon EC2 인스턴스의 AMI를 생성합니다.
- `aws:branch` - `DestinationSubnetId` 파라미터에 대해 지정된 값을 기반으로 분기합니다.
- `aws:runInstances` - EC2-Classic에서 중지된 Amazon EC2 인스턴스에서 생성된 AMI에서 새 인스턴스를 시작합니다.
- `aws:approve` - 어떤 이유로든 이전 단계가 실패할 경우, 새로 시작한 인스턴스 종료 승인을 기다리고, EC2-Classic에서 Amazon EC2 인스턴스를 시작합니다.
- `aws:changeInstanceState` - 새로 시작한 Amazon EC2 인스턴스를 종료합니다.
- `aws:runInstances` - `DestinationSubnetId` 파라미터에서 EC2-Classic의 중지된 Amazon EC2 인스턴스에서 생성된 AMI에서 새 인스턴스를 시작합니다.
- `aws:approve` - 어떤 이유로든 이전 단계가 실패할 경우, 새로 시작한 인스턴스 종료 승인을 기다리고, EC2-Classic에서 Amazon EC2 인스턴스를 시작합니다.
- `aws:changeInstanceState` - 새로 시작한 Amazon EC2 인스턴스를 종료합니다.
- `aws:changeInstanceState` - EC2-Classic에서 중지된 Amazon EC2 인스턴스를 시작합니다.
- `aws:branch` - Amazon EC2 인스턴스에 퍼블릭 IP 주소가 있는지 여부를 기반으로 분기합니다.
- `aws:executeAwsApi` - 퍼블릭 IP 주소가 탄력적 IP 주소인지 확인합니다.
- `aws:branch` - `MigrationType` 파라미터에서 사용자가 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - 탄력적 IP 주소를 VPC로 이동합니다.
- `aws:executeAwsApi` - VPC로 이동된 탄력적 IP 주소의 할당 ID를 수집합니다.
- `aws:branch` - VPC에서 실행 중인 Amazon EC2 인스턴스가 시작된 서브넷을 기반으로 분기합니다.
- `aws:executeAwsApi` - VPC에서 새로 시작한 인스턴스에 탄력적 IP 주소를 연결합니다.
- `aws:executeScript` - VPC에서 실행 중인 새로 시작한 Amazon EC2 인스턴스가 퍼블릭 서브넷인지 확인합니다.

출력

`getInstanceProperties.virtualizationType` - EC2-Classic에서 실행 중인 Amazon EC2 인스턴스의 가상화 유형입니다.

`getInstanceProperties.rootDeviceType` - EC2-Classic에서 실행 중인 Amazon EC2 인스턴스의 루트 디바이스 유형입니다.

`createAMIWithoutReboot.ImageId` - EC2-Classic에서 실행 중인 Amazon EC2 인스턴스를 재부팅하지 않은 상태로 생성한 AMI의 ID입니다.

`getDefaultVPC.VpcId` - `DestinationSubnetId` 파라미터에 대한 값을 제공하지 않은 경우 새 Amazon EC2 인스턴스가 시작되는 기본 VPC의 ID입니다.

`getSubnetIdinDefaultVPC.subnetIdFromDefaultVpc` - `DestinationSubnetId` 파라미터에 대한 값을 제공하지 않은 경우 새 Amazon EC2 인스턴스가 시작되는 기본 VPC의 서브넷 ID입니다.

`launchTestInstanceDefaultVPC.InstanceIds` - `Test` 마이그레이션 유형 도중 기본 VPC에서 새로 시작한 Amazon EC2 인스턴스의 ID입니다.

`launchTestInstanceProvidedSubnet.InstanceIds` - `Test` 마이그레이션 유형 도중 지정한 `DestinationSubnetId`에서 새로 시작한 Amazon EC2 인스턴스의 ID입니다.

`createAMIAfterStoppingInstance.ImageId` - EC2-Classic에서 실행 중인 Amazon EC2 인스턴스를 중지한 후 생성되는 AMI의 ID입니다.

`launchCutOverInstanceProvidedSubnet.InstanceIds` - `CutOver` 마이그레이션 유형 도중 지정한 `DestinationSubnetId`에서 새로 시작한 Amazon EC2 인스턴스의 ID입니다.

`launchCutOverInstanceDefaultVPC.InstanceIds` - `CutOver` 마이그레이션 유형 도중 기본 VPC에서 새로 시작한 Amazon EC2 인스턴스의 ID입니다.

`verifySubnetIsPublicTestDefaultVPC.IsSubnetPublic` - 기본 VPC에서 자동화를 통해 선택한 서브넷이 퍼블릭인지 여부입니다.

`verifySubnetIsPublicTestProvidedSubnet.IsSubnetPublic` - `DestinationSubnetId`에서 지정한 서브넷이 퍼블릭인지 여부입니다.

AWSSupport-MigrateXenToNitroLinux

설명

`AWSSupport-MigrateXenToNitroLinux` 실행서는 Amazon Elastic Compute Cloud(Amazon EC2)의 Linux Xen 인스턴스를 복제 및 준비하고 Nitro 인스턴스 유형으로 마이그레이션합니다. 이 실행서는 작업 유형에 대한 두 가지 옵션을 제공합니다.

- `Clone&Migrate` - 이 옵션의 워크플로는 예비 검사, 테스트 및 Clone&Migrate 단계로 구성됩니다. 워크플로는 `AWSSupport-CloneXenEC2InstanceAndMigrateToNitro` 실행서를 사용하여 실행됩니다.
- `FullMigration` - 이 옵션은 `Clone&Migrate` 워크플로를 실행한 다음 루트 Amazon EBS 볼륨 교체라는 추가 단계를 수행합니다.

> **Important**
>
> 이 실행서를 사용하면 Amazon EC2 인스턴스의 실행 시간, Amazon Elastic Block Store(Amazon EBS) 볼륨 생성 및 AMIs에 대한 비용이 계정에 발생합니다. 자세한 내용은 Amazon EC2 요금 및 Amazon EBS 요금을 참조하세요.

예비 검사

자동화는 마이그레이션을 계속하기 전에 다음과 같은 예비 검사를 수행합니다. 검사 중 하나라도 실패하면 자동화가 종료됩니다. 이 단계는 `Clone&Migrate` 워크플로의 일부일 뿐입니다.

- 대상 인스턴스가 이미 Nitro 인스턴스 유형인지 확인합니다.
- 대상 인스턴스에 스팟 인스턴스 구매 옵션이 사용되었는지 확인합니다.
- 인스턴스 스토어 볼륨이 대상 인스턴스에 연결되어 있는지 확인합니다.
- 대상 인스턴스 운영 체제(OS) 가 Linux인지 확인합니다.
- 대상 인스턴스가 Amazon EC2 Auto Scaling 그룹의 일부인지 확인합니다. Auto Scaling 그룹의 일부인 경우에는 자동화를 통해 인스턴스가 `standby` 상태에 있는지 확인합니다.
- 인스턴스가 AWS Systems Manager에 의해 관리되는지 확인합니다.

테스트

자동화는 대상 인스턴스에서 Amazon Machine Image(AMI)를 생성하고 새로 생성된 AMI 인스턴스에서 테스트 인스턴스를 시작합니다. 이 단계는 오직 `Clone&Migrate` 워크플로의 일부입니다.

테스트 인스턴스가 모든 상태 검사를 통과하면 자동화가 일시 중지되고 Amazon Simple Notification Service(Amazon SNS) 알림을 통해 지정된 보안 주체의 승인을 요청합니다. 승인이 제공되면 자동화

가 테스트 인스턴스를 종료하며 대상 인스턴스를 중지하고 마이그레이션을 계속합니다. 새로 생성된 AMI은 `Clone&Migrate` 워크플로가 끝나면 등록이 해제됩니다.

> **Note**
>
> 승인을 제공하기 전에 대상 인스턴스에서 실행 중인 모든 애플리케이션이 정상적으로 종료되었는지 확인하는 것이 좋습니다.

복제 및 마이그레이션

자동화는 대상 인스턴스에서 다른 AMI을 생성하고 새 인스턴스를 시작하여 Nitro 인스턴스 유형으로 변경합니다. 자동화는 마이그레이션을 계속하기 전에 다음 필수 조건을 완료합니다. 검사 중 하나라도 실패하면 자동화가 종료됩니다. 이 단계 또한 `Clone&Migrate` 워크플로의 일부일 뿐입니다.

- 향상된 네트워킹(ENA) 속성을 활성화합니다.
- ENA 드라이버가 아직 설치되지 않은 경우, 최신 버전을 설치하거나 ENA 드라이버 버전을 최신 버전으로 업데이트합니다. 네트워크 성능을 극대화하려면, Nitro 인스턴스 유형이 6세대인 경우 최신 ENA 드라이버 버전으로 업데이트해야 합니다.
- NVMe 모듈이 설치되었는지 확인합니다. 모듈이 설치되면 자동화는 모듈이 `initramfs`에 로드되었는지 확인합니다.
- `/etc/fstab`을 분석하고 블록 디바이스 이름(`/dev/sd*` 또는 `/dev/xvd*`)이 있는 항목을 해당 UUID로 교체합니다. 구성을 수정하기 전에 자동화를 통해 경로 `/etc/fstab*`에 파일 백업본이 생성됩니다.
- 옵션이 존재하는 경우, `/etc/default/grub` 파일의 `GRUB_CMDLINE_LINUX` 줄에, 또는 `/boot/grub/menu.lst`의 커널에 `net.ifnames=0` 옵션을 추가하여 예측 가능한 인터페이스 이름 지정을 비활성화합니다.
- 파일이 존재하는 경우 해당 `/etc/udev/rules.d/70-persistent-net.rules` 파일을 제거합니다. 파일을 제거하기 전에 자동화를 통해 경로 `/etc/udev/rules.d/`에 파일 백업본이 생성됩니다.

모든 요구 사항을 확인한 후, 인스턴스 유형이 지정한 Nitro 인스턴스 유형으로 변경됩니다. 자동화는 Nitro 인스턴스 유형으로 시작한 후 새로 생성한 인스턴스가 모든 상태 검사를 통과할 때까지 기다립니다. 그런 다음, 자동화는 지정된 보안 주체의 승인을 기다려서 성공적으로 시작된 Nitro 인스턴스의 AMI을 생성합니다. 승인이 거부되면, 자동화가 종료되고 새로 생성한 인스턴스는 계속 실행되며 대상 인스턴스는 중지된 상태로 유지됩니다.

루트 Amazon EBS 볼륨 교체

`FullMigration`을 `OperationType`로 선택하면 자동화가 대상 Amazon EC2 인스턴스를 지정한 Nitro 인스턴스 유형으로 마이그레이션합니다. 자동화는 지정된 보안 주체에게 승인을 요청하여 대상 Amazon EC2 인스턴스의 루트 Amazon EBS 볼륨을 복제된 Amazon EC2 인스턴스의 루트 볼륨으로 교체합니다. 마이그레이션이 성공한 후, 복제된 Amazon EC2 인스턴스가 종료됩니다. 자동화가 실패할 경우, 원래 Amazon EBS 루트 볼륨이 대상 Amazon EC2 인스턴스에 연결됩니다. 대상 Amazon EC2 인스턴스에 연결된 루트 Amazon EBS 볼륨에 `aws:` 접두사가 적용된 태그가 있는 경우 `FullMigration` 작업이 지원되지 않습니다.

시작하기 전에

대상 인스턴스는 아웃바운드 인터넷 액세스 권한이 있어야 합니다. 이는 kernel-devel, gcc, patch, rpm-build, wget, dracut, make, linux-headers 및 unzip 같은 드라이버 및 종속 항목의 리포지토리에 액세스하기 위한 것입니다. 필요한 경우 패키지 관리자를 사용합니다.

승인 및 업데이트 알림을 보내려면 Amazon SNS 주제가 필요합니다. Amazon SNS 주제 생성 방법에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 주제 생성을 참조하세요.

이 실행서는 다음 운영 체제를 지원합니다.

- RHEL 7.x - 8.5
- Amazon Linux (2018.03), Amazon Linux 2
- Debian 서버
- Ubuntu Server 18.04 LTS, 20.04 LTS 및 20.10 STR
- SUSE Linux Enterprise Server (SUSE12SP5, SUSE15SP2)

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 확인

  유형: 문자열

  설명: (필수) 이 자동화 실행서에서 수행한 작업의 전체 세부 정보를 읽고 실행서 사용을 계속하려면 **`Yes, I understand and acknowledge`**을 입력하세요.
- ApproverIAM

  유형: 문자열

  설명: (필수) 자동화에 대한 승인을 제공할 수 있는 IAM 역할, 사용자 또는 사용자 이름의 ARN입니다. 최대 10개의 승인자를 지정할 수 있습니다.
- DeleteResourcesOnFailure

  유형: 부울

  설명: (선택 사항) 자동화가 실패할 경우 새로 생성한 인스턴스와 마이그레이션용 AMI을 삭제할지 여부를 결정합니다.

  유효한 값: True | False

  기본값: True
- MinimumRequiredApprovals

  유형: 문자열

  설명: (선택 사항) 승인 요청 시 자동화를 계속 실행하는 데 필요한 최소 승인 수입니다.

  유효한 값: 1~10

기본값: 1

- NitroInstanceType

  유형: 문자열

  설명: (필수) 인스턴스를 변경하려는 Nitro 인스턴스 유형입니다. 지원되는 인스턴스 유형에는 M5, M6, C5, C6, R5, R6, T3이 포함됩니다.

  기본값: m5.xlarge

- OperationType

  유형: 문자열

  설명: (필수) 수행하려는 작업입니다. 이 `FullMigration` 옵션은 `Clone&Migrate`와 동일한 작업을 수행하며 대상 인스턴스의 루트 볼륨을 추가로 대체합니다. 대상 인스턴스의 루트 볼륨은 다음 마이그레이션 프로세스에 따라 새로 생성한 인스턴스의 루트 볼륨으로 대체됩니다. 이 `FullMigration` 작업은 논리적 볼륨 관리자(LVM)에서 정의한 루트 볼륨을 지원하지 않습니다.

  유효한 값: Clone&Migrate | FullMigration

- SNSTopicArn

  유형: 문자열

  설명: (필수) 알림을 게시할 Amazon SNS 주제의 ARN입니다. Amazon SNS 주제는 자동화 도중 필수 승인 알림을 보내는 데 사용됩니다.

- TargetInstanceId

  유형: 문자열

  설명: (필수) 마이그레이션하려는 Amazon EC2 인스턴스의 ID입니다.

Clone&Migrate 워크플로

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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

문서 단계

- startOfPreliminaryChecksBranch - 예비 검사 워크플로로 분기합니다.
- getTargetInstanceProperties - 대상 인스턴스에서 세부 정보를 수집합니다.

- `checkIfNitroInstanceTypeIsSupportedInAZ` - 대상 Amazon EC2 인스턴스 유형이 대상 인스턴스와 동일한 가용 영역에서 지원되는지 확인합니다.
- `getXenInstanceTypeDetails` - 소스 인스턴스 유형에 대한 세부 정보를 수집합니다.
- `checkIfInstanceHypervisorIsNitroAlready` - 대상 인스턴스가 이미 Nitro 인스턴스 유형으로 실행 중인지 확인합니다.
- `checkIfTargetInstanceLifecycleIsSpot` - 대상 인스턴스의 구매 옵션이 Spot인지 확인합니다.
- `checkIfOperatingSystemIsLinux` - 대상 인스턴스 OS가 Linux인지 확인합니다.
- `verifySSMConnectivityForTargetInstance` - 대상 인스턴스가 Systems Manager에서 관리되고 있는지 확인합니다.
- `checkIfEphemeralVolumeAreSupported` - 대상 인스턴스의 현재 인스턴스 유형이 인스턴스 스토어 볼륨을 지원하는지 확인합니다.
- `verifyIfTargetInstanceHasEphemeralVolumesAttached` - 대상 인스턴스에 인스턴스 스토어 볼륨이 연결되어 있는지 확인합니다.
- `checkIfRootVolumeIsEBS` - 대상 인스턴스의 루트 볼륨 유형이 EBS인지 확인합니다.
- `checkIfTargetInstanceIsInASG` - 대상 인스턴스가 Auto Scaling 그룹의 일부인지 확인합니다.
- `endOfPreliminaryChecksBranch` - 예비 검사 브랜치를 종료합니다.
- `startOfTestBranch` - 테스트 워크플로로 분기합니다.
- `createTestImage` - 대상 인스턴스의 테스트 AMI를 생성합니다.
- `launchTestInstanceInSameSubnet` - 대상 인스턴스와 동일한 구성을 사용하여 테스트 AMI에서 테스트 인스턴스를 시작합니다.
- `cleanupTestInstance` - 테스트 인스턴스를 종료합니다.
- `endOfTestBranch` - 테스트 브랜치를 종료합니다.
- `checkIfTestingBranchSucceeded` - 테스트 브랜치의 상태를 확인합니다.
- `approvalToStopTargetInstance` - 대상 인스턴스를 중지하기 위해 지정된 보안 주체의 승인을 기다립니다.
- `stopTargetEC2Instance` - 대상 인스턴스를 중지합니다.
- `forceStopTargetEC2Instance` - 이전 단계에서 인스턴스를 중지하지 못한 경우에만 대상 인스턴스를 강제 중지합니다.
- `startOfCloneAndMigrateBranch` - Clone&Migrate 워크플로로 분기합니다.
- `createBackupImage` - 백업으로 사용할 대상 인스턴스의 AMI를 생성합니다.

- `launchInstanceInSameSubnet` - 소스 인스턴스와 동일한 구성을 사용하여 백업 AMI에서 새 인스턴스를 시작합니다.
- `waitForClonedInstanceToPassStatusChecks` - 새로 생성한 인스턴스가 모든 상태 검사를 통과할 때까지 기다립니다.
- `verifySSMConnectivityForClonedInstance` - 새로 생성한 인스턴스가 Systems Manager에서 관리되는지 확인합니다.
- `checkAndInstallENADrivers` - 새로 생성한 인스턴스에 ENA 드라이버가 설치되어 있는지 확인하고 필요한 경우 드라이버를 설치합니다.
- `checkAndAddNVMEDrivers` - 새로 생성한 인스턴스에 NVMe 드라이버가 설치되어 있는지 확인하고 필요한 경우 드라이버를 설치합니다.
- `checkAndModifyFSTABEntries` - 디바이스 이름이 `/etc/fstab`에서 사용되었는지 확인하고 필요한 경우 UUID로 대체합니다.
- `stopClonedInstance` - 새로 생성한 인스턴스를 중지합니다.
- `forceStopClonedInstance` - 이전 단계에서 인스턴스를 중지하지 못한 경우에만 새로 생성한 인스턴스를 강제 중지합니다.
- `checkENAAttributeForClonedInstance` - 새로 생성한 인스턴스에 향상된 네트워킹 속성이 켜져 있는지 확인합니다.
- `setNitroInstanceTypeForClonedInstance` - 새로 생성한 인스턴스의 인스턴스 유형을 지정하는 Nitro 인스턴스 유형으로 변경합니다.
- `startClonedInstance` - 인스턴스 유형을 변경한 새로 생성한 인스턴스를 시작합니다.
- `approvalForCreatingImageAfterDriversInstallation` - 인스턴스가 Nitro 인스턴스 유형으로 성공적으로 시작되면 자동화는 필수 보안 주체의 승인을 기다립니다. 승인이 제공되면 Golden AMI로 사용할 AMI을 생성합니다.
- `createImageAfterDriversInstallation` - Golden AMI으로 사용할 AMI를 생성합니다.
- `endOfCloneAndMigrateBranch` - Clone&Migrate 브랜치를 종료합니다.
- `cleanupTestImage` - 테스트를 위해 생성된 AMI의 등록을 해제합니다.
- `failureHandling` - 실패 시 리소스를 종료하도록 선택했는지 확인합니다.
- `onFailureTerminateClonedInstance` - 자동화가 실패하면 새로 생성한 인스턴스를 종료합니다.
- `onFailurecleanupTestImage` - 테스트를 위해 생성된 AMI의 등록을 해제합니다.
- `onFailureApprovalToStartTargetInstance` - 자동화가 실패하면 지정된 보안 주체의 승인을 기다려 대상 인스턴스를 시작합니다.

- `onFailureStartTargetInstance` - 자동화가 실패하면 대상 인스턴스를 시작합니다.

FullMigration 워크플로

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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

문서 단계

FullMigration 워크플로는 Clone&Migrate 워크플로와 동일한 단계를 실행하며 다음 단계를 추가로 수행합니다.

- checkConcurrency - 지정하는 Amazon EC2 인스턴스를 대상으로 하는 이 실행서의 자동화가 하나뿐인지 확인합니다. 실행서에서 동일한 인스턴스를 대상으로 진행 중인 또 다른 자동화가 발견되면 자동화가 종료됩니다.
- getTargetInstanceProperties - 대상 인스턴스에서 세부 정보를 수집합니다.
- checkRootVolumeTags - 대상 Amazon EC2 인스턴스의 루트 볼륨에 AWS 예약된 태그가 포함되어 있는지 확인합니다.
- cloneTargetInstanceAndMigrateToNitro - AWS-CloneXenInstanceToNitro 실행서를 사용하여 하위 자동화를 시작합니다.
- branchOnTheOperationType - OperationType 파라미터에 지정한 값을 기반으로 분기합니다.
- getClonedInstanceId - 하위 자동화에서 새로 시작한 인스턴스의 ID를 검색합니다.
- checkIfRootVolumeIsBasedOnLVM - 루트 파티션을 LVM에서 관리하는지 여부를 결정합니다.
- branchOnTheRootVolumeLVMStatus - 보안 주체부터 필요한 최소 승인을 받으면 자동화가 루트 볼륨 교체를 진행합니다.
- manualInstructionsInCaseOfLVM - LVM에서 루트 볼륨을 관리하는 경우, 자동화는 루트 볼륨을 수동으로 교체하는 방법에 대한 지침이 포함된 출력본을 보냅니다.
- startOfReplaceRootEBSVolumeBranch - 루트 EBS 볼륨 교체 브랜치 워크플로를 시작합니다.
- checkIfTargetInstanceIsManagedByCFN - 대상 인스턴스가 AWS CloudFormation 스택으로 관리되는지 여부를 결정합니다.
- branchOnCFNStackStatus - CloudFormation 스택의 상태를 기반으로 분기합니다.
- approvalForRootVolumesReplacement(WithCFN) - 대상 인스턴스가 CloudFormation에서 시작된 경우 자동화는 새로 시작된 인스턴스가 Nitro 인스턴스 유형으로 성공적으로 시작된 후 승인

을 기다립니다. 승인이 제공되면 대상 인스턴스의 Amazon EBS 볼륨이 새로 시작된 인스턴스의 루트 볼륨으로 교체됩니다.

- `approvalForRootVolumesReplacement` - 새로 시작한 인스턴스가 Nitro 인스턴스 유형으로 성공적으로 시작된 후 승인을 기다립니다. 승인이 제공되면 대상 인스턴스의 Amazon EBS 볼륨이 새로 시작된 인스턴스의 루트 볼륨으로 교체됩니다.
- `assertIfTargetEC2InstanceIsStillStopped` - 루트 볼륨을 교체하기 전에 대상 인스턴스가 `stopped` 상태인지 확인합니다.
- `stopTargetInstanceForRootVolumeReplacement` - 대상 인스턴스가 실행 중인 경우, 자동화는 루트 볼륨을 교체하기 전에 인스턴스를 중지합니다.
- `forceStopTargetInstanceForRootVolumeReplacement` - 이전 단계가 실패할 경우 대상 인스턴스를 강제 중지합니다.
- `stopClonedInstanceForRootVolumeReplacement` - Amazon EBS 볼륨을 교체하기 전에 새로 생성한 인스턴스를 중지합니다.
- `forceStopClonedInstanceForRootVolumeReplacement` - 이전 단계가 실패할 경우 새로 생성한 인스턴스를 강제 중지합니다.
- `getBlockDeviceMappings` - 대상 인스턴스와 새로 생성된 인스턴스 모두에 대한 블록 디바이스 매핑을 검색합니다.
- `replaceRootEbsVolumes` - 대상 인스턴스의 루트 볼륨을 새로 생성된 인스턴스의 루트 볼륨으로 교체합니다.
- `EndOfReplaceRootEBSVolumeBranch` - 루트 EBS 볼륨 교체 브랜치 워크플로를 종료합니다.
- `checkENAAttributeForTargetInstance` - 대상 Amazon EC2 인스턴스에 대해 향상된 네트워킹(ENA) 속성이 켜져 있는지 확인합니다.
- `enableENAAttributeForTargetInstance` - 필요한 경우 대상 Amazon EC2 인스턴스의 ENA 속성을 활성화합니다.
- `setNitroInstanceTypeForTargetInstance` - 대상 인스턴스를 지정한 Nitro 인스턴스 유형으로 변경합니다.
- `replicateRootVolumeTags` - 대상 Amazon EC2 인스턴스에서 루트 Amazon EBS 볼륨에 태그를 복제합니다.
- `startTargetInstance` - 인스턴스 유형을 변경한 후 대상 Amazon EC2 인스턴스를 시작합니다.
- `onFailureStopTargetEC2Instance` - 대상 Amazon EC2 인스턴스가 Nitro 인스턴스 유형으로 시작되지 않을 경우 이를 중지합니다.
- `onFailureForceStopTargetEC2Instance` - 이전 단계가 실패할 경우 대상 Amazon EC2 인스턴스를 강제 중지합니다.

- `OnFailureRevertOriginalInstanceType` - 대상 인스턴스가 Nitro 인스턴스 유형으로 시작하지 못할 경우 대상 Amazon EC2 인스턴스를 원래 인스턴스 유형으로 되돌립니다.
- `onFailureRollbackRootVolumeReplacement` - 필요한 경우 `replaceRootEbsVolumes`단계에서 변경한 내용을 모두 되돌립니다.
- `onFailureApprovalToStartTargetInstance` - 이전 변경 내용을 롤백한 후 대상 Amazon EC2 인스턴스를 시작하도록 지정된 보안 주체의 승인을 기다립니다.
- `onFailureStartTargetInstance` - 대상 Amazon EC2 인스턴스를 시작합니다.
- `terminateClonedEC2Instance` - 루트 Amazon EBS 볼륨을 교체한 후 복제된 Amazon EC2 인스턴스를 종료합니다.

AWSSupport-ResetAccess

설명

이 실행서는 지정된 EC2 인스턴스에서 EC2Rescue 도구를 사용하여 EC2 콘솔(Windows)을 사용하는 암호 해독을 다시 활성화하거나 새 SSH 키 페어(Linux)를 생성 및 추가합니다. 키 페어를 분실한 경우 이 자동화는 사용자 고유의 키 페어를 사용하여 새 EC2 인스턴스를 시작하는 데 사용할 수 있는 암호 활성화된 AMI를 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- EC2RescueInstanceType

  유형: 문자열

  유효한 값: t2.small | t2.medium | t2.large

  기본값: t2.small

  설명: (필수) EC2Rescue 인스턴스의 EC2 인스턴스 유형입니다. 권장 크기: t2.small.

- InstanceId

  유형: 문자열

  설명: (필수) 액세스 권한을 재설정할 EC2 인스턴스의 ID입니다.

  > **Important**
  >
  > Systems Manager Automation은 이 인스턴스를 중지하고, 작업을 시도하기 전에 AMI를 생성합니다. 인스턴스 스토어 볼륨에 저장되어 있는 데이터가 손실됩니다. 탄력적 IP를 사용하지 않는 경우 퍼블릭 IP 주소가 변경됩니다.

- SubnetId

  유형: 문자열

  기본값: CreateNewVPC

  설명: (선택 사항) EC2Rescue 인스턴스의 서브넷 ID입니다. 기본적으로, Systems Manager Automation은 새 VPC를 생성합니다. 또는 SelectedInstanceSubnet을 사용하여 인스턴스와 동일한 서브넷을 사용하거나 사용자 지정 서브넷 ID를 지정합니다.

  > **Important**
  >
  > 서브넷은 InstanceId와 동일한 가용 영역이어야 하며 SSM 엔드포인트와의 통신을 허용해야 합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

자동화 출력을 읽을 수 있으려면 적어도 ssm:StartAutomationExecution, ssm:GetParameter(SSH 키 파라미터 이름 검색용) 및 ssm:GetAutomationExecution이 있어야 합니다. 필요한 권한에 대한 자세한 정보는 `AWSSupport-StartEC2RescueWorkflow` 단원을 참조하십시오.

문서 단계

1. `aws:assertAwsResourceProperty` - 제공된 인스턴스가 Windows인 경우를 단정합니다.
   a. (Windows용 EC2Rescue) 제공된 인스턴스가 Windows인 경우:
      i. `aws:executeAutomation` - Windows 오프라인 암호 재설정 스크립트용 EC2Rescue를 사용하여 `AWSSupport-StartEC2RescueWorkflow`를 간접적으로 호출합니다.
      ii. `aws:executeAwsApi` - 중첩된 자동화에서 백업 AMI ID를 검색합니다.
      iii. `aws:executeAwsApi` - 중첩된 자동화에서 암호 활성화된 AMI ID를 검색합니다.
      iv. `aws:executeAwsApi` - 중첩된 자동화에서 EC2Rescue 요약을 검색합니다.
   b. (Linux용 EC2Rescue) 제공된 인스턴스가 Linux인 경우:
      i. `aws:executeAutomation` - Linux 오프라인 SSH 키 삽입 스크립트용 EC2Rescue를 사용하여 `AWSSupport-StartEC2RescueWorkflow`를 간접적으로 호출합니다.
      ii. `aws:executeAwsApi` - 중첩된 자동화에서 백업 AMI ID를 검색합니다.
      iii. `aws:executeAwsApi` - 주입된 SSH 키에 대한 SSM 파라미터를 검색합니다.
      iv. `aws:executeAwsApi` - 중첩된 자동화에서 EC2Rescue 요약을 검색합니다.

출력

getEC2RescueForWindowsResult.Output

getWindowsBackupAmi.ImageId

getWindowsPasswordEnabledAmi.ImageId

getEC2RescueForLinuxResult.Output

getLinuxBackupAmi.ImageId

getLinuxSSHKeyParameter.Name

AWSSupport-ResetLinuxUserPassword

설명

AWSSupport-ResetLinuxUserPassword 실행서는 로컬 운영 체제(OS) 사용자의 암호를 재설정하는 데 도움이 됩니다. 이 런북은 직렬 콘솔을 사용하여 Amazon Elastic Compute Cloud (AmazonEC2) 인스턴스에 액세스해야 하는 사용자에게 특히 유용합니다. Runbook은 and AWS Identity and Access Management (IAM) 역할에 암호가 포함된 AWS Secrets Manager 비밀 값을 검색할 수 AWS 계정 있는 권한을 가진 임시 Amazon EC2 인스턴스를 생성합니다.

런북은 대상 Amazon EC2 인스턴스를 중지하고 루트 Amazon 엘라스틱 블록 스토어 EBS (Amazon) 볼륨을 분리하여 임시 Amazon 인스턴스에 연결합니다. EC2 Run Command를 사용하면, 임시 인스턴스에서 스크립트가 실행되어 지정한 OS 사용자의 암호를 설정합니다. 그러면 루트 Amazon EBS 볼륨이 대상 인스턴스에 다시 연결됩니다. 실행서는 또한 자동화를 시작할 때 루트 볼륨의 스냅샷을 생성하는 옵션도 제공합니다.

시작하기 전에

OS 사용자에게 할당하려는 암호 값을 사용하여 Secrets Manager 보안 암호를 생성합니다. 값은 일반 텍스트여야 합니다. 자세한 정보는 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager 보안 암호 생성을 참조하세요.

고려 사항

- 이 실행서를 사용하기 전에 인스턴스를 백업해 두는 것이 좋습니다. CreateSnapshot 파라미터 값을 **Yes**로 설정하는 것을 고려해 보세요.
- 로컬 사용자 암호를 변경하려면 실행서에서 인스턴스를 중지해야 합니다. 인스턴스가 중지되면, 메모리 또는 인스턴스 스토어 볼륨에 저장된 데이터가 손실됩니다. 또한 자동으로 할당된 공용 IPv4 주소도 모두 해제됩니다. 인스턴스를 중지하면 어떻게 되는지에 대한 자세한 내용은 Amazon EC2 User Guide의 인스턴스 중지 및 시작을 참조하십시오.
- 대상 Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨이 고객 관리 AWS Key Management Service (AWS KMS) 키로 암호화된 경우, 키가 암호화되지 않았는지 확인하십시오. 그렇지 않으면 인스턴스가 시작되지 않습니다deleted. AWS KMS disabled

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) 재설정하려는 OS 사용자 암호가 포함된 Amazon EC2 Linux 인스턴스의 ID입니다.
- LinuxUserName

  유형: 문자열

  기본값: ec2-user

  설명: (선택 사항) 재설정하려는 암호가 있는 OS 사용자 계정입니다.
- SecretArn

  유형: 문자열

  설명: (필수) 새 비밀번호가 포함된 Secrets Manager ARN 시크릿의 비밀번호입니다.
- SecurityGroupId

  유형: 문자열

  설명: (선택 사항) 임시 Amazon EC2 인스턴스에 연결할 보안 그룹의 ID입니다. 이 파라미터의 값을 제공하지 않으면 기본 Amazon Virtual Private Cloud (AmazonVPC) 보안 그룹이 사용됩니다.

- SubnetId

  유형: 문자열

  설명: (선택 사항) Amazon EC2 임시 인스턴스를 시작하려는 서브넷의 ID입니다. 기본적으로, 자동화는 대상 인스턴스와 동일한 서브넷을 선택합니다. 다른 서브넷을 제공하려면, 대상 인스턴스와 동일한 가용 영역에 있고 Systems Manager 엔드포인트에 액세스할 수 있어야 합니다.

- CreateSnapshot

  유형: 문자열

  유효한 값: Yes | No

  기본값: Yes

  설명: (선택 사항) 자동화가 실행되기 전에 대상 Amazon EC2 인스턴스의 루트 볼륨 스냅샷을 생성할지 여부를 결정합니다.

- StopConsent

  유형: 문자열

  유효한 값: Yes | No

  기본값: 아니요

  설명: 이 자동화 중에 대상 Amazon EC2 인스턴스가 중지된다는 것을 **`Yes`** 확인하려면 입력하십시오. Amazon EC2 인스턴스가 중지되면 메모리 또는 인스턴스 스토어 볼륨에 저장된 모든 데이터가 손실되고 자동 공개 IPv4 주소가 해제됩니다. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 중지 및 시작을 참조하십시오.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

1. `aws:branch`— 브랜치는 대상 Amazon EC2 인스턴스 중지에 대한 동의 여부를 기반으로 합니다.

2. `aws:assertAwsResourceProperty`— Amazon EC2 인스턴스 상태가 `running` or `stopped` 상태인지 확인합니다. 그렇지 않으면, 자동화가 종료됩니다.
3. `aws:executeAwsApi`— Amazon EC2 인스턴스 속성을 가져옵니다.
4. `aws:executeAwsApi`— 루트 볼륨 속성을 가져옵니다.
5. `aws:branch`— 임시 Amazon EC2 인스턴스의 서브넷 ID가 제공되었는지 여부에 따라 자동화를 분기합니다.
6. `aws:assertAwsResourceProperty`— `SubnetId` 파라미터에 지정한 서브넷이 대상 Amazon EC2 인스턴스와 동일한 가용 영역에 있는지 확인합니다.
7. `aws:assertAwsResourceProperty`— 대상 Amazon EC2 인스턴스 루트 볼륨이 Amazon EBS 볼륨인지 확인합니다.
8. `aws:assertAwsResourceProperty`— Amazon EC2 인스턴스 아키텍처가 `arm64` 또는인지 확인합니다`x86_64`.
9. `aws:assertAwsResourceProperty`— Amazon EC2 인스턴스 종료 동작이 `stop` 유효한지 아닌지 `terminate` 확인합니다.
10. `aws:branch`— Amazon EC2 인스턴스가 스팟 인스턴스가 아닌지 확인합니다. 그렇지 않으면, 자동화가 종료됩니다.
11. `aws:executeScript`— Amazon EC2 인스턴스가 Auto Scaling 그룹에 속하지 않도록 합니다. 인스턴스가 Auto Scaling 그룹의 일부인 경우, 자동화를 통해 Amazon EC2 인스턴스가 `Standby` 수명 주기 상태에 있음을 확인합니다.
12. `aws:createStack`— 지정한 OS 사용자의 암호를 재설정하는 데 사용되는 임시 Amazon EC2 인스턴스를 생성합니다.
13. `aws:waitForAwsResourceProperty`— 새로 시작한 임시 Amazon EC2 인스턴스가 실행될 때까지 기다립니다.
14. `aws:executeAwsApi`— 임시 Amazon EC2 인스턴스의 ID를 가져옵니다.
15. `aws:waitForAwsResourceProperty`— 임시 Amazon EC2 인스턴스가 Systems Manager에서 관리하는 것으로 보고될 때까지 기다립니다.
16. `aws:changeInstanceState`— 대상 Amazon EC2 인스턴스를 중지합니다.
17. `aws:changeInstanceState`— 대상 Amazon EC2 인스턴스가 중지 상태에서 멈추는 경우 강제로 중지합니다.
18. `aws:branch`— 대상 Amazon EC2 인스턴스의 루트 볼륨 스냅샷이 요청되었는지 여부에 따라 자동화를 분기합니다.
19. `aws:executeAwsApi`— 대상 Amazon EC2 인스턴스 루트 Amazon EBS 볼륨의 스냅샷을 생성합니다.

20. `aws:waitForAwsResourceProperty`— 스냅샷이 `completed` 상태가 될 때까지 기다립니다.
21. `aws:executeAwsApi`— 대상 Amazon EC2 인스턴스에서 Amazon EBS 루트 볼륨을 분리합니다.
22. `aws:waitForAwsResourceProperty`— Amazon EBS 루트 볼륨이 대상 Amazon 인스턴스에서 분리될 때까지 기다립니다. EC2
23. `aws:executeAwsApi`— 루트 Amazon EBS 볼륨을 임시 Amazon EC2 인스턴스에 연결합니다.
24. `aws:waitForAwsResourceProperty`— Amazon EBS 루트 볼륨이 임시 Amazon EC2 인스턴스에 연결될 때까지 기다립니다.
25. `aws:runCommand`— 임시 Amazon EC2 인스턴스에서 Run Command를 사용하여 셸 스크립트를 실행하여 대상 사용자 암호를 재설정합니다.
26. `aws:executeAwsApi`— Amazon EBS 루트 볼륨을 임시 Amazon EC2 인스턴스에서 분리합니다.
27. `aws:waitForAwsResourceProperty`— Amazon EBS 루트 볼륨이 임시 Amazon 인스턴스에서 분리될 때까지 기다립니다. EC2
28. `aws:executeAwsApi`— 오류 발생 후 임시 Amazon EC2 인스턴스에서 Amazon EBS 루트 볼륨을 분리합니다.
29. `aws:waitForAwsResourceProperty`— 오류 발생 후 Amazon EBS 루트 볼륨이 임시 Amazon EC2 인스턴스에서 분리될 때까지 기다립니다.
30. `aws:branch`— 오류 발생 시 복구 경로를 확인하기 위해 루트 볼륨의 스냅샷을 요청했는지 여부에 따라 자동화를 분기합니다.
31. `aws:executeAwsApi`— 루트 Amazon EBS 볼륨을 대상 Amazon 인스턴스에 다시 연결합니다. EC2
32. `aws:waitForAwsResourceProperty`— Amazon EBS 루트 볼륨이 Amazon EC2 인스턴스에 연결될 때까지 기다립니다.
33. `aws:executeAwsApi`— 대상 Amazon EC2 인스턴스 루트 EBS 볼륨 스냅샷에서 새 Amazon 볼륨을 생성합니다.
34. `aws:waitForAwsResourceProperty`— 새 Amazon EBS 볼륨이 `available` 상태가 될 때까지 기다립니다.
35. `aws:executeAwsApi`— 새 Amazon EBS 볼륨을 대상 인스턴스에 루트 볼륨으로 연결합니다.
36. `aws:waitForAwsResourceProperty`— Amazon EBS 볼륨이 특정 `attached` 상태가 될 때까지 기다립니다.
37. `aws:executeAwsApi`— Runbook에서 AWS CloudFormation 스택을 생성하거나 업데이트하지 못하는 경우의 AWS CloudFormation 스택 이벤트를 설명합니다.
38. `aws:branch`— 이전 Amazon EC2 인스턴스 상태에 따라 자동화를 분기합니다. 상태가 `running`이면, 인스턴스가 시작됩니다. 인스턴스가 `stopped` 상태였다면, 자동화는 계속됩니다.

39. `aws:changeInstanceState`— 필요한 경우 Amazon EC2 인스턴스를 시작합니다.
40. `aws:waitForAwsResourceProperty`— AWS CloudFormation 스택이 터미널 상태가 될 때까지 기다린 후 삭제합니다.
41. `aws:executeAwsApi`— 임시 Amazon EC2 인스턴스를 포함한 AWS CloudFormation 스택을 삭제합니다.

AWSPremiumSupport-ResizeNitroInstance

설명

`AWSPremiumSupport-ResizeNitroInstance` 실행서는 Nitro 시스템에 구축된 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 크기를 조정하기 위한 자동화된 솔루션을 제공합니다.

데이터 손실 및 가동 중지 시간의 잠재적 위험을 줄이기 위해, 실행서는 다음을 확인합니다.

- 인스턴스 중지 동작
- 인스턴스가 Amazon EC2 Auto Scaling 그룹의 일부이고 `standby` 모드에 있는 경우
- 인스턴스 상태 및 테넌시
- 변경하려는 인스턴스 유형은 현재 인스턴스에 연결된 네트워크 인터페이스 수를 지원합니다.
- 현재 인스턴스 유형과 대상 인스턴스 유형의 프로세서 아키텍처 및 가상화 유형은 동일한 내용입니다.
- 인스턴스가 실행 중이면 모든 상태 검사를 통과한 것입니다.
- 변경하려는 인스턴스 유형을 동일한 가용 영역에서 사용할 수 있습니다.

Amazon EC2가 인스턴스 유형을 변경한 후 상태 검사를 통과하지 못하면, 실행서는 자동으로 이전 인스턴스 유형으로 롤백됩니다.

기본적으로, 이 실행서는 실행 중이고 인스턴스 스토어 볼륨이 연결되어 있는 경우, 인스턴스 유형을 변경하지 않습니다. 또한 인스턴스가 AWS CloudFormation 스택의 일부인 경우, 실행서는 인스턴스 유형을 변경하지 않습니다. 이러한 동작 중 하나를 변경하려면 `AllowInstanceStoreInstances` 및 `AllowCloudFormationInstances` 파라미터의 `yes`을 지정하세요.

실행서는 변경하려는 인스턴스 유형을 지정하는 두 가지 방법을 제공합니다.

- 단일 인스턴스를 대상으로 하는 단순 자동화의 경우, `TargetInstanceTypeFromParameter` 파라미터를 사용하여 변경하려는 인스턴스 유형을 지정합니다.

- 대규모로 자동화를 실행하여 여러 인스턴스의 인스턴스 유형을 변경하려면, `TargetInstanceTypeFromTagValue` 파라미터를 사용하여 인스턴스 유형을 지정합니다. 대규모 자동화 실행에 대한 자세한 내용은 대규모 자동화 실행을 참조하세요.

두 파라미터 중 하나에 값을 지정하지 않으면, 자동화가 실패합니다.

> **Important**
>
> `AWSPremiumSupport-*` 실행서에 액세스하려면 Enterprise 또는 Business Support Subscription이 필요합니다. 자세한 내용은 AWS Support 플랜 비교를 참조하세요.

고려 사항

- 이 실행서를 사용하기 전에 인스턴스를 백업해 두는 것이 좋습니다.
- 인스턴스 유형 변경의 호환성에 대한 자세한 내용은 인스턴스 유형 변경 호환성을 참조하세요.
- 자동화가 실패하고 원래 인스턴스 유형으로 롤백되는 경우, 인스턴스 유형 변경 문제 해결을 참조하세요.
- 인스턴스 유형을 변경하려면 실행서에서 인스턴스를 중지해야 합니다. 인스턴스가 중지되면, 메모리 또는 인스턴스 스토어 볼륨에 저장된 데이터가 손실됩니다. 또한, 자동으로 할당된 임의의 퍼블릭 IPv4 주소가 해제됩니다. 인스턴스를 중지할 경우 발생하는 상황에 대한 자세한 내용은 인스턴스 중지 및 시작을 참조하세요.
- `SkipInstancesWithTagKey` 파라미터를 사용하면, 특정 Amazon EC2 태그 키가 적용된 인스턴스를 건너뛸 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 확인

  유형: 문자열

  설명: (필수) **yes**을 입력하여 현재 실행 중인 인스턴스가 중지될 것임을 확인합니다.

- AllowInstanceStoreInstances

  유형: 문자열

  유효한 값: no | yes

  기본값: 아니요

  설명: (선택 사항) yes을 지정하는 경우, 인스턴스 스토어 볼륨이 연결된 인스턴스에서 실행서가 실행되도록 허용합니다.

- AllowCloudFormationInstances

  유형: 문자열

  유효한 값: no | yes

  기본값: 아니요

  설명: (선택 사항) yes을 지정하는 경우, 실행서는 AWS CloudFormation 스택의 일부인 인스턴스에서 실행됩니다.

- DryRun

  유형: 문자열

  유효한 값: no | yes

기본값: 아니요

설명: (선택 사항) `yes`을 지정하는 경우, 실행서는 인스턴스 유형을 변경하지 않고 크기 조정 요구 사항을 검증합니다.

- InstanceId

  유형: 문자열

  설명: (필수) 변경하려는 유형이 있는 Amazon EC2 인스턴스의 ID입니다.

- SkipInstancesWithTagKey

  유형: 문자열

  설명: (선택 사항) 지정한 태그 키가 인스턴스에 적용되면, 자동화가 대상 인스턴스를 건너뜁니다.

- SleepTime

  유형: 문자열

  기본값: 3

  설명: (선택 사항) 이 실행서가 완료 후 대기 상태로 유지되는 시간(초)입니다.

- TagInstance

  유형: 문자열

  설명: (선택 사항) *`Key=ChangingType,Value=True`* 형식을 사용하여 선택한 키와 값으로 인스턴스에 태그를 지정합니다. 이 옵션을 사용하면 이 실행서가 대상으로 지정한 인스턴스를 추적할 수 있습니다. 태그 키와 값은 대/소문자를 구분합니다.

- TargetInstanceTypeFromParameter

  유형: 문자열

  설명: (선택 사항) 인스턴스를 변경하려는 인스턴스 유형입니다. `TargetInstanceTypeFromTagValue` 파라미터에 제공된 태그 키 값을 사용하려는 경우, 이 파라미터를 비워 두세요.

- TargetInstanceTypeFromTagValue

  유형: 문자열

설명: (선택 사항) 변경하려는 인스턴스 유형이 값에 포함된 대상 인스턴스에 적용되는 태그 키입니다. `TargetInstanceTypeFromParameter` 파라미터의 값을 지정하면, 이 파라미터에 지정한 파라미터의 모든 값을 무시합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

1. `aws:assertAwsResourceProperty`: `SkipInstancesWithTagKey` 파라미터에 지정된 리소스 태그 키로 Amazon EC2 인스턴스에 태그가 지정되지 않았는지 확인합니다. 태그 키가 인스턴스에 적용된 것으로 확인되면, 단계가 실패하고 자동화가 종료됩니다.
2. `aws:assertAwsResourceProperty`: 대상 Amazon EC2 인스턴스의 상태가`running`, `pending`, `stopped` 또는 `stopping`인지 확인합니다. 그렇지 않으면, 자동화가 종료됩니다.
3. `aws:executeAwsApi`: Amazon EC2 인스턴스에서 속성을 수집합니다.
4. `aws:executeAwsApi`: 현재 Amazon EC2 인스턴스 유형에 대한 세부 정보를 수집합니다.
5. `aws:branch`: 현재 인스턴스 유형과 `TargetInstanceTypeFromParameter` 파라미터에 지정된 인스턴스 유형이 동일한지 확인합니다. 그럴 경우, 자동화가 종료됩니다.

6. `aws:assertAwsResourceProperty`: 인스턴스가 Nitro 시스템에서 실행되는지 확인합니다.
7. `aws:branch`: Amazon EC2 인스턴스 루트 볼륨 유형이 Amazon Elastic Block Store(Amazon EBS) 볼륨인지 확인합니다.
8. `aws:assertAwsResourceProperty`: 인스턴스 종료 동작이 `terminate`이 아닌 `stop`인지 확인합니다.
9. `aws:branch`: Amazon EC2 인스턴스가 스팟 인스턴스가 아닌지 확인합니다.
10. `aws:branch`: Amazon EC2 인스턴스 테넌시가 전용 호스트나 전용 인스턴스가 아닌 기본값인지 확인합니다.
11. `aws:executeScript`: 현재 인스턴스 ID를 대상으로 하는 이 실행서의 자동화가 하나만 존재한다는 점을 확인합니다. 동일한 인스턴스를 대상으로 하는 다른 자동화가 이미 진행 중인 경우, 자동화가 오류를 반환하고 종료됩니다.
12. `aws:branch`: Amazon EC2 인스턴스의 상태를 기반으로 자동화를 분기합니다.
    a. `stopped` 또는 `stopping`인 경우, Amazon EC2 인스턴스가 완전히 중지될 때까지 자동화가 `aws:waitForAwsResourceProperty`을 실행합니다.
    b. `running` 또는 `pending`인 경우, Amazon EC2 인스턴스가 상태 검사를 통과할 때까지 자동화가 `aws:waitForAwsResourceProperty`을 실행합니다.
13. `aws:assertAwsResourceProperty`: `DescribeAutoScalingInstances` API 작업을 호출하여 Amazon EC2 인스턴스가 Auto Scaling 그룹의 일부가 아닌지 확인합니다. 인스턴스가 Auto Scaling 그룹의 일부인 경우, Amazon EC2 인스턴스가 `standby` 모드에 있는지 확인하세요.
14. `aws:branch`: 자동화를 통해 Amazon EC2 인스턴스가 AWS CloudFormation 스택의 일부인지 확인하려는지 여부에 따라 자동화를 분기합니다.
    a. `aws:executeScript` `DescribeStackResources` API 작업을 호출하여 Amazon EC2 인스턴스가 AWS CloudFormation 스택의 일부가 아닌지 확인합니다.
15. `aws:executeAwsApi`: 프로세서 아키텍처 유형, 가상화 유형이 동일하고, 대상 인스턴스에 현재 연결된 네트워크 인터페이스 수를 지원하는 인스턴스 유형 목록을 반환합니다.
16. `aws:executeAwsApi`: `TargetInstanceTypeFromTagValue` 파라미터에 지정된 태그 키에서 대상 인스턴스 유형 값을 가져옵니다.
17. `aws:executeScript`: 현재 인스턴스 유형과 대상 인스턴스 유형이 호환되는지 확인합니다. 대상 인스턴스 유형을 동일한 서브넷에서 사용할 수 있는지 확인합니다. 실행서를 시작한 보안 주체가 인스턴스 유형을 변경하고 실행 중인 경우, 인스턴스를 중지하고 시작할 수 있는 권한이 있는지 확인합니다.
18. `aws:branch`: `DryRun` 파라미터 값이 `yes`으로 설정되었는지 여부에 따라 자동화를 분기합니다. `yes`인 경우, 자동화가 종료됩니다.

19. `aws:branch`: 원본 인스턴스 유형과 대상 인스턴스 유형이 동일한 내용인지 확인합니다. 동일하면, 자동화가 종료됩니다.
20. `aws:executeAwsApi`: 현재 인스턴스 상태를 가져옵니다.
21. `aws:changeInstanceState`: Amazon EC2 인스턴스를 중지합니다.
22. `aws:changeInstanceState`: 인스턴스가 `stopping` 상태에서 멈춘 경우, 인스턴스를 강제로 중지합니다.
23. `aws:executeAwsApi`: 인스턴스 유형을 대상 인스턴스 유형으로 변경합니다.
24. `aws:sleep`: 최종 일관성을 위해 인스턴스 유형을 변경한 후 3초 동안 기다립니다.
25. `aws:branch`: 이전 인스턴스 상태를 기반으로 자동화를 분기합니다. 해당 내용이 `running`이었을 경우, 인스턴스가 시작됩니다.
    a. `aws:changeInstanceState`: 인스턴스 유형을 변경하기 전에 Amazon EC2 인스턴스가 실행 중이었다면, 해당 인스턴스를 시작합니다.
    b. `aws:waitForAwsResourceProperty`: Amazon EC2 인스턴스가 상태 검사를 통과할 때까지 기다립니다. 인스턴스가 상태 확인을 통과하지 못하면, 원래 인스턴스 유형으로 다시 변경됩니다.
        i. `aws:changeInstanceState`: 원래 인스턴스 유형으로 변경하기 전에 Amazon EC2 인스턴스를 중단합니다.
        ii. `aws:changeInstanceState`: 중지 상태에서 멈출 경우를 대비하여 해당 내용을 원래 인스턴스 유형으로 변경하기 전에 Amazon EC2 인스턴스를 강제로 중지합니다.
        iii. `aws:executeAwsApi`: Amazon EC2 인스턴스를 해당하는 원래 유형으로 변경합니다.
        iv. `aws:sleep`: 최종 일관성을 위해 인스턴스 유형을 변경한 후 3초 동안 기다립니다.
        v. `aws:changeInstanceState`: 인스턴스 유형을 변경하기 전에 Amazon EC2 인스턴스가 실행 중이었다면, 해당 인스턴스를 시작합니다.
        vi. `aws:waitForAwsResourceProperty`: Amazon EC2 인스턴스가 상태 검사를 통과할 때까지 기다립니다.
26. `aws:sleep`: 실행서를 종료하기 전에 기다립니다.

AWSSupport-RestoreEC2InstanceFromSnapshot

설명

`AWSSupport-RestoreEC2InstanceFromSnapshot` 실행서는 루트 볼륨의 작동 중인 Amazon Elastic Block Store(Amazon EBS) 스냅샷에서 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 식별하고 복원하는 데 도움이 됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- EndDate

  유형: 문자열

  설명: (선택 사항) 자동화를 통해 스냅샷을 찾도록 하려는 마지막 날짜입니다.
- InplaceSwap

  유형: 부울

  유효한 값: true | false

  설명: (선택 사항) 이 파라미터의 값을 `true`로 설정하면 스냅샷에서 새로 생성된 볼륨이 인스턴스에 연결된 기존 루트 볼륨을 대체합니다.
- InstanceId

  유형: 문자열

  설명: (필수) 스냅샷에서 복원할 인스턴스의 ID입니다.

- LookForInstanceStatusCheck

  유형: 부울

  유효한 값: true | false

  기본값: true

  설명: (선택 사항) 이 파라미터의 값을 `true`로 설정하면 자동화가 스냅샷에서 시작된 테스트 인스턴스의 인스턴스 상태 확인이 실패하는지 여부를 확인합니다.

- SkipSnapshotsBy

  유형: 문자열

  설명: (선택 사항) 인스턴스를 복원할 스냅샷을 검색할 때 스냅샷을 건너뛰는 간격입니다. 예를 들어, 사용 가능한 스냅샷이 100개이고 이 파라미터에 값을 2로 지정하면 모든 세 번째 스냅샷이 검토됩니다.

  기본값: 0

- SnapshotId

  유형: 문자열

  설명: (선택 사항) 인스턴스를 복원하려는 스냅샷의 ID입니다.

- StartDate

  유형: 문자열

  설명: (선택 사항) 자동화를 통해 스냅샷을 찾도록 하려는 첫 번째 날짜입니다.

- TotalSnapshotsToLook

  유형: 문자열

  설명: (선택 사항) 자동화가 검토하는 스냅샷의 수입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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

문서 단계

1. aws:executeAwsApi - 대상 인스턴스에 대한 세부 정보를 수집합니다.
2. aws:assertAwsResourceProperty - 대상 인스턴스가 존재하는지 확인합니다.
3. aws:assertAwsResourceProperty - 루트 볼륨이 Amazon EBS 볼륨인지 확인합니다.
4. aws:assertAwsResourceProperty - 이 인스턴스를 대상으로 하는 다른 자동화가 이미 실행되고 있지 않은지 확인합니다.
5. aws:executeAwsApi - 대상 인스턴스에 태그를 지정합니다.
6. aws:executeAwsApi - 인스턴스의 AMI를 만듭니다.
7. aws:executeAwsApi - 이전 단계에서 생성한 AMI에 대한 세부 정보를 수집합니다.

8. `aws:waitForAwsResourceProperty` - 진행하기 전에 AMI의 상태가 `available`이 될 때까지 기다립니다.
9. `aws:executeScript` - 새로 만든 AMI에서 새 인스턴스를 시작합니다.
10. `aws:assertAwsResourceProperty` - 인스턴스 상태가 `available`인지 확인합니다.
11. `aws:executeAwsApi` - 새로 시작한 인스턴스에 대한 세부 정보를 수집합니다.
12. `aws:branch` - `SnapshotId` 파라미터에 대한 값을 제공했는지 여부를 기반으로 분기합니다.
13. `aws:executeScript` - 지정된 기간 내의 스냅샷 목록을 반환합니다.
14. `aws:executeAwsApi` - 인스턴스를 중지합니다.
15. `aws:waitForAwsResourceProperty` - 볼륨 상태가 `available`가 될 때까지 기다립니다.
16. `aws:waitForAwsResourceProperty` - 인스턴스 상태가 `stopped`가 될 때까지 기다립니다.
17. `aws:executeAwsApi` - 루트 볼륨을 분리합니다.
18. `aws:waitForAwsResourceProperty` - 루트 볼륨이 분리될 때까지 기다립니다.
19. `aws:executeAwsApi` - 새 루트 볼륨을 연결합니다.
20. `aws:waitForAwsResourceProperty` - 새 볼륨이 연결될 때까지 기다립니다.
21. `aws:executeAwsApi` - 인스턴스를 시작합니다.
22. `aws:waitForAwsResourceProperty` - 인스턴스 상태가 `available`가 될 때까지 기다립니다.
23. `aws:waitForAwsResourceProperty` - 인스턴스에 대한 시스템 및 인스턴스 상태 확인이 통과할 때까지 기다립니다.
24. `aws:executeScript` - 스크립트를 실행하여 볼륨을 성공적으로 생성하는 데 사용할 수 있는 스냅샷을 찾습니다.
25. `aws:executeScript` - 스크립트를 실행하여 자동화가 식별한 스냅샷에서 새로 생성된 볼륨을 사용하거나 `SnapshotId` 파라미터에 지정한 스냅샷에서 생성한 볼륨을 사용하여 인스턴스를 복구합니다.
26. `aws:executeScript` - 자동화를 통해 생성된 리소스를 삭제합니다.

출력

launchCloneInstance.InstanceIds

ListSnapshotByDate.finalSnapshots

ListSnapshotByDate.remainingSnapshotToBeCheckedInSameDateRange

findWorkingSnapshot.workingSnapshot

InstanceRecovery.result

AWSSupport-SendLogBundleToS3Bucket

설명

AWSSupport-SendLogBundleToS3Bucket 실행서는 EC2Rescue 도구로 생성된 로그 번들을 대상 인스턴스에서 지정된 S3 버킷으로 업로드합니다. 실행서는 대상 인스턴스의 플랫폼을 기반으로 플랫폼별 EC2Rescue 버전을 설치합니다. 그 다음에는 사용 가능한 모든 운영 체제(OS) 로그를 수집하는 데 EC2Rescue가 사용됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) 로그를 수집할 Windows 또는 Linux 관리형 인스턴스의 ID입니다.
- S3BucketName

  유형: 문자열

설명: (필수) 로그를 업로드할 S3 버킷입니다.

- S3Path

  유형: 문자열

  기본값: `AWSSupport-SendLogBundleToS3Bucket/`

  설명: (선택 사항) 수집한 로그의 S3 경로입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

이 명령을 수신하는 EC2 인스턴스에 AmazonSSMManagedInstanceCore Amazon 관리형 정책이 연결된 IAM 역할을 지정하는 것이 좋습니다. 자동화를 실행하고 인스턴스로 명령을 전송하려면 사용자에게 적어도 ssm:StartAutomationExecution 및 ssm:SendCommand가 있어야 하며, 추가로 자동화 출력을 읽을 수 있으려면 ssm:GetAutomationExecution도 있어야 합니다.

문서 단계

1. `aws:runCommand` - `AWS-ConfigureAWSPackage`를 통해 EC2Rescue를 설치합니다.
2. `aws:runCommand` - EC2Rescue를 사용하여 Windows 문제 해결 로그를 수집하는 PowerShell 스크립트를 실행합니다.
3. `aws:runCommand` - EC2Rescue를 사용하여 Linux 문제 해결 로그를 수집하는 bash 스크립트를 실행합니다.

출력

collectAndUploadWindowsLogBundle.Output

collectAndUploadLinuxLogBundle.Output

AWSSupport-StartEC2RescueWorkflow

설명

`AWSSupport-StartEC2RescueWorkflow` 실행서는 인스턴스를 복구하기 위해 생성된 헬퍼 인스턴스에서 제공된 base64로 인코딩된 스크립트(Bash 또는 Powershell)를 실행합니다. 인스턴스의 루트 볼륨은 인스턴스라고도 하는 도우미 인스턴스에 연결되고 마운트됩니다. EC2Rescue 인스턴스가

Windows이면 Powershell 스크립트를 제공합니다. 그렇지 않은 경우 Bash를 사용합니다. 이 실행서는 스크립트에서 사용할 수 있는 환경 변수를 설정합니다. 환경 변수에는 제공된 입력에 대한 정보와 오프라인 루트 볼륨에 대한 정보가 포함됩니다. 오프라인 볼륨이 이미 탑재되었고 사용할 수 있습니다. 예를 들면 원하는 상태 구성 파일을 오프라인 Windows 루트 볼륨에 저장하거나 chroot를 오프라인 Linux 루트 볼륨에 저장하고 오프라인 수정을 수행할 수 있습니다.

이 자동화 실행(콘솔)

> **Important**
>
> Marketplace Amazon 머신 이미지 (AMIs) 에서 생성된 Amazon EC2 인스턴스는 이 자동화에 의해 지원되지 않습니다.

추가 정보

스크립트를 base64로 인코딩하려는 경우 Powershell 또는 Bash를 사용할 수 있습니다. Powershell:

```
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes([System.IO.File]::ReadA
```

Bash:

```
base64 PATH_TO_FILE
```

다음은 대상 OS에 따라 오프라인 스크립트에서 사용할 수 있는 환경 변수의 목록입니다.

Windows:

변수	설명	예시 값
$env: _ _ID EC2RESCUE ACCOUNT	{{글로벌: ACCOUNT _ID}}	123456789012
$env: _ EC2RESCUE DATE	{{글로벌:DATE}}	2018-09-07
$env: _ _ EC2RESCUE DATE TIME	{{글로벌: DATE _TIME}}	2018-09-07_18.09.59
$env: _ _ EC2RESCUE EC2RW DIR	EC2Rescue윈도우용 설치 경로	C:\Program 파일\ 아마존\ EC2Rescue

변수	설명	예시 값
$env: _ _ EC2RESCUE EC2RW DIR	EC2Rescue윈도우용 설치 경로	C:\Program 파일\ 아마존\ EC2Rescue
$env: _ _ID EC2RESCUE EXECUTION	{{자동화: EXECUTION _ID}}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
$env: EC2RESCUE _ _ _ _ OFFLINE CURRENT CONTROL SET	오프라인 Windows 현재 제어 설정 경로	`HKLM:\AWSTempSystem \ControlSet001`
$env: _ _ EC2RESCUE OFFLINE DRIVE	오프라인 Windows 드라이브 문자	D:\
$env: _ _ _ EC2RESCUE OFFLINE EBS DEVICE	오프라인 루트 볼륨 디바이스 EBS	xvdf
$env: EC2RESCUE _ _ _ OFFLINE KERNEL VER	오프라인 Windows 커널 버전	6.1.7601.24214
$env: _ _OS_ EC2RESCUE OFFLINE ARCHITECTURE	오프라인 Windows 아키텍처	AMD64
$env: _ _OS_ EC2RESCUE OFFLINE CAPTION	오프라인 Windows 캡션	Windows Server 2008 R2 Datacenter
$env: _ _OS_ EC2RESCUE OFFLINE TYPE	오프라인 Windows OS 유형	Server
$env: _ _ _ _ EC2RESCUE OFFLINE PROGRAM FILES DIR	오프라인 Windows 프로그램 파일 디렉터리 경로	D:\Program Files
$env: EC2RESCUE _ _ _ _X86_ OFFLINE PROGRAM FILES DIR	오프라인 Windows 프로그램 파일 x86 디렉터리 경로	D:\Program Files (x86)

변수	설명	예시 값
$env: _ _ _ EC2RESCUE OFFLINE REGISTRY DIR	오프라인 Windows 레지스트리 디렉터리 경로	D:\Windows\System32\config
$env: _ _ _ EC2RESCUE OFFLINE SYSTEM ROOT	오프라인 Windows 시스템 루트 디렉터리 경로	D:\Windows
$env: _ EC2RESCUE REGION	{{글로벌:REGION}}	us-west-1
$env: _S3_ EC2RESCUE BUCKET	{{S3}} BucketName	amzn-s3-데모 버킷
$env: _S3_ EC2RESCUE PREFIX	{{ S3Prefix }}	myprefix/
$env: EC2RESCUE _ _ SOURCE INSTANCE	{{ InstanceId }}	i-abcdefgh123456789
$스크립트: _ _ _ EC2RESCUE OFFLINE WINDOWS INSTALL	오프라인 Windows 설치 메타데이터	고객 Powershell 객체

Linux:

변수	설명	예시 값
EC2RESCUE_ _아이디 ACCOUNT	{{글로벌: ACCOUNT _ID}}	123456789012
EC2RESCUE_DATE	{{글로벌:DATE}}	2018-09-07
EC2RESCUE_DATE_TIME	{{글로벌: DATE _TIME}}	2018-09-07_18.09.59
EC2RESCUE_EC2RL_DIR	EC2Rescue리눅스용 설치 경로	/usr/local/ec2rl-1.1.3

변수	설명	예시 값
EC2RESCUE_ EXECUTION _ID	{{자동화: EXECUTION _ID}}	7ef8008e-219b-4aca -8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_ DEVICE	오프라인 디바이스 이름	/dev/xvdf1
EC2RESCUE_OFFLINE_ EBS_DEVICE	오프라인 루트 볼륨 디바이스 EBS	/dev/sdf
EC2RESCUE_OFFLINE_ SYSTEM_ROOT	오프라인 루트 볼륨 탑재 지점	/mnt/mount
EC2RESCUE_PYTHON	Python 버전	python2.7
EC2RESCUE_REGION	{{글로벌:REGION}}	us-west-1
EC2RESCUE_S3_ BUCKET	{{S3}} BucketName	amzn-s3-데모 버킷
EC2RESCUE_S3_ PREFIX	{{ S3Prefix }}	myprefix/
EC2RESCUE_SOURCE_I NSTANCE	{{ InstanceId }}	i-abcdefgh123456789

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AMIPrefix

  유형: 문자열

기본값: `AWSSupport-EC2Rescue`

설명: (선택 사항) 백업 이름의 접두사. AMI

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- CreatePostEC2RescueBackup

  유형: 문자열

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) 스크립트를 실행한 AMI InstanceId 후 시작하기 전에 of를 `true` 생성하도록 설정합니다. 자동화가 완료된 후에도 AMI 지속됩니다. 에 대한 액세스를 보호하거나 삭제하는 것은 사용자의 책임입니다. AMI

- CreatePreEC2RescueBackup

  유형: 문자열

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) 스크립트를 InstanceId 실행하기 전에 AMI of를 `true` 생성하도록 설정합니다. 자동화가 완료된 후에도 AMI 지속됩니다. 에 대한 액세스를 보호하거나 삭제하는 것은 사용자의 책임입니다. AMI

- EC2RescueInstanceType

  유형: 문자열

  유효한 값: t2.small | t2.medium | t2.large

  기본값: t2.small

설명: (선택 사항) EC2 인스턴스의 EC2Rescue 인스턴스 유형.

- InstanceId

  유형: 문자열

  설명: (필수) EC2 인스턴스의 ID. IMPORTANT: AWS Systems Manager 자동화로 이 인스턴스가 중지됩니다. 인스턴스 스토어 볼륨에 저장되어 있는 데이터가 손실됩니다. 탄력적 IP를 사용하지 않는 경우 퍼블릭 IP 주소가 변경됩니다.

- OfflineScript

  유형: 문자열

  설명: (필수) 헬퍼 인스턴스에 대해 실행할 Base64로 인코딩된 스크립트입니다. 소스 인스턴스가 Linux이고 Windows인 PowerShell 경우 Bash를 사용하십시오.

- S3 BucketName

  유형: 문자열

  설명: (선택 사항) 문제 해결 로그를 업로드할 계정의 S3 버킷 이름입니다. 버킷 정책에서 수집된 로그에 액세스할 필요가 없는 당사자에 대해 불필요한 읽기/쓰기 권한을 부여하지 않도록 해야 합니다.

- S3Prefix

  유형: 문자열

  기본값: `AWSSupport-EC2Rescue`

  설명: (선택 사항) S3 로그의 접두사입니다.

- SubnetId

  유형: 문자열

  기본값: SelectedInstanceSubnet

  설명: (선택 사항) EC2Rescue 인스턴스의 서브넷 ID. 기본적으로 제공된 인스턴스가 상주하는 동일 서브넷이 사용됩니다. IMPORTANT: 사용자 지정 서브넷을 제공하는 경우 해당 서브넷은 동일한 가용 영역에 있어야 InstanceId 하며 엔드포인트에 대한 액세스를 허용해야 합니다. SSM

- UniqueId

  유형: 문자열

기본값: {{자동화: EXECUTION _ID}}

설명: (선택 사항) 자동화의 고유한 식별자입니다.

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

자동화를 실행하는 사용자는 A mazonSSMAutomation Role IAM 관리 정책을 연결하는 것이 좋습니다. 해당 정책 외에도, 사용자에게 다음이 필요합니다.

```
{
                "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"
                  }
               ]
```

```
            }
```

문서 단계

1. `aws:executeAwsApi` - 제공된 인스턴스를 설명합니다.
2. `aws:executeAwsApi` - 제공된 인스턴스의 루트 볼륨을 설명합니다.
3. `aws:assertAwsResourceProperty`- 루트 볼륨 디바이스 유형이 다음과 같은지 확인하세요. EBS
4. `aws:assertAwsResourceProperty` - 루트 볼륨이 암호화되지 않았는지 확인합니다.
5. `aws:assertAwsResourceProperty`- 제공된 서브넷 ID를 확인합니다.
   a. (현재 인스턴스 서브넷 사용) - SelectedInstanceSubnet * SubnetId = *인 경우 `aws:createStack` 실행하여 스택을 배포합니다. EC2Rescue CloudFormation
   b. (새로 생성VPC) - CreateNew VPC * SubnetId = *인 경우 `aws:createStack` 실행하여 스택을 배포합니다. EC2Rescue CloudFormation
   c. (사용자 지정 서브넷 사용) - 그 밖의 모든 경우:

      `aws:assertAwsResourceProperty` - 제공된 서브넷이 제공된 인스턴스와 동일한 가용 영역에 있는지 확인합니다.

      `aws:createStack`- EC2Rescue CloudFormation 스택 배포
6. `aws:invokeLambdaFunction` - 추가 입력 검증을 수행합니다.
7. `aws:executeAwsApi`- EC2Rescue CloudFormation 스택을 업데이트하여 EC2Rescue 헬퍼 인스턴스를 생성합니다.
8. `aws:waitForAwsResourceProperty`- EC2Rescue CloudFormation 스택 업데이트가 완료될 때까지 기다립니다.
9. `aws:executeAwsApi`- EC2Rescue CloudFormation 스택 출력을 설명하여 EC2Rescue 헬퍼 인스턴스 ID를 얻습니다.
10. `aws:waitForAwsResourceProperty`- EC2Rescue 도우미 인스턴스가 관리형 인스턴스가 될 때까지 기다립니다.
11. `aws:changeInstanceState` - 제공된 인스턴스를 중지합니다.
12. `aws:changeInstanceState` - 제공된 인스턴스를 중지합니다.
13. `aws:changeInstanceState` - 제공된 인스턴스를 강제 중지합니다.
14. `aws:assertAwsResourceProperty`- CreatePre EC2RescueBackup 입력 값 확인
    a. (사전 EC2Rescue 백업 생성) - *가 true인 CreatePre EC2RescueBackup 경우*

   b. `aws:executeAwsApi`- 제공된 인스턴스의 AMI 백업 생성
   c. `aws:createTags`- AMI 백업에 태그 지정
15. `aws:runCommand`- EC2Rescue 헬퍼 인스턴스에 설치 EC2Rescue
16. `aws:executeAwsApi` - 제공된 인스턴스의 루트 볼륨을 분리합니다.
17. `aws:assertAwsResourceProperty` - 제공된 인스턴스 플랫폼을 확인합니다.
   a. (인스턴스가 Windows인 경우):

      `aws:executeAwsApi`- 루트 볼륨을 EC2Rescue 헬퍼 인스턴스에 *xvdf*로 연결

      `aws:sleep` - 10초 동안 대기 상태로 유지합니다.

      `aws:runCommand` - Powershell에서 제공된 오프라인 스크립트를 실행합니다.
   b. (인스턴스가 Linux인 경우):

      `aws:executeAwsApi`- 루트 볼륨을*/dev/sdf*로 헬퍼 인스턴스에 연결 EC2Rescue

      `aws:sleep` - 10초 동안 대기 상태로 유지합니다.

      `aws:runCommand` - Bash에서 제공된 오프라인 스크립트를 실행합니다.
18. `aws:changeInstanceState`- 헬퍼 인스턴스 중지 EC2Rescue
19. `aws:changeInstanceState`- EC2Rescue 헬퍼 인스턴스 강제 중지
20. `aws:executeAwsApi`- 헬퍼 인스턴스에서 루트 볼륨 분리 EC2Rescue
21. `aws:executeAwsApi` - 루트 볼륨을 제공된 인스턴스에 다시 연결합니다.
22. `aws:assertAwsResourceProperty`- 입력 값 CreatePost EC2RescueBackup 확인
   a. (사후 EC2Rescue 백업 생성) - *가 true인 CreatePost EC2RescueBackup 경우*
   b. `aws:executeAwsApi`- 제공된 인스턴스의 AMI 백업 생성
   c. `aws:createTags`- AMI 백업에 태그 지정
23. `aws:executeAwsApi` - 제공된 인스턴스의 루트 볼륨에 대해 초기 종료 시 삭제 상태를 복원합니다.
24. `aws:changeInstanceState` - 제공된 인스턴스의 초기 상태(running/stopped)를 복원합니다.
25. `aws:deleteStack`- EC2Rescue CloudFormation 스택 삭제

출력

runScriptFor리눅스. 아웃풋

runScriptFor윈도우. 출력

preScriptBackup.ImageId

postScriptBackup.ImageId

AWSPremiumSupport-TroubleshootEC2DiskUsage

설명

AWSPremiumSupport-TroubleshootEC2DiskUsage 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 루트 및 루트가 아닌 디스크 사용과 관련된 문제를 조사하고 잠재적으로 해결하는 데 도움이 됩니다. 가능한 경우, 실행서는 볼륨과 해당 파일 시스템을 확장하여 문제 해결을 시도합니다. 이러한 작업을 수행하기 위해, 이 실행서는 영향을 받는 인스턴스의 운영 체제를 기반으로 여러 실행서의 실행을 조정합니다.

첫 번째 실행서 AWSPremiumSupport-DiagnoseDiskUsageOnWindows 또는 AWSPremiumSupport-DiagnoseDiskUsageOnLinux는 볼륨을 확장하여 디스크 문제를 완화할 수 있는지 여부를 결정합니다.

두 번째 실행서 AWSPremiumSupport-ExtendVolumesOnWindows 또는 AWSPremiumSupport-ExtendVolumesOnLinux는 첫 번째 실행서의 출력을 사용하여 볼륨을 수정하는 Python 코드를 실행합니다. 볼륨이 수정되고 난 후, 실행서는 영향을 받는 볼륨의 파티션과 파일 시스템을 확장합니다.

> **Important**
>
> AWSPremiumSupport-* 실행서에 액세스하려면 Enterprise 또는 Business Support 구독이 필요합니다. 자세한 내용은 AWS Support 플랜 비교를 참조하세요.

이 문서는 AWS Managed Services(AMS)와 공동으로 작성되었습니다. AMS는 AWS 인프라를 보다 효율적이고 안전하게 관리하는 데 도움이 됩니다. 또한 AMS는 운영 유연성, 향상된 보안 및 규정 준수, 용량 최적화, 비용 절감 식별을 제공합니다. 자세한 내용은 AWS Managed Services 섹션을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, Windows

파라미터

- InstanceId

  유형: 문자열

  허용되는 값: ^i-[a-z0-9]{8,17}$

  설명: (필수) Amazon EC2 인스턴스의 ID입니다.
- VolumeExpansionEnabled

  유형: 부울

  설명: (선택 사항) 문서가 영향을 받는 볼륨 및 파티션을 확장할지 여부를 제어하는 플래그입니다.

  기본값: true
- VolumeExpansionUsageTrigger

  유형: 문자열

  설명: (선택 사항) 확장을 트리거하는 데 필요한 파티션 공간의 최소 사용량(백분율)입니다.

  허용되는 값: ^[0-9]{1,2}$

  기본값: 85
- VolumeExpansionCapSize

  유형: 문자열

  설명: (선택 사항) Amazon Elastic Block Store(Amazon EBS) 볼륨이 늘어나는 최대 크기(GiB)입니다.

  허용되는 값: ^[0-9]{1,4}$

  기본값: 2048

- VolumeExpansionGibIncrease

  유형: 문자열

  설명: (선택 사항) 볼륨의 GiB를 늘립니다. VolumeExpansionGibIncrease와 VolumeExpansionPercentageIncrease 사이의 가장 큰 순 증가분이 사용됩니다.

  허용되는 값: ^[0-9]{1,4}$

  기본값: 20
- VolumeExpansionPercentageIncrease

  유형: 문자열

  설명: (선택 사항) 볼륨의 비율을 늘립니다. VolumeExpansionGibIncrease와 VolumeExpansionPercentageIncrease 사이의 가장 큰 순 증가분이 사용됩니다.

  허용되는 값: ^[0-9]{1,2}$

  기본값: 20
- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

1. `aws:assertAwsResourceProperty` - 인스턴스가 Systems Manager에서 관리되는지 확인합니다.
2. `aws:executeAwsApi` - 플랫폼을 가져오는 인스턴스를 설명합니다.
3. `aws:branch` - 인스턴스의 플랫폼을 기반으로 자동화를 분기합니다.
   a. 인스턴스가 Windows인 경우:
      i. `aws:executeAutomation` - `AWSPremiumSupport-DiagnoseDiskUsageOnWindows` 실행서를 실행하여 인스턴스의 디스크 사용 문제를 진단합니다.
      ii. `aws:executeAwsApi` - 이전 자동화의 출력을 가져옵니다.
      iii. `aws:branch` - 진단 출력 및 경고를 완화하기 위해 확장할 수 있는 볼륨이 있는지 여부를 기반으로 분기합니다.
         A. 확장해야 할 볼륨이 없습니다. 자동화를 종료합니다.
         B. 확장해야 할 볼륨이 있습니다.
            I. `aws:executeAwsApi` - 인스턴스의 Amazon Machine Image(AMI)을 생성합니다.
            II. `aws:waitForAwsResourceProperty` - AMI 상태가 `available`이 될 때까지 기다립니다.
            III. `aws:executeAutomation` - `AWSPremiumSupport-ExtendVolumesOnWindows` 실행서를 실행하여 볼륨 수정 및 운영 체제(OS)에서 새 공간을 사용할 수 있도록 필요한 단계를 수행합니다.

b. (플랫폼은 Windows가 아님) 입력 인스턴스가 Windows가 아닌 경우:

   i. `aws:executeAutomation` - `AWSPremiumSupport-DiagnoseDiskUsageOnLinux` 실행서를 실행하여 인스턴스의 디스크 사용 문제를 진단합니다.

   ii. `aws:executeAwsApi` - 이전 자동화의 출력을 가져옵니다.

   iii. `aws:branch` - 진단 출력 및 경고를 완화하기 위해 확장할 수 있는 볼륨이 있는지 여부를 기반으로 분기합니다.

      A. 확장해야 할 볼륨이 없습니다. 자동화를 종료합니다.

      B. 확장해야 할 볼륨이 있습니다.

         I. `aws:executeAwsApi` - 인스턴스의 AMI를 만듭니다.

         II. `aws:waitForAwsResourceProperty` - AMI 상태가 `available`이 될 때까지 기다립니다.

         III. `aws:executeAutomation` - `AWSPremiumSupport-ExtendVolumesOnLinux` 실행서를 실행하여 볼륨 수정 및 OS에서 새 공간을 사용할 수 있도록 필요한 단계를 수행합니다.

출력

diagnoseDiskUsageAlertOnWindows.Output

extendVolumesOnWindows.Output

diagnoseDiskUsageAlertOnLinux.Output

extendVolumesOnLinux.Output

BackupAMILinux.ImageId

BackupAMIWindows.ImageId

AWSSupport-TroubleshootEC2InstanceConnect

설명

`AWSSupport-TroubleshootEC2InstanceConnect`자동화는 Amazon Instance Connect를 사용하여 Amazon Elastic Compute Cloud (AmazonEC2) 인스턴스로의 연결을 방해하는 오류를 분석하고 감지하는 데 도움이 됩니다. EC2 지원되지 않는 Amazon Machine Image (AMI), OS 수준 패키지 설치 또는 구성 누락, AWS Identity and Access Management (IAM) 권한 누락 또는 네트워크 구성 문제로 인해 발생하는 문제를 식별합니다.

어떻게 작동하나요?

이 런북에는 Amazon EC2 인스턴스 ID, 사용자 이름, 연결 모드, 소스 IPCIDR, SSH 포트, Amazon EC2 인스턴스 연결 관련 문제가 발생한 IAM 역할 또는 사용자의 Amazon 리소스 이름 (ARN) 이 포함됩니다. 그런 다음 Amazon Instance EC2 Connect를 사용하여 Amazon EC2 인스턴스에 연결하기 위한 사전 요구 사항을 확인합니다.

- 인스턴스가 실행 중이며 정상 상태입니다.
- 인스턴스는 Amazon EC2 Instance Connect에서 지원하는 AWS 지역에 있습니다.
- AMIAmazon 인스턴스 Connect는 EC2 해당 인스턴스를 지원합니다.
- 인스턴스는 인스턴스 메타데이터 서비스 (IMDSv2) 에 도달할 수 있습니다.
- Amazon EC2 Instance Connect 패키지가 OS 수준에서 제대로 설치 및 구성되어 있습니다.
- 네트워크 구성 (보안 그룹ACL, 네트워크 및 라우팅 테이블 규칙) 을 사용하면 Amazon Instance Connect를 통해 EC2 인스턴스에 연결할 수 있습니다.
- Amazon EC2 Instance Connect를 활용하는 데 사용되는 IAM 역할 또는 사용자는 Amazon 인스턴스의 푸시 키에 액세스할 수 있습니다. EC2

> **Important**
>
> - 인스턴스AMI, 연결 IMDSv2 가능성 및 Amazon Instance EC2 Connect 패키지 설치를 확인하려면 인스턴스를 관리해야 SSM 합니다. 그렇지 않으면 해당 단계를 건너뛰게 됩니다. 자세한 내용은 Amazon EC2 인스턴스가 관리형 노드로 표시되지 않는 이유를 참조하십시오.
> - 네트워크 검사는 입력 파라미터로 제공된 경우 보안 그룹 및 네트워크 ACL 규칙이 트래픽을 차단하는지 SourceIp CIDR 여부만 감지합니다. 그렇지 않으면 SSH 관련 규칙만 표시됩니다.
> - Amazon EC2 Instance Connect 엔드포인트를 사용하는 연결은 이 런북에서 검증되지 않았습니다.
> - 프라이빗 연결의 경우, 자동화는 클라이언트가 소스 시스템에 설치되어 있는지, 그리고 해당 SSH 클라이언트가 인스턴스의 프라이빗 IP 주소에 도달할 수 있는지 여부를 확인하지 않습니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ec2:DescribeInstances`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeInternetGateways`
- `iam:SimulatePrincipalPolicy`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommands`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`

지침

다음 단계에 따라 자동화를 구성합니다.

1. `AWSSupport-TroubleshootEC2InstanceConnect` AWS Systems Manager 콘솔에서 로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - InstanceId (필수):

     Amazon EC2 인스턴스 연결을 사용하여 연결할 수 없는 대상 Amazon EC2 인스턴스의 ID입니다.
   - AutomationAssumeRole (선택 사항):

Systems Manager 자동화가 사용자를 대신하여 작업을 수행할 수 있도록 하는 IAM 역할입니다. ARN 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.

- 사용자 이름 (필수):

  Amazon 인스턴스 연결을 사용하여 Amazon EC2 EC2 인스턴스에 연결하는 데 사용되는 사용자 이름입니다. 이 특정 사용자에게 IAM 액세스 권한이 부여되었는지 평가하는 데 사용됩니다.

- EC2InstanceConnectRoleOrUser(필수):

  Amazon EC2 Instance Connect를 활용하여 키를 인스턴스로 푸시하는 IAM 역할 또는 사용자의 이름입니다. ARN

- SSHPort(선택 사항):

  Amazon EC2 인스턴스에 구성된 SSH 포트입니다. 기본값은 22입니다. 포트 번호는 다음 사이여야 합니다1-65535.

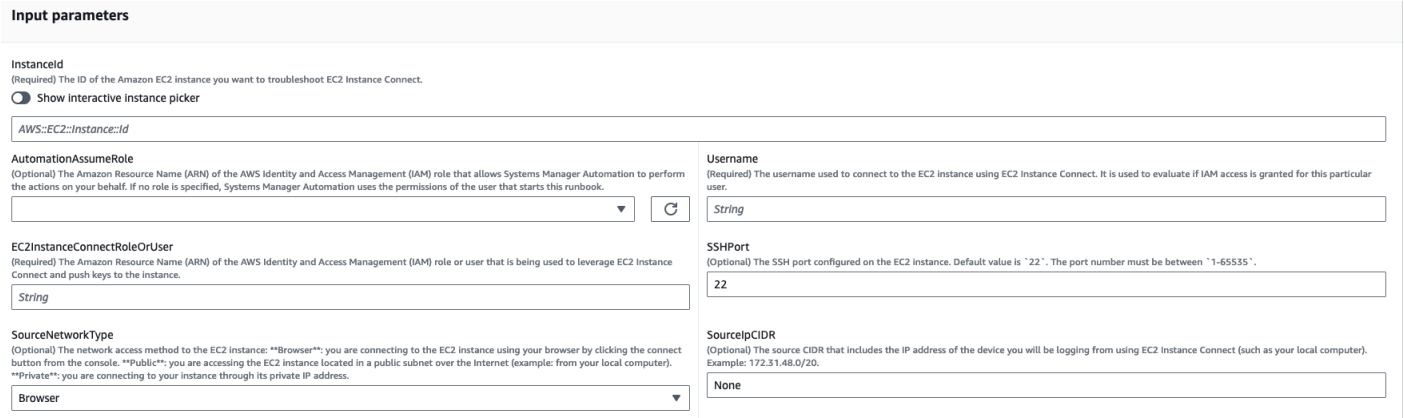
- SourceNetworkType (선택 사항):

  Amazon EC2 인스턴스에 대한 네트워크 액세스 방법:

  - 브라우저: AWS 관리 콘솔에서 연결합니다.
  - 퍼블릭: 인터넷을 통해 퍼블릭 서브넷에 있는 인스턴스 (예: 로컬 컴퓨터) 에 연결합니다.
  - 프라이빗: 인스턴스의 프라이빗 IP 주소를 통해 연결합니다.

- SourceIpCIDR(선택 사항):

  Amazon EC2 Instance Connect를 사용하여 로그인한 디바이스 (예: 로컬 컴퓨터) 의 IP 주소가 CIDR 포함된 소스입니다. 예: 172.31.48.6/32. 공개 또는 비공개 액세스 모드에서 값을 제공하지 않는 경우, Runbook은 Amazon EC2 인스턴스 보안 그룹 및 네트워크 ACL 규칙이 SSH 트래픽을 허용하는지 여부를 평가하지 않습니다. 대신 SSH 관련 규칙이 표시됩니다.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - AssertInitialState:

     Amazon EC2 인스턴스 상태가 실행 중인지 확인합니다. 그렇지 않으면, 자동화가 종료됩니다.
   - GetInstanceProperties:

     현재 Amazon EC2 인스턴스 속성 (PlatformDetails, PublicIpAddress VpcId, SubnetId 및 MetadataHttpEndpoint) 을 가져옵니다.
   - GatherInstanceInformationFromSSM:

     인스턴스가 관리되는 경우 Systems Manager 인스턴스의 핑 상태와 운영 체제 세부 정보를 가져옵니다. SSM
   - CheckIfAWSRegionSupported:

     Amazon 인스턴스가 Amazon EC2 EC2 인스턴스 연결 지원 AWS 지역에 있는지 확인합니다.
   - BranchOnIfAWSRegionSupported:

     Amazon EC2 Instance Connect에서 해당 AWS 지역을 지원하는 경우 실행을 계속합니다. 그렇지 않으면 출력을 생성하고 자동화를 종료합니다.
   - CheckIfInstanceAMIIsSupported:

     Amazon Instance Connect에서 해당 인스턴스와 AMI 연결된 EC2 인스턴스를 지원하는지 확인합니다.
   - BranchOnIfInstanceAMIIsSupported:

     AMI인스턴스가 지원되는 경우 메타데이터 도달 가능성, Amazon EC2 Instance Connect 패키지 설치 및 구성과 같은 OS 수준 검사를 수행합니다. 그렇지 않으면 를 사용하여 HTTP 메타데이터가 활성화되었는지 확인한 다음 AWS API 네트워크 검사 단계로 진행합니다.
   - C heckIMDSReachabilityFromOs:

     대상 Amazon EC2 Linux 인스턴스에서 Bash 스크립트를 실행하여 해당 인스턴스가 에 도달할 수 있는지 확인합니다. IMDSv2
   - C heckEICPackage 설치:

대상 Amazon EC2 Linux 인스턴스에서 Bash 스크립트를 실행하여 Amazon Instance Connect 패키지가 제대로 설치 및 구성되었는지 확인합니다. EC2

- C heckSSHConfigFromOs:

  대상 Amazon EC2 Linux 인스턴스에서 Bash 스크립트를 실행하여 구성된 SSH 포트가 입력 매개변수 SSHPort `와 일치하는지 확인합니다. `

- CheckMetadataHTTPEndpointIsEnabled:

  인스턴스 메타데이터 서비스 HTTP 엔드포인트가 활성화되었는지 확인합니다.

- C heckEICNetwork 액세스:

  네트워크 구성 (보안 그룹ACL, 네트워크 및 라우팅 테이블 규칙) 이 Amazon EC2 Instance Connect를 통한 인스턴스 연결을 허용하는지 확인합니다.

- C heckIAMRoleOrUserPermissions:

  Amazon EC2 Instance Connect를 활용하는 데 사용된 IAM 역할 또는 사용자가 제공된 사용자 이름을 사용하여 Amazon EC2 인스턴스의 푸시 키에 액세스할 수 있는지 확인합니다.

- MakeFinalOutput:

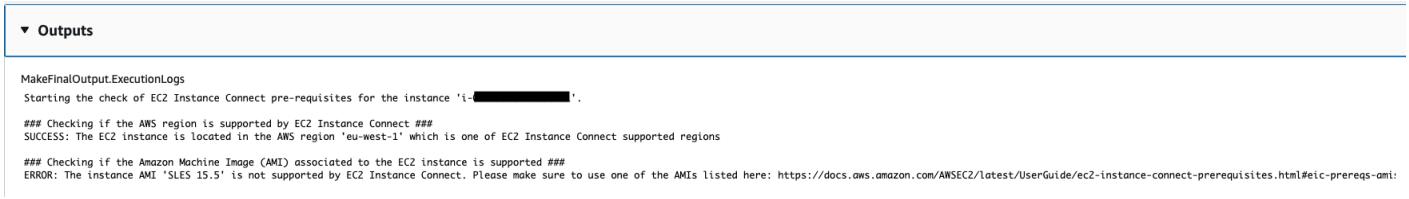
  이전 단계의 출력을 모두 통합합니다.

7. 완료 후 출력 섹션에서 실행의 세부 결과를 검토하십시오.

   대상 인스턴스에 필요한 모든 사전 요구 사항이 있는 경우 실행:

```
▼ Outputs

MakeFinalOutput.ExecutionLogs
Starting the check of EC2 Instance Connect pre-requisites for the instance 'i-[redacted]'.

### Checking if the AWS region is supported by EC2 Instance Connect ###
SUCCESS: The EC2 instance is located in the AWS region 'eu-west-1' which is one of EC2 Instance Connect supported regions

### Checking if the Amazon Machine Image (AMI) associated to the EC2 instance is supported ###
SUCCESS: The instance AMI 'Ubuntu 22.04' is supported by EC2 Instance Connect

### Checking if Instance Metadata service (IMDSv2) is reachable ###
SUCCESS: Instance metadata is reachable.


### Checking if EC2 Instance Connect package is installed and configured on the instance: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-set-up.html ###
SUCCESS: 'ec2-instance-connect' package is installed
SUCCESS: 'ec2-instance-connect' is properly configured

### Checking SSH configuration at the OS-level ###
WARNING: If you configured a firewall in the EC2 instance make sure that it allows SSH traffic from the source ip CIDR
INFO: SSH is configured to listen on port 22.
SUCCESS: The configured SSH port (22) matches the provided input port (22).


### Checking Network configuration requirements to access the instance through EC2 Instance Connect using 'Browser' access mode and port '22' ###
SUCCESS: The instance has a public IPv4 address.
SUCCESS: Subnet subnet [redacted] is public.
SUCCESS: SSH access is allowed by security group id 'sg-[redacted]'
SUCCESS: 'Inbound' NACL allows connection through EC2 instance connect. using the rule: '100'
SUCCESS: 'Outbound' NACL allows connection through EC2 instance connect. using the rule: '100'
SUCCESS: Network requirements to connect to the instance 'i-[redacted]' using EC2 instance connect are satisfied

### Checking if the required permissions are granted to the IAM identity 'arn:aws:iam:[redacted]:role/Admin' used to connect to the instance 'i-[redacted]' through EC2 Instance Connect with the username 'ubuntu' ###
SUCCESS: The IAM identity 'arn:aws:iam::[redacted]role/Admin' includes the 'ec2:DescribeInstances' access permission
SUCCESS: The IAM identity 'arn:aws:iam::[redacted]role/Admin' includes the 'ec2:SendSSHPublicKey' access permission
```

   대상 인스턴스가 AMI 지원되지 않는 경우 실행:



참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 설명서

- Amazon 인스턴스 연결을 사용하여 Amazon EC2 EC2 인스턴스에 연결할 때 발생하는 문제를 해결하려면 어떻게 해야 합니까?

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

설명

`AWSSupport-TroubleshootLinuxMGNDRSAgentLogs`자동화 런북은 Linux 서버에 AWS Application Migration Service (AWS MGN) 및 AWS Elastic Disaster Recovery (AWS DRS) 복제 에이전트를 설치하여 원본 서버를 AWS 클라우드로 마이그레이션할 때 흔히 발생하는 오류를 탐지하는 데 사용됩니다.

어떻게 작동하나요?

`AWSSupport-TroubleshootLinuxMGNDRSAgentLogs`런북은 AWS DRS 또는 설치 `aws_replication_agent_installer.log` 로그가 파라미터로 업로드되는 AWS MGN Amazon Simple Storage 서비스 (Amazon S3) 경로를 사용합니다. 그런 다음 다음 작업을 수행합니다.

- 검증: 제공된 로그 파일이 유효하고 이 파일에 하나 이상의 에이전트 설치가 포함되어 있는지 확인합니다.
- 구문 분석: 로그 파일에 있는 최신 에이전트 설치를 철저하게 분석하여 알려진 AWS MGN 오류나 AWS DRS 오류가 있는지 확인합니다.

- 오류 감지 및 해결: 구문 분석을 기반으로 에이전트 설치 프로세스 중에 발생하는 모든 오류나 문제를 감지하고 나열합니다. 발견된 각 오류에 대해 런북은 문제를 해결하거나 완화하는 데 도움이 되는 세부 단계를 제공합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `s3:GetObject`
- `s3:ListBucket`

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems `AWSSupport-TroubleshootLinuxMGNDRSAgentLogs`Manager의 문서 아래로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 () ARN 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.

- BucketName (필수):

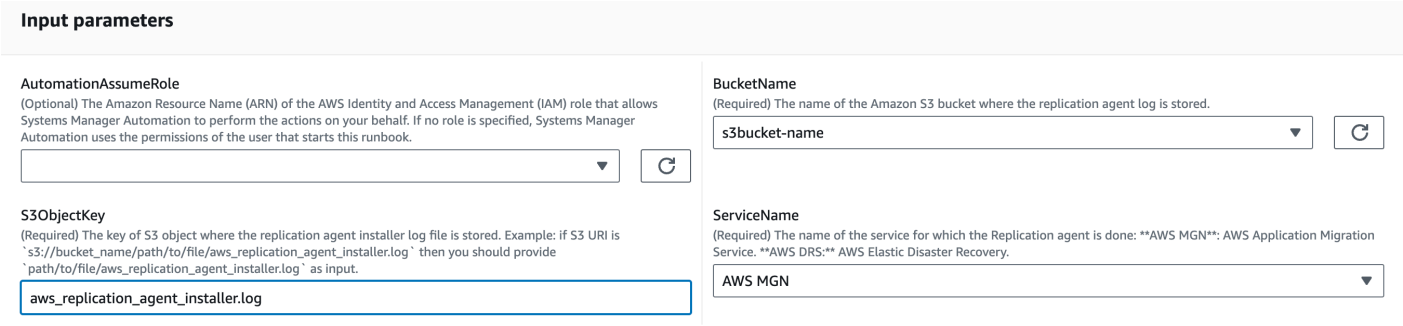
  복제 에이전트 로그가 저장되는 Amazon S3 버킷의 이름.

- S3 ObjectKey (필수):

  복제 에이전트 설치 관리자 로그 파일이 저장되는 Amazon S3 객체의 키입니다. 예: Amazon URI `s3://bucket_name/path/to/file/aws_replication_agent_installer.log` S3인 경우 다음을 입력해야 `path/to/file/aws_replication_agent_installer.log` 합니다.

- ServiceName (필수):

  복제 에이전트가 설치된 서비스의 이름. 허용되는 값: `AWS MGN` 또는 `AWS DRS`



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.

   - **`ValidateInput`**

     제공된 Amazon S3 버킷 이름과 객체 경로를 사용하여 복제 에이전트 로그 파일이 유효하고 액세스할 수 있는지 확인한 다음 최신 에이전트 설치의 바이트 번호를 반환합니다.

   - **`CheckReplicationAgentLogErrors`**

     최신 설치 바이트부터 시작하여 복제 에이전트 로그 파일을 읽고 알려진 AWS MGN 오류나 AWS DRS 오류를 검색합니다.

   - **`MakeFinalOutput`**

     발견된 오류에 대한 정보와 문제 해결 권장 사항을 포함하여 이전 검사의 출력을 생성합니다.

7. 완료 후 출력 섹션에서 실행의 세부 결과를 검토하십시오.

▼ **Outputs**

```
MakeFinalOutput.Output
### Input Validation Step ###

✅ The replication agent log file is valid and accessible using the provided S3 path.

### Log file error checking results ###

❌ Detected error: Kernel development package for [redacted] are missing from repositories

✅ Recommendations and troubleshooting steps:

During agent installation, the installer downloads a matching "kernel-devel/linux-headers" package from the repository configured in your Linux operating system.
This error occurs when the agent installation workflow can't install the matching "kernel-devel/linux-headers" package to the Linux OS current running kernel.

1. Check the current kernel version on the source server:

    $ sudo uname -r

2. Make sure to install the version that corresponds exactly to the current kernel version that you are running (displayed in the output of "sudo uname -r" command).

Use the following commands to install "kernel-devel/linux-headers" package for the running kernel:

    + For all Red Hat and CentOS source servers:

        $ sudo yum install kernel-devel-`uname -r`

    + For all Ubuntu/Debian source servers:

        $ sudo apt-get install linux-headers-`uname -r`

    + For all SUSE source servers:

        $ sudo zypper install kernel-default-devel-`uname -r`

Note: When the "kernel-devel/linux-headers" packages are installed for both the running kernel and other installed kernels, you will find the following directories generated for each installed kernel.
They are located under "/usr/src/kernels" for all Red Hat-based operating systems and under "/usr/src" for Ubuntu and Debian-based operating systems:

    $ sudo ls -la /usr/src/kernels

    $ sudo ls -la /usr/src

3. Sometimes, you will find that the "kernel-devel/linux-headers" package for the running kernel is not available in your server repositories.
In that case, you have three options:
```

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWSSupport-TroubleshootRDP

설명

사용자는 AWSSupport-TroubleshootRDP 실행서를 사용하여 RDP 포트, 네트워크 계층 인증(NLA), Windows 방화벽 프로파일 등 원격 데스크톱 프로토콜(RDP) 연결에 영향을 미치는 대상 인스턴스의 일반 설정을 확인하거나 수정할 수 있습니다. 또는, 사용자에게 오프라인 수정이 명시적으로 허용되는 경우 인스턴스를 중지했다가 시작하여 변경 내용을 오프라인으로 적용할 수 있습니다. 기본적으로, 이 실행서는 설정 값을 읽고 출력합니다.

> **Important**
>
> 이 실행서를 사용하기 전에 RDP 설정, RDP 서비스 및 Windows 방화벽 프로파일에 대한 변경 내용을 신중히 검토해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

- 작업

  유형: 문자열

  유효한 값: CheckAll | FixAll | Custom

  기본값: Custom

  설명: (선택 사항) [Custom] Firewall, RDPServiceStartupType, RDPServiceAction, RDPPortAction, NLASettingAction 및 RemoteConnections의 값을 사용하여 설정을 관리합니다. [CheckAll] 설정 값을 변경하지 않은 상태로 해당 내용을 읽습니다. [FixAll] RDP 기본 설정을 복원하고, Windows 방화벽을 비활성화합니다.

- AllowOffline

  유형: 문자열

  유효한 값: true | false

  기본값: false

설명: (선택 사항) Fix only - 온라인 문제 해결에 실패하거나 제공된 인스턴스가 관리형 인스턴스가 아닌 경우 오프라인으로 RDP를 수정할 수 있도록 하려면 true로 설정합니다. 참고: 오프라인 수정의 경우, SSM Systems Manager Automation은 해당 인스턴스를 중지하고, 작업을 시도하기 전에 AMI를 생성합니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 방화벽

  유형: 문자열

  유효한 값: Check | Disable

  기본값: Check

  설명: (선택 사항) Windows 방화벽(모든 프로파일)을 확인하거나 비활성화합니다.

- InstanceId

  유형: 문자열

  설명: (필수) RDP 설정 문제를 해결할 인스턴스의 ID입니다.

- NLASettingAction

  유형: 문자열

  유효한 값: Check | Disable

  기본값: Check

  설명: (선택 사항) 네트워크 계층 인증(NLA)를 확인하거나 비활성화합니다.

- RDPPortAction

  유형: 문자열

유효한 값: Check | Modify

기본값: Check

설명: (선택 사항) RDP 연결에 사용되는 현재 포트를 확인하거나, RDP 포트를 3389로 다시 수정하고 서비스를 다시 시작합니다.

- RDPServiceAction

  유형: 문자열

  유효한 값: Check | Start | Restart | Force-Restart

  기본값: Check

  설명: (선택 사항) RDP 서비스(TermService)를 확인, 시작, 다시 시작 또는 강제로 다시 시작합니다.

- RDPServiceStartupType

  유형: 문자열

  유효한 값: Check | Auto

  기본값: Check

  설명: (선택 사항) RDP 서비스를 확인하거나 Windows 부팅 시 자동으로 시작하도록 설정합니다.

- RemoteConnections

  유형: 문자열

  유효한 값: Check | Enable

  기본값: Check

  설명: (선택 사항) fDenyTSConnections 설정에 대해 수행할 작업(Check, Enable)입니다.

- S3BucketName

  유형: 문자열

  설명: (선택 사항) 오프라인에만 해당 - 문제 해결 로그를 업로드할 계정의 S3 버킷 이름입니다. 버킷 정책에서 수집된 로그에 액세스할 필요가 없는 당사자에 대해 불필요한 읽기/쓰기 권한을 부여하지 않도록 해야 합니다.

- SubnetId

  유형: 문자열

  기본값: SelectedInstanceSubnet

  설명: (선택 사항) 오프라인 전용 - 오프라인 문제 해결을 수행하는 데 사용하는 EC2Rescue 인스턴스용 서브넷 ID. 서브넷 ID를 지정하지 않으면 AWS Systems Manager Automation에서 새 VPC를 생성합니다. 중요: 서브넷이 InstanceId와 동일한 가용 영역이어야 하며 SSM 엔드포인트와의 통신을 허용해야 합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

이 명령을 수신하는 EC2 인스턴스에 AmazonSSMManagedInstanceCore Amazon 관리형 정책이 연결된 IAM 역할을 지정하는 것이 좋습니다. 온라인 수정의 경우, 자동화를 실행하고 인스턴스로 명령을 전송하려면 사용자에게 적어도 ssm:DescribeInstanceInformation, ssm:StartAutomationExecution 및 ssm:SendCommand가 있어야 하며, 자동화 출력을 읽을 수 있으려면 ssm:GetAutomationExecution도 있어야 합니다. 오프라인 수정의 경우, 자동화 출력을 읽을 수 있으려면 사용자에게 적어도 ssm:DescribeInstanceInformation, ssm:StartAutomationExecution, ec2:DescribeInstances 및 ssm:GetAutomationExecution이 있어야 합니다. `AWSSupport-TroubleshootRDP`는 `AWSSupport-ExecuteEC2Rescue`을 호출하여 오프라인 수정을 수행합니다 - `AWSSupport-ExecuteEC2Rescue`에 대한 권한을 검토하여 자동화를 성공적으로 실행할 수 있는지 확인하세요.

문서 단계

1. `aws:assertAwsResourceProperty` - 인스턴스가 Windows Server 인스턴스인지 확인합니다.
2. `aws:assertAwsResourceProperty` - 인스턴스가 관리형 인스턴스인지 확인합니다.
3. (온라인 문제 해결) 인스턴스가 관리형 인스턴스인 경우:
   a. `aws:assertAwsResourceProperty` - 제공된 Action 값을 확인합니다.
   b. (온라인 확인) Action = CheckAll인 경우:

      `aws:runPowerShellScript` - Windows 방화벽 프로파일 상태를 가져오는 PowerShell 스크립트를 실행합니다.

      `aws:executeAutomation` - RDP 서비스 상태를 가져오는 `AWSSupport-ManageWindowsService`를 호출합니다.

`aws:executeAutomation` - RDP 설정을 가져오는 `AWSSupport-ManageRDPSettings`를 호출합니다.

c. (온라인 수정) Action = FixAll인 경우:

`aws:runPowerShellScript` - 모든 Windows 방화벽 프로파일을 비활성화하는 PowerShell 스크립트를 실행합니다.

`aws:executeAutomation`- RDP 서비스를 시작하는 `AWSSupport-ManageWindowsService`를 호출합니다.

`aws:executeAutomation` - 원격 연결을 활성화하고 NLA를 비활성화하는 `AWSSupport-ManageRDPSettings`를 호출합니다.

d. (온라인 관리) Action = Custom인 경우:

`aws:runPowerShellScript` - Windows 방화벽 프로파일을 관리하는 PowerShell 스크립트를 실행합니다.

`aws:executeAutomation` - RDP 서비스를 관리하는 `AWSSupport-ManageWindowsService`를 호출합니다.

`aws:executeAutomation` - RDP 설정을 관리하는 `AWSSupport-ManageRDPSettings`를 호출합니다.

4. (오프라인 수정) 인스턴스가 관리형 인스턴스가 아닌 경우:

a. `aws:assertAwsResourceProperty` – AllowOffline = true를 단정합니다

b. `aws:assertAwsResourceProperty` - Action = FixAll를 단정합니다.

c. `aws:assertAwsResourceProperty` - SubnetId의 값을 단정합니다.

(제공된 인스턴스의 서브넷 사용) SubnetId가 SELECTED_INSTANCE_SUBNET인 경우

`aws:executeAwsApi` - 현재 인스턴스의 서브넷을 검색합니다.

`aws:executeAutomation` - 제공된 인스턴스의 서브넷을 사용하여 `AWSSupport-ExecuteEC2Rescue`를 실행합니다.

d. (제공된 사용자 지정 서브넷 사용) SubnetId가 SELECTED_INSTANCE_SUBNET이 아닌 경우

`aws:executeAutomation` - 제공된 SubnetId 값을 사용하여 `AWSSupport-ExecuteEC2Rescue`를 실행합니다.

출력

manageFirewallProfiles.Output

manageRDPServiceSettings.Output

manageRDPSettings.Output

checkFirewallProfiles.Output

checkRDPServiceSettings.Output

checkRDPSettings.Output

disableFirewallProfiles.Output

restoreDefaultRDPServiceSettings.Output

restoreDefaultRDPSettings.Output

troubleshootRDPOffline.Output

troubleshootRDPOfflineWithSubnetId.Output

AWSSupport-TroubleshootSSH

설명

AWSSupport-TroubleshootSSH 실행서는 Linux용 Amazon EC2Rescue 도구를 설치한 다음, EC2Rescue 도구를 사용하여 SSH를 통한 Linux 시스템에 대한 원격 연결을 방해하는 일반적인 문제를 확인하거나 수정하려고 합니다. 또는, 사용자에게 오프라인 수정이 명시적으로 허용되는 경우 인스턴스를 중지했다가 시작하여 변경 내용을 오프라인으로 적용할 수 있습니다. 기본적으로, 이 실행서는 읽기 전용 모드로 작동합니다.

이 자동화 실행(콘솔)

AWSSupport-TroubleshootSSH 실행서 사용에 대한 자세한 내용은 AWS Premium Support의 이 AWSSupport-TroubleshootSSH문제 해결 주제를 참조하세요.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

- 작업

  유형: 문자열

  유효한 값: CheckAll | FixAll

  기본값: CheckAll

  설명: (필수) 문제를 수정 없이 문제가 있는지 여부만 확인할지 아니면 검색된 문제를 확인하고 자동으로 수정할지 여부를 지정합니다.

- AllowOffline

  유형: 문자열

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) Fix only - 온라인 문제 해결에 실패하거나 제공된 인스턴스가 관리형 인스턴스가 아닌 경우 오프라인으로 SSH를 수정할 수 있도록 하려면 true로 설정합니다. 참고: 오프라인 수정의 경우, SSM Systems Manager Automation은 해당 인스턴스를 중지하고, 작업을 시도하기 전에 AMI를 생성합니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  유형: 문자열

설명: (필수) Linux용 EC2 인스턴스의 ID입니다.

- S3BucketName

  유형: 문자열

  설명: (선택 사항) 오프라인에만 해당 - 문제 해결 로그를 업로드할 계정의 S3 버킷 이름입니다. 버킷 정책에서 수집된 로그에 액세스할 필요가 없는 당사자에 대해 불필요한 읽기/쓰기 권한을 부여하지 않도록 해야 합니다.

- SubnetId

  유형: 문자열

  기본값: SelectedInstanceSubnet

  설명: (선택 사항) 오프라인 전용 - 오프라인 문제 해결을 수행하는 데 사용하는 EC2Rescue 인스턴스용 서브넷 ID. 서브넷 ID를 지정하지 않으면 AWS Systems Manager Automation에서 새 VPC를 생성합니다.

> **Important**
>
> 서브넷은 InstanceId와 동일한 가용 영역이어야 하며 SSM 엔드포인트와의 통신을 허용해야 합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

이 명령을 수신하는 EC2 인스턴스에 AmazonSSMManagedInstanceCore Amazon 관리형 정책이 연결된 IAM 역할을 지정하는 것이 좋습니다. 온라인 수정의 경우, 자동화를 실행하고 인스턴스로 명령을 전송하려면 사용자에게 적어도 ssm:DescribeInstanceInformation, ssm:StartAutomationExecution 및 ssm:SendCommand가 있어야 하며, 자동화 출력을 읽을 수 있으려면 ssm:GetAutomationExecution도 있어야 합니다. 오프라인 수정의 경우, 자동화 출력을 읽을 수 있으려면 사용자에게 적어도 ssm:DescribeInstanceInformation, ssm:StartAutomationExecution, ec2:DescribeInstances 및 ssm:GetAutomationExecution이 있어야 합니다. `AWSSupport-TroubleshootSSH`는 `AWSSupport-ExecuteEC2Rescue`을 호출하여 오프라인 수정을 수행합니다 - `AWSSupport-ExecuteEC2Rescue`에 대한 권한을 검토하여 자동화를 성공적으로 실행할 수 있는지 확인하세요.

문서 단계

1. `aws:assertAwsResourceProperty` - 인스턴스가 관리형 인스턴스인지 확인하세요.
   a. (온라인 수정) 인스턴스가 관리형 인스턴스가 아닌 경우:
      i. `aws:configurePackage` - `AWS-ConfigureAWSPackage`를 통해 Linux용 EC2Rescue를 설치합니다.
      ii. `aws:runCommand` - Linux용 EC2Rescue를 실행하는 Bash 스크립트를 실행합니다.
   b. (오프라인 수정) 인스턴스가 관리형 인스턴스가 아닌 경우:
      i. `aws:assertAwsResourceProperty` – AllowOffline = true를 단정합니다
      ii. `aws:assertAwsResourceProperty` - Action = FixAll를 단정합니다.
      iii. `aws:assertAwsResourceProperty` - SubnetId의 값을 단정합니다.
      iv. (제공된 인스턴스의 서브넷 사용) SubnetId가 SelectedInstanceSubnet이면 `aws:executeAutomation`을 통해 제공된 인스턴스의 서브넷을 사용하여 `AWSSupport-ExecuteEC2Rescue`를 실행합니다.
      v. (제공된 사용자 지정 서브넷 사용) SubnetId가 SelectedInstanceSubnet이 아니면 `aws:executeAutomation`을 통해 제공된 SubnetId 값을 사용하여 `AWSSupport-ExecuteEC2Rescue`를 실행합니다.

출력

troubleshootSSH.Output

troubleshootSSHOffline.Output

troubleshootSSHOfflineWithSubnetId.Output

AWSSupport-TroubleshootSUSERegistration

설명

`AWSSupport-TroubleshootSUSERegistration` 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) SUSE Linux Enterprise Server 인스턴스를 SUSE 업데이트 인프라에 등록하지 못한 이유를 식별하는 데 도움이 됩니다. 자동화 출력은 문제 해결 단계를 제공하거나 문제를 해결하는 데 도움이 됩니다. 인스턴스가 자동화 중에 모든 검사를 통과하면 인스턴스가 SUSE 업데이트 인프라에 등록됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) 문제를 해결하려는 Amazon EC2 인스턴스의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:DescribeInstanceProperties`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:SendCommand`
- `ssm:ListCommands`

문서 단계

- `aws:assertAwsResourceProperty` - Amazon EC2 인스턴스가 AWS Systems Manager에서 관리되는지 확인합니다.
- `aws:runCommand` - Amazon EC2 인스턴스 플랫폼이 SLES인지 확인합니다.
- `aws:runCommand` - 패키지 `cloud-regionsrv-client` 버전이 필수 버전 9.0.10 이상인지 확인합니다.
- `aws:runCommand` - 기본 제품의 심볼 연결이 끊어졌는지 확인하고, 연결이 끊어진 경우 해당 연결을 수정합니다.
- `aws:runCommand` - 호스트 파일(`/etc/hosts`)에 `smt-ec2-suscloud.net`에 대한 레코드가 있는지 확인합니다. 자동화가 모든 중복 항목을 제거합니다.
- `aws:runCommand` - `curl` 명령이 설치되었는지 확인합니다.
- `aws:runCommand` - Amazon EC2 인스턴스가 인스턴스 메타데이터 서비스(IMDS) 주소 169.254.169.254에 액세스할 수 있는지 확인합니다.
- `aws:runCommand` - Amazon EC2 인스턴스에 결제 코드 또는 AWS Marketplace 제품 코드가 있는지 확인합니다.
- `aws:runCommand` - Amazon EC2 인스턴스가 HTTPS를 통해 적어도 1개의 리전 서버에 도달할 수 있는지 확인합니다.
- `aws:runCommand` - Amazon EC2 인스턴스가 HTTP를 통해 구독 관리 도구(SMT) 서버에 도달할 수 있는지 확인합니다.
- `aws:runCommand` - Amazon EC2 인스턴스가 HTTPS를 통해 구독 관리 도구(SMT) 서버에 도달할 수 있는지 확인합니다.
- `aws:runCommand` - Amazon EC2 인스턴스가 HTTPS를 통해 `smt-ec2.susecloud.net` 주소에 도달할 수 있는지 확인합니다.
- `aws:runCommand` - Amazon EC2 인스턴스를 SUSE 업데이트 인프라를 통해 등록합니다.
- `aws:executeScript` - 이전 단계의 결과를 모두 수집하여 출력합니다.

AWSSupport-TroubleshootWindowsPerformance

설명

런북은 Amazon Elastic Compute Cloud EC2 (Amazon) Windows 인스턴스에서 진행 중인 성능 문제를 해결하는 `AWSSupport-TroubleshootWindowsPerformance` 데 도움이 됩니다. 런북은 대상 인스턴스의 로그를 캡처하고 메모리CPU, 디스크 및 네트워크 성능 지표를 분석합니다. 선택적으로 자동화를 통해 프로세스 덤프를 캡처하여 성능 저하의 잠재적 원인을 파악할 수 있습니다. 또한 이 런북에서

설치하도록 허용한 경우 자동화는 최신 EC2Rescue도구를 사용하여 이벤트 및 시스템 로그를 캡처합니다.

어떻게 작동하나요?

런북은 다음 단계를 수행합니다.

- Amazon EC2 인스턴스에서 사전 요구 사항을 확인합니다.
- Amazon EC2 Windows 인스턴스의 루트 디스크에 성능 로그를 생성합니다.
- 캡처한 로그를 폴더에 저장합니다. `C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance`
- Amazon Simple Storage Service (Amazon S3) 버킷이 제공되고 자동화 담당자 역할에 필요한 권한이 있는 경우 캡처된 로그는 Amazon S3 버킷에 업로드됩니다.
- 설치하기로 선택한 경우 Amazon EC2 Windows 인스턴스에 최신 `EC2Rescue` 도구를 설치하여 이벤트와 시스템 로그를 캡처하지만 에서 캡처한 프로세스 덤프와 로그는 분석하지 않습니다. `EC2Rescue`

Important

- 이 런북을 실행하려면 Amazon EC2 Windows 인스턴스를 에서 관리해야 합니다. AWS Systems Manager자세한 내용은 Amazon EC2 인스턴스가 관리형 노드로 표시되지 않는 이유를 참조하십시오.
- 이 런북을 실행하려면 Amazon EC2 Windows 인스턴스가 4.0 이상의 Windows 8.1/Windows Server 2012 R2 (6.3) 이상 버전에서 실행되고 있어야 합니다. PowerShell 자세한 내용은 Windows 운영 체제 버전을 참조하십시오.
- 성능 로그를 생성하려면 루트 디바이스에 최소 10GB의 여유 공간이 필요합니다. 루트 디스크가 100GB보다 큰 경우 사용 가능한 공간은 디스크 크기의 10% 이상이어야 합니다. 실행 중에 프로세스를 덤프하는 경우 여유 공간은 프로세스가 10GB 이상의 메모리를 사용할 때 프로세스에서 소비한 총 메모리 크기를 더한 10GB보다 커야 합니다.
- 루트 디바이스에서 생성된 로그는 자동으로 삭제되지 않습니다.
- 런북은 도구를 제거하지 않습니다. `EC2Rescue` 자세한 내용은 Windows EC2Rescue Server용 사용을 참조하십시오.

- 성능에 영향을 미치는 경우 이 자동화를 실행하는 것이 가장 좋습니다. AWS Systems Manager State Manager 연결을 사용하거나 AWS Systems Manager 유지 관리 기간을 예약하여 정기적으로 실행할 수도 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

Parameters

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

(선택 사항) 인스턴스 프로필 또는 인스턴스에 구성된 IAM 사용자에 연결된 IAM 역할을 사용하려면 파라미터에 지정된 Amazon S3 버킷에 로그를 업로드하려면 다음 작업이 필요합니다*LogUploadBucketName*.

- `s3:PutObject`
- `s3:GetObject`
- `s3:ListBucket`

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems `AWSSupport-TroubleshootWindowsPerformance`Manager의 문서 아래로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 () ARN 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - InstanceId (필수):

     자동화를 실행하려는 대상 Amazon EC2 Windows 인스턴스의 ID입니다. 자동화를 실행하려면 Systems Manager에서 인스턴스를 관리해야 합니다.
   - CaptureProcessDump (선택 사항):

     캡처할 프로세스 덤프 유형입니다. 자동화는 자동화 초기에 성능에 영향을 줄 수 있는 프로세스의 프로세스 덤프 하나를 캡처할 수 있습니다. 인스턴스 루트 볼륨에는 최소 10GB의 여유 공간이 필요합니다 (루트 볼륨 크기가 100GB보다 큰 경우 디스크 크기의 10% 초과, 프로세스가 10GB 이상의 메모리를 사용하는 경우 프로세스에서 소비한 총 메모리 크기 10GB를 더한 값).
   - LogCaptureDuration (선택 사항):

     문제가 발생하는 동안 이 자동화가 로그를 캡처하는 데 걸리는 시간 (1~분) 입니다. 15 기본값은 5입니다.

- LogUploadBucketName (선택 사항):

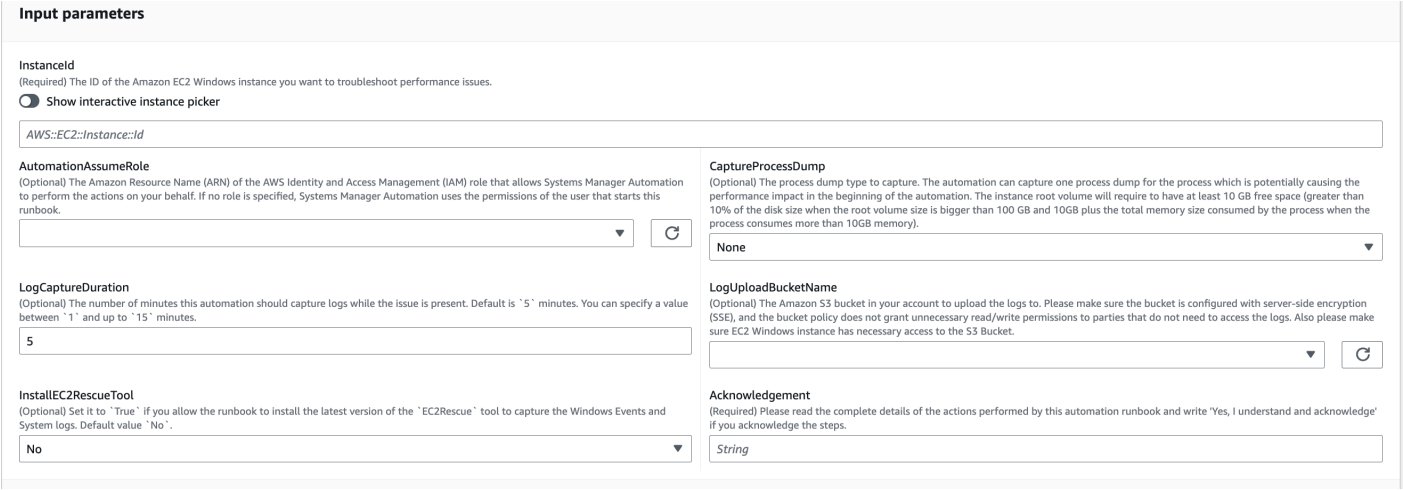
  로그를 업로드하려는 계정의 Amazon S3 버킷 버킷은 서버 측 암호화 (SSE) 로 구성되어야 하며, 버킷 정책은 캡처된 로그에 액세스할 필요가 없는 당사자에게 불필요한 읽기/쓰기 권한을 부여해서는 안 됩니다. 아마존 EC2 윈도우 인스턴스는 Amazon S3 버킷에 액세스할 수 있어야 합니다.

- 설치 EC2RescueTool (선택 사항):

  런북이 최신 버전의 `EC2Rescue` 도구를 설치하여 Windows 이벤트 및 시스템 로그를 캡처할 수 있도록 설정합니다. `Yes` 기본값은 `No`입니다.

- 승인 (필수):

  이 자동화 런북에서 수행한 작업의 전체 세부 정보를 읽고 동의하면 입력하십시오. `Yes, I understand and acknowledge`



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.

   - **`CheckConcurrency`:**

     인스턴스를 대상으로 하는 이 런북이 한 번만 실행되도록 합니다. Runbook에서 동일한 인스턴스를 대상으로 하는 다른 실행을 발견하면 오류가 반환되고 종료됩니다.

   - **`AssertInstanceIsWindows`:**

     Amazon EC2 인스턴스가 Windows 운영 체제에서 실행되고 있는지 확인합니다. 그렇지 않으면, 자동화가 종료됩니다.

   - **`AssertInstanceIsManagedInstance`:**

Amazon EC2 인스턴스를 에서 관리한다고 주장합니다. AWS Systems Manager그렇지 않으면 자동화가 종료됩니다.

- **`VerifyPrerequisites:`**

  인스턴스 OS의 PowerShell 버전을 확인하고 Systems Manager를 통해 인스턴스를 연결하여 PowerShell 명령을 실행할 수 있는지 확인합니다. 이 자동화는 Windows 8.1/서버 2012 R2 (6.3) 이상 버전에서 실행되는 PowerShell 4.0 이상을 지원합니다. 이전 버전인 경우 자동화가 실패합니다. Amazon S3 버킷에 로그를 업로드하도록 선택하면 이 자동화는 PowerShell 모듈용 AWS 도구가 사용 가능한지 확인합니다. 그렇지 않으면 자동화가 종료됩니다.

- **`BranchOnProcessDump:`**

  브랜치는 성능에 영향을 미치는 프로세스 덤프를 캡처하도록 설정했는지 여부에 따라 달라집니다.

- **`CaptureProcessDump:`**

  인스턴스에 이 자동화를 실행할 수 있는 충분한 공간이 있는지 확인합니다 ([CPUHiest/Memory]를 선택한 경우).

- **`CapturePerformanceLogs:`**

  디스크 공간을 다시 확인하고 인스턴스에서 PowerShell 스크립트를 실행하여 perfmon 카운터를 만들고 성능 모니터 및 Windows 성능 레코더 로깅을 시작합니다. 정의된 값이 충족되면 스크립트가 `LogCaptureDuration` 중지됩니다.

- **`SummarizePerformanceLogs:`**

  이전 단계에서 생성된 XML 보고서를 요약하여 가장 많은 WorkingSet 64 (메모리) 및% 프로세서 시간 (CPU) 을 소비하는 담당 프로세스를 찾아 자동화의 출력으로 표시합니다. `CapturePerformanceLogs` 네트워크 인터페이스, 메모리 LogicalDisk,, 의 사용에 대한 유사한 정보를 생성하여 `analysis_output.log` 출력 폴더에 저장합니다. TCPv4 IPv4 UDPv4

- **`BranchOnInstallEC2Rescue:`**

  Amazon EC2 인스턴스에 최신 `EC2Rescue` 도구를 설치하도록 설정하면 브랜치가 발생합니다.

- **`InstallEC2RescueTool:`**

  를 사용하여 `EC2Rescue` `AWS-ConfigureAWSPackage` 로그를 캡처할 `EC2Rescue` 도구를 인스턴스 OS에 설치합니다.

- **`RunEC2RescueTool:`**

인스턴스 OS에서 `EC2Rescue` 도구를 실행하여 필요한 모든 로그를 캡처합니다. `EC2Rescue`필요한 로그만 캡처하여 공간을 절약합니다.

- **`BranchOnIfS3BucketProvided:`**

  로그를 업로드하는 데 사용할 수 있는 버킷 이름이 있는지 확인하기 `LogUploadBucketName` 위해 사용자 입력을 기반으로 분기합니다.

- **`GetS3BucketPublicStatus:`**

  Amazon S3 버킷이 제공되는지 확인하고, 제공된다면 Amazon S3 버킷이 퍼블릭이 아니며 퍼블릭으로 SSE 구성되어 있는지 확인합니다.

- **`UploadLogResult:`**

  제공된 Amazon S3 버킷에 로그를 업로드합니다. PowerShell 버전이 5.0 이상이면 로그를 ZIP 아카이브로 압축하여 업로드합니다. 업로드가 완료되면 ZIP 파일이 삭제됩니다. PowerShell 버전이 5.0 미만인 경우 파일을 폴더에 직접 업로드합니다.

- **`CleanUpLogsOnFailure:`**

  실패 시 `CapturePerformanceLogs` 단계에서 생성된 모든 로그를 정리합니다. SSM에이전트가 제대로 작동하지 않거나 Windows 시스템이 응답하지 않는 경우 단계가 실패하거나 제한 시간이 초과될 수 있습니다. `CleanUpLogsOnFailure`

7. 완료 후 출력 섹션에서 실행의 세부 결과를 검토하십시오.

대상 인스턴스에 필요한 모든 사전 요구 사항이 있는 경우 실행.

Outputs

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

CapturePerformanceLogs.Output

```
The instance has enough space to capture performance logs.
WPR capture process is in 'Stopped' state.
Data Collector Set TroubleshootWindowsPerformance_[redacted] was not found.
Attempting to create Performance monitor Data Collector Set TroubleshootWindowsPerformance_[redacted].....
Data Collector Set TroubleshootWindowsPerformance_[redacted] created successfully.
Attempting to start Performance monitor Data Collector Set TroubleshootWindowsPerformance[redacted].....
Data Collector Set TroubleshootWindowsPerformance_[redacted] started successfully.
Current CPU usage is '54.73'% and Memory usage is '17.15'%
Not both CPU and Memory usage are over 95% at this moment hence continue to capture WPR log.
Starting Windows Performance Recording (WPR) capture process.
Stopping WPR capture process.
WPR capture process is in 'Stopped' state.
The Data Collector Set TroubleshootWindowsPerformance_[redacted] is currently generating logs.
The Data Collector Set TroubleshootWindowsPerformance_[redacted] has finished generating logs and is currently in 'Stopped' state.
Attempting to delete Data Collector Set TroubleshootWindowsPerformance_[redacted]
Data Collector Set TroubleshootWindowsPerformance_[redacted] deleted successfully.

[PASSED] Performance logs are captured successfully inside the folder: C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\[redacted]
The captured log files will not be deleted by this automation, please manually delete it after analysis.
```

RunEC2RescueTool.Output

[PASSED] EC2Rescue log collection is completed. Log saved in folder: 'C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance\[redacted]_EC2Rescue_23-05-48.zip'. The latest EC2Rescue tool is installed by this automation and please manually remove it if you don't need it. Its installed path is C:\Program Files\Amazon\EC2Rescue\EC2RescueCmd.exe.

SummarizePerformanceLogs.Output

```
Top 5 Processes which consumed most CPU in percentage as below. If you see a percentage higher than 100 that means the process is using more than one CPU core.
Process                 Counter         Min %           Max %           Avg %
sppsvc                  Processor       0.00            106.00          9.00
WmiPrvSE##2             Processor       0.00            90.00           2.00
MsMpEng                 Processor       0.00            38.00           0.75
GenValObj               Processor       0.00            30.00           0.28
svchost##42             Processor       0.00            29.00           0.17

Top 5 Processes which consumed most WorkingSet64 memory as below (in MB):
Process                 Counter         Min MB          Max MB          Avg MB
MsMpEng                 WorkingSet      220.00          260.00          236.00
Registry                WorkingSet      78.00           193.00          120.00
powershell              WorkingSet      90.00           92.00           92.00
LogonUI                 WorkingSet      43.00           43.00           43.00
dwm                     WorkingSet      38.00           38.00           38.00
```

대상 인스턴스가 Linux 플랫폼에 있고 실행이 실패한 경우 실행 단계 ID를 선택하면 실패 세부 정보를 볼 수 있습니다.

Outputs

CapturePerformanceLogs.Output

No output available yet because the step is not successfully executed

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

RunEC2RescueTool.Output

No output available yet because the step is not successfully executed

SummarizePerformanceLogs.Output

No output available yet because the step is not successfully executed

UploadLogResult.Output

No output available yet because the step is not successfully executed

VerifyPrerequisites.Output

No output available yet because the step is not successfully executed

Execution status

Overall status	All executed steps	# Succeeded
Failed	2	1
# Failed	**# Cancelled**	**# TimedOut**
1	0	0

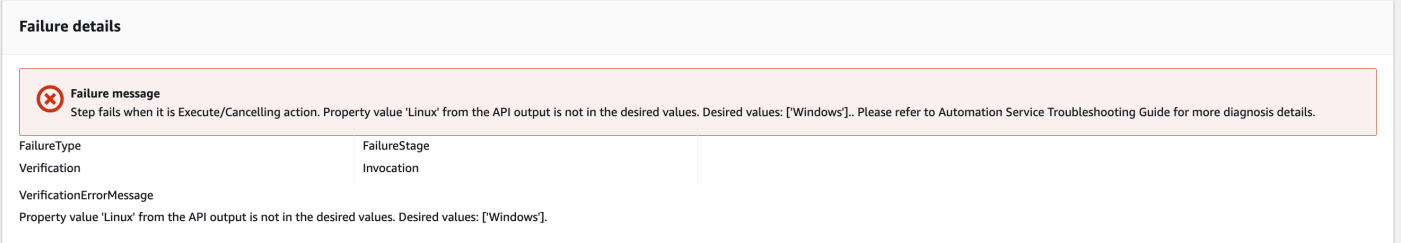
Executed steps (2)

Find Steps

1

Step ID	Step #	Step name	Action	Status	Start time	End time
[redacted]	1	CheckConcurrency	aws:executeScript	Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT
[redacted]0a3a9	2	AssertInstanceIsWindows	aws:assertAwsResourceProperty	Failed	Tue, 19 Mar 2024 16:15:00 GMT	Tue, 19 Mar 2024 16:15:01 GMT

단계의 실패 세부 정보`AssertInstanceIsWindows`.



참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWSSupport-TroubleshootWindowsUpdate

설명

`AWSSupport-TroubleshootWindowsUpdate`런북은 Amazon Elastic Compute Cloud (Amazon EC2) Windows 인스턴스에 대한 Windows 업데이트에 실패할 수 있는 문제를 식별하는 데 사용됩니다.

어떻게 작동하나요?

런북은 다음 단계를 수행합니다.

- 대상 Amazon EC2 인스턴스가 에서 관리되는지 확인합니다. AWS Systems Manager
- Systems Manager 패치 작업에 AWS Systems Manager 에이전트 (SSM 에이전트) 및 Windows Server 버전이 지원되는지 확인합니다.
- Windows 업데이트에 권장되는 사용 가능한 디스크 공간과 재부팅이 보류 중인지 확인합니다. 일반적으로 재부팅 보류는 업데이트가 보류 중임을 나타내며 추가 업데이트를 수행하기 전에 재부팅해야 합니다.
- 운영 체제 수준에서 프록시 설정을 구성하여 연결 문제를 해결하는 데 도움이 될 수 있습니다.
- Amazon Simple Storage Service (Amazon S3) 엔드포인트 연결 테스트를 수행하고 API 작업을 `GetDeployablePatchSnapshotForInstance`호출하여 관리형 노드가 사용하는 패치 기준에 대한 현재 스냅샷을 검색합니다.

- 연결이 실패할 경우, `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 런북을 실행하여 Amazon S3 엔드포인트에 대한 인스턴스의 연결을 분석할 수 있는 옵션을 제공합니다.
- Windows 업데이트 구성을 검증하고 Windows 서버 업데이트 서비스 (WSUS) 를 테스트합니다 (해당하는 경우).

> **Important**
>
> - Active Directory 도메인 컨트롤러는 지원되지 않습니다.
> - 윈도우 서버 버전 2008 R2 또는 이전 버전은 지원되지 않습니다.
> - SSM 에이전트 1.2.371 또는 이전 버전은 지원되지 않습니다.
> - `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`런북은 소스와 서비스 엔드포인트 간의 네트워크 연결을 분석하는 `VPC Reachability Analyzer`데 사용합니다. 소스와 대상 간의 분석 실행당 요금이 부과됩니다. 자세한 내용은 Amazon VPC 요금을 참조하세요.
> - Systems Manager가 지원되는 일부 지역에서는 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 런북을 사용할 수 없습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

Parameters

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`

> **Note**
>
> 하위 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 런북을 실행하려면 이 문서에 나열된 권한을 추가하십시오.

지침

다음 단계에 따라 자동화를 구성합니다.

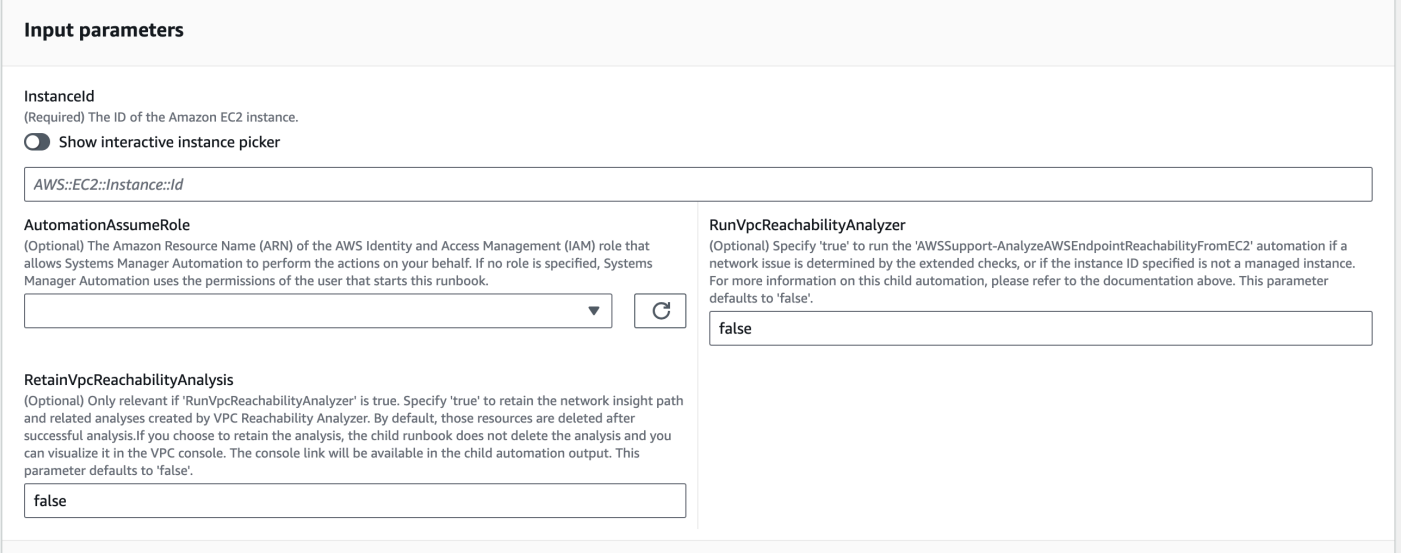
1. Systems `AWSSupport-TroubleshootWindowsUpdate`Manager의 문서 아래로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (ARN) 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - InstanceId (필수):

     윈도우 업데이트가 실패한 Amazon EC2 인스턴스의 ID를 입력합니다.
   - RunVpcReachabilityAnalyzer(선택 사항):

     확장 검사를 통해 네트워크 문제가 확인되거나 지정된 인스턴스 ID가 관리형 인스턴스가 아닌 경우 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 자동화를 `true` 실행하도록 지정합니다. 이 하위 자동화에 대한 자세한 내용은 설명서를 참조하십시오. 기본 값은 `false`입니다.
   - RetainVpcReachabilityAnalysis(선택 사항):

해당되는 경우에만 `RunVpcReachabilityAnalyzer` 해당됩니다`true`. 에서 생성한 `Reachability Analyzer` 네트워크 인사이트 경로 및 관련 분석을 `true` 보존하도록 지정하십시오. 기본적으로 이러한 리소스는 분석 성공 후 삭제됩니다. 분석을 보존하기로 선택한 경우 하위 런북은 분석을 삭제하지 않으므로 Amazon VPC 콘솔에서 분석을 시각화할 수 있습니다. 콘솔 링크는 하위 자동화 출력에서 사용할 수 있습니다. 디폴트 `false` 값입니다.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - **`getWindowsServerAndSSMAgentVersion:`**

     대상 인스턴스가 SSM 에이전트 AWS Systems Manager 버전과 Windows 버전에 의해 관리되는지 확인하고 SSM 에이전트 버전과 Windows 버전에 대한 세부 정보를 가져옵니다.
   - **`assertifInstanceIsSsmManaged:`**

     Amazon EC2 인스턴스가 AWS Systems Manager (SSM) 에 의해 관리되는지 확인합니다. 그렇지 않으면 자동화가 종료됩니다.
   - **`CheckProxy:`**

     Windows 인스턴스의 모든 프록시 유형을 확인합니다.
   - **`CheckPrerequisites:`**

     SSM 에이전트 버전과 Windows 버전을 가져와서 액티브 디렉터리 도메인 컨트롤러 (DC) 인지 확인합니다. 인스턴스가 DC이거나 SSM 에이전트 또는 Windows 버전이 지원되지 않는 경우 런북이 중지됩니다.

- **`CheckDiskSpace:`**

  Windows 인스턴스를 통해 사용 가능한 디스크 공간이 Windows 업데이트를 수행하기에 충분한 경우 이를 가져오고 유효성을 검사합니다.

- **`CheckPendingReboot:`**

  Windows 인스턴스에서 보류 중인 재부팅이 있는지 확인합니다.

- **`CheckS3Connectivity:`**

  인스턴스가 Amazon S3 엔드포인트에 `Patchbaseline` 도달할 수 있는지 확인합니다.

- **`branchOnRunVpcReachabilityAnalyzer:`**

  `RunVpcReachabilityAnalyzer`이 true인 경우 자동화를 분기하여 Amazon S3 연결 디버깅에 대한 심층 분석을 실행합니다.

- **`GenerateEndpoints:`**

  Amazon S3 엔드포인트에 대한 확장 연결 검사를 수행할 엔드포인트를 생성합니다.

- **`analyzeAwsEndpointReachabilityFromEC2:`**

  자동화 런북,`AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`. 을 호출하여 선택한 인스턴스가 필요한 엔드포인트에 도달할 수 있는지 확인합니다.

- **`CheckWindowsUpdateServices:`**

  Windows Update 서비스 상태 및 시작 유형을 확인합니다.

- **`CheckWindowsUpdateSettings:`**

  Windows 인스턴스에 구성된 Windows 업데이트 정책을 확인합니다.

- **`CheckWSUSSettings:`**

  Windows 업데이트가 WSUS 또는 Microsoft 업데이트 카탈로그로 구성되어 있는지 확인하고 연결을 확인합니다.

- **`CheckWUGlobalSettings:`**

  Windows 인스턴스에 구성된 Windows Update 글로벌 설정을 확인합니다.

- **`GenerateLogs:`**

  Windows Update 로그와 CBS 로그를 인스턴스 데스크톱에 다운로드하고 Windows 이벤트 로그에서 실패를 확인합니다.

- **FinalReport:**

  모든 단계에 대한 전체 보고서를 생성합니다.

7. 완료 후 출력 섹션에서 실행의 세부 결과를 검토하십시오.

```
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
"
```

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 관련 문서

- 자세한 내용은 TroubleShoot Windows 업데이트 문서를 참조하십시오.

AWSSupport-UpgradeWindowsAWSDrivers

설명

AWSSupport-UpgradeWindowsAWSDrivers 실행서는 지정된 EC2 인스턴스의 스토리지 및 네트워크 AWS 드라이버를 업그레이드 또는 복구합니다. 실행서는 SSM Agent를 호출하여 온라인으로 AWS 드라이버의 최신 버전 설치를 시도합니다. SSM Agent에 접촉할 수 없다면 실행서는 명시적으로 요청된 경우 AWS 드라이버의 오프라인 설치를 수행할 수 있습니다.

> **Note**
>
> 온라인 및 오프라인 업그레이드 둘 다 작업을 시도하기 전에 AMI를 생성하며, 이 업그레이드 작업은 자동화가 완료된 후에 계속됩니다. AMI에 대한 액세스를 보호하거나 AMI를 삭제하는 일은 고객의 책임입니다. 온라인 방법에서는 업그레이드 프로세스의 일부로서 인스턴스를 다시 시작하는 반면, 오프라인 방법에서는 제공된 EC2 인스턴스를 중지했다가 시작해야 합니다.

> **Important**
>
> 인스턴스가 VPC 엔드포인트를 사용하여 AWS Systems Manager에 연결하는 경우, us-east-1 리전에서 사용하는 경우를 제외하고 이 실행서는 실패합니다. 이 실행서는 도메인 컨트롤러에서도 실패합니다. 도메인 컨트롤러에서 AWS PV 드라이버를 업데이트하려면 도메인 컨트롤러 업그레이드(AWS PV 업그레이드)를 참조하십시오.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AllowOffline

  유형: 문자열

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) 온라인 설치를 수행할 수 없을 때 오프라인 드라이버 업그레이드를 허용하는 경우 true로 설정합니다. 참고: 오프라인 방법을 사용하려면 제공된 EC2 인스턴스를 중지했다가 다시 시작해야 합니다. 인스턴스 스토어 볼륨에 저장되어 있는 데이터가 손실됩니다. 탄력적 IP를 사용하지 않는 경우 퍼블릭 IP 주소가 변경됩니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ForceUpgrade

  유형: 문자열

  유효한 값: true | false

  기본값: false

설명: (선택 사항) 오프라인에만 해당 - 인스턴스에 이미 최신 드라이버가 설치되었어도 오프라인 드라이버 업그레이드를 계속 진행할 수 있도록 하려면 true로 설정합니다.

- InstanceId

  유형: 문자열

  설명: (필수) Windows Server용 EC2 인스턴스의 ID입니다.

- SubnetId

  유형: 문자열

  기본값: SelectedInstanceSubnet

  설명: (선택 사항) 오프라인에만 해당 - 오프라인 드라이버 업그레이드를 수행하는 데 사용하는 EC2Rescue 인스턴스용 서브넷 ID. 서브넷 ID를 지정하지 않으면 Systems Manager Automation에서 새 VPC를 생성합니다.

> **Important**
>
> 서브넷은 동일한 가용 영역에 있어야 InstanceId 하며 SSM 엔드포인트에 대한 액세스를 허용해야 합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

명령을 수신하는 EC2 인스턴스는 최소한 ssm: StartAutomationExecution 및 ssm:가 자동화를 실행하고 인스턴스에 명령을 전송할 수 있는 권한과 자동화 출력을 읽을 수 있는 SendCommandssm: 에 대한 권한을 포함하는 IAM 역할을 가지고 있어야 합니다. GetAutomationExecution `AmazonSSMManagedInstanceCore` Amazon 관리형 정책을 IAM 역할에 연결하여 이러한 권한을 제공할 수 있습니다. 그러나 이러한 `AmazonSSMAutomationRole` 목적으로 자동화 IAM 역할을 사용하는 것이 좋습니다. 자세한 내용은 IAM을 사용하여 자동화를 위한 역할 구성을 참조하십시오.

오프라인 업그레이드를 수행하려는 경우 `AWSSupport-StartEC2RescueWorkflow`에 필요한 권한을 참조하십시오.

문서 단계

1. `aws:assertAwsResourceProperty` - 입력 인스턴스가 Windows인지 확인합니다.

2. `aws:assertAwsResourceProperty` - 입력 인스턴스가 관리형 인스턴스인지 확인합니다. 이 경우에 해당하면 온라인 업그레이드가 시작되며, 그렇지 않은 경우 오프라인 업그레이드가 평가됩니다.
   a. (온라인 업그레이드) 입력 인스턴스가 관리형 인스턴스인 경우:
      i. `aws:createImage` - AMI 백업을 생성합니다.
      ii. `aws:createTags` - AMI 백업에 태그를 지정합니다.
      iii. `aws:runCommand` - `AWS-ConfigureAWSPackage`를 통해 ENA 네트워크 드라이버를 설치합니다.
      iv. `aws:runCommand` - `AWS-ConfigureAWSPackage`를 통해 NVMe 드라이버를 설치합니다.
      v. `aws:runCommand` - `AWS-ConfigureAWSPackage`을 통해 AWS PV 드라이버를 설치합니다.
   b. (오프라인 업그레이드) 입력 인스턴스가 관리형 인스턴스가 아닌 경우:
      i. `aws:assertAwsResourceProperty` - AllowOffline 플래그가 `true`으로 설정되었는지 확인합니다. 이 경우에 해당하면 오프라인 업그레이드가 시작되며, 그렇지 않은 경우 자동화가 종료됩니다.
      ii. `aws:changeInstanceState` - 소스 인스턴스를 중지합니다.
      iii. `aws:changeInstanceState` - 소스 인스턴스를 강제 중지합니다.
      iv. `aws:createImage` - 소스 인스턴스의 AMI 백업을 생성합니다.
      v. `aws:createTags` - 소스 인스턴스의 AMI 백업에 태그를 지정합니다.
      vi. `aws:executeAwsApi` - 인스턴스의 ENA를 활성화합니다.
      vii. `aws:assertAwsResourceProperty`- 플래그를 설정하세요. ForceUpgrade
      viii. 강제 오프라인 업그레이드) ForceUpgrade =true인 경우 드라이버 강제 업그레이드 `AWSSupport-StartEC2RescueWorkflow` 스크립트와 함께 `aws:executeAutomation` 실행하여 호출합니다. 그러면 설치된 현재 버전과 관계 없이 드라이버가 설치됩니다.
      ix. (오프라인 업그레이드) ForceUpgrade =false인 경우 드라이버 업그레이드 `AWSSupport-StartEC2RescueWorkflow` 스크립트와 함께 `aws:executeAutomation` 실행하여 호출합니다.

출력

preUpgradeBackup.ImageId

preOfflineUpgradeBackup. ImageId

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

upgradeDriversOffline. 출력

forceUpgradeDrivers오프라인. 출력

Amazon ECS

AWS Systems Manager 자동화는 Amazon Elastic Container Service에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-CollectECSInstanceLogs
- AWS-InstallAmazonECSAgent
- AWS-ECSRunTask
- AWSSupport-TroubleshootECSContainerInstance
- AWSSupport-TroubleshootECSTaskFailedToStart
- AWS-UpdateAmazonECSAgent

AWSSupport-CollectECSInstanceLogs

설명

`AWSSupport-CollectECSInstanceLogs` 런북은 Amazon Elastic Compute Cloud(AmazonECS) 인스턴스에서 운영 체제 및 Amazon Elastic Container Service(AmazonEC2) 관련 로그 파일을 수집하여 일반적인 Amazon ECS 문제를 해결하는 데 도움이 됩니다. 자동화가 관련 로그 파일을 수집하고 있는 동안, 변경내용이 파일 시스템에 적용됩니다. 이러한 변경내용에는 임시 디렉터리 및 로그 디렉터리 생성, 이러한 디렉터리에 대한 로그 파일 복사, 로그 파일을 아카이브로 압축하기 등이 포함됩니다.

`LogDestination` 파라미터에 대한 값을 지정하는 경우, 지정하는 Amazon Simple Storage Service(Amazon S3) 버킷의 정책 상태를 자동화에서 평가합니다. Amazon EC2 인스턴스에서 수집된 로그의 보안을 지원하기 위해 정책 상태가 `true` 로 설정되거나 액세스 제어 목록(ACL)`isPublic`이 `All Users` Amazon S3 사전 정의된 그룹에 `READ|WRITE` 권한을 부여하는 경우 로그가 업로드되지 않습니다. 또한, 제공된 버킷을 계정에서 사용할 수 없는 경우, 로그가 업로드되지 않습니다. Amazon

S3의 미리 정의된 그룹에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 Amazon S3의 미리 정의된 그룹을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ECSInstanceId

  유형: 문자열

  설명: (필수) 로그를 수집하려는 인스턴스의 ID입니다. 지정하는 인스턴스는 Systems Manager에서 관리해야 합니다.
- LogDestination

  유형: 문자열

  설명: (선택 사항) 보관된 로그를 업로드 AWS 계정 할 의 Amazon S3 버킷입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:SendCommand
- ssm:DescribeInstanceInformation

ECSInstanceId 파라미터에 지정한 Amazon EC2 인스턴스에 AmazonSSMManagedInstanceCore Amazon 관리형 정책이 연결된 IAM 역할이 있는 것이 좋습니다. LogDestination 파라미터에서 지정하는 Amazon S3 버킷에 로그 아카이브를 업로드하려면 다음 권한을 추가해야 합니다.

- s3:PutObject
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl

문서 단계

- assertInstanceIsManaged - ECSInstanceId 파라미터에서 지정하는 인스턴스가 Systems Manager에서 관리되는지 여부를 확인합니다.
- getInstancePlatform - ECSInstanceId 파라미터에서 지정된 인스턴스의 운영 체제(OS) 플랫폼에 대한 정보를 가져옵니다.
- verifyInstancePlatform - OS 플랫폼을 기반으로 자동화를 분기합니다.
- runLogCollectionScriptOnLinux - Linux 인스턴스에서 운영 체제 및 Amazon ECS 관련 로그 파일을 수집하고 /var/log/collectECSlogs 디렉터리에 아카이브 파일을 생성합니다.
- runLogCollectionScriptOnWindows - Windows 인스턴스에서 운영 체제 및 Amazon ECS 관련 로그 파일을 수집하고 C:\ProgramData\collectECSlogs 디렉터리에 아카이브 파일을 생성합니다.
- verifyIfS3BucketProvided - LogDestination 파라미터에 대해 값이 지정되었는지 여부를 확인합니다.
- runUploadScript - OS 플랫폼을 기반으로 자동화 단계를 분기합니다.
- runUploadScriptOnLinux - LogDestination 파라미터에서 지정된 Amazon S3 버킷에 로그 아카이브를 업로드하고 OS로부터 아카이브된 로그 파일을 삭제합니다.
- runUploadScriptOnWindows - LogDestination 파라미터에서 지정된 Amazon S3 버킷에 로그 아카이브를 업로드하고 OS로부터 아카이브된 로그 파일을 삭제합니다.

AWS-InstallAmazonECSAgent

설명

`AWS-InstallAmazonECSAgent` 실행서는 지정한 Amazon Elastic Compute Cloud(AmazonECS) 인스턴스에 Amazon Elastic Container Service(AmazonEC2) 에이전트를 설치합니다. 이 실행서는 Amazon Linux 및 Amazon Linux 2 인스턴스만 지원합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceIds

  유형: StringList

  설명: (필수) Amazon ECS 에이전트를 설치하려는 Amazon EC2 인스턴스IDs의 입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeInstances`

문서 단계

`aws:executeScript` - `InstanceIds` 파라미터에서 지정한 Amazon EC2 인스턴스에 Amazon ECS 에이전트를 설치합니다.

출력

InstallAmazonECSAgent.SuccessfulInstances - Amazon ECS 에이전트 설치에 성공한 인스턴스의 ID입니다.

InstallAmazonECSAgent.FailedInstances - Amazon ECS 에이전트 설치에 실패한 인스턴스의 ID입니다.

InstallAmazonECSAgent.InProgressInstances - Amazon ECS 에이전트 설치가 진행 중인 인스턴스의 ID입니다.

AWS-ECSRunTask

설명

`AWS-ECSRunTask` 런북은 지정한 Amazon Elastic Container Service(AmazonECS) 작업을 실행합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- capacityProviderStrategy

  유형: 문자열

  설명: (선택 사항) 작업에 사용할 용량 공급자 전략입니다.
- cluster

  유형: 문자열

  설명: (선택 사항) 작업을 실행할 클러스터ARN의 짧은 이름입니다. 클러스터를 지정하지 않으면 기본 클러스터가 사용됩니다.
- count

  유형: 문자열

  설명: (선택 사항) 클러스터에 배치할 지정된 작업의 인스턴스 수입니다. 각 요청에 대해 최대 10개의 작업을 지정할 수 있습니다.
- enableECSManaged태그

  타입: 부울

  설명: (선택 사항) 작업에 Amazon ECS 관리형 태그를 사용할지 여부를 지정합니다. 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 Amazon ECS 리소스 태그 지정을 참조하세요.
- enableExecuteCommand

  타입: 부울

  설명: (선택 사항) 이 태스크의 컨테이너에 대해 실행 명령 기능을 활성화할지 여부를 결정합니다. true인 경우 태스크의 모든 컨테이너에서 실행 명령 기능을 활성화합니다.
- 그룹

유형: 문자열

설명: (선택 사항) 태스크와 연결할 태스크 그룹의 이름입니다. 기본값은 작업 정의의 성입니다. 예: `family:my-family-name`.

- launchType

  유형: 문자열

  유효한 값: EC2 | FARGATE | EXTERNAL

  설명: (선택 사항) 독립 실행형 작업을 실행할 인프라입니다.

- networkConfiguration

  유형: 문자열

  설명: (선택 사항) 태스크의 네트워크 구성입니다. 이 파라미터는 `awsvpc` 네트워크 모드를 사용하여 자체 탄력적 네트워크 인터페이스를 수신하는 작업 정의에 필요하며 다른 네트워크 모드에서는 지원되지 않습니다.

- 재정의

  유형: 문자열

  설명: (선택 사항) 지정된 작업 정의에서 컨테이너 이름을 지정하는 JSON 형식의 컨테이너 재정의 목록과 수신해야 하는 재정의 목록입니다. 명령 재정의를 사용하여 작업 정의 또는 Docker 이미지에 지정된 컨테이너에 대한 기본 명령을 재정의할 수 있습니다. 컨테이너의 작업 정의 또는 Docker 이미지에 지정된 기존 환경 변수를 재정의할 수도 있습니다. 또한 환경 재정의를 사용하여 새 환경 변수를 추가할 수 있습니다.

- placementConstraints

  유형: 문자열

  설명: (선택 사항) 작업에 사용할 배치 제약 조건 객체의 배열입니다. 태스크 정의의 제약 조건과 런타임에 지정된 제약 조건을 포함하여 각 태스크에 최대 10개의 제약 조건을 지정할 수 있습니다.

- placementStrategy

  유형: 문자열

  설명: (선택 사항) 작업에 사용할 배치 전략 객체입니다. 각 작업에 대해 최대 5개의 전략 규칙을 지정할 수 있습니다.

- platformVersion

  유형: 문자열

  설명: (선택 사항) 태스크가 사용하는 플랫폼 버전입니다. 플랫폼 버전은 Fargate에서 호스팅되는 작업에 대해서만 지정됩니다. 플랫폼 버전을 지정하지 않으면 `LATEST` 플랫폼 버전이 사용됩니다.
- propagateTags

  유형: 문자열

  설명: (선택 사항) 태그가 태스크 정의에서 태스크로 전파되는지 여부를 결정합니다. 값을 지정하지 않으면 태그가 전파되지 않습니다. 태그는 태스크 생성 중에만 태스크로 전파될 수 있습니다.
- referenceId

  유형: 문자열

  설명: (선택 사항) 작업에 사용할 참조 ID입니다. 참조 ID의 최대 길이는 1,024자입니다.
- startedBy

  유형: 문자열

  설명: (선택 사항) 작업이 시작될 때 지정된 선택적 태그입니다. 이렇게 하면 `ListTasks` API 작업 결과를 필터링하여 특정 작업에 속하는 태스크를 식별할 수 있습니다. 최대 36개의 문자(대문자 및 소문자), 숫자, 하이픈(-) 및 밑줄(_)이 허용됩니다.
- tags

  유형: 문자열

  설명: (선택 사항) 태스크를 분류하고 구성하는 데 도움이 되도록 태스크에 적용할 메타데이터입니다. 각 태그는 사용자 정의 키와 값으로 구성됩니다.
- taskDefinition

  유형: 문자열

  설명: (선택 사항) 실행할 작업 정의ARN의 `family` 및 `revision` (`family:revision`) 또는 전체입니다. 개정이 지정되지 않은 경우 최신 `ACTIVE` 개정이 사용됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ecs:RunTask`

문서 단계

`aws:executeScript` - 실행서 입력 파라미터에 대해 지정한 값을 기반으로 Amazon ECS 작업을 실행합니다.

AWSSupport-TroubleshootECSContainerInstance

설명

`AWSSupport-TroubleshootECSContainerInstance` 실행서는 Amazon ECS 클러스터에 등록하지 못하는 Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스 문제를 해결하는 데 도움이 됩니다. 이 자동화는 인스턴스의 사용자 데이터에 올바른 클러스터 정보가 포함되어 있는지 여부, 인스턴스 프로파일에 필요한 권한이 포함되어 있는지 여부, 그리고 네트워크 구성 문제를 검토합니다.

> **Important**
>
> 이 자동화를 성공적으로 실행하려면 Amazon EC2 인스턴스의 상태가 `running` 이고 Amazon ECS 클러스터 상태가 `ACTIVE` 여야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ClusterName

  유형: 문자열

  설명: (필수) 인스턴스가 등록하지 못한 Amazon ECS 클러스터의 이름입니다.

- InstanceId

  유형: 문자열

  설명: (필수) 문제를 해결하려는 Amazon EC2 인스턴스의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

aws:executeScript: Amazon EC2 인스턴스가 Amazon ECS 클러스터에 등록하는 데 필요한 사전 요구 사항을 충족하는지 검토합니다.

AWSSupport-TroubleshootECSTaskFailedToStart

설명

`AWSSupport-TroubleshootECSTaskFailedToStart` 실행서는 Amazon ECS 클러스터의 Amazon Elastic Container Service(Amazon ECS) 작업이 시작되지 않은 이유를 해결하는 데 도움이 됩니다. 시작에 실패한 작업 AWS 리전 과 동일한 에서 이 런북을 실행해야 합니다. 실행서는 작업 시작을 방해할 수 있는 다음과 같은 일반적인 문제를 분석합니다.

- 구성된 컨테이너 레지스트리에 대한 네트워크 연결
- 작업 실행 역할에 필요한 IAM 권한 누락
- VPC 엔드포인트 연결
- 보안 그룹 규칙 구성
- AWS Secrets Manager 보안 암호 참조
- 로깅 구성

> **Note**
>
> 분석에 따라 네트워크 연결을 테스트해야 하는 것으로 결정되면 계정에 Lambda 함수와 필수 IAM 역할이 생성됩니다. 이러한 리소스는 실패한 작업의 네트워크 연결을 시뮬레이션하는 데 사용됩니다. 자동화를 통해 더 이상 필요하지 않은 리소스는 삭제됩니다. 하지만, 자동화로 리소스가 삭제되지 않는 경우 수동으로 삭제해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ClusterName

  유형: 문자열

  설명: (필수) 작업이 시작되지 않은 Amazon ECS 클러스터의 이름입니다.
- CloudwatchRetentionPeriod

  유형: 정수

  설명: (선택 사항) Lambda 함수 로그가 Amazon CloudWatch Logs에 저장되는 보존 기간입니다. 이는 분석 결과 네트워크 연결성을 테스트해야 한다고 판단되는 경우에만 필요합니다.

  유효한 값: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90

  기본값: 30
- TaskId

  유형: 문자열

  설명: (필수) 실패한 작업의 ID입니다. 가장 최근에 실패한 작업을 사용하십시오.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeScript` - 자동화를 시작한 사용자 또는 역할에 필요한 IAM 권한이 있는지 확인합니다. 이 실행서를 사용할 수 있는 충분한 권한이 없는 경우, 누락된 필수 권한이 자동화 출력에 포함됩니다.
- `aws:branch` - 실행서에 필요한 모든 작업에 대한 권한이 있는지 여부를 기반으로 분기합니다.
- `aws:executeScript` - 분석에서 네트워크 연결을 테스트해야 한다고 결정하는 VPC 경우 에 Lambda 함수를 생성합니다.
- `aws:branch` - 이전 단계의 결과를 기반으로 분기합니다.
- `aws:executeScript` - 작업 시작 실패의 가능한 원인을 분석합니다.
- `aws:executeScript` - 이 자동화로 생성된 리소스를 삭제합니다.
- `aws:executeScript` - 분석 결과를 콘솔에 반환하도록 자동화 출력의 형식을 지정합니다. 이 단계 이후에 자동화가 완료되기 전에 분석을 검토할 수 있습니다.
- `aws:branch` - Lambda 함수 및 관련 리소스가 생성되었고 삭제해야 하는지 여부를 기반으로 분기합니다.
- `aws:sleep` - Lambda 함수의 탄력적 네트워크 인터페이스를 삭제할 수 있도록 30분 동안 휴면 모드로 전환합니다.
- `aws:executeScript` - Lambda 함수 네트워크 인터페이스를 삭제합니다.
- `aws:executeScript` - Lambda 함수 네트워크 인터페이스 삭제 단계의 출력 형식을 지정합니다.

AWS-UpdateAmazonECSAgent

설명

`AWS-UpdateAmazonECSAgent` 런북은 지정한 Amazon Elastic Compute Cloud(Amazon ECS) 인스턴스에서 Amazon Elastic Container Service(Amazon EC2) 에이전트를 업데이트합니다. 이 실행서는 Amazon Linux 및 Amazon Linux 2 인스턴스만 지원합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 클러스터ARN

  유형: StringList

  설명: (필수) 컨테이너 인스턴스가 등록된 Amazon ECS 클러스터의 Amazon 리소스 이름(ARN)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:GetCommandInvocation`
- `ec2:DescribeImages`
- `ec2:DescribeInstanceAttribute`

- `ec2:DescribeImage`
- `ec2:DescribeInstance`
- `ec2:DescribeInstanceAttribute`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeClusters`
- `ecs:ListContainerInstances`
- `ecs:UpdateContainerAgent`

문서 단계

`aws:executeScript` - `ClusterARN` 파라미터에서 지정한 Amazon ECS 클러스터의 Amazon ECS 에이전트를 업데이트합니다.

출력

UpdateAmazonECSAgent.UpdatedContainers - Amazon ECS 에이전트 업데이트에 성공한 인스턴스의 ID입니다.

UpdateAmazonECSAgent.FailedContainers - Amazon ECS 에이전트 업데이트에 실패한 인스턴스의 ID입니다.

UpdateAmazonECSAgent.InProgressContainers - Amazon ECS 에이전트 업데이트가 진행 중인 인스턴스의 ID입니다.

Amazon EFS

AWS Systems Manager 자동화는 Amazon Elastic File System 에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-CheckAndMountEFS

`AWSSupport-CheckAndMountEFS`

설명

`AWSSupport-CheckAndMountEFS` 런북은 Amazon Elastic File System(AmazonEFS) 파일 시스템을 탑재하기 위한 사전 조건을 확인하고 지정한 Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스에 파일 시스템을 탑재합니다. 이 런북은 Amazon EFS 파일 시스템을 DNS 이름으로 탑재하거나 탑재 대상의 IP 주소를 사용하는 것을 지원합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 작업

  유형: 문자열

  유효한 값: 확인 | CheckAndMount

  설명: (필수) 실행서가 사전 요구 사항을 확인하는지, 아니면 사전 요구 사항을 확인하고 파일 시스템을 탑재하는지 결정합니다.
- EfsId

  유형: 문자열

  설명: (필수) 탑재할 파일 시스템의 ID입니다.

- InstanceId

  유형: 문자열

  설명: (필수) 파일 시스템을 탑재하려는 Amazon EC2 인스턴스의 ID입니다.
- MountOptions

  유형: 문자열

  설명: (선택 사항) 파일 시스템을 탑재할 때 사용하려는 Amazon EFS 탑재 도우미에서 지원하는 옵션입니다. `tls` 옵션을 지정하는 경우 대상 인스턴스에서 stunnel이 업그레이드되었는지 확인하십시오.
- MountPoint

  유형: 문자열

  설명: (선택 사항) 파일 시스템을 탑재하려는 디렉터리입니다. `Action` 파라미터에 대해 `Check` 값을 지정하는 경우, 이 파라미터를 지정하지 않아야 합니다.
- MountTargetIP

  유형: 문자열

  설명: (선택 사항) 탑재 대상의 IP 주소입니다. IP 주소별 탑재DNS는 DNS 호스트 이름이 비활성화된 가상 프라이빗 클라우드(VPCs)와 같이 이 비활성화된 환경에서 작동합니다. 또한 환경이 Amazon Route 53(Route 53) 이외의 DNS 공급자를 사용하는 경우 이 옵션을 사용할 수 있습니다.
- 리전

  유형: 문자열

  설명: (필수) Amazon EC2 인스턴스 및 파일 시스템이 AWS 리전 있는 위치입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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:*

문서 단계

- aws:executeScript - InstanceId 파라미터에서 지정한 Amazon EC2 인스턴스에 대한 세부 정보를 수집합니다.
- aws:executeScript - EfsId 파라미터에서 지정하는 파일 시스템에 대한 세부 정보를 수집합니다.
- aws:executeScript - 파일 시스템과 연결된 보안 그룹이 InstanceId 파라미터에 지정한 Amazon EC2 인스턴스에서 포트 2049의 트래픽을 허용하는지 확인합니다.
- aws:assertAwsResourceProperty - InstanceId 파라미터에서 지정한 Amazon EC2 인스턴스가 Systems Manager에서 관리되고 상태가 Online 인지 확인합니다.
- aws:branch - Action 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- aws:runCommand - EfsId 파라미터에서 지정하는 파일 시스템을 탑재하기 위한 사전 요구 사항을 확인합니다.
- aws:runCommand - EfsId 파라미터에 지정한 파일 시스템을 탑재하기 위한 사전 조건을 확인하고 InstanceId 파라미터에 지정한 Amazon EC2 인스턴스에 파일 시스템을 탑재합니다.

Amazon EKS

AWS Systems Manager 자동화는 Amazon Elastic Kubernetes Service에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-CollectEKSInstanceLogs
- AWS-CreateEKSClusterWithFargateProfile
- AWS-CreateEKSClusterWithNodegroup
- AWS-DeleteEKSCluster
- AWS-MigrateToNewEKSSelfManagedNodeGroup
- AWSPremiumSupport-TroubleshootEKSCluster
- AWSSupport-TroubleshootEKSWorkerNode
- AWS-UpdateEKSCluster
- AWS-UpdateEKSManagedNodeGroup
- AWS-UpdateEKSSelfManagedLinuxNodeGroups

`AWSSupport-CollectEKSInstanceLogs`

설명

`AWSSupport-CollectEKSInstanceLogs` 런북은 Amazon Elastic Compute Cloud(AmazonEKS) 인스턴스에서 운영 체제 및 Amazon Elastic Kubernetes Service(AmazonEC2) 관련 로그 파일을 수집하여 일반적인 문제를 해결하는 데 도움이 됩니다. 자동화가 관련 로그 파일을 수집하고 있는 동안, 임시 디렉터리 생성, 임시 디렉터리에 대한 로그 파일 복사, 아카이브로 로그 파일 압축하기 등 파일 시스템 구조에 대한 변경내용이 적용됩니다. 이 활동을 수행하면 EC2 인스턴스`CPUUtilization`가 증가할 수 있습니다. `CPUUtilization` 에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 인스턴스 지표를 참조하세요.

`LogDestination` 파라미터에 대한 값을 지정하는 경우, 지정하는 Amazon Simple Storage Service(Amazon S3) 버킷의 정책 상태를 자동화에서 평가합니다. EC2 인스턴스에서 수집한 로그의 보안을 지원하기 위해 정책 상태가 `true` 로 설정되어 있거나 액세스 제어 목록(ACL)`isPublic`이 `All Users` Amazon S3 사전 정의된 그룹에 `READ|WRITE` 권한을 부여하는 경우 로그가 업로드되지 않습

니다. Amazon S3의 미리 정의된 그룹에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 Amazon S3의 미리 정의된 그룹을 참조하세요.

> **Note**
>
> 이 자동화에는 EC2 인스턴스에 연결된 루트 Amazon Elastic Block Store(Amazon EBS) 볼륨에 사용 가능한 디스크 공간의 10% 이상이 필요합니다. 루트 볼륨에 사용 가능한 디스크 공간이 충분하지 않으면 자동화가 중지됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- EKSInstanceId

  유형: 문자열

  설명: 로그를 수집할 Amazon EKS EC2 인스턴스의 (필수) ID입니다.

- LogDestination

유형: 문자열

설명: (선택 사항) 보관된 로그를 업로드할 사용자의 계정에 있는 S3 버킷입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

명령을 수신하는 EC2 인스턴스에는 AmazonmazonSSMManagedInstanceCore 관리형 정책이 연결된 IAM 역할이 있는 것이 좋습니다. `LogDestination` 파라미터에서 지정하는 S3 버킷에 로그 아카이브를 업로드하려면 `s3:PutObject` 권한을 추가해야 합니다.

문서 단계

- `aws:assertAwsResourceProperty` - `EKSInstanceId` 파라미터에서 지정된 값의 운영 체제가 Linux인지 확인합니다.
- `aws:runCommand` - 운영 체제 및 Amazon EKS 관련 로그 파일을 수집하여 `/var/log` 디렉터리의 아카이브로 압축합니다.
- `aws:branch` - `LogDestination` 파라미터에 대해 값이 지정되었는지 확인합니다.
- `aws:runCommand` - `LogDestination` 파라미터에서 지정하는 S3 버킷에 로그 아카이브를 업로드합니다.

AWS-CreateEKSClusterWithFargateProfile

설명

`AWS-CreateEKSClusterWithFargateProfile` 실행서는 를 사용하여 Amazon Elastic Kubernetes Service(AmazonEKS) 클러스터를 생성합니다 AWS Fargate.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ClusterName

  유형: 문자열

  설명: (필수) 클러스터의 고유한 이름입니다.
- ClusterRoleArn

  유형: 문자열

  설명: (필수) Kubernetes 제어 영역이 사용자를 대신하여 작업에 호출 AWS API할 수 있는 권한을 제공하는 IAM 역할ARN의 입니다.
- FargateProfileName

  유형: 문자열

  설명: (필수) Fargate 프로필의 이름입니다.
- FargateProfileRoleArn

  유형: 문자열

  설명: (필수) Amazon EKS Pod 실행 IAM 역할ARN의 입니다.

- FargateProfileSelectors

  유형: 문자열

  설명: (필수) 포드를 Fargate 프로필과 일치시키는 선택기입니다.

- SubnetIds

  유형: StringList

  설명: (필수) Amazon EKS 클러스터에 사용할 서브넷IDs의 입니다. Amazon은 노드와 Kubernetes 제어 영역 간의 통신을 위해 이러한 서브넷에 탄력적 네트워크 인터페이스를 EKS 생성합니다. 서브넷 를 두 개 이상 지정해야 합니다IDs.

- EKSEndpointPrivateAccess

  타입: 부울

  기본값: True

  설명: (선택 사항) 클러스터의 Kubernetes API 서버 엔드포인트에 대한 프라이빗 액세스를 허용`True`하려면 이 값을 로 설정합니다. 프라이빗 액세스를 활성화하면 클러스터 내의 Kubernetes API 요청이 프라이빗 VPC 엔드포인트를 VPC 사용합니다. 프라이빗 액세스를 비활성화하고 클러스터에 노드 또는 AWS Fargate 포드가 있는 경우 에 노드 또는 Fargate 포드와의 통신에 필요한 CIDR 블록이 `publicAccessCidrs` 포함되어 있는지 확인합니다.

- EKSEndpointPublicAccess

  타입: 부울

  기본값: False

  설명: (선택 사항) 클러스터의 Kubernetes API 서버 엔드포인트에 대한 퍼블릭 액세스를 비활성화`False`하려면 이 값을 로 설정합니다. 퍼블릭 액세스를 비활성화하면 클러스터의 Kubernetes API 서버가 시작된 의 요청만 수신할 수 VPC 있습니다.

- PublicAccessCIDRs

  유형: StringList

  설명: (선택 사항) 클러스터의 퍼블릭 Kubernetes API 서버 엔드포인트에 대한 액세스가 허용되는 CIDR 블록입니다. 지정한 CIDR 블록 외부의 주소에서 엔드포인트로의 통신이 거부됩니다. 프라이빗 엔드포인트 액세스를 비활성화하고 클러스터에 노드 또는 Fargate 포드가 있는 경우 필요한 CIDR 블록을 지정해야 합니다.

- SecurityGroupIds

  유형: StringList

  설명: (선택 사항) Amazon 에서 계정에 생성한 탄력적 네트워크 인터페이스와 연결할 보안 그룹을 하나 이상 지정합니다EKS.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- CreateEKSCluster (aws:executeAwsApi) - Amazon EKS 클러스터를 생성합니다.
- VerifyEKSClusterIsActive (aws:waitForAwsResourceProperty) - 클러스터 상태가 인지 확인합니다`ACTIVE`.
- CreateFargateProfile (aws:executeAwsApi) - 클러스터에 대한 Fargate를 생성합니다.
- VerifyFargateProfileIsActive (aws:waitForAwsResourceProperty) - Fargate 프로필 상태가 인지 확인합니다`ACTIVE`.

출력

`CreateEKSCluster.CreateClusterResponse`

설명: `CreateCluster` API 통화에서 수신된 응답입니다.

`CreateFargateProfile.CreateFargateProfileResponse`

설명: `CreateFargateProfile` API 통화에서 수신된 응답입니다.

AWS-CreateEKSClusterWithNodegroup

설명

`AWS-CreateEKSClusterWithNodegroup` 실행서는 용량에 대한 노드 그룹을 사용하여 Amazon Elastic Kubernetes Service(AmazonEKS) 클러스터를 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ClusterName

  유형: 문자열

  설명: (필수) 클러스터의 고유한 이름입니다.
- ClusterRoleArn

  유형: 문자열

  설명: (필수) Kubernetes 제어 영역이 사용자를 대신하여 작업에 호출 AWS API할 수 있는 권한을 제공하는 IAM 역할ARN의 입니다.
- NodegroupName

  유형: 문자열

  설명: (필수) 노드 그룹의 고유 이름입니다.
- NodegroupRoleArn

  유형: 문자열

  설명: (필수) 노드 그룹과 연결할 IAM 역할ARN의 입니다. Amazon EKS 작업자 노드 kubelet 데몬은 사용자를 대신하여 APIs를 AWS 호출합니다. 노드는 IAM 인스턴스 프로파일 및 관련 정책을 통해 이러한 API 호출에 대한 권한을 받습니다. 노드를 시작하고 클러스터에 등록하려면 먼저 해당 노드가 시작될 때 사용할 IAM 역할을 생성해야 합니다.
- SubnetIds

  유형: StringList

  설명: (필수) Amazon EKS 클러스터에 사용할 서브넷IDs의 입니다. Amazon은 노드와 Kubernetes 제어 영역 간의 통신을 위해 이러한 서브넷에 탄력적 네트워크 인터페이스를 EKS 생성합니다. 서브넷 를 두 개 이상 지정해야 합니다IDs.
- EKSEndpointPrivateAccess

  타입: 부울

  기본값: True

  설명: (선택 사항) 클러스터의 Kubernetes API 서버 엔드포인트에 대한 프라이빗 액세스를 허용`True`하려면 이 값을 로 설정합니다. 프라이빗 액세스를 활성화하면 클러스터 내의 Kubernetes API 요청이 프라이빗 VPC 엔드포인트를 VPC 사용합니다. 프라이빗 액세스를 비활성화하고 클러스

터에 노드 또는 AWS Fargate 포드가 있는 경우 에 노드 또는 Fargate 포드와의 통신에 필요한 CIDR 블록이 `publicAccessCidrs` 포함되어 있는지 확인합니다.

- EKSEndpointPublicAccess

  타입: 부울

  기본값: False

  설명: (선택 사항) 클러스터의 Kubernetes API 서버 엔드포인트에 대한 퍼블릭 액세스를 비활성화`False`하려면 이 값을 로 설정합니다. 퍼블릭 액세스를 비활성화하면 클러스터의 Kubernetes API 서버가 시작된 의 요청만 수신할 수 VPC 있습니다.

- PublicAccessCIDRs

  유형: StringList

  설명: (선택 사항) 클러스터의 퍼블릭 Kubernetes API 서버 엔드포인트에 대한 액세스가 허용되는 CIDR 블록입니다. 지정한 CIDR 블록 외부의 주소에서 엔드포인트로의 통신이 거부됩니다. 프라이빗 엔드포인트 액세스를 비활성화하고 클러스터에 노드 또는 Fargate 포드가 있는 경우 필요한 CIDR 블록을 지정해야 합니다.

- SecurityGroupIds

  유형: StringList

  설명: (선택 사항) Amazon 에서 계정에 생성한 탄력적 네트워크 인터페이스와 연결할 보안 그룹을 하나 이상 지정합니다EKS.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DescribeCluster`
- `eks:DescribeNodegroup`

- `iam:CreateServiceLinkedRole`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:PassRole`

문서 단계

- CreateEKSCluster (aws:executeAwsApi) - Amazon EKS 클러스터를 생성합니다.
- VerifyEKSClusterIsActive (aws:waitForAwsResourceProperty) - 클러스터 상태가 인지 확인합니다`ACTIVE`.
- CreateNodegroup (aws:executeAwsApi) - 클러스터에 대한 노드 그룹을 생성합니다.
- VerifyNodegroupIsActive (aws:waitForAwsResourceProperty) - 노드 그룹 상태가 인지 확인합니다`ACTIVE`.

출력

- `CreateEKSCluster.CreateClusterResponse`: `CreateCluster` API 통화에서 수신된 응답입니다.
- `CreateNodegroup.CreateNodegroupResponse`: `CreateNodegroup` API 통화에서 수신된 응답입니다.

AWS-DeleteEKSCluster

설명

이 런북은 노드 그룹 및 Fargate 프로파일을 포함하여 Amazon EKS 클러스터와 연결된 리소스를 삭제합니다. 선택적으로 모든 자체 관리형 노드, 노드를 생성하는 데 사용되는 AWS CloudFormation 스택 및 클러스터의 VPC CloudFormation 스택을 삭제하도록 선택할 수 있습니다. 클러스터 삭제에 대한 자세한 내용은 Amazon EKS 사용 설명서의 클러스터 삭제를 참조하세요.

> **Note**
>
> 클러스터의 활성 서비스가 로드 밸런서와 연결된 경우 클러스터 삭제 전에 해당 서비스를 삭제해야 합니다. 그렇지 않으면, 시스템에서 로드 밸런서를 삭제할 수 없습니다. `AWS-DeleteEKSCluster` 실행서를 실행하기 전에 다음 절차에 따라 서비스를 찾아 삭제합니다.

클러스터에서 서비스를 찾아 삭제하려면

1. Kubernetes 명령줄 유틸리티를 설치합니다.`kubectl` 자세한 내용은 Amazon EKS 사용 설명서의 kubectl 설치를 참조하세요.
2. 다음 명령을 실행하여 클러스터에서 실행 중인 모든 서비스를 나열합니다.

```
kubectl get svc --all-namespaces
```

3. 연결된 EXTERNAL-IP 값이 있는 서비스를 삭제하려면 다음 명령을 실행합니다. 이러한 서비스는 로드 밸런서에 의해 설정되고, Kubernetes에서 이를 삭제하여 로드 밸런서와 연결된 리소스가 적절하게 릴리스되어야 합니다.

```
kubectl delete svc
service-name
```

이제 `AWS-DeleteEKSCluster` 실행서를 실행할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역

할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- EKSClusterName

  유형: 문자열

  설명: (필수) 삭제할 Amazon EKS 클러스터의 이름입니다.

- VPCCloudFormationStack

  유형: 문자열

  설명: 삭제 중인 EKS 클러스터의 에 VPC 대한 (선택 사항) AWS CloudFormation 스택 이름입니다. 이렇게 하면 의 AWS CloudFormation 스택VPC과 스택에서 생성한 모든 리소스가 삭제됩니다.

- VPCCloudFormationStackRole

  유형: 문자열

  설명: (선택 사항) 가 VPC CloudFormation 스택을 삭제하도록 AWS CloudFormation 맡는 IAM 역할 ARN의 입니다. 는 역할의 자격 증명을 AWS CloudFormation 사용하여 사용자를 대신하여 전화를 겁니다.

- SelfManagedNodeStacks

  유형: 문자열

  설명: (선택 사항) 자체 관리형 노드의 AWS CloudFormation 스택 이름 목록을 쉼표로 구분하면 자체 관리형 노드의 AWS CloudFormation 스택이 삭제됩니다.

- SelfManagedNodeStacksRole

  유형: 문자열

  설명: (선택 사항) 가 자체 관리형 노드 스택을 삭제하도록 AWS CloudFormation 맡는 IAM 역할ARN의 입니다. 는 역할의 자격 증명을 AWS CloudFormation 사용하여 사용자를 대신하여 전화를 겁니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `sts:AssumeRole`

- `eks:ListNodegroups`
- `eks:DeleteNodegroup`
- `eks:ListFargateProfiles`
- `eks:DeleteFargateProfile`
- `eks:DeleteCluster`
- `cfn:DescribeStacks`
- `cfn:DeleteStack`

문서 단계

- `aws:executeScript` - DeleteNodeGroups: EKS 클러스터의 모든 노드 그룹을 찾아 삭제합니다.
- `aws:executeScript` - DeleteFargateProfiles: EKS 클러스터의 모든 Fargate 프로파일을 찾아 삭제합니다.
- `aws:executeScript` - DeleteSelfManagedNodes: 노드를 생성하는 데 사용되는 모든 자체 관리형 노드와 CloudFormation 스택을 삭제합니다.
- `aws:executeScript` - D eleteEKSCluster: EKS 클러스터를 삭제합니다.
- `aws:executeScript` - D eleteVPCCloudFormationStack: VPC CloudFormation 스택을 삭제합니다.

AWS-MigrateToNewEKSSelfManagedNodeGroup

설명

`AWS-MigrateToNewEKSSelfManagedNodeGroup` 실행서는 기존 애플리케이션을 로 마이그레이션할 새 Amazon Elastic Kubernetes Service(AmazonEKS) Linux 노드 그룹을 생성하는 데 도움이 됩니다. 자세한 내용은 Amazon EKS 사용 설명서의 새 노드 그룹으로 마이그레이션을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- OldStackName

  유형: 문자열

  설명: (필수) 기존 AWS CloudFormation 스택의 이름 또는 스택 ID입니다.

- NewStackName

  유형: 문자열

  설명: (선택 사항) 새 노드 그룹에 대해 생성된 새 AWS CloudFormation 스택의 이름입니다. 이 파라미터의 값을 지정하지 않으면 스택 이름이 형식을 사용하여 생성됩니다`NewNodeGroup-`*`ClusterName`*`-`*`AutomationExecutionID`*.

- ClusterControlPlaneSecurityGroup

  유형: 문자열

  설명: (선택 사항) 노드가 Amazon EKS 제어 영역과 통신하는 데 사용할 보안 그룹의 ID입니다. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 보안 그룹이 사용됩니다.

- NodeInstanceType

  유형: 문자열

  설명: (선택 사항) 새 노드 그룹에 사용할 인스턴스 유형입니다. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 인스턴스 유형이 사용됩니다.

- NodeGroupName

유형: 문자열

설명: (선택 사항) 새 노드 그룹의 이름입니다. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 노드 그룹 이름이 사용됩니다.

- NodeAutoScalingGroupDesiredCapacity

  유형: 문자열

  설명: (선택 사항) 새 스택이 생성될 때 확장할 노드의 원하는 수입니다. 이 숫자는 `NodeAutoScalingGroupMinSize` 값보다 크거나 같아야 하며 보다 작거나 같아야 합니다`NodeAutoScalingGroupMaxSize`. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 노드 그룹 원하는 용량이 사용됩니다.

- NodeAutoScalingGroupMaxSize

  유형: 문자열

  설명: (선택 사항) 노드 그룹이 확장할 수 있는 최대 노드 수입니다. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 노드 그룹 최대 크기가 사용됩니다.

- NodeAutoScalingGroupMinSize

  유형: 문자열

  설명: (선택 사항) 노드 그룹이 확장할 수 있는 최소 노드 수입니다. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 노드 그룹 최소 크기가 사용됩니다.

- NodeImageId

  유형: 문자열

  설명: (선택 사항) 의 ID Amazon Machine Image (AMI)를 사용합니다.

- NodeImageIdSSMParam

  유형: 문자열

  설명: (선택 사항) 에 대한 퍼블릭 Systems Manager 파라미터 AMI 노드 그룹이 사용할 노드 그룹입니다.

- NodeVolumeSize

  유형: 문자열

설명: (선택 사항) GiB. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 노드 볼륨 크기가 사용됩니다.

- NodeVolumeType

  유형: 문자열

  설명: (선택 사항) 노드의 루트 EBS 볼륨에 사용할 Amazon 볼륨의 유형입니다. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 볼륨 유형이 사용됩니다.

- KeyName

  유형: 문자열

  설명: (선택 사항) 노드에 할당하려는 키 페어입니다. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 키 페어가 사용됩니다.

- 서브넷

  유형: StringList

  설명: (선택 사항) 새 노드 그룹에 IDs 사용할 서브넷의 쉼표로 구분된 목록입니다. 이 파라미터의 값을 지정하지 않으면 기존 AWS CloudFormation 스택에 지정된 서브넷이 사용됩니다.

- D isableIMDSv1

  타입: 부울

  설명: (선택 사항) 를 지정`true`하여 인스턴스 메타데이터 서비스 버전 1()을 비활성화합니다 IMDSv1. 기본적으로 노드는 IMDSv1 및 를 지원합니다IMDSv2.

- BootstrapArguments

  유형: 문자열

  설명: (선택 사항) 노드 부트스트랩 스크립트에 전달하려는 추가 인수입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- DetermineParameterValuesForNewNodeGroup (aws:executeScript) - 새 노드 그룹에 사용할 파라미터 값을 수집합니다.
- CreateStack (aws:createStack) - 새 노드 그룹의 AWS CloudFormation 스택을 생성합니다.
- GetNewStackNodeInstanceRole (aws:executeAwsApi) - 노드 인스턴스 역할을 가져옵니다.
- GetNewStackSecurityGroup (aws:executeAwsApi) - 단계가 노드 보안 그룹을 가져옵니다.
- AddIngressRulesToNewNodeSecurityGroup (aws:executeAwsApi) - 새로 생성된 보안 그룹에 수신 규칙을 추가하여 이전 노드 그룹에 할당된 보안 그룹의 트래픽을 수락할 수 있습니다.
- AddIngressRulesToOldNodeSecurityGroup (aws:executeAwsApi) - 새로 생성된 노드 그룹에 할당된 보안 그룹의 트래픽을 수락할 수 있도록 이전 보안 그룹에 수신 규칙을 추가합니다.
- VerifyStackComplete (aws:assertAwsResourceProperty) - 새 스택 상태가 인지 확인합니다`CREATE_COMPLETE`.

출력

DetermineParameterValuesForNewNodeGroup.NewStackParameters - 새 스택을 생성하는 데 사용되는 파라미터입니다.

GetNewStackNodeInstanceRole.NewNodeInstanceRole - 새 노드 그룹의 노드 인스턴스 역할입니다.

GetNewStackSecurityGroup.NewNodeSecurityGroup - 새 노드 그룹에 대한 보안 그룹의 ID입니다.

DetermineParameterValuesForNewNodeGroup.NewStackName - 새 노드 그룹의 AWS CloudFormation 스택 이름입니다.

CreateStack.StackId - 새 노드 그룹의 AWS CloudFormation 스택 ID입니다.

`AWSPremiumSupport-TroubleshootEKSCluster`

설명

`AWSPremiumSupport-TroubleshootEKSCluster` 런북은 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터, 기본 인프라의 일반적인 문제를 진단하고 권장 개선 단계를 제공합니다.

> **Important**
>
> `AWSPremiumSupport-*` 실행서에 액세스하려면 Enterprise 또는 Business Support Subscription이 필요합니다. 자세한 내용은 AWS 지원 플랜 비교를 참조하세요.

`S3BucketName` 파라미터에 대한 값을 지정하는 경우, 지정하는 Amazon Simple Storage Service(Amazon S3) 버킷의 정책 상태를 자동화에서 평가합니다. EC2 인스턴스에서 수집한 로그의 보안을 지원하기 위해 정책 상태가 `true` 로 설정되어 있거나 액세스 제어 목록(ACL)`isPublic`이 `All Users` Amazon S3 사전 정의된 그룹에 `READ|WRITE` 권한을 부여하는 경우 로그가 업로드되지 않습니다. Amazon S3의 미리 정의된 그룹에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 Amazon S3의 미리 정의된 그룹을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ClusterName

  유형: 문자열

  설명: (필수) 문제를 해결하려는 Amazon EKS 클러스터의 이름입니다.

- S3BucketName

  유형: 문자열

  설명: (선택 사항) 실행서에서 생성한 보고서를 업로드해야 하는 프라이빗 Amazon S3 버킷의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

또한 자동화를 시작하는 사용자 또는 역할에 연결된 AWS Identity and Access Management (IAM) 정책은 `ssm:GetParameter` 작업을 다음 퍼블릭 AWS Systems Manager 파라미터로 허용하여 최신 권장 Amazon을 얻어야 합니다. EKS Amazon Machine Image (AMI)를 사용합니다.

- `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`

실행서에서 생성된 보고서를 Amazon S3 버킷에 업로드하려면 지정된 Amazon S3 버킷에 대해 다음과 같은 권한이 필요합니다.

- `s3:GetBucketPolicyStatus`
- `s3:GetBucketAcl`
- `s3:PutObject`

문서 단계

- `aws:executeAwsApi` - 지정된 Amazon EKS 클러스터에 대한 세부 정보를 수집합니다.
- `aws:executeScript` - Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스, Auto Scaling 그룹,AMI및 Amazon EC2 GPU 그래픽 인스턴스 유형.
- `aws:executeScript` - Amazon EKS 클러스터의 가상 프라이빗 클라우드(VPC), 서브넷, 네트워크 주소 변환(NAT) 게이트웨이, 서브넷 경로, 보안 그룹 및 네트워크 액세스 제어 목록(ACLs)에 대한 세부 정보를 수집합니다.
- `aws:executeScript` - 연결된 IAM 인스턴스 프로파일 및 역할 정책의 세부 정보를 수집합니다.
- `aws:executeScript` - `S3BucketName` 파라미터에서 지정하는 Amazon S3 버킷의 세부 정보를 수집합니다.
- `aws:executeScript` - Amazon VPC 서브넷을 퍼블릭 또는 프라이빗으로 분류합니다.
- `aws:executeScript` - Amazon VPC 서브넷에 Amazon EKS 클러스터의 일부로 필요한 태그가 있는지 확인합니다.
- `aws:executeScript` - Amazon VPC 서브넷에 Elastic Load Balancing 서브넷에 필요한 태그가 있는지 확인합니다.
- `aws:executeScript` - 작업자 노드 Amazon EC2 인스턴스가 최신 Amazon EKS 최적화를 사용하는지 확인합니다.AMIs
- `aws:executeScript` - 작업자 노드에 연결된 Amazon VPC 보안 그룹이 필요한 태그인지 확인합니다.
- `aws:executeScript` - Amazon EKS 클러스터 및 작업자 노드 Amazon VPC 보안 그룹 규칙에서 Amazon EKS 클러스터에 대한 권장 수신 규칙을 확인합니다.
- `aws:executeScript` - Amazon EKS 클러스터 및 작업자 노드 Amazon VPC 보안 그룹 규칙에서 Amazon EKS 클러스터의 권장 송신 규칙을 확인합니다.
- `aws:executeScript` - Amazon VPC 서브넷의 네트워크 ACL 구성을 확인합니다.
- `aws:executeScript` - 작업자 노드 Amazon EC2 인스턴스에 필요한 관리형 정책이 있는지 확인합니다.
- `aws:executeScript` - Auto Scaling 그룹에 클러스터 자동 스케일링에 필요한 태그가 있는지 확인합니다.
- `aws:executeScript` - 작업자 노드 Amazon EC2 인스턴스가 인터넷에 연결되어 있는지 확인합니다.
- `aws:executeScript` - 이전 단계의 출력을 기반으로 보고서를 생성합니다. `S3BucketName` 파라미터에 대해 값이 지정된 경우, 생성된 보고서가 Amazon S3 버킷에 업로드됩니다.

AWSSupport-TroubleshootEKSWorkerNode

설명

AWSSupport-TroubleshootEKSWorkerNode 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 작업자 노드와 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 분석하여 작업자 노드가 클러스터에 가입하지 못하게 하는 일반적인 원인을 식별하고 해결하는 데 도움이 됩니다. 실행서는 식별된 문제를 해결하는 데 도움이 되는 지침을 출력합니다.

> **Important**
>
> 이 자동화를 성공적으로 실행하려면 Amazon EC2 작업자 노드의 상태가 running 이고 Amazon EKS 클러스터 상태가 ACTIVE 여야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ClusterName

유형: 문자열

설명: (필수) Amazon EKS 클러스터의 이름입니다.

- WorkerID

  유형: 문자열

  설명: (필수) 클러스터에 조인하지 못한 Amazon EC2 작업자 노드의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:assertAwsResourceProperty` - `ClusterName` 파라미터에 지정한 Amazon EKS 클러스터가 존재하고 `ACTIVE` 상태인지 확인합니다.
- `aws:assertAwsResourceProperty` - `WorkerID` 파라미터에 지정한 Amazon EC2 작업자 노드가 존재하고 `running` 상태인지 확인합니다.
- `aws:executeScript` - 워커 노드가 클러스터에 가입하지 못하는 가능한 원인을 식별하는 데 도움이 되는 Python 스크립트를 실행합니다.

AWS-UpdateEKSCluster

설명

`AWS-UpdateEKSCluster` 실행서는 Amazon Elastic Kubernetes Service(AmazonEKS) 클러스터를 사용하려는 Kubernetes 버전으로 업데이트하는 데 도움이 됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ClusterName

  유형: 문자열

  설명: (필수) Amazon EKS 클러스터의 이름입니다.

- 버전

  유형: 문자열

  설명: (필수) 클러스터를 업데이트하려는 Kubernetes 버전입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `eks:DescribeUpdate`
- `eks:UpdateClusterVersion`

문서 단계

- `aws:executeAwsApi` - Amazon EKS 클러스터에서 사용하는 Kubernetes 버전을 업데이트합니다.
- `aws:waitForAwsResourceProperty` - 업데이트 상태가 가 될 때까지 기다립니다`Successful`.

AWS-UpdateEKSManagedNodeGroup

설명

`AWS-UpdateEKSManagedNodeGroup` 실행서는 Amazon Elastic Kubernetes Service(AmazonEKS) 관리형 노드 그룹을 업데이트하는 데 도움이 됩니다. `Version` 또는 `Configuration` 업데이트 중 하나를 선택할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ClusterName

  유형: 문자열

  설명: (필수) 업데이트하려는 노드 그룹이 있는 클러스터의 이름입니다.
- NodeGroupName

  유형: 문자열

  설명: (필수) 업데이트할 노드 그룹의 이름입니다.
- UpdateType

  유형: 문자열

  유효한 값: Update Node Group Version | Update Node Group Configurations

  기본값: Update Node Group Version

  설명: (필수) 노드 그룹에서 수행하려는 업데이트 유형입니다.

다음 파라미터는 `Version` 업데이트 유형에만 적용됩니다.

- AMIReleaseVersion

  유형: 문자열

  설명: (선택 사항) EKS 최적화된 Amazon 버전 AMI 사용하려는 입니다. 기본적으로 최신 버전이 사용됩니다.

- ForceUpgrade

  타입: 부울

  설명: (선택 사항) true인 경우, 포드 중단 예산 위반에 대응하여 업데이트가 실패하지 않습니다.

- KubernetesVersion

  유형: 문자열

  설명: (선택 사항) 노드 그룹을 업데이트할 Kubernetes 버전입니다.

- LaunchTemplateId

  유형: 문자열

  설명: (선택 사항) 시작 템플릿의 ID입니다.

- LaunchTemplateName

  유형: 문자열

  설명: (선택 사항) 시작 템플릿의 이름입니다.

- LaunchTemplateVersion

  유형: 문자열

  설명: (선택 사항) Amazon Elastic Compute Cloud(Amazon EC2) 시작 템플릿 버전입니다. 이 파라미터는 시작 템플릿에서 노드 그룹을 생성한 경우에만 유효합니다.

다음 파라미터는 `Configuration` 업데이트 유형에만 적용됩니다.

- AddOrUpdateNodeGroupLabels

  유형: StringMap

  설명: (선택 사항) 추가하거나 업데이트하려는 Kubernetes 레이블입니다.

- AddOrUpdateKubernetesTaintsEffect

  유형: StringList

  설명: (선택 사항) 추가하거나 업데이트하려는 Kubernetes 테인트입니다.
- MaxUnavailableNodeGroups

  유형: 정수

  기본값: 0

  설명: (선택 사항) 버전 업데이트 중 한 번에 사용할 수 없는 최대 노드 수입니다.
- MaxUnavailablePercentageNodeGroup

  유형: 정수

  기본값: 0

  설명: (선택 사항) 버전 업데이트 중 사용할 수 없는 노드 비율입니다.
- NodeGroupDesiredSize

  유형: 정수

  기본값: 0

  설명: (선택 사항) 관리형 노드 그룹에서 유지해야 하는 노드 수입니다.
- NodeGroupMaxSize

  유형: 정수

  기본값: 0

  설명: (선택 사항) 관리형 노드 그룹이 확장될 수 있는 최대 노드 수입니다.
- NodeGroupMinSize

  유형: 정수

  기본값: 0

  설명: (선택 사항) 관리형 노드 그룹이 확장될 수 있는 최소 노드 수입니다.
- RemoveKubernetesTaintsEffect

유형: StringList

설명: (선택 사항) 제거하려는 Kubernetes 테인트입니다.

- RemoveNodeGroupLabels

  유형: StringList

  설명: (선택 사항) 제거하려는 레이블의 쉼표로 구분된 목록입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `eks:UpdateNodegroupConfig`
- `eks:UpdateNodegroupVersion`

문서 단계

- `aws:executeScript` - 실행서 입력 파라미터에 대해 지정한 값에 따라 Amazon EKS 클러스터 노드 그룹을 업데이트합니다.
- `aws:waitForAwsResourceProperty` - 클러스터 업데이트 상태가 `Successful`이 될 때까지 기다립니다.

AWS-UpdateEKSSelfManagedLinuxNodeGroups

설명

`AWS-UpdateEKSSelfManagedLinuxNodeGroups` 실행서는 AWS CloudFormation 스택을 사용하여 Amazon Elastic Kubernetes Service(AmazonEKS) 클러스터의 자체 관리형 노드 그룹을 업데이트합니다.

클러스터에서 Auto Scaling을 사용하는 경우 이 실행서를 사용하기 전에 배포를 복제본 2개로 조정하는 것이 좋습니다.

배포를 복제본 2개로 조정하려면

1. Kubernetes 명령줄 유틸리티를 설치합니다.`kubectl` 자세한 내용은 설치를 참조하세요.kubectl Amazon EKS 사용 설명서의 .

2. 다음 명령을 실행합니다.

```
kubectl scale deployments/cluster-autoscaler --replicas=2 -n kube-system
```

3. `AWS-UpdateEKSSelfManagedLinuxNodeGroups` 실행서를 실행합니다.
4. 다음 명령어를 실행하여 배포를 원하는 복제본 수로 다시 조정합니다.

```
kubectl scale deployments/cluster-autoscaler --replicas=number -n kube-system
```

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ClusterName

  유형: 문자열

  설명: (필수) Amazon EKS 클러스터의 이름입니다.
- NodeGroupName

  유형: 문자열

설명: (필수) 관리형 노드 그룹의 이름입니다.

- ClusterControlPlaneSecurityGroup

  유형: 문자열

  설명: (필수) 컨트롤 플레인 보안 그룹의 ID입니다.

- D isableIMDSv1

  타입: 부울

  설명: (선택 사항) 인스턴스 메타데이터 서비스 버전 1(IMDSv1) 및 를 허용할지 여부를 결정합니다 IMDSv2.

- KeyName

  유형: 문자열

  설명: (선택 사항) 인스턴스의 키 이름입니다.

- NodeAutoScalingGroupDesiredCapacity

  유형: 문자열

  설명: (선택 사항) 노드 그룹에서 유지해야 하는 노드 수입니다.

- NodeAutoScalingGroupMaxSize

  유형: 문자열

  설명: (선택 사항) 노드 그룹이 확장될 수 있는 최대 노드 수입니다.

- NodeAutoScalingGroupMinSize

  유형: 문자열

  설명: (선택 사항) 노드 그룹이 축소될 수 있는 최소 노드 수입니다.

- NodeInstanceType

  유형: 문자열

  기본값: t3.large

  설명: (선택 사항) 노드 그룹에 대해 사용하려는 인스턴스 유형입니다.

- NodeImageId

  유형: 문자열

  설명: (선택 사항) 의 ID Amazon Machine Image (AMI)를 사용합니다.
- NodeImageIdSSMParam

  유형: 문자열

  기본값: /aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

  설명: (선택 사항) 에 대한 퍼블릭 Systems Manager 파라미터 AMI 노드 그룹이 사용할 노드 그룹입니다.
- StackName

  유형: 문자열

  설명: (필수) 노드 그룹을 업데이트하는 데 사용되는 AWS CloudFormation 스택의 이름입니다.
- 서브넷

  유형: 문자열

  설명: (필수) 클러스터에서 사용할 서브넷에 IDs 대한 의 쉼표로 구분된 목록입니다.
- VpcId

  유형: 문자열

  기본값: Default

  설명: (필수) 클러스터가 배포되는 가상 프라이빗 클라우드(VPC)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `eks:CreateCluster`
- `eks:CreateNodegroup`
- `eks:DeleteNodegroup`
- `eks:DeleteCluster`

- `eks:DescribeCluster`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListNodegroups`
- `eks:UpdateClusterConfig`
- `eks:UpdateNodegroupConfig`

문서 단계

- `aws:executeScript` - 실행서 입력 파라미터에 대해 지정한 값에 따라 Amazon EKS 클러스터 노드 그룹을 업데이트합니다.
- `aws:waitForAwsResourceProperty` - AWS CloudFormation 스택 업데이트 상태가 반환될 때까지 기다립니다.

Elastic Beanstalk

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Elastic Beanstalk. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-CollectElasticBeanstalkLogs
- AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming
- AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications
- AWSSupport-TroubleshootElasticBeanstalk

`AWSSupport-CollectElasticBeanstalkLogs`

설명

`AWSSupport-CollectElasticBeanstalkLogs` 실행서는 Amazon Elastic Compute Cloud(AmazonEC2)에서 관련 로그 파일을 수집합니다. AWS Elastic Beanstalk Windows Server 일반적인 문제를 해결하는 데 도움이 되도록 Elastic Beanstalk에서 시작한 인스턴스입니다. 자동화가 관련 로그 파일을 수집하고 있는 동안, 임시 디렉터리 생성, 임시 디렉터리에 대한 로그 파일 복사, 아카이브로 로그 파일 압축하기 등 파일 시스템 구조에 대한 변경내용이 적용됩니다. 이 활동을 수행하면

Amazon EC2 인스턴스`CPUUtilization`가 증가할 수 있습니다. `CPUUtilization` 에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 인스턴스 지표를 참조하세요.

`S3BucketName` 파라미터에 대한 값을 지정하는 경우, 지정하는 Amazon Simple Storage Service(Amazon S3) 버킷의 정책 상태를 자동화에서 평가합니다. Amazon EC2 인스턴스에서 수집한 로그의 보안을 지원하기 위해 정책 상태가 `true` 로 설정되어 있거나 액세스 제어 목록(ACL)`isPublic`이 `All Users` Amazon S3 미리 정의된 그룹에 `READ|WRITE` 권한을 부여하는 경우 로그가 업로드되지 않습니다. Amazon S3의 미리 정의된 그룹에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 Amazon S3의 미리 정의된 그룹을 참조하세요.

`S3BucketName` 파라미터 값을 지정하지 않으면 자동화가 로그 번들을 자동화를 실행하는 AWS 리전 에서 기본 Elastic Beanstalk Amazon S3 버킷에 업로드합니다. 디렉터리 이름은 다음 구조인 `elasticbeanstalk-` *`region`* `-` *`accountID`* 에 따라 지정됩니다. 는 *`region`* 그리고 *`accountID`* 값은 리전에 따라 다르며 자동화를 AWS 계정 실행합니다. 로그 번들은 `resources/environments/logs/bundle/` *`environmentID`* `/` *`instanceID`* 디렉터리에 저장됩니다. 는 *`environmentID`* 그리고 *`instanceID`* 값은 Elastic Beanstalk 환경과 로그를 수집하는 Amazon EC2 인스턴스에 따라 달라집니다.

기본적으로 Elastic Beanstalk 환경의 Amazon 인스턴스에 연결된 AWS Identity and Access Management (IAM) EC2 인스턴스 프로필에는 환경의 기본 Elastic Beanstalk Amazon S3 버킷에 번들을 업로드하는 데 필요한 권한이 있습니다. `S3BucketName` 파라미터의 값을 지정하는 경우 Amazon 인스턴스에 연결된 EC2 인스턴스 프로파일에서 지정된 Amazon S3 버킷 및 경로에 대한 `s3:GetBucketAcl` , `s3:GetBucketPolicy` `s3:GetBucketPolicyStatus` , 및 `s3:PutObject` 작업을 허용해야 합니다.

> **Note**
>
> 이 자동화에는 Amazon EC2 인스턴스에 연결된 루트 Amazon Elastic Block Store(Amazon EBS) 볼륨에 최소 500MB의 사용 가능한 디스크 공간이 필요합니다. 루트 볼륨에 사용 가능한 디스크 공간이 충분하지 않으면 자동화가 중지됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- EnvironmentId

  유형: 문자열

  설명: (필수) 로그 번들을 수집하려는 Elastic Beanstalk 환경의 ID입니다.
- InstanceId

  유형: 문자열

  (필수) 로그 번들을 수집할 Elastic Beanstalk 환경의 Amazon EC2 인스턴스 ID입니다.
- S3BucketName

  유형: 문자열

  (선택 사항) 보관된 로그를 업로드하려는 Amazon S3 버킷입니다.
- S3BucketPath

  유형: 문자열

  (선택 사항) 보관된 로그를 업로드하려는 Amazon S3 버킷 경로입니다. `S3BucketName` 파라미터의 값을 지정하지 않은 경우, 이 파라미터는 무시됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ssm:SendCommand`
- `ssm:DescribeInstanceInformation`
- `ec2:DescribeInstances`

문서 단계

- `aws:assertAwsResourceProperty` - `InstanceId` 파라미터에 지정한 Amazon EC2 인스턴스가 에서 관리되는지 확인합니다 AWS Systems Manager.
- `aws:assertAwsResourceProperty` - `InstanceId` 파라미터에 지정한 Amazon EC2 인스턴스가 Windows Server 인스턴스.
- `aws:runCommand` - 인스턴스가 Elastic Beanstalk 환경에 속하는지, 로그를 번들링하기에 충분한 디스크 공간이 있는지, 로그를 업로드할 Amazon S3 버킷이 퍼블릭인지 확인합니다.
- `aws:runCommand` - 로그 파일을 수집하고 아카이브를 `S3BucketName` 파라미터에 지정된 Amazon S3 버킷에 또는 값이 지정되지 않은 경우 Elastic Beanstalk 환경의 기본 버킷에 업로드합니다.

AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming

설명

`AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming` 런북을 사용하면 지정한 AWS Elastic Beanstalk (Elastic Beanstalk) 환경에 로깅할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- EnvironmentId

  유형: 문자열

  설명: (필수) 로그온을 활성화하려는 Elastic Beanstalk 환경의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

문서 단계

- `aws:executeAwsApi` - `EnvironmentId` 파라미터에서 지정하는 Elastic Beanstalk 환경에서 로그온을 활성화합니다.
- `aws:waitForAwsResourceProperty` - 환경 상태가 `Ready`로 변경될 때까지 기다립니다.
- `aws:executeScript` - Elastic Beanstalk 환경에서 로깅이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications

설명

`AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications` 실행서는 지정한 AWS Elastic Beanstalk (Elastic Beanstalk) 환경에 대한 알림을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- EnvironmentId

  유형: 문자열

  설명: (필수) 일림을 활성화하려는 Elastic Beanstalk 환경의 ID입니다.
- TopicArn

  유형: 문자열

  설명: (필수) 알림을 보내려는 Amazon Simple Notification Service(AmazonSNS) 주제ARN의 입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `elasticbeanstalk:DescribeConfigurationSettings`
- `elasticbeanstalk:DescribeEnvironments`
- `elasticbeanstalk:UpdateEnvironment`

문서 단계

- `aws:executeAwsApi` - `EnvironmentId` 파라미터에서 지정하는 Elastic Beanstalk 환경에 대한 알림을 활성화합니다.
- `aws:waitForAwsResourceProperty` - 환경 상태가 `Ready`로 변경될 때까지 기다립니다.
- `aws:executeScript` - Elastic Beanstalk 환경에서 알림이 활성화되었는지 확인합니다.

AWSSupport-TroubleshootElasticBeanstalk

설명

`AWSSupport-TroubleshootElasticBeanstalk` 실행서는 AWS Elastic Beanstalk 환경이 `Degraded` 또는 `Severe` 상태에 있는 잠재적 이유를 해결하는 데 도움이 됩니다. 이 자동화는 Elastic Beanstalk 환경과 연결된 다음 AWS 리소스를 확인합니다.

- 로드 밸런서, AWS CloudFormation 스택, Amazon EC2 Auto Scaling 그룹, Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 및 가상 프라이빗 클라우드()에 대한 구성 세부 정보입니다 VPC.
- 서브넷과 연결된 보안 그룹 규칙, 라우팅 테이블 및 네트워크 액세스 제어 목록(ACLs)과 관련된 네트워크 구성 문제입니다.
- Elastic Beanstalk 엔드포인트에 대한 연결 및 공용 인터넷 액세스를 확인합니다.
- 로드 밸런서의 상태를 확인합니다.
- Amazon EC2 인스턴스의 상태를 확인합니다.
- Elastic Beanstalk 환경에서 로그 번들을 검색하고 선택적으로 파일을 에 업로드합니다 AWS Support.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ApplicationName

  유형: 문자열

  설명: (필수) Elastic Beanstalk 애플리케이션의 이름입니다.
- EnvironmentName

  유형: 문자열

  설명: (필수) Elastic Beanstalk 환경의 이름입니다.
- AWSS3UploaderLink

  유형: 문자열

  설명: (선택 사항) Elastic Beanstalk 환경에서 로 로그 번들을 업로드 AWS Support 하기 위해 가 URL 제공합니다. 이 옵션은 AWS Support 플랜을 구매하고 지원 사례를 연 고객만 사용할 수 있습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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*`

문서 단계

- `aws:executeScript` - 자동화를 시작한 AWS Identity and Access Management (IAM) 보안 주체가 실행서에 정의된 모든 작업을 수행하는 데 필요한 권한을 가지고 있는지 확인합니다.
- `aws:branch` - 이전 단계의 결과를 기반으로 워크플로를 분기합니다.
- `aws:executeScript` - 로드 밸런서, AWS CloudFormation 스택, Auto Scaling 그룹, Amazon EC2 인스턴스 및 VPC 구성을 포함한 Elastic Beanstalk 환경에 대한 정보를 수집합니다.
- `aws:executeScript` - 라우팅 테이블 및 의 서브넷과 ACLs 연결된 네트워크 연결 문제를 확인합니다VPC.

- `aws:executeScript` - Amazon EC2 인스턴스와 연결된 보안 그룹 규칙과 관련된 네트워크 연결 문제를 확인합니다.
- `aws:executeScript` - Amazon EC2 인스턴스의 상태 확인을 확인합니다.
- `aws:executeScript` - Elastic Beanstalk 환경의 로그 번들에 대한 링크를 생성합니다.
- `aws:executeScript` - 로그 번들을 에 업로드합니다 AWS Support.
- `aws:executeScript` - Elastic Beanstalk 환경 상태에 영향을 미칠 수 있는 문제를 해결하는 데 도움이 되는 작업 항목 보고서를 출력합니다.

Elastic Load Balancing

AWS Systems Manager Automation은 Elastic Load Balancing 에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-DropInvalidHeadersForALB
- AWS-EnableCLBAccessLogs
- AWS-EnableCLBConnectionDraining
- AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing
- AWSConfigRemediation-EnableELBDeletionProtection
- AWSConfigRemediation-EnableLoggingForALBAndCLB
- AWSSupport-TroubleshootCLBConnectivity
- AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing
- AWS-UpdateALBDesyncMitigationMode
- AWS-UpdateCLBDesyncMitigationMode

`AWSConfigRemediation-DropInvalidHeadersForALB`

설명

`AWSConfigRemediation-DropInvalidHeadersForALB` 실행서를 사용하면 지정한 애플리케이션 로드 밸런서가 잘못된 HTTP 헤더가 있는 헤더를 제거할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- LoadBalancerArn

  유형: 문자열

  설명: (필수) 잘못된 헤더를 삭제하려는 로드 밸런서의 Amazon 리소스 이름(ARN)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

문서 단계

- `aws:executeAwsApi` - `LoadBalancerArn` 파라미터에서 사용자가 지정하는 로드 밸런서에 대해 유효하지 않은 헤더 삭제 설정을 활성화합니다.

- `aws:executeScript` - `LoadBalancerArn` 파라미터에서 사용자가 지정하는 로드 밸런서에 대해 유효하지 않은 헤더 삭제 설정이 활성화되었는지 확인합니다.

AWS-EnableCLBAccessLogs

설명

`AWS-EnableCLBAccessLogs` 실행서는 Classic Load Balancer 에 대한 액세스 로그를 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- EmitInterval

  유형: 정수

  유효한 값: 5 | 60

  기본값: 60

  설명: (선택 사항) 몇 분 안에 액세스 로그를 게시하는 간격입니다.

- LoadBalancerNames

  유형: 문자열

  설명: (필수) 액세스 로그를 활성화하려는 Classic Load Balancer의 쉼표로 구분된 목록입니다.
- S3BucketName

  유형: 문자열

  설명: (필수) 액세스 로그가 저장되는 Amazon Simple Storage Service(Amazon S3) 버킷의 이름입니다.
- S3BucketPrefix

  유형: 문자열

  설명: (선택 사항) Amazon S3 버킷에 대해 생성한 논리적 계층 구조, 예: `my-bucket-prefix/prod`. 접두사를 제공하지 않으면 로그가 버킷의 루트 수준에 저장됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `elasticloadbalancing:ModifyLoadBalancerAttributes`

문서 단계

- `aws:executeAwsApi` - `LoadBalancerNames` 파라미터에 지정한 Classic Load Balancer에 대한 액세스 로그를 활성화합니다.

출력

E nableCLBAccessLogs. SuccessesLoadBalancers - 액세스 로그가 성공적으로 활성화된 로드 밸런서 이름의 목록입니다.

E 액세스 nableCLBAccess로그 활성화가 실패한 FailedLoadBalancers MapList 로드 밸런서 이름과 실패 이유.

AWS-EnableCLBConnectionDraining

설명

`AWS-EnableCLBConnectionDraining` 실행서를 사용하면 Classic Load Balancer(CLB)에서 지정된 제한 시간 값으로 연결을 드레이닝할 수 있습니다. 연결 드레이닝CLB을 사용하면 가 등록 취소 중이거나 비정상인 인스턴스에 대한 전송 중 요청을 완료할 수 있습니다. 지정된 제한 시간은 인스턴스를 등록 취소된 것으로 보고하기 전에 연결을 유지하는 시간입니다. 의 연결 드레이닝에 대한 자세한 내용은 Classic Load Balancer 사용 설명서의 Classic Load Balancer에 대한 연결 드레이닝 구성을 CLBs참조하세요. Load Balancer

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- LoadBalancerName

  유형: 문자열

  설명: (필수) 연결 드레이닝을 활성화하려는 로드 밸런서의 이름입니다.

- ConnectionTimeout

  유형: 정수

  유효한 값: 1-3600

기본값: 300

설명: (필수) 로드 밸런서의 연결 제한 시간 값입니다. 제한 시간 값은 1~3,600초로 설정할 수 있습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

문서 단계

- ModifyLoadBalancerConnectionDraining (aws:executeAwsApi): 연결 드레이닝을 활성화하고 지정한 로드 밸런서에 지정된 제한 시간 값을 설정합니다.
- VerifyLoadBalancerConnectionDrainingEnabled (aws:assertAwsResourceProperty): 로드 밸런서에 연결 드레이닝이 활성화되어 있는지 확인합니다.
- VerifyLoadBalancerConnectionDrainingTimeout (aws:assertAwsResourceProperty): 로드 밸런서의 연결 제한 시간 값이 지정한 값과 일치하는지 확인합니다.

AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing

설명

`AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing` 런북을 사용하면 지정한 Classic Load Balancer(CLB)에 대해 영역 간 로드 밸런싱을 사용할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- LoadBalancerName

  유형: 문자열

  설명: (필수) 교차 영역 로드 밸런싱을 활성화CLB하려는 의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elb:DescribeLoadBalancerAttributes`
- `elb:ModifyLoadBalancerAttributes`

문서 단계

- `aws:executeAwsApi` - `LoadBalancerName` 파라미터에 CLB 지정한 에 대해 크로스 영역 로드 밸런싱을 활성화합니다.
- `aws:assertAwsResourceProperty` - 에서 영역 간 로드 밸런싱이 활성화되었는지 확인합니다 CLB.

AWSConfigRemediation-EnableELBDeletionProtection

설명

`AWSConfigRemediation-EnableELBDeletionProtection` 실행서는 지정한 탄력적 로드 밸런서(ELB)에 대한 삭제 방지를 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- LoadBalancerArn

  유형: 문자열

  설명: (필수) 삭제 보호를 활성화ELB하려는 의 Amazon 리소스 이름(ARN)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

문서 단계

- `aws:executeScript` - `LoadBalancerArn` 파라미터에 ELB 지정한 에서 삭제 방지를 활성화합니다.

AWSConfigRemediation-EnableLoggingForALBAndCLB

설명

`AWSConfigRemediation-EnableLoggingForALBAndCLB` 실행서는 지정된 AWS Application Load Balancer 또는 Classic Load Balancer()에 대한 로깅을 활성화합니다CLB.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- LoadBalancerId

  유형: 문자열

  설명: (필수) Classic Load Balancer 이름 또는 Application Load Balancer 입니다ARN.

- S3BucketName

유형: 문자열

설명: (필수) Amazon S3 버킷 이름입니다.

- S3BucketPrefix

  유형: 문자열

  설명: (선택 사항) Amazon Simple Storage Service(Amazon S3) 버킷에 대해 생성한 논리적 계층 구조입니다(예를 들면, `my-bucket-prefix/prod`). 접두사를 제공하지 않으면 로그가 버킷의 루트 수준에 저장됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

문서 단계

- `aws:executeScript` - Classic Load Balancer 또는 Application Load Balancer에 대한 로깅을 활성화하고 확인합니다.

`AWSSupport-TroubleshootCLBConnectivity`

설명

`AWSSupport-TroubleshootCLBConnectivity` 실행서는 Classic Load Balancer(CLB)와 Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스 간의 연결 문제를 해결하는 데 도움이 됩니다. 또한 클라이언트와 간의 연결 문제가 검토CLB됩니다. 또한 이 런북은 에 대한 상태 확인을 검토하고CLB, 모범 사례를 따르고 있는지 확인하고, 문제 해결 대시보드를 생성합니다. 선택적으로, Amazon Simple Storage Service(Amazon S3) 버킷에 Automation 출력을 업로드할 수 있습니다. 그러나, 이 실행서는 공개적으로 액세스할 수 있는 S3 버킷에 출력을 업로드하는 것을 지원하지 않습니다. 이 자동화를 위해 임시 S3 버킷을 생성하는 것이 좋습니다.

> **Important**
>
> 이 실행서를 사용하면 생성된 대시보드에 대한 요금이 부과될 수 있습니다. 자세한 내용은 Amazon CloudWatch 요금을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InvestigationType

  유형: 문자열

  유효한 값: Best Practices | Connectivity Issues | Troubleshooting Dashboard

  설명: (필수) 실행서에서 수행하려는 작업입니다.
- LoadBalancerName

  유형: 문자열

  설명: (필수) 의 이름입니다CLB.

- S3Location

  유형: 문자열

  설명: (선택 사항) 자동화 결과를 보내려는 S3 버킷의 이름입니다. 공개적으로 액세스할 수 있는 버킷은 지원되지 않습니다. S3 버킷이 서버 측 암호화를 사용하는 경우 이 자동화를 실행하는 사용자에게 또는 역할에 AWS KMS 키에 대한 `kms:GenerateDataKey` 권한이 있어야 합니다.
- S3LocationPrefix

  유형: 문자열

  설명: (선택 사항) 자동화 출력을 업로드하려는 Amazon S3 키 접두사(하위 폴더)입니다. 형식 출력은 amzn-s3-demo-bucket/ 형식으로 저장됩니다.*S3LocationPrefix*/{{*InvestigationType*}}_{{자동화:*EXECUTION_ID*}}.txt.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeScript` - `LoadBalancerName` 파라미터에 CLB 지정한 이 존재하는지 확인합니다.
- `aws:branch` - `InvestigationType` 파라미터에 대해 지정된 값을 기반으로 분기합니다.
- `aws:executeScript` - 에 대한 연결 확인을 수행합니다CLB.
- `aws:executeScript` - CLB 구성이 Elastic Load Balancing 모범 사례를 준수하는지 확인합니다.
- `aws:executeScript` - 에 대한 Amazon CloudWatch 대시보드를 생성합니다CLB.
- `aws:executeScript` - 자동화 결과가 포함된 텍스트 파일을 생성하여 `S3Location` 파라미터에서 지정하는 Amazon S3 버킷에 업로드합니다.

출력

RunBestPractices.Summary

RunConnectivityChecks.Summary

CreateTroubleshootingDashboard.출력

UploadOutputToS3.출력

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

설명

`AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` 런북을 사용하면 지정한 네트워크 로드 밸런서(NLB)에 대해 크로스 영역 로드 밸런싱이 활성화됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- LoadBalancerArn

  유형: 문자열

  설명: (필수) 교차 영역 로드 밸런싱을 활성화NLB하려는 의 Amazon 리소스 이름(ARN)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

문서 단계

- `aws:executeAwsApi` - `LoadBalancerArn` 파라미터에 NLB 지정한 에 대해 크로스 영역 로드 밸런싱을 활성화합니다.
- `aws:executeScript` - 에서 교차 영역 로드 밸런싱이 활성화되었는지 확인합니다NLB.

AWS-UpdateALBDesyncMitigationMode

설명

`AWS-UpdateALBDesyncMitigationMode` 실행서는 Application Load Balancer(ALB)의 비동기화 완화 모드를 지정된 완화 모드로 업데이트합니다. 비동기화 완화 모드는 로드 밸런서가 애플리케이션에 보안 위험을 초래할 수 있는 요청을 처리하는 방법을 결정합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역

할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- LoadBalancerArn

  유형: 문자열

  설명: (필수) 의 비동기화 완화 모드를 수정ALB하려는 의 Amazon 리소스 이름(ARN)입니다.

- DesyncMitigationMode

  유형: 문자열

  유효한 값: 모니터 | 방어 | 가장 엄격

  설명: (필수) 에서 사용할 완화 모드ALB입니다. 비동기화 완화 모드에 대한 자세한 내용은 Application Load Balancer 사용 설명서의 비동기화 완화 모드를 참조하세요.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancers`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

문서 단계

- VerifyLoadBalancerType (aws:assertAwsResourceProperty) - 다음 단계로 진행하기 전에 `LoadBalancerArn` 입력 파라미터에 지정된 값이 애플리케이션 로드 밸런서용인지 확인합니다.
- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - 지정된 ALB를 사용하도록 를 업데이트합니다`DesyncMitigationMode`.
- VerifyLoadBalancerDesyncMitigationMode (aws:executeScript) - 대상 에 대해 비동기화 완화 모드가 업데이트되었는지 확인합니다ALB.

출력

VerifyLoadBalancerDesyncMitigationMode.ModificationResult - 에 대한 수정을 확인하는 스크립트의 메시지 페이로드입니다ALB.

AWS-UpdateCLBDesyncMitigationMode

설명

`AWS-UpdateCLBDesyncMitigationMode` 실행서는 Classic Load Balancer(CLB)의 비동기화 완화 모드를 지정된 완화 모드로 업데이트합니다. 비동기화 완화 모드는 로드 밸런서가 애플리케이션에 보안 위험을 초래할 수 있는 요청을 처리하는 방법을 결정합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- LoadBalancerName

  유형: 문자열

  설명: (필수) 의 비동기화 완화 모드를 수정CLB하려는 의 이름입니다.
- DesyncMitigationMode

  유형: 문자열

유효한 값: 모니터 | 방어 | 가장 엄격

설명: (필수) 에서 사용할 완화 모드CLB입니다. 비동기화 완화 모드에 대한 자세한 내용은 Application Load Balancer 사용 설명서의 비동기화 완화 모드를 참조하세요.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `elasticloadbalancing:DescribeLoadBalancerAttributes`
- `elasticloadbalancing:ModifyLoadBalancerAttributes`

문서 단계

- ModifyLoadBalancerDesyncMode (aws:executeAwsApi) - 지정된 CLB를 사용하도록 를 업데이트합니다`DesyncMitigationMode`.
- VerifyLoadBalancerDesyncMitigationMode (aws:executeScript) - 대상 에 대해 비동기화 완화 모드가 업데이트되었는지 확인합니다CLB.

출력

VerifyLoadBalancerDesyncMitigationMode.ModificationResult - 에 대한 수정을 확인하는 스크립트의 메시지 페이로드입니다CLB.

Amazon EMR

AWS Systems Manager 자동화는 Amazon 에 사전 정의된 실행서를 제공합니다EMR. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-AnalyzeEMRLogs
- AWSSupport-DiagnoseEMRLogsWithAthena

AWSSupport-AnalyzeEMRLogs

설명

이 실행서는 Amazon EMR 클러스터에서 작업을 실행하는 동안 오류를 식별하는 데 도움이 됩니다. 실행서는 파일 시스템에 정의된 로그 목록을 분석하고 미리 정의된 키워드 목록을 찾습니다. 이러한 로그 항목은 이벤트를 기반으로 필요한 작업을 수행할 수 있도록 Amazon CloudWatch Events 이벤트를 생성하는 데 사용됩니다. 선택적으로 실행서는 선택한 Amazon CloudWatch Logs 로그 그룹에 로그 항목을 게시합니다. 이 실행서는 현재 로그 파일에서 다음과 같은 오류 및 패턴을 찾습니다.

- container_out_of_memory – YARN 컨테이너에 메모리가 부족하여 작업을 실행하지 못할 수 있습니다.
- yarn_nodemanager_health: CORE 또는 TASK 노드의 디스크 공간이 부족하여 작업을 실행할 수 없습니다.
- node_state_change: CORE 또는 TASK 노드가 MASTER 노드에 연결할 수 없습니다.
- step_failure: EMR 단계가 실패했습니다.
- no_core_nodes_running: 현재 실행 중인 CORE 노드가 없으며 클러스터가 비정상입니다.
- hdfs_missing_blocks: 데이터 손실로 이어질 수 있는 누락된 HDFS 블록이 있습니다.
- hdfs_high_util: HDFS 사용률이 높아 작업 및 클러스터 상태에 영향을 미칠 수 있습니다.
- instance_controller_restart: Instance-Controller 프로세스가 다시 시작되었습니다. 이 프로세스는 클러스터 상태를 유지하는 데 필수적입니다.
- instance_controller_restart_legacy: Instance-Controller 프로세스가 다시 시작되었습니다. 이 프로세스는 클러스터 상태를 유지하는 데 필수적입니다.
- high_load: High Load Average가 감지되어 노드 상태 보고에 영향을 미치거나 시간 초과 또는 속도 저하를 초래할 수 있습니다.
- yarn_node_blacklisted: CORE 또는 TASK 노드가 실행 중인 작업YARN에서 에 의해 블랙리스트에 올랐습니다.
- yarn_node_lost: CORE 또는 TASK 노드가 LOST로 표시되었습니다. 연결 문제가 YARN발생할 수 있습니다.

지정하는 인스턴스와 `ClusterID`(와)과 연결된 인스턴스는 AWS Systems Manager에 의해 관리되어야 합니다. 이 자동화를 한 번 실행하거나, 특정 시간 간격으로 실행되도록 자동화를 예약하거나, 자동화로 이전에 생성한 일정을 제거할 수 있습니다. 이 런북은 Amazon EMR 릴리스 버전 5.20~6.30을 지원합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ClusterID

  유형: 문자열

  설명: (필수) 분석하려는 노드 로그가 있는 클러스터의 ID입니다.
- Operation

  유형: 문자열

  유효한 값: Run Once | Schedule | Remove Schedule

  설명: (필수) 클러스터에서 수행할 작업입니다.
- IntervalTime

  유형: 문자열

  유효한 값: 5 minutes | 10 minutes | 15 minutes

설명: (선택 사항) 자동화 실행 사이의 시간입니다. 이 파라미터는 `Operation` 파라미터에 대해 `Schedule` 값을 지정하는 경우에만 적용할 수 있습니다.

- LogToCloudWatchLogs

  유형: 문자열

  유효한 값: yes | no

  설명: (선택 사항) 이 파라미터의 값에 `yes` 를 지정하면 자동화는 `CloudWatchLogGroup` 파라미터에 지정된 이름으로 CloudWatch 로그 로그 로그 그룹을 생성하여 일치하는 로그 항목을 저장합니다.

- CloudWatchLogGroup

  유형: 문자열

  설명: (선택 사항) 일치하는 CloudWatch 로그 항목을 저장할 로그 로그 로그 그룹의 이름입니다. 이 파라미터는 `LogToCloudWatchLogs` 파라미터에 대해 `yes` 값을 지정하는 경우에만 적용할 수 있습니다.

- CreateLogInsightsDashboard

  유형: 문자열

  유효한 값: yes | no

  설명: (선택 사항) `yes` 를 지정하면 CloudWatch 대시보드가 아직 존재하지 않는 경우 대시보드가 생성됩니다. 이 파라미터는 `LogToCloudWatchLogs` 파라미터에 대해 `yes` 값을 지정하는 경우에만 적용할 수 있습니다.

- CreateMetricFilters

  유형: 문자열

  유효한 값: yes | no

  설명: (선택 사항) CloudWatch 로그 로그 그룹에 대한 지표 필터를 생성할`yes`지 여부를 지정합니다. 이 파라미터는 `LogToCloudWatchLogs` 파라미터에 대해 `yes` 값을 지정하는 경우에만 적용할 수 있습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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

문서 단계

- aws:executeAwsApi - ClusterID 파라미터에 지정된 Amazon EMR 클러스터에 대한 정보를 수집합니다.
- aws:branch - 입력을 기반으로 분기합니다.
  - 제공된 작업이 Run Once 또는 Schedule인 경우:
    - aws:assertAwsResourceProperty - 클러스터를 사용할 수 있는지 확인합니다.
    - aws:executeAwsApi - 클러스터에서 실행되는 모든 인스턴스IDs의 를 수집합니다.
    - aws:assertAwsResourceProperty - SSM 에이전트가 클러스터의 모든 인스턴스에서 실행 중인지 확인합니다.
    - aws:branch - 자동화를 한 번 실행하도록 지정했는지, 또는 일정에 따라 실행하도록 지정했는지에 따라 분기합니다.
      - 제공된 작업이 Run Once인 경우:
        - aws:branch - LogToCloudWatchLogs 파라미터에서 지정된 값을 기반으로 분기합니다.
          - LogToCloudWatchLogs 값이 yes인 경우:
            - aws:executeScript - 파라미터에 지정된 이름을 가진 CloudWatch 로그 로그 그룹이 CloudWatchLogGroup 이미 존재하는지 확인합니다. 그렇지 않은 경우, 지정된 이름으로 그룹이 생성됩니다.
            - aws:branch - CreateMetricFilters 파라미터에서 지정된 값을 기반으로 분기합니다.
              - CreateMetricFilters 값이 yes인 경우:
                - aws:executeAwsApi - 각 지표 필터에 대해 12단계가 실행됩니다.
                - aws:branch - CreateLogInsightsDashboard 파라미터에서 지정된 값을 기반으로 분기합니다.
                - CreateLogInsightsDashboard 값이 yes인 경우:
                - aws:executeAwsApi - 파라미터가 아직 존재하지 않는 경우 CloudWatchLogGroup 파라미터에 지정된 것과 동일한 이름으로 대시보드를 생성합니다 CloudWatch.
                - CreateLogInsightsDashboard 값이 no인 경우:
                - aws:runCommand - 쉘 스크립트를 실행하여 클러스터의 각 인스턴스에서 로그 패턴을 찾습니다.

- `CreateMetricFilters` 값이 no인 경우:
  - `aws:branch` - `CreateLogInsightsDashboard` 파라미터에서 지정된 값을 기반으로 분기합니다.
    - `CreateLogInsightsDashboard` 값이 yes인 경우:
      - `aws:executeAwsApi` - 파라미터가 아직 존재하지 않는 경우 `CloudWatchLogGroup` 파라미터에 지정된 것과 동일한 이름으로 대시보드를 생성합니다 CloudWatch.
    - `CreateLogInsightsDashboard` 값이 no인 경우:
      - `aws:runCommand` - 쉘 스크립트를 실행하여 클러스터의 각 인스턴스에서 로그 패턴을 찾습니다.
  - `LogToCloudWatchLogs` 값이 no인 경우:
    - `aws:executeAwsApi` - 쉘 스크립트를 실행하여 클러스터의 각 인스턴스에서 로그 패턴을 찾습니다.
- 제공된 작업이 `Schedule`인 경우:
  - `aws:createStack` - 이 런북을 대상으로 하는 Amazon EventBridge 이벤트를 생성합니다.
- 제공된 작업이 `Remove Schedule`인 경우:
  - `aws:executeAwsApi` - 클러스터에 일정이 있는지 확인합니다.
  - `aws:deleteStack` - 일정을 삭제합니다.

출력

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstances.InstanceIDs

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists.출력

FindLogPatternOnEMRNode.CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

설명

`AWSSupport-DiagnoseEMRLogsWithAthena`런북은 Amazon Athena를 데이터 AWS Glue 카탈로그와 통합하여 사용하여 Amazon EMR 로그를 진단하는 데 도움이 됩니다. Amazon Athena는 특정 날짜 범위 또는 키워드 기반 검색을 위한 선택적 파라미터를 사용하여 Amazon EMR 로그 파일에서 컨테이너, 노드 로그 또는 둘 다를 쿼리하는 데 사용됩니다.

Runbook은 기존 클러스터의 Amazon EMR 로그 위치를 자동으로 검색하거나 Amazon S3 로그 위치를 지정할 수 있습니다. 로그를 분석하려면 런북을 참조하십시오.

- AWS Glue 데이터베이스를 생성하고 Amazon Amazon EMR S3 로그 위치에서 Amazon Athena 데이터 정의 언어 DDL () 쿼리를 실행하여 클러스터 로그에 대한 테이블과 알려진 문제 목록을 생성합니다.
- 데이터 조작 언어 (DML) 쿼리를 실행하여 Amazon EMR 로그에서 알려진 문제 패턴을 검색합니다. 쿼리는 탐지된 문제 목록, 발생 횟수, Amazon S3 파일 경로별로 일치하는 키워드 수를 반환합니다.
- 접두사 `saw_diagnose_EMR_known_issues` 아래에 지정한 Amazon S3 버킷에 결과가 업로드됩니다.
- 런북은 사전 정의된 하위 집합에서 가져온 Amazon Knowledge Center (KC) 문서에 대한 결과, 권장 사항 및 참조를 강조하여 Amazon Athena 쿼리 결과를 반환합니다.
- 완료 또는 실패 시 Amazon S3 버킷에 업로드된 AWS Glue 데이터베이스 및 알려진 문제 파일이 삭제됩니다.

어떻게 작동하나요?

Amazon Athena를 사용하여 Amazon EMR 로그를 분석하여 오류를 탐지하고 결과, 권장 사항 및 관련 지식 센터 문서를 강조 표시합니다. `AWSSupport-DiagnoseEMRLogsWithAthena`

런북은 다음 단계를 수행합니다.

- 클러스터 ID를 사용하여 Amazon EMR 클러스터 로그 위치를 가져오거나 Amazon S3 위치를 입력하여 로그 위치 및 크기를 검색합니다.
- 로그 위치 크기를 기반으로 Athena 비용 추정치를 제공합니다.
- Athena 쿼리를 실행하기 전에 지정된 IAM 담당자에게 승인을 요청하고 다음 단계를 계속 진행하여 진행 승인을 받으세요.

- 알려진 문제를 지정된 Amazon S3 버킷에 업로드하고 AWS Glue 데이터베이스와 테이블을 생성합니다.
- Amazon EMR 로그 데이터에 대해 Athena 쿼리를 실행합니다. 쿼리는 날짜 범위, 키워드 또는 두 가지 기준 모두를 기준으로 검색하거나 제공된 입력에 따라 필터 없이 실행할 수 있습니다.
- 결과를 분석하여 결과, 권장 사항 및 관련 KC 문서를 강조하세요.
- Amazon Athena DML 쿼리 결과를 위한 출력 링크입니다.
- 생성된 데이터베이스, 테이블 및 업로드된 알려진 문제를 제거하여 환경을 정리합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

/

런북을 성공적으로 사용하려면 AutomationAssumeRole 매개 변수에 다음 작업이 필요합니다.

- 아테나: GetQueryExecution
- 아테나: StartQueryExecution
- 아테나: GetPreparedStatement
- 아테나: CreatePreparedStatement
- 글루: GetDatabase
- 접착제: CreateDatabase
- 접착제: DeleteDatabase
- 접착제: CreateTable
- 접착제: GetTable
- 접착제: DeleteTable
- 엘라스틱 맵 리듀스: DescribeCluster
- s3: ListBucket
- s3: GetBucketVersioning
- s3: ListBucketVersions

- s3: GetBucketPublicAccessBlock
- s3: GetBucketPolicyStatus
- s3: GetObject
- s3: GetBucketLocation
- 가격: GetProducts
- 가격: GetAttributeValues
- 가격: DescribeServices
- 가격: ListPriceLists

> **Important**
>
> 이 자동화에 필요한 리소스에만 액세스를 제한하려면 SSM 서비스를 신뢰하는 IAM 역할에 다음 정책을 추가하세요. 파티션, 리전, 계정을 런북이 실행되는 파티션, 리전, 계정 번호의 적절한 값으로 바꾸십시오.

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

지침

다음 단계에 따라 자동화를 구성합니다.

1. 문서 AWS Systems Manager 아래에서 AWSSupport-D를 iagnoseEMRLogs WithAthena 탐색하십시오.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터의 경우, 다음 내용을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
   - 클러스터ID (필수):

     아마존 EMR 클러스터 ID.
   - S3 LogLocation (선택 사항):

     아마존 S3 아마존 EMR 로그 위치. 경로 스타일의 URL Amazon S3 위치를 입력합니다 (예:). `s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/` Amazon EMR 클러스터가 종료된 지 `30` 며칠 이상인 경우 이 파라미터를 제공하십시오.

- S3 BucketName (필수):

  알려진 문제의 목록과 Amazon Athena 쿼리의 출력을 업로드하기 위한 Amazon S3 버킷 이름입니다. 버킷에는 퍼블릭 액세스 차단이 활성화되어 있어야 하며 Amazon EMR 클러스터와 동일한 AWS 리전 및 계정에 있어야 합니다.

- 승인자 (필수):

  작업을 승인하거나 거부할 수 있는 AWS 인증된 주도자 목록. 사용자 이름, 사용자ARN, 역할 또는 역할 수임 형식 중 하나를 사용하여 주도자를 지정할 수 있습니다. IAM ARN IAM ARN 최대 승인자자 수는 10명입니다.

- FetchNodeLogsOnly (선택 사항):

  로 `true` 설정하면 자동화가 Amazon EMR 애플리케이션 컨테이너 로그를 진단합니다. 기본값은 `false`입니다.

- FetchContainersLogsOnly(선택 사항):

  로 `true` 설정하면 자동화가 Amazon EMR 컨테이너 로그를 진단합니다. 기본값은 `false`입니다.

- EndSearchDate (선택 사항):

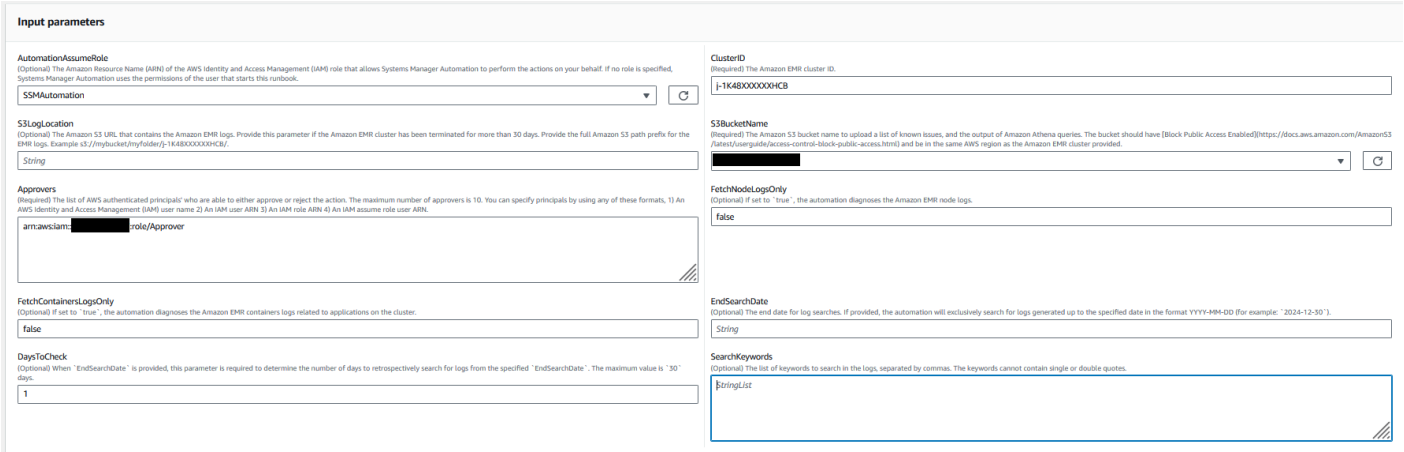
  로그 검색 종료일. 제공된 경우 자동화는 YYYY -MM-DD 형식으로 지정된 날짜까지 생성된 로그만 검색합니다 (예:). `2024-12-30`

- DaysToCheck (선택 사항):

  이 매개 변수가 제공되는 경우 지정된 로그를 소급하여 검색할 일수를 결정하는 데 이 매개 변수가 필요합니다. `EndSearchDate` `EndSearchDate` 최대값은 `30` 일수입니다. 기본값은 `1`입니다.

- SearchKeywords (선택 사항):

  로그에서 검색할 키워드 목록 (쉼표로 구분됨). 키워드에는 작은따옴표나 큰따옴표를 포함할 수 없습니다.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - getLogLocation:

     지정된 Amazon 클러스터 ID를 쿼리하여 Amazon S3 로그 위치를 검색합니다. EMR 자동화가 Amazon EMR 클러스터 ID에서 로그 위치를 쿼리할 수 없는 경우, Runbook은 `S3LogLocation` 입력 파라미터를 사용합니다.
   - branchOnValid로그:

     Amazon EMR 로그 위치를 확인합니다. 위치가 유효하다면 Amazon 로그에서 쿼리를 실행할 때 Amazon Athena의 잠재적 비용을 추정해 보십시오. EMR
   - estimateAthenaCosts:

     Amazon EMR 로그의 크기를 결정하고 로그 데이터세트에서 Athena 스캔을 실행하는 데 드는 예상 비용을 제공합니다. 비상업 지역 (AWS 비파티션) 의 경우 이 단계에서는 비용을 추정하지 않고 로그 크기만 제공합니다. 비용은 지정된 지역의 Athena 가격 책정 설명서를 사용하여 계산할 수 있습니다.
   - approveAutomation:

     지정된 담당자의 승인을 IAM 기다려 자동화의 다음 단계를 진행합니다. 승인 알림에는 Amazon 로그의 EMR Amazon Athena 스캔 예상 비용과 자동화를 통해 프로비저닝되는 리소스에 대한 세부 정보가 포함됩니다.
   - uploadKnownIssuesExecuteAthenaQueries:

미리 정의된 알려진 문제를 파라미터에 지정된 Amazon S3 버킷에 `S3BucketName` 업로드합니다. AWS Glue 데이터베이스와 테이블을 생성합니다. 입력 파라미터를 기반으로 데이터베이스에서 Amazon Athena 쿼리를 실행합니다. AWS Glue

- getQueryExecution상태:

  Amazon Athena 쿼리 실행 상태가 `SUCCEEDED` 될 때까지 기다립니다. Amazon Athena DML 쿼리는 Amazon EMR 클러스터 로그에서 오류와 예외를 검색합니다.

- analyzeAthenaResults:

  Amazon Athena 결과를 분석하여 사전 정의된 매핑 세트에서 가져온 결과, 권장 사항 및 KC (지식 센터) 문서를 제공합니다.

- getAnalyzeResults쿼리 ExecutionStatus 1:

  쿼리 실행 상태가 될 때까지 기다립니다. `SUCCEEDED` Amazon Athena DML 쿼리는 이전 DML 쿼리의 결과를 분석합니다. 이 분석 쿼리는 해결 방법 및 KC 문서와 일치하는 예외를 반환합니다.

- getAnalyzeResults쿼리 2ExecutionStatus:

  쿼리 실행 상태가 될 때까지 기다립니다. `SUCCEEDED` Amazon Athena DML 쿼리는 이전 DML 쿼리의 결과를 분석합니다. 이 분석 쿼리는 각 Amazon S3 로그 경로에서 감지된 예외/오류 목록을 반환합니다.

- printAthenaQueries메시지:

  Amazon Athena DML 쿼리 결과에 대한 링크를 인쇄합니다.

- cleanupResources:

  생성된 AWS Glue 데이터베이스를 삭제하여 리소스를 정리하고 Amazon EMR logs 버킷에 생성된 알려진 문제 파일을 삭제합니다.

7. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토하십시오.

   출력은 Athena 쿼리 결과에 대한 세 개의 링크를 제공합니다.

   - Amazon EMR 클러스터 로그에서 발견된 모든 오류 및 자주 발생하는 예외를 해당 로그 위치 (Amazon S3 접두사) 와 함께 나열합니다.
   - 문제 해결에 도움이 되는 권장 해결 방법 및 KC 문서와 함께 Amazon EMR 로그에 일치하는 알려진 고유한 예외 요약을 제공합니다.
   - Amazon S3 로그 경로에서 특정 오류 및 예외가 나타나는 위치에 대한 세부 정보를 제공하여 추가 진단을 지원합니다.

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 설명서

- 자세한 내용은 Amazon EMR 클러스터 문제 해결을 참조하십시오.

Amazon OpenSearch Service

AWS Systems Manager 자동화는 Amazon OpenSearch Service에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-DeleteOpenSearchDomain
- AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain
- AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups
- AWSSupport-TroubleshootOpenSearchRedYellowCluster
- AWSSupport-TroubleshootOpenSearchHighCPU

`AWSConfigRemediation-DeleteOpenSearchDomain`

설명

`AWSConfigRemediation-DeleteOpenSearchDomain` 실행서는 DeleteDomain 를 사용하여 지정된 Amazon OpenSearch Service 도메인을 삭제합니다API.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- DomainName

  유형: 문자열

  유효한 값: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  설명: (필수) 삭제하려는 Amazon OpenSearch Service 도메인의 이름입니다.
- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DeleteDomain`

- `es:DescribeDomain`

문서 단계

- `aws:executeScript` - Amazon OpenSearch Service 도메인 이름을 입력으로 수락하고 삭제한 다음 삭제를 확인합니다.

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

설명

`AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain` 런북은 를 사용하여 지정된 Amazon OpenSearch Service 도메인`EnforceHTTPS`에서 UpdateDomainConfig 를 활성화합니다API.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- DomainName

  유형: 문자열

  유효한 값: (\d{12}/)?[a-z]{1}[a-z0-9-]{2,28}

  설명: (필수) 를 적용하는 데 사용할 Amazon OpenSearch Service 도메인의 이름입니다HTTPS.
- AutomationAssumeRole

  유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

문서 단계

- `aws:executeScript` - `DomainName` 파라미터에 지정한 Amazon OpenSearch Service 도메인에서 `EnforceHTTPS` 엔드포인트 옵션을 활성화합니다.

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

설명

`AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups` 실행서는 를 사용하여 지정된 Amazon OpenSearch Service 도메인의 보안 그룹 구성을 업데이트합니다UpdateDomainConfigAPI.

> **Note**
> AWS 보안 그룹은 Amazon Virtual Private Cloud(VPC) 액세스용으로 구성된 Amazon OpenSearch Service 도메인에만 적용할 수 있으며 퍼블릭 액세스용으로 구성된 Amazon OpenSearch Service 도메인에는 적용할 수 없습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- DomainName

  유형: 문자열

  설명: (필수) 보안 그룹을 업데이트하는 데 사용할 Amazon OpenSearch Service 도메인의 이름입니다.
- SecurityGroupList

  유형: StringList

  설명: (필수) Amazon OpenSearch Service 도메인에 할당IDs하려는 보안 그룹입니다.
- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `es:DescribeDomain`
- `es:UpdateDomainConfig`

문서 단계

- `aws:executeScript` - `DomainName` 파라미터에 지정한 Amazon OpenSearch Service 도메인의 보안 그룹 구성을 업데이트합니다.

AWSSupport-TroubleshootOpenSearchRedYellowCluster

설명

`AWSSupport-TroubleshootOpenSearchRedYellowCluster`자동화 런북은 빨간색 또는 노란색 클러스터 상태의 원인을 식별하고 클러스터를 다시 녹색으로 변경하는 과정을 안내하는 데 사용됩니다.

어떻게 작동하나요?

런북은 빨간색 또는 노란색 클러스터의 원인을 해결하는 `AWSSupport-TroubleshootOpenSearchRedYellowCluster` 데 도움이 되며 클러스터 구성 및 리소스 사용률을 분석하여 이 문제를 해결하기 위한 다음 단계를 제공합니다.

런북은 다음 단계를 수행합니다.

- 대상 도메인에 DescribeDomainAPI대해 를 호출하여 클러스터 구성을 가져옵니다.
- OpenSearch 서비스 도메인이 인터넷 기반 (퍼블릭) 인지 아니면 Amazon Virtual Private Cloud (VPC) 기반인지 확인합니다.
- 클러스터 구성에 따라 공용 또는 Amazon VPC 기반 AWS Lambda 함수를 생성합니다. 참고: Lambda 함수에는 클러스터에 대해 APIs 서비스를 OpenSearch 실행하여 클러스터가 빨간색 또는 노란색 상태인 이유를 확인하는 문제 해결 코드가 포함되어 있습니다.
- Lambda 함수를 삭제합니다.
- 빨간색 또는 노란색 클러스터 문제를 해결하기 위해 수행된 검사 및 다음 권장 단계를 표시합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

런북을 성공적으로 사용하려면 `LambdaExecutionRole` 파라미터에 다음 작업이 필요합니다.

- `es:ESHttpGet`

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DeleteNetworkInterface`

`LambdaExecutionRole`정책 개요:

다음은 이 런북에 필요한 서비스 및 리소스에 AWS 액세스할 수 있는 권한을 함수에 부여하는 Lambda 함수의 실행 역할AWS Identity and Access Management IAM (() 역할) 의 예입니다. 자세한 내용을 알아보려면 Lambda 실행 역할을 참조하세요.

> **Note**
>
> `ec2:DescribeNetworkInterfaces`,`ec2:CreateNetworkInterface`, 및 `ec2:DeleteNetworkInterface` 는 Lambda 함수가 Amazon 네트워크 인터페이스를 생성하고 관리할 수 있도록 Amazon VPC 기반 OpenSearch 서비스 클러스터인 경우에만 필요합니다. VPC 자세한 내용은 Amazon VPC 및 Lambda 실행 역할의 리소스에 아웃바운드 네트워킹 연결을 참조하십시오.

```
        {
            "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"
                }

            ]
        }
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. TroubleshootOpenSearchRedYellowCluster콘솔에서 AWSSupport-로 이동하십시오. AWS Systems Manager
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터의 경우, 다음 내용을 입력합니다.
   - AutomationAssumeRole (선택 사항):

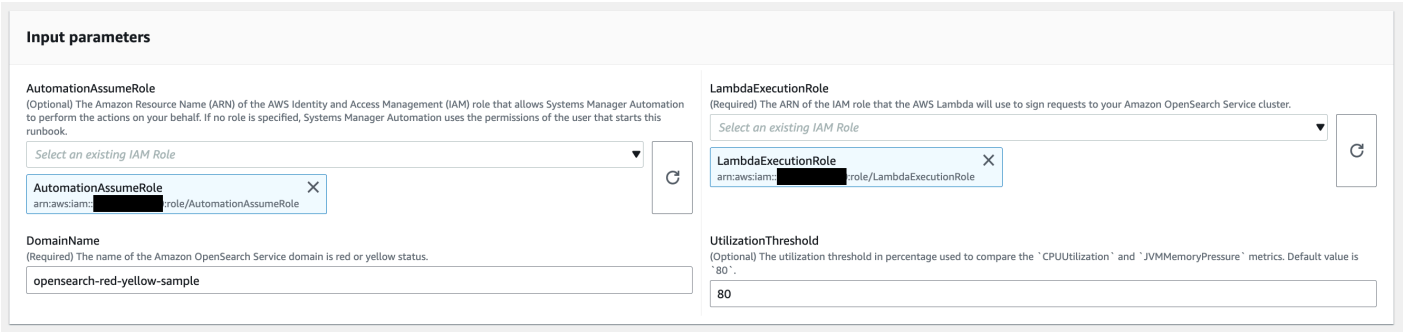
     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
   - LambdaExecutionRole (필수):

     Lambda가 Amazon OpenSearch 서비스 클러스터에 대한 요청에 서명하는 데 사용할 IAM 역할. ARN
   - DomainName (필수):

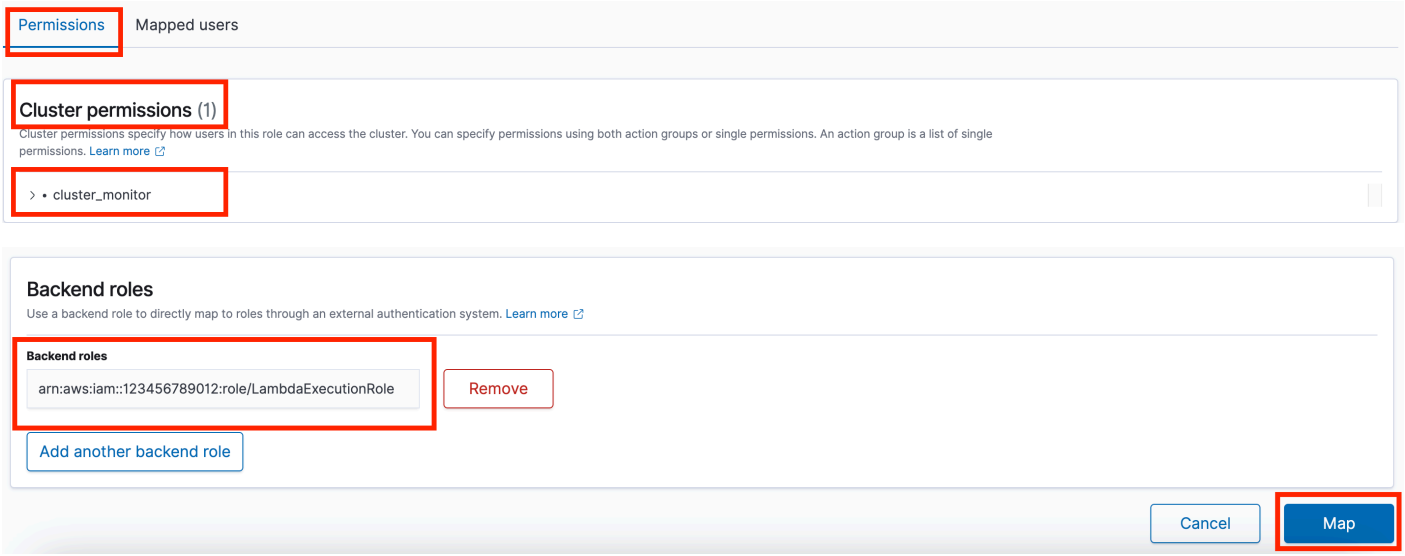
     빨간색 또는 노란색 클러스터 상태가 있는 OpenSearch 서비스 도메인의 이름.

- UtilizationThreshold (선택 사항):

  CPUUtilization및 JVMMemoryPressure 지표를 비교하는 데 사용되는 사용률 임계값 백분율. 기본값은 80입니다.



4. OpenSearch 서비스 클러스터에서 세분화된 액세스 제어를 활성화한 경우, `LambdaExecutionRole` 역할 arn이 최소한 권한이 있는 역할에 매핑되었는지 확인하세요. `cluster_monitor`



5. 실행을 선택합니다.
6. 자동화가 시작됩니다.
7. 자동화 실행서는 다음 단계를 수행합니다.
   - GetClusterConfiguration:

     서비스 클러스터 구성을 가져옵니다. OpenSearch
   - C: reateAWSLambda FunctionStack

     를 사용하여 계정에 임시 Lambda 함수를 생성합니다. AWS CloudFormation Lambda 함수는 서비스를 실행하는 데 사용됩니다. OpenSearch APIs

- WaitForAWSLambdaFunctionStack:

  CloudFormation 스택이 완료될 때까지 기다립니다.

- GetClusterMetricsFromCloudWatch:

  Amazon CloudWatch ClusterStatusCPUUtilization, 및 JVMMemoryPressure OpenSearch Service 클러스터 관련 지표와 생성 날짜를 가져옵니다.

- RunOpenSearchAPIs:

  Lambda 함수를 사용하여 APIs 서비스를 OpenSearch 호출하고 클러스터 지표 데이터를 분석하여 빨간색 또는 노란색 클러스터 상태의 원인을 진단합니다.

- D: eleteAWSLambda FunctionStack

  계정에서 이 자동화로 생성된 Lambda 함수를 삭제합니다.

8. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.

   - RootCause:

     클러스터 상태가 빨간색 또는 노란색 상태인 식별된 원인의 개요를 제공합니다.

   - IssueDescription:

     클러스터가 빨간색 또는 노란색 상태인 이유와 클러스터를 녹색 상태로 되돌릴 수 있는 방법에 대한 세부 정보를 제공합니다.

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 설명서

- 자세한 내용은 Amazon OpenSearch 서비스 문제 해결을 참조하십시오.

AWSSupport-TroubleshootOpenSearchHighCPU

설명

AWSSupport-TroubleshootOpenSearchHighCPU런북은 Amazon OpenSearch Service 도메인에서 진단 데이터를 수집하여 심각한 문제를 해결하는 자동화된 솔루션을 제공합니다. CPU

어떻게 작동하나요?

AWSSupport-TroubleshootOpenSearchHighCPU런북은 Amazon OpenSearch Service 도메인의 높은 CPU 사용률 문제를 해결하는 데 도움이 됩니다.

런북은 다음 단계를 수행합니다.

- 제공된 Amazon OpenSearch Service 도메인에 DescribeDomainAPI대해 를 실행하여 클러스터 메타데이터를 가져옵니다.
- Amazon OpenSearch 서비스 도메인이 퍼블릭 기반인지 Amazon VPC 기반인지 확인하고 의 AWS CloudFormation도움을 받아 퍼블릭 또는 Amazon VPC 기반 AWS Lambda 함수를 생성합니다.
- Lambda 함수는 Amazon 서비스 도메인에서 진단 데이터를 가져옵니다. OpenSearch
- AWS Step Functions 상태 머신을 사용하여 여러 Lambda 함수 실행을 오케스트레이션하여 보다 포괄적인 데이터를 수집합니다.
- 수집된 데이터를 Amazon CloudWatch 로그 그룹에 기본적으로 24시간 동안 저장합니다.
- CloudWatch 로그 그룹을 제외하고 생성된 리소스를 삭제합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

필수 권한 IAM

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- 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`

런북을 성공적으로 사용하려면 `LambdaExecutionRole` 파라미터에 다음 작업이 필요합니다.

- `es:ESHttpGet`
- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DeleteNetworkInterface`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Lambda 실행 역할은 이 런북에 필요한 서비스 및 리소스에 AWS 액세스할 수 있는 권한을 함수에 부여합니다. 자세한 내용을 알아보려면 Lambda 실행 역할을 참조하세요.

> **Note**
>
> `ec2:DescribeNetworkInterfaces`,`ec2:CreateNetworkInterface`, 및 `ec2:DeleteNetworkInterface` 는 Lambda 함수가 Amazon 네트워크 인터페이스를 생성하고 관리할 수 있도록 Amazon VPC 기반 OpenSearch 서비스 클러스터인 경우에만 필요합니다. VPC 자세한 내용은 Amazon VPC 및 Lambda 실행 역할의 리소스에 아웃바운드 네트워킹 연결을 참조하십시오.

지침

다음 단계에 따라 자동화를 구성합니다.

1. TroubleshootOpenSearchHighCPU콘솔에서 AWSSupport-로 이동하십시오. AWS Systems Manager
2. Execute automation(자동화 실행)을 선택합니다.

3. 입력 파라미터의 경우, 다음 내용을 입력합니다.
   - AutomationAssumeRole (선택 사항):

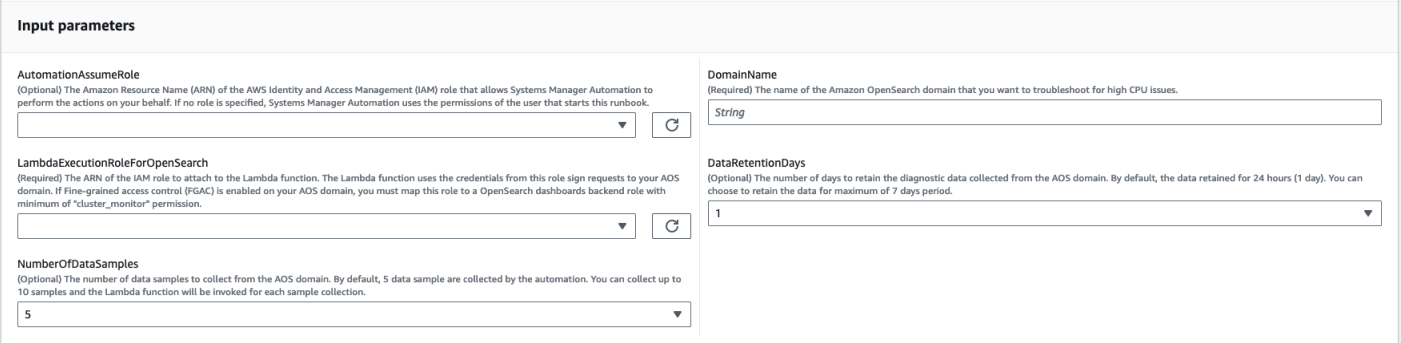
     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 () ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
   - DomainName (필수):

     심각한 CPU 문제로 문제를 해결하려는 Amazon OpenSearch 서비스 도메인의 이름.
   - LambdaExecutionRoleForOpenSearch(필수):

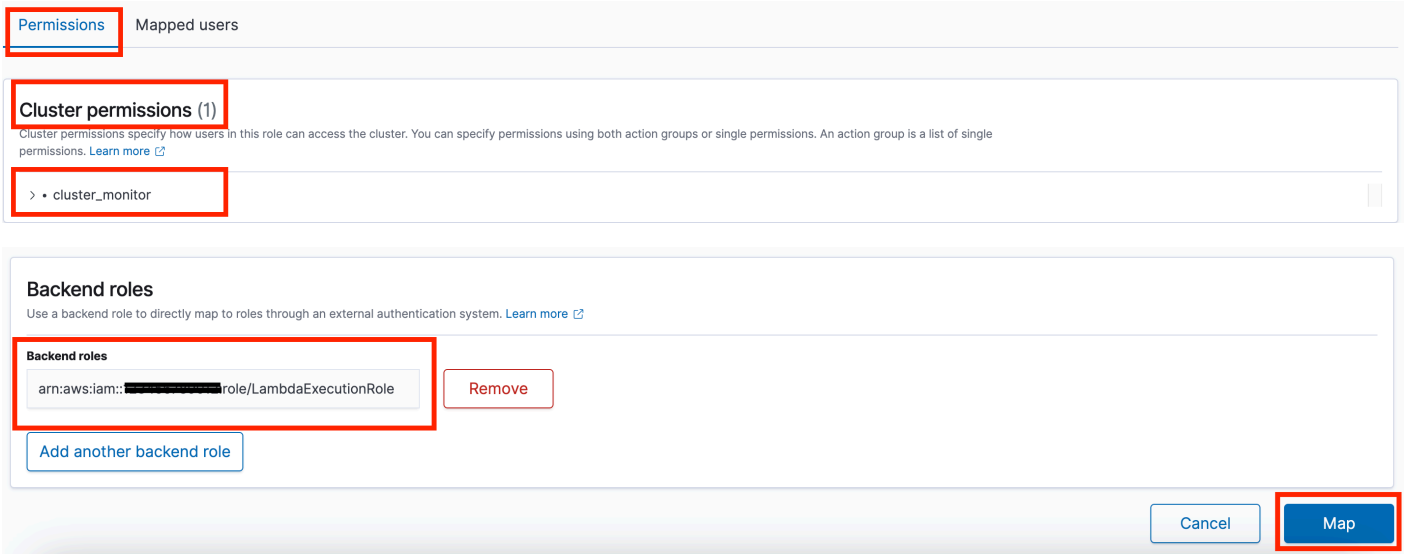
     Lambda 함수에 연결할 IAM 역할의 이름입니다. ARN Lambda 함수는 이 역할의 자격 증명을 사용하여 Amazon OpenSearch 서비스 도메인에 대한 요청에 서명합니다. Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화된 경우, 최소 “cluster_monitor” 권한을 가진 OpenSearch 서비스 대시보드 백엔드 역할에 이 역할을 매핑해야 합니다.
   - DataRetentionDays (선택 사항):

     Amazon OpenSearch 서비스 도메인에서 수집한 진단 데이터를 보관하는 기간 (일). 기본적으로 데이터는 24시간 (1일) 동안 보관됩니다. 데이터를 최대 30일 동안 보존하도록 선택할 수 있습니다.
   - NumberOfDataSamples (선택 사항):

     Amazon OpenSearch 서비스 도메인에서 수집할 데이터 샘플 수. 기본적으로 5개의 데이터 샘플이 수집됩니다. 최대 10개의 샘플을 수집할 수 있으며 각 샘플 수집에 대해 Lambda 함수가 호출됩니다.



4. OpenSearch 서비스 클러스터에서 세분화된 액세스 제어를 활성화한 경우, `LambdaExecutionRole` 역할 arn이 최소한 권한이 있는 역할에 매핑되었는지 확인하십시오. `cluster_monitor`



5. 실행을 선택합니다.
6. 자동화가 시작됩니다.
7. 자동화 실행서는 다음 단계를 수행합니다.
   - checkConcurrency:

     지정된 Amazon OpenSearch Service 도메인을 대상으로 하는 이 런북이 한 번만 실행되도록 합니다. Runbook에서 동일한 도메인 이름을 대상으로 하는 다른 실행을 발견하면 오류가 반환되고 종료됩니다.
   - getDomainConfig:

     대상 OpenSearch 서비스 도메인의 구성 세부 정보를 가져옵니다.
   - provisionResources:

     를 사용하여 데이터를 수집할 수 있도록 리소스를 AWS CloudFormation프로비저닝합니다.
   - waitForStack생성:

     AWS CloudFormation 스택이 완료될 때까지 기다립니다.
   - describeStackResources:

     AWS CloudFormation 스택을 설명하고 상태 머신의 정보를 가져옵니다. ARN
   - runStateMachine:

     Step Functions 상태 머신을 실행하여 데이터 수집기 Lambda 함수를 한 번 이상 호출합니다.
   - describeErrorsFromStackEvents:

AWS CloudFormation 스택의 오류에 대한 설명을 제공합니다.

- unstageOpenSearchHighCPUAutomation:

  `AWSSupport-TroubleshootOpenSearchHighCPU` AWS CloudFormation 스택을 삭제합니다.

- describeErrorsFromStackDeletion:

  스택을 삭제하는 동안 발생한 오류에 AWS CloudFormation 대해 설명합니다.

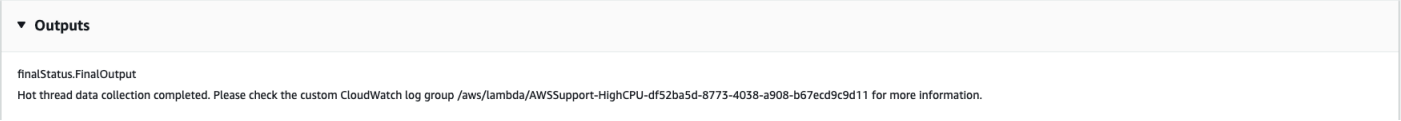
- finalStatus:

  `AWSSupport-TroubleshootOpenSearchHighCPU`런북의 최종 출력을 반환합니다.

8. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.

   - finalStatus.FinalOutput:

     진단 데이터가 저장되는 CloudWatch 로그 그룹을 제공합니다.



참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 설명서

- 자세한 내용은 Amazon OpenSearch 서비스 문제 해결을 참조하십시오.

EventBridge

AWS Systems Manager 자동화는 Amazon 에 사전 정의된 실행서를 제공합니다 EventBridge. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-AddOpsItemDedupStringToEventBridgeRule
- AWS-DisableEventBridgeRule

AWS-AddOpsItemDedupStringToEventBridgeRule

설명

`AWS-AddOpsItemDedupStringToEventBridgeRule` 실행서는 Amazon EventBridge 규칙과 AWS Systems Manager OpsItems 연결된 모든 에 대한 중복 제거 문자열을 추가합니다. 규칙에 이미 적용된 경우, 이 실행서는 중복 제거 문자열을 추가하지 않습니다. 중복 제거 문자열 및 에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 중복 감소를 OpsItems참조하세요. OpsItems

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- DedupString

  유형: 문자열

  설명: (필수) 규칙에 추가하려는 중복 제거 문자열입니다.

- RuleName

  유형: 문자열

  설명: (필수) 중복 제거 문자열을 추가하려는 규칙의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:ListTargetsByRule`
- `events:PutTargets`

문서 단계

- `aws:executeScript` - `RuleName` 파라미터에서 EventBridge 지정한 규칙에 중복 제거 문자열을 추가합니다.

AWS-DisableEventBridgeRule

설명

`AWS-DisableEventBridgeRule` 실행서는 specify.To 사용자가 사용하는 Amazon EventBridge 규칙을 비활성화합니다. EventBridge 규칙에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 규칙을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- EventBusName

  유형: 문자열

  기본값: default

  설명: (선택 사항) 비활성화하려는 규칙과 연결된 이벤트 버스입니다.

- RuleName

  유형: 문자열

  설명: (필수) 비활성화하려는 규칙의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `events:DisableRule`

문서 단계

- `aws:executeAwsApi` - `RuleName` 파라미터에 지정한 EventBridge 규칙을 비활성화합니다.

AWS Glue

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Glue. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-TroubleshootGlueConnection

AWSSupport-TroubleshootGlueConnection

설명

AWSSupport-TroubleshootGlueConnections 실행서는 AWS Glue 연결 문제를 해결하는 데 도움이 됩니다. 테스트된 연결의 대상은 JDBC 연결을 통해 도달해야 하며 Amazon Relational Database Service(Amazon RDS) 클러스터/인스턴스, 클러스터 또는 를 통해 액세스할 수 있는 기타 대상일 수 있습니다JDBC. 처음 두 경우에서는 Reachability Analyzer 도구를 사용하여 소스(AWS Glue)와 대상(Amazon RDS 또는 Amazon Redshift) 간의 연결이 부여되었는지 확인합니다.

연결 대상이 Amazon RDS 또는 Amazon Redshift가 아닌 경우에도 연결과 동일한 서브넷(네트워크 존재 지점)에서 AWS Lambda 함수를 생성하고 대상 이름을 확인할 수 있는지, 대상 포트에서 연결할 수 있는지 확인하여 AWS Glue 연결을 테스트합니다.

> **Important**
>
> Reachability Analyzer 검사를 실행하기 위해 각 연결의 데이터 소스 서브넷에 탄력적 네트워크 인터페이스가 생성됩니다. 이 자동화를 실행하기 전에 해당 서브넷IPs에 충분한 여유 공간이 있고 하나의 IP를 사용하더라도 워크로드에 영향을 주지 않는지 확인하세요.

> **Important**
>
> 이 자동화에서 생성된 모든 리소스에는 태그를 지정하여 쉽게 찾을 수 있습니다. 사용되는 태그는 다음과 같습니다.
>
> - `AWSSupport-TroubleshootGlueConnection`: true
> - `AutomationExecutionId`: *Amazon EC2 Systems Manager Execution Id*

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- AWS Glue 연결 확인을 위한 소스 정보(서브넷 및 보안 그룹)를 가져오는 연결을 설명합니다.
- 에 참조된 데이터 소스 또는 `DatasourceSecurityGroups` 및 `DatasourceSubnets` 파라미터가 있는 경우 JDBC URL 해당 파라미터에서 대상 정보(서브넷 및 보안 그룹)를 가져옵니다.
- 에 있는 데이터 소스JDBCURL가 Amazon RDS 인스턴스 또는 클러스터이거나 Amazon Redshift 클러스터인 경우 이 자동화는 이전 단계에서 수집된 소스 및 대상 정보를 모두 ENIs 사용하여 를 생성하고 Reachability Analyzer를 사용하여 이들 간에 연결 확인을 수행합니다.
- Lambda 함수(이 자동화의 맥락에서 네트워크 존재 지점)는 L4 연결 및 이름 확인 검사를 수행하는 데 사용됩니다.
- 동일한 Lambda 함수를 사용하여 Amazon S3 엔드포인트에 대한 검사를 수행합니다.
- 정책 시뮬레이터는 연결에 사용되는 IAM 역할에 필요한 권한이 있는지 확인하는 데 사용됩니다.
- 자동화는 연결에 사용되는 보안 그룹에 예상 구성이 있는지 확인합니다.
- 테스트 연결 작업 실패의 가능한 원인 및/또는 수행된 성공한 테스트가 포함된 보고서가 생성됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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**
>
> 위에서 언급한 작업 외에도 Reachability Analyzer 테스트가 성공적으로 수행되도록 에는 AmazonVPCReachabilityAnalyzerFullAccessPolicy가 연결된 관리형 정책으로 `AutomationAssumeRole` 있어야 합니다.

다음은 에 부여할 수 있는 정책의 예입니다`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"
                }
            }
```

```
        }
    ]
}
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager`AWSSupport-TroubleshootGlueConnection`의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 AWS AWS Identity and Access Management 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 Amazon 리소스 이름(IAM)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - TestConnectionRole (필수)

     연결 테스트 중에 사용되는 IAM 역할의 Amazon 리소스 이름(ARN)입니다.
   - ConnectionName (필수)

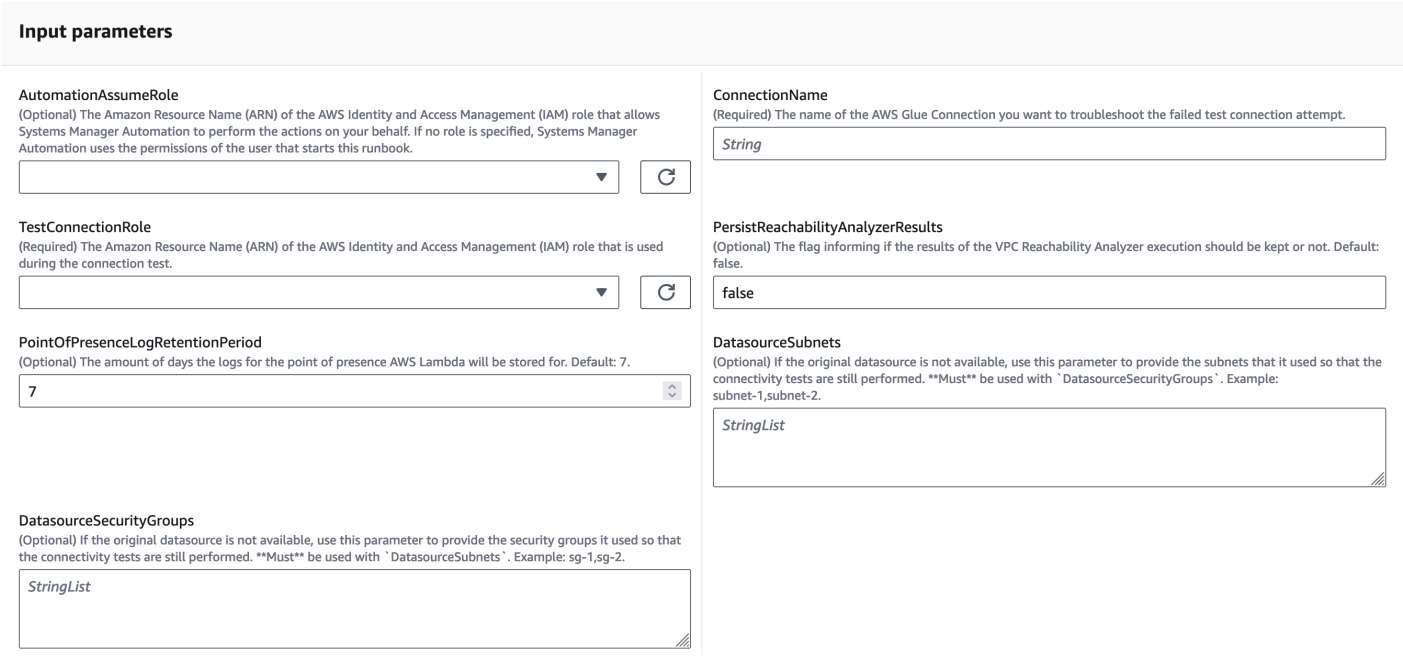
     AWS Glue 문제를 해결하려는 테스트 연결 이름이 실패했습니다.
   - PersistReachabilityAnalyzerResults (선택 사항)

     Reachability Analyzer 실행 결과를 유지해야 하는지 여부를 알려주는 플래그입니다. 기본값: `false.`
   - PointOfPresenceLogRetentionPeriod (선택 사항)

     현재 위치 Lambda의 로그가 저장되는 일수입니다. 기본값: 7.
   - DatasourceSubnets (선택 사항)

     원본 데이터 소스를 사용할 수 없는 경우 이 파라미터를 사용하여 연결 테스트가 계속 수행되도록 사용한 서브넷을 제공합니다. 와 함께 사용해야 합니다`DatasourceSecurityGroups`. 예: `subnet-1,subnet-2`.
   - DatasourceSecurityGroups (선택 사항)

원본 데이터 소스를 사용할 수 없는 경우 이 파라미터를 사용하여 연결 테스트가 계속 수행되도록 사용한 보안 그룹을 제공합니다. 와 함께 사용해야 합니다`DatasourceSubnets`. 예: `sg-1,sg-2`.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 자동화 실행서는 다음 단계를 수행합니다.
   - ParseInputs:

     이 단계에서는 입력의 조합을 검증합니다. `DatasourceSecurityGroups` 및 `DatasourceSubnets`가 모두 제공되는 경우 유효하며 그대로 반환됩니다. 아무 것도 제공되지 않으면 두 개의 빈 목록이 반환됩니다. 이 중 하나만 제공되면 단계가 를 올립니다`ValueException`.
   - GetConnectionDetails:

     이 단계에서는 제공된 AWS Glue 연결의 세부 정보를 반환합니다.
   - ParseSecurityGroupList:

     이 단계는 향후 이 자동화에서 사용할 `String` 수 있도록 `SecurityGroupIdList`의 를 연결하는 데 사용됩니다.
   - GetConnectionData:

URL, JDBC `RedShiftRdsInstance`, 사이의 연결 유형을 에 따라 결정합니다`RdsCluster0ther`. 또한 는 JDBC 연결에 사용되는 도메인 및 포트, 연결의 Amazon VPC 및 해당 도메인 이름 서버를 반환합니다.

- GetNetworkDetails:

  Amazon RDS 또는 Amazon Redshift 대상에서 서브넷 및 보안 그룹 정보를 가져옵니다.

- C reateENITemplate:

  연결을 테스트하는 데 사용되는 네트워크 인터페이스를 생성하는 데 사용되는 AWS CloudFormation 템플릿을 생성합니다. 이는 Reachability Analyzer 도구를 실행하는 데 필요합니다.

- C reateENIStack:

  이전 단계에서 생성된 템플릿에서 AWS CloudFormation 스택을 생성합니다.

- GetStackDetails:

  이전 AWS CloudFormation 스택에서 생성된 스택을 설명하고 `SourceNetworkInterface` `TargetNetworkInterfaces` 정보를 검색합니다.

- RunSourceToTargetCheck:

  Reachability Analyzer 도구를 사용하여 이전 단계에서 ENIs 생성된 소스와 대상 간에 검사를 실행합니다.

- D eleteENIStack:

  네트워크 인터페이스를 생성하는 AWS CloudFormation 스택을 삭제합니다.

- CreateNetworkPointOfPresence:

  AWS CloudFormation 는 네트워크 존재 지점으로 사용되는 Lambda 함수를 생성합니다.

- GetFunctionName:

  AWS CloudFormation 설명 스택 API 호출을 수행하여 이전 단계에서 생성된 Lambda 함수의 이름을 검색합니다.

- RunEndpointChecks:

  네트워크 존재 지점을 사용하여 JDBC 연결에 있는 엔드포인트가 선언된 포트에서 확인 가능하고 도달할 수 있는지 확인합니다.

- CheckS3Connectivity :

Amazon S3 서비스에 대한 AWS Glue 연결에서 네트워크 연결을 확인합니다.

- DeletePointOfPresence:

  Lambda의 네트워크 존재 지점을 생성하는 AWS CloudFormation 스택을 삭제합니다.

- T estIAMRole권한:

  테스트에 사용되는 IAM 역할에 이를 실행하는 데 필요한 권한이 있는지 확인합니다.

- CheckConnectionSecurityGroupReferencingRule:

  AWS Glue 연결에 사용되는 보안 그룹이 자체적으로 모든 수신 트래픽을 허용하는지 확인합니다. 이 규칙이 없는 경우 보안 그룹 목록이 반환됩니다.

- GenerateReport:

  결과 목록(연결 테스트 실패의 가능한 이유)과 다음 단계(연결 테스트 실패 해결 시도)가 포함된 보고서를 생성합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- 자동화 결과

  이 섹션에서는 테스트 연결 작업이 실패할 수 있는 원인(결과)과 이를 해결하는 방법(다음 단계)을 설명하는 시나리오를 찾을 수 있습니다. 자동화에서 테스트 실패의 원인을 찾을 수 없는 경우 이 단원에서도 이를 확인할 수 있습니다.

- 성공적인 테스트

  이 섹션에서는 이 자동화에서 성공적으로 테스트한 내용을 알려주는 시나리오를 찾을 수 있습니다. 성공한 테스트는 테스트 연결 장애의 원인을 식별할 수 없는 경우 문제의 원인이 아닌 것을 알려 조사 범위를 줄일 수 있으므로 유용합니다.

- 자동화 오류

  이 섹션에서는 자동화 중에 발생한 문제를 설명하는 시나리오를 찾을 수 있습니다. 이 시나리오는 자동화가 수행할 수 있는 테스트 수를 제한했을 수 있습니다. 시나리오에 대한 설명은 실패한 단계를 알려줍니다.

```
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.
```

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

Amazon FSx

AWS Systems Manager 자동화는 Amazon 에 사전 정의된 실행서를 제공합니다FSx. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-ValidateFSxWindowsADConfig

AWSSupport-ValidateFSxWindowsADConfig

설명

AWSSupport-ValidateFSxWindowsADConfig런북은 Windows 파일 FSx 서버용 Amazon의 자체 관리형 Active Directory (AD) 구성을 검증하는 데 사용됩니다.

어떻게 작동하나요?

런북은 Amazon 서브넷의 런북에서 시작한 임시 Amazon Elastic Compute Cloud EC2 (Amazon) Windows 인스턴스에서 Amazon FSx 검증 스크립트를 AWSSupport-ValidateFSxWindowsADConfig 실행합니다. FSx 스크립트는 여러 검사를 수행하여 자체 관리형 AD/ DNS 서버에 대한 네트워크 연결과 Amazon FSx 서비스 계정의 권한을 검증합니다. 런북은 실패하거나 잘못 구성된 FSx Windows용 Amazon 파일 서버의 유효성을 검사하거나 자체 관리형 AD를 사용하여 FSx Windows용 Amazon 파일 서버를 새로 만들 수 있습니다.

기본적으로 런북은 Amazon FSx 서브넷에서 Amazon EC2 Windows 인스턴스, AWS Systems Manager (SSM) 액세스를 위한 보안 그룹, AWS Identity and Access Management (IAM) 역할 및 정책을 생성합니다. AWS CloudFormation 기존 Amazon EC2 인스턴스에서 스크립트를 실행하려면 파라미터에 ID를 제공하십시오InstanceId. 실행에 성공하면 CloudFormation 리소스가 삭제됩니다. 하지만 리소스를 유지하려면 RetainCloudFormationStack true 파라미터를 로 설정하십시오.

CloudFormation 템플릿은 Amazon FSx 검증 스크립트를 실행하기 위해 Amazon EC2 인스턴스에 연결하는 데 필요한 권한을 가진 IAM 역할을 사용자 대신 생성합니다. 임시 IAM 인스턴스의 기존 인스턴스 프로필을 지정하려면 InstanceProfileName 파라미터를 사용하십시오. 관련 IAM 역할에는 다음 권한이 포함되어야 합니다.

- ec2:DescribeSubnets및 ec2:DescribeVpcs 권한 및 Amazon 관리형 정책 AmazonSSMManagedInstanceCore
- 를 호출하여 Systems Manager로부터 Amazon FSx 서비스 계정 사용자 이름 및 암호를 가져올 수 있는 GetSecretValue API 권한입니다.
- Amazon Simple Storage Service (Amazon S3) 버킷에 스크립트 출력을 위해 객체를 넣을 수 있는 권한

사전 조건

Run Command를 사용하여 AmazonFSxADValidation SSM 스크립트를 실행하려면 임시 Amazon EC2 인스턴스가 생성되는 서브넷 (또는 InstanceId 파라미터에 제공된 기존 인스턴스) 이 AWS

Systems Manager AWS Secrets Manager,, Amazon S3 엔드포인트에 대한 액세스를 허용해야 합니다.

AWS Secrets Manager 설정

검증 스크립트는 Secrets Manager에 대한 런타임 호출을 통해 Amazon FSx 서비스 계정 사용자 이름과 암호를 검색하여 Microsoft AD 도메인에 연결합니다. AWS Secrets Manager 시크릿 생성의 단계에 따라 새 Secrets Manager 시크릿을 생성하십시오. 사용자 이름과 비밀번호가 다음과 같은 형식의 키/값 쌍을 사용하여 저장되었는지 확인하십시오. `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}"` 비밀에 대한 액세스 보안에 AWS Secrets Manager 대한 자세한 내용은 인증 및 액세스 제어를 참조하십시오.

도구에 대한 자세한 내용은 A mazonFSx ADValidation 파일의 `TROUBLESHOOTING.md` 및 `README.md` 파일을 참조하십시오.

런북 실행

Amazon FSx ID 또는 AD 파라미터를 사용하여 런북을 실행합니다. 다음은 런북 워크플로입니다.

- Amazon FSx ID에서 파라미터를 가져오거나 입력된 AD 파라미터를 사용합니다.
- SSM액세스를 위한 보안 그룹, IAM 역할 및 정책 (조건부) 을 사용하여 CloudFormation Amazon FSx 서브넷에 임시 검증 Amazon EC2 Windows 인스턴스를 생성합니다. `InstanceId`파라미터가 지정되면 해당 파라미터가 사용됩니다.
- Amazon FSx 기본 서브넷의 대상 Amazon EC2 인스턴스에서 검증 스크립트를 다운로드하고 실행합니다.
- 자동화 출력에 AD 검증 결과 코드를 제공합니다. 또한 전체 스크립트 출력이 Amazon S3 버킷에 업로드됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

Parameters

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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

자동화 역할 수임 IAM 정책에 대한 예제

```
                {
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Sid": "AllowDescribe",
                            "Effect": "Allow",
                            "Action": [
                                "ec2:DescribeSubnets",
                                "ec2:DescribeSecurityGroups",
                                "ec2:DescribeImages",
                                "ec2:DescribeInstances",
                                "ec2:DescribeLaunchTemplates",
                                "ec2:DescribeLaunchTemplateVersions",
                                "ssm:DescribeInstanceInformation",
                                "ssm:DescribeAutomationExecutions",
                                "ssm:DescribeAutomationStepExecutions",
                                "fsx:DescribeFileSystems",
                                "ds:DescribeDirectories"
                            ],
                            "Resource": "*"
                        },
                        {
                            "Sid": "CloudFormation",
                            "Effect": "Allow",
                            "Action": [
                                "cloudformation:DescribeStacks",
                                "cloudformation:DescribeStackResources",
                                "cloudformation:DescribeStackEvents",
                                "cloudformation:CreateStack",
                                "cloudformation:DeleteStack"
                            ],
                            "Resource": "arn:*:cloudformation:*:*:stack/AWSSupport-
ValidateFSxWindowsADConfig-*"
                        },
                        {
                            "Sid": "AllowCreateLaunchTemplate",
                            "Effect": "Allow",
                            "Action": [
                                "ec2:CreateLaunchTemplate",
                                "ec2:CreateTags"
                            ],
```

```
                "Resource": [
                    "arn:aws:ec2:*:*:launch-template/*"
                ]
            },
            {
                "Sid": "AllowEC2RunInstances",
                "Effect": "Allow",
                "Action": [
                    "ec2:RunInstances",
                    "ec2:CreateTags"
                ],
                "Resource": [
                    "arn:aws:ec2:*::image/*",
                    "arn:aws:ec2:*::snapshot/*",
                    "arn:aws:ec2:*:*:subnet/*",
                    "arn:aws:ec2:*:*:network-interface/*",
                    "arn:aws:ec2:*:*:security-group/*",
                    "arn:aws:ec2:*:*:key-pair/*",
                    "arn:aws:ec2:*:*:launch-template/*"
                ]
            },
            {
                "Sid": "AllowEC2RunInstancesWithTags",
                "Effect": "Allow",
                "Action": [
                    "ec2:RunInstances",
                    "ec2:CreateTags"
                ],
                "Resource": [
                    "arn:aws:ec2:*:*:instance/*",
                    "arn:aws:ec2:*:*:volume/*"
                ]
            },
            {
                "Sid": "EC2SecurityGroup",
                "Effect": "Allow",
                "Action": [
                    "ec2:CreateSecurityGroup",
                    "ec2:RevokeSecurityGroupEgress",
                    "ec2:AuthorizeSecurityGroupEgress",
                    "ec2:CreateTags"
                ],
                "Resource": [
                    "arn:*:ec2:*:*:security-group/*",
```

```
                "arn:*:ec2:*:*:vpc/*"
            ]
        },
        {
            "Sid": "EC2Remove",
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:launch-template/*",
                "arn:*:ec2:*:*:security-group/*"
            ]
        },
        {
            "Sid": "IAMInstanceProfile",
            "Effect": "Allow",
            "Action": [
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:GetInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile"
            ],
            "Resource": "arn:*:iam::*:instance-profile/*"
        },
        {
            "Sid": "IAM",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:getRolePolicy",
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:GetRole",
                "iam:TagRole"
            ],
            "Resource": "arn:*:iam::*:role/*"
```

```
                        },
                        {
                            "Sid": "SSM",
                            "Effect": "Allow",
                            "Action": [
                                "ssm:StartAutomationExecution",
                                "ssm:GetDocument",
                                "ssm:GetAutomationExecution",
                                "ssm:ListCommandInvocations",
                                "ssm:GetParameters",
                                "ssm:ListCommands",
                                "ssm:GetCommandInvocation"
                            ],
                            "Resource": "*"
                        },
                        {
                            "Sid": "SSMSendCommand",
                            "Effect": "Allow",
                            "Action": [
                                "ssm:SendCommand"
                            ],
                            "Resource": "arn:aws:ssm:*:*:document/AWS-
RunPowerShellScript"
                        },
                        {
                            "Sid": "SSMSendCommandOnlyFsxInstance",
                            "Effect": "Allow",
                            "Action": [
                                "ssm:SendCommand"
                            ],
                            "Resource": [
                                "arn:aws:ec2:*:*:instance/*"
                            ],
                            "Condition": {
                                "StringLike": {
                                    "ssm:resourceTag/CreatedBy": [
                                        "AWSSupport-ValidateFSxWindowsADConfig"
                                    ]
                                }
                            }
                        },
                        {
                            "Effect": "Allow",
                            "Action": "iam:PassRole",
```

```
                            "Resource": "*",
                            "Condition": {
                                "StringEquals": {
                                    "iam:PassedToService": [
                                        "ec2.amazonaws.com"
                                    ]
                                }
                            }
                        },
                        {
                            "Effect": "Allow",
                            "Action": [
                                "s3:GetEncryptionConfiguration",
                                "s3:GetBucketPublicAccessBlock",
                                "s3:GetAccountPublicAccessBlock",
                                "s3:GetBucketPolicyStatus",
                                "s3:GetBucketAcl",
                                "s3:GetBucketLocation"
                            ],
                            "Resource": "*"
                        }
                    ]
                }
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems `AWSSupport-ValidateFSxWindowsADConfig`Manager의 문서 아래로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 오류가 발생하거나 잘못 구성된 기존 FSx Amazon으로 자체 관리형 AD를 검증하려면 다음 매개변수를 입력하십시오.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 () ARN 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - FSxId(조건부):

FSx윈도우용 아마존 파일 서버 ID. 이는 실패하거나 잘못 구성된 기존 FSx Amazon을 검증하는 데 필요합니다.

- SecretArn (필수):

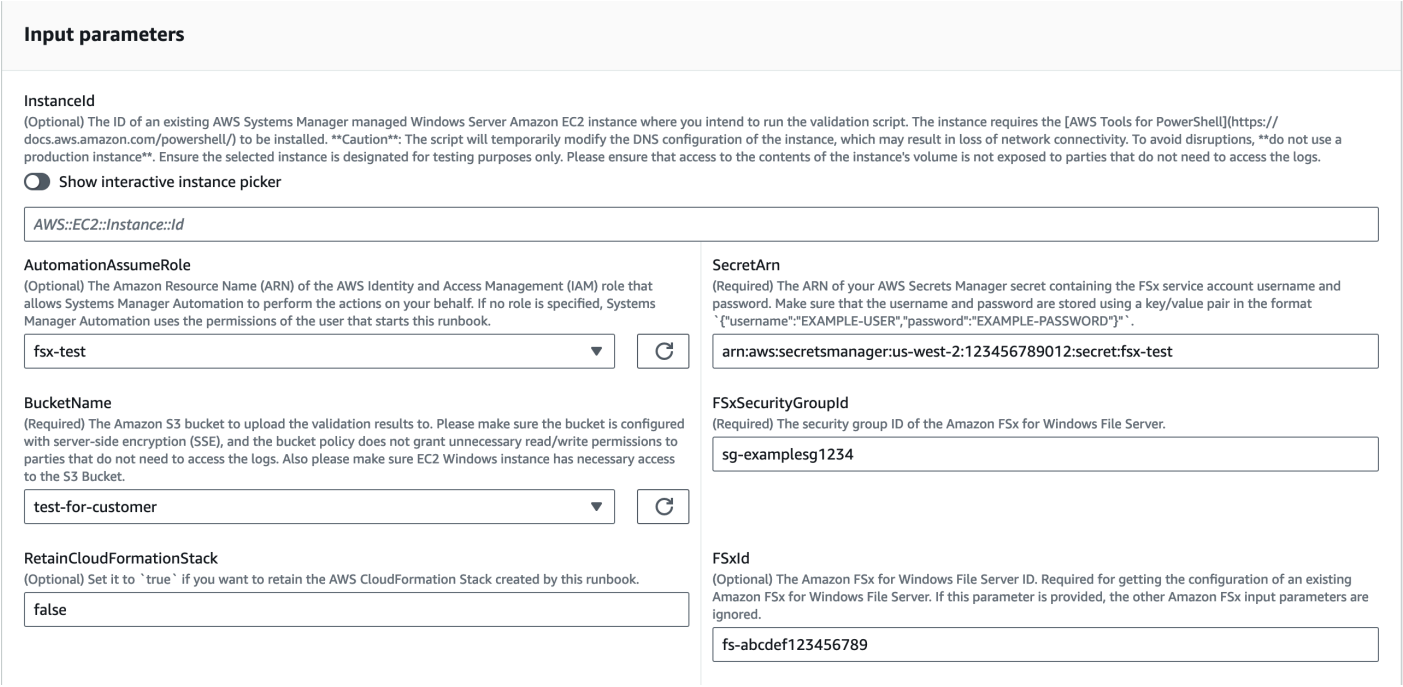
  Amazon FSx 서비스 계정 사용자 이름과 비밀번호가 포함된 Secrets Manager 시크릿의 비밀번호입니다. ARN 사용자 이름과 암호는 형식의 키/값 쌍을 사용하여 저장해야 합니다. `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}` CloudFormation 스택은 `GetSecretValue` 이를 수행할 수 있는 권한이 있는 검증 인스턴스를 생성합니다. ARN

- FSxSecurityGroupId(필수):

  FSx윈도우용 Amazon 파일 서버의 보안 그룹 ID입니다.

- BucketName (필수):

  검증 결과를 업로드할 Amazon S3 버킷입니다. 버킷이 서버 측 암호화 (SSE) 로 구성되어 있고 버킷 정책이 로그에 액세스할 필요가 없는 당사자에게 불필요한 읽기/쓰기 권한을 부여하지 않는지 확인하십시오. 또한 Amazon EC2 Windows 인스턴스에 Amazon S3 버킷에 필요한 액세스 권한이 있는지 확인하십시오.



4. 새 Amazon FSx 생성에 대한 자체 관리형 AD 구성을 검증하려면 다음 매개변수를 입력하십시오.

   - AutomationAssumeRole (선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 () ARN 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.

- SecretArn (필수):

  Amazon FSx 서비스 계정 사용자 이름과 비밀번호가 포함된 Secrets Manager 시크릿의 비밀번호입니다. ARN 사용자 이름과 암호는 형식의 키/값 쌍을 사용하여 저장해야 합니다. `{"username":"EXAMPLE-USER","password":"EXAMPLE-PASSWORD"}` CloudFormation 스택은 `GetSecretValue` 이를 수행할 수 있는 권한이 있는 검증 인스턴스를 생성합니다. ARN

- FSxSecurityGroupId(필수):

  FSx윈도우용 Amazon 파일 서버의 보안 그룹 ID입니다.

- BucketName (필수):

  검증 결과를 업로드할 Amazon S3 버킷입니다. 버킷이 서버 측 암호화 (SSE) 로 구성되어 있고 버킷 정책이 로그에 액세스할 필요가 없는 당사자에게 불필요한 읽기/쓰기 권한을 부여하지 않는지 확인하십시오. 또한 Amazon EC2 Windows 인스턴스에 Amazon S3 버킷에 필요한 액세스 권한이 있는지 확인하십시오.

- FSxPreferredSubnetId(조건부):

  FSxWindows용 Amazon 파일 서버 선호 서브넷입니다.

- DomainName (조건부):

  자체 관리형 Microsoft AD 도메인의 정규화된 도메인 이름입니다.

- DnsIpAddresses (조건부):

  자체 관리형 AD 도메인에 있는 최대 2개의 DNS 서버 또는 도메인 컨트롤러 IP 주소 목록. 최대 IPs 2개까지는 쉼표로 구분하여 입력합니다.

- FSxAdminsGroup(조건부):

  FSxWindows용 Amazon 파일 서버는 파일 시스템 관리자 그룹을 위임했습니다. 기본 이름은 `Domain Admins`입니다.

- FSxOrganizationalUnit(조건부):

  파일 시스템에 가입하려는 조직 구성 단위 (OU). OU의 고유 경로 이름을 입력합니다. 예: `OU=org,DC=example,DC=com`.

RetainCloudFormationStack
(Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.
false

TestServiceAccountPermissions
(Optional) Enable service account permission validation. This validation will create test Active Directory computer objects in the Microsoft Active Directory Organizational Unit. The resources are cleaned up by the script unless delete permissions are not properly configured on the provided service account in which case manual cleanup may be necessary.
true

DnsIpAddresses
(Conditional) A list of up to two DNS server or domain controller IP addresses in your self-managed AD domain. Required if the `FSxId` parameter is not specified. For up to two IPs, enter them separated by a comma.
10.0.1.10

FSxSecondarySubnetId
(Conditional) The Amazon FSx for Windows File Server secondary subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Optional if the `FSxId` parameter is not specified.
String

FSxOrganizationalUnit
(Conditional) The Organizational Unit (OU) within which you want to join your file system. Provide the distinguished path name of the OU. Example: `OU=org,DC=example,DC=com`. Optional if the `FSxId` parameter is not specified.
OU=testou,DC=example,DC=com

FSxId
(Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.
String

DomainName
(Conditional) The fully qualified domain name of your self-managed Microsoft Active Directory domain. Required if the `FSxId` parameter is not specified.
example.com

FSxPreferredSubnetId
(Conditional) The Amazon FSx for Windows File Server preferred subnet. Amazon FSx serves traffic from this subnet except in the event of a failover to the secondary file server. Required if the `FSxId` parameter is not specified.
subnet-test1234example

FSxAdminsGroup
(Conditional) The Amazon FSx for Windows File Server delegated file system administrators group. Optional if the `FSxId` parameter is not specified. By default, this is `Domain Admins`.
Domain Admins

InstanceKeyPairName
(Conditional) An existing Amazon EC2 key pair you want to associate to the temporary Amazon EC2 instance. Optional when the `InstanceId` parameter is not specified.
String

5. 실행을 선택합니다.
6. 자동화가 시작됩니다.
7. 문서는 다음 단계를 수행합니다.
   - CheckBucketPublicStatus(aws:executeScript):

     대상 Amazon S3 버킷이 잠재적으로 해당 객체에 대한 읽기 및/또는 쓰기 공개 액세스 권한을 부여하는지 확인합니다.
   - BranchOnInputParameters(aws:branch):

     제공된 입력 파라미터 (예: Amazon FSx ID 또는 Amazon FSx 파라미터) 를 기반으로 분기합니다.
   - AssertFileSystemTypeIsWindows(aws: assertAwsResource 속성):

     Amazon FSx ID가 제공되면 파일 시스템 유형이 FSx Windows용 Amazon 파일 서버인지 확인합니다.
   - GetValidationInputs(aws:executeScript):

     Amazon EC2 인스턴스를 생성하기 위해 CloudFormation 템플릿에 필요한 자체 관리형 Microsoft AD 구성을 반환합니다.
   - BranchOnInstanceId (aws:branch):

제공된 입력에 따른 브랜치 `InstanceId` 제공된 경우 `InstanceId` 검증 스크립트는 자동화를 통해 대상 Amazon EC2 인스턴스에서 실행됩니다`step:RunValidationScript`.

- 생성 EC2InstanceStack (aws:createStack):

  `AmazonFSxADValidation`도구가 실행될 AWS CloudFormation 위치를 사용하여 선호 서브넷에 Amazon EC2 인스턴스를 생성합니다.

- DescribeStackResources(aws:executeAwsApi):

  임시 Amazon EC2 인스턴스 ID를 가져오기 위한 CloudFormation 스택을 설명합니다.

- WaitForEC2InstanceToBeManaged(aws: waitForAwsResourceProperty):

  Run Command를 사용하여 SSM 검증 스크립트를 실행하기 위해 Systems Manager에서 Amazon EC2 인스턴스를 관리할 때까지 기다립니다.

- GetAmazonFSxADValidationAttachment(aws:executeAwsApi):

  런북 첨부 URL 파일에서 `AmazonFSxADValidation` 도구를 가져옵니다.

- RunValidationScript(aws:runCommand):

  임시 Amazon EC2 인스턴스에서 `AmazonFSxADValidation` 도구를 실행하고 `BucketName` 파라미터에 지정된 Amazon S3 버킷에 결과를 저장합니다.

- DescribeErrorsFromStackEvents(aws:executeScript):

  런북이 CloudFormation 스택을 생성하지 못하는 경우의 스택 이벤트를 설명합니다.

- BranchOnRetainCloudFormationStack(aws:branch):

  `RetainCloudFormationStack`및 `InstanceId` 파라미터를 브랜치하여 CloudFormation 스택 삭제 여부를 결정합니다.

- DeleteCloudFormationStack(aws:deleteStack):

  AWS CloudFormation 스택을 삭제합니다.

8. 완료 후 출력 섹션에서 실행 결과를 검토하십시오.

▼ **Outputs**

DescribeInstanceIdAndSubnet.InstanceId

i-06[redacted]

CreateEC2InstanceStack.CloudFormationStackId

arn:aws:cloudformation:us-east-1:3[redacted]:stack/AWSSupport-ValidateFSxWindowsADConfig-3428bd96-f8ca-4c8d-9b02-57d81560bac8/67c23cc0-3585-11ef-868f-0efb7b77b54b

RunValidationScript.Output

```
AmazonFSxADValidation tool downloaded and extracted successfully.
RSAT-AD-PowerShell installed successfully.

Running Test-FSxADConfiguration with parameters:
DomainDNSRoot: self.msf.com
DnsIpAddresses: 10.10.1.191
SubnetIds: subnet-0[redacted]
TestServiceAccountPermissions: True
TranscriptDirectory: C:\ProgramData\Amazon\AmazonFSxADValidation\3428bd96-f8ca-4c8d-9b02-57d81560bac8
AdminGroup: Domain Admins
OrganizationalUnit:

==========================================================================================
The validation details and logs can be found in the bucket test-for-customer.

ERRORS: 1
- InvalidCredentials

WARNINGS: 0

For detailed information about a given warning or error, see C:\ProgramData\Amazon\AmazonFSxADValidation\AmazonFSxADValidation\TROUBLESHOOTING.md.

==========================================================================================
The local DNS configuration has been reset successfully.
```

런북은 검증 스크립트 실행 결과를 Amazon S3 버킷에 업로드합니다.

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 설명서

- FSx윈도우용 Amazon 파일 서버란 무엇입니까?
- Windows 파일 FSx 서버용 Amazon의 자체 관리형 AD 구성 검증

GuardDuty

AWS Systems Manager 자동화는 Amazon 에 사전 정의된 실행서를 제공합니다 GuardDuty. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-CreateGuardDutyDetector

AWSConfigRemediation-CreateGuardDutyDetector

설명

`AWSConfigRemediation-CreateGuardDutyDetector` 실행서는 자동화를 실행하는 AWS 리전에 Amazon GuardDuty (GuardDuty) 탐지기를 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `guardduty:CreateDetector`
- `guardduty:GetDetector`

문서 단계

- `aws:executeAwsApi` - GuardDuty 감지기를 생성합니다.
- `aws:assertAwsResourceProperty` - 감지기의 `Status`가 `ENABLED`인지 확인합니다.

IAM

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Identity and Access Management. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-AttachIAMToInstance
- AWS-DeleteIAMInlinePolicy
- AWSConfigRemediation-DeleteIAMRole
- AWSConfigRemediation-DeleteIAMUser
- AWSConfigRemediation-DeleteUnusedIAMGroup
- AWSConfigRemediation-DeleteUnusedIAMPolicy
- AWSConfigRemediation-DetachIAMPolicy
- AWSConfigRemediation-EnableAccountAccessAnalyzer
- AWSSupport-GrantPermissionsToIAMUser
- AWSConfigRemediation-RemoveUserPolicies
- AWSConfigRemediation-ReplaceIAMInlinePolicy
- AWSConfigRemediation-RevokeUnusedIAMUserCredentials
- AWSConfigRemediation-SetIAMPasswordPolicy

`AWS-AttachIAMToInstance`

설명

AWS Identity and Access Management (IAM) 역할을 관리형 인스턴스에 연결합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ForceReplace

  타입: 부울

  설명: (선택 사항) 기존 IAM 프로파일을 교체할지 여부를 지정하는 플래그입니다.

  기본값: true
- InstanceId

  유형: 문자열

  설명: (필수) IAM 역할을 할당하려는 인스턴스의 ID입니다.
- RoleName

  유형: 문자열

  설명: (필수) 관리형 인스턴스에 추가할 IAM 역할 이름입니다.

문서 단계

1. `aws:executeAwsApi` - DescribeInstanceProfile - IAM 인스턴스에 연결된 EC2 인스턴스 프로파일을 찾습니다.
2. `aws:branch` - CheckInstanceProfileAssociations - IAM 인스턴스에 연결된 EC2 인스턴스 프로파일을 확인합니다.
   a. IAM 인스턴스 프로파일이 연결되어 있고 `true` 로 `ForceReplace` 설정된 경우:
      i. `aws:executeAwsApi` - DisassociateIamInstanceProfile - IAM 인스턴스에서 EC2 인스턴스 프로파일의 연결을 해제합니다.
   b. `aws:executeAwsApi` - ListInstanceProfilesForRole - 제공된 IAM 역할의 인스턴스 프로파일을 나열합니다.
   c. `aws:branch` - CheckInstanceProfileCreated - 제공된 IAM 역할에 연결된 인스턴스 프로파일이 있는지 확인합니다.
      i. IAM 역할에 연결된 인스턴스 프로파일이 있는 경우:
         A. `aws:executeAwsApi` - A ttachIAMProfileToInstance - IAM 인스턴스 프로필 역할을 EC2 인스턴스에 연결합니다.
      i. IAM 역할에 연결된 인스턴스 프로파일이 없는 경우:
         A. `aws:executeAwsApi` - CreateInstanceProfileForRole - 지정된 역할에 대한 인스턴스 프로파일 IAM 역할을 생성합니다.
         B. `aws:executeAwsApi` - AddRoleToInstanceProfile - 인스턴스 프로필 역할을 지정된 IAM 역할에 연결합니다.
         C. `aws:executeAwsApi` - GetInstanceProfile - 지정된 IAM 역할에 대한 인스턴스 프로파일 데이터를 가져옵니다.
         D. `aws:executeAwsApi` - A ttachIAMProfileToInstanceWithRetry - IAM 인스턴스 프로필 역할을 EC2 인스턴스에 연결합니다.

출력

A ttachIAMProfileToInstanceWithRetry.AssociationId

GetInstanceProfile.InstanceProfileName

GetInstanceProfile.InstanceProfileArn

A ttachIAMProfileToInstance.AssociationId

ListInstanceProfilesForRole.InstanceProfileName

ListInstanceProfilesForRole.InstanceProfileArn

AWS-DeleteIAMInlinePolicy

설명

`AWS-DeleteIAMInlinePolicy` 실행서는 지정한 IAM 자격 증명에 연결된 모든 AWS Identity and Access Management (IAM) 인라인 정책을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- IamArns

  유형: 문자열

  설명: (필수) 인라인 정책을 삭제할 IAM 자격 증명에 ARNs 대한 의 쉼표로 구분된 목록입니다. 이 목록에는 IAM 사용자, 그룹 또는 역할이 포함될 수 있습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `iam:DeleteGroupPolicy`
- `iam:DeleteRolePolicy`
- `iam:DeleteUserPolicy`
- `iam:ListGroupPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`

문서 단계

- `aws:executeScript` - 대상 IAM 자격 증명에 연결된 IAM 인라인 정책을 삭제합니다.

AWSConfigRemediation-DeleteIAMRole

설명

`AWSConfigRemediation-DeleteIAMRole` 런북은 지정한 (IAM) 역할을 삭제합니다 AWS Identity and Access Management . 이 자동화는 IAM 역할 또는 서비스 연결 역할과 연결된 인스턴스 프로파일을 삭제하지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- IAMRoleID

  유형: 문자열

  설명: (필수) 삭제하려는 IAM 역할의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:ListAttachedRolePolicies`
- `iam:ListInstanceProfilesForRole`
- `iam:ListRolePolicies`
- `iam:ListRoles`
- `iam:RemoveRoleFromInstanceProfile`

문서 단계

- `aws:executeScript` - `IAMRoleID` 파라미터에 지정한 IAM 역할의 이름을 수집합니다.
- `aws:executeScript` - IAM 역할과 연결된 정책 및 인스턴스 프로파일을 수집합니다.
- `aws:executeScript` - 연결된 정책을 삭제합니다.
- `aws:executeScript` - IAM 역할을 삭제하고 역할이 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteIAMUser

설명

`AWSConfigRemediation-DeleteIAMUser` 실행서는 지정한 (IAM) 사용자를 삭제합니다 AWS Identity and Access Management . 이 자동화는 IAM 사용자와 연결된 다음 리소스를 삭제하거나 분리합니다.

- 액세스 키
- 연결된 관리형 정책
- Git 보안 인증
- IAM 그룹 멤버십
- IAM 사용자 암호
- 인라인 정책
- 다중 인증(MFA) 디바이스
- 인증서 서명
- SSH 퍼블릭 키

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- IAMUserId

유형: 문자열

설명: (필수) 삭제하려는 IAM 사용자의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeScript` - `IAMUserId` 파라미터에 지정한 IAM 사용자의 사용자 이름을 수집합니다.
- `aws:executeScript` - IAM 사용자와 연결된 액세스 키, 인증서, 자격 증명, MFA 디바이스 및 SSH 키를 수집합니다.
- `aws:executeScript` - IAM 사용자의 그룹 멤버십 및 정책을 수집합니다.
- `aws:executeScript` - IAM 사용자와 연결된 액세스 키, 인증서, 자격 증명, MFA 디바이스 및 SSH 키를 삭제합니다.
- `aws:executeScript` - IAM 사용자의 그룹 멤버십 및 정책을 삭제합니다.
- `aws:executeScript` - IAM 사용자를 삭제하고 사용자가 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteUnusedIAMGroup

설명

`AWSConfigRemediation-DeleteUnusedIAMGroup` 실행서는 사용자가 포함되지 않은 IAM 그룹을 삭제합니다.

`AWSConfigRemediation-DeleteUnusedIAMGroup` 실행서는 사용자가 포함되지 않은 IAM 그룹을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- GroupName

  유형: 문자열

  설명: (필수) 삭제하려는 IAM 그룹의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteGroup`
- `iam:DeleteGroupPolicy`
- `iam:DetachGroupPolicy`

문서 단계

- `aws:executeScript` - 대상 IAM 그룹에 연결된 관리형 및 인라인 IAM 정책을 제거한 다음 IAM 그룹을 삭제합니다.

AWSConfigRemediation-DeleteUnusedIAMPolicy

설명

`AWSConfigRemediation-DeleteUnusedIAMPolicy` 실행서는 사용자, 그룹 또는 역할에 연결되지 않은 AWS Identity and Access Management (IAM) 정책을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- IAMResourceId

  유형: 문자열

  설명: (필수) 삭제하려는 IAM 정책의 리소스 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `config:ListDiscoveredResources`
- `iam:DeletePolicy`
- `iam:DeletePolicyVersion`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`
- `iam:ListPolicyVersions`

문서 단계

- `aws:executeScript` - `IAMResourceId` 파라미터에서 지정하는 정책을 삭제하고 정책이 삭제되었는지 확인합니다.

AWSConfigRemediation-DetachIAMPolicy

설명

`AWSConfigRemediation-DetachIAMPolicy` 실행서는 지정한 AWS Identity and Access Management (IAM) 정책을 분리합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- IAMResourceId

  유형: 문자열

  설명: (필수) 분리하려는 IAM 정책의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `config:ListDiscoveredResources`
- `iam:DetachGroupPolicy`
- `iam:DetachRolePolicy`
- `iam:DetachUserPolicy`
- `iam:GetPolicy`
- `iam:ListEntitiesForPolicy`

문서 단계

- `aws:executeScript` - 모든 리소스에서 IAM 정책을 분리합니다.

AWSConfigRemediation-EnableAccountAccessAnalyzer

설명

`AWSConfigRemediation-EnableAccountAccessAnalyzer` 실행서는 에 AWS Identity and Access Management (IAM) Access Analyzer를 생성합니다 AWS 계정. Access Analyzer에 대한 자세한 내용은 IAM 사용 설명서의 AWS IAM Access Analyzer 사용을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AnalyzerName

  유형: 문자열

  설명: (필수) 생성할 분석기의 이름입니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `access-analyzer:CreateAnalyzer`
- `access-analyzer:GetAnalyzer`

문서 단계

- `aws:executeAwsApi` - 계정에 대한 Access Analyzer를 생성합니다.
- `aws:waitForAwsResourceProperty` - Access Analyzer의 상태가 `ACTIVE`가 될 때까지 기다립니다.
- `aws:assertAwsResourceProperty` - Access Analyzer의 상태가 `ACTIVE`인지 확인합니다.

AWSSupport-GrantPermissionsToIAMUser

설명

이 런북은 IAM 그룹(신규 또는 기존)에 지정된 권한을 부여하고 기존 IAM 사용자를 추가합니다. 선택할 수 있는 정책은 결제 또는 지원입니다. 에 대한 결제 액세스를 활성화하려면 IAM 결제 및 비용 관리 페이지에 대한 사용자 및 페더레이션 사용자 액세스도 활성화해야 IAM합니다.

> **Important**
>
> 기존 IAM 그룹을 제공하는 경우 그룹의 모든 현재 IAM 사용자는 새 권한을 받습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- IAMGroupName

  유형: 문자열

  기본값: ExampleSupportAndBillingGroup

  설명: (필수) 신규 또는 기존 그룹일 수 있습니다. IAM 엔터티 이름 제한 을 준수해야 합니다.
- IAMUserName

  유형: 문자열

  기본값: ExampleUser

  설명: (필수) 기존 사용자여야 합니다.
- LambdaAssumeRole

  유형: 문자열

  설명: (선택 사항) lambda가 맡은 역할ARN의 입니다.
- 권한

유형: 문자열

유효한 값: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

기본값: SupportAndBillingFullAccess

설명: (필수) 다음 중 하나 선택: `SupportFullAccess`에서 지원 센터에 대한 모든 액세스 권한 부여. `BillingFullAccess`에서 결제 대시보드에 대한 모든 액세스 권한 부여. `SupportAndBillingFullAccess`에서 지원 센터 및 결제 대시보드 모두에 대해 모든 액세스 권한 부여. 문서 세부 정보의 정책에 대한 추가 정보를 참조하세요.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

필요한 `AWSSupport-GrantPermissionsToIAMUser` 권한은 실행 방식에 따라 달라집니다.

현재 로그인한 사용자 또는 역할로 실행

Lambda 함수와 Lambda에 전달할 IAM 역할을 생성할 수 있도록 `AmazonSSMAutomationRole` Amazon 관리형 정책을 연결하고 다음과 같은 추가 권한을 부여하는 것이 좋습니다.

```
{
                    "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 및 사용 LambdaAssumeRole

사용자는 실행서에 대한 ssm:StartAutomationExecution 권한과 AutomationAssumeRole 및 로 전달된 IAM 역할에 대한 iam:PassRole 권한이 있어야 합니다LambdaAssumeRole. 각 IAM 역할에 필요한 권한은 다음과 같습니다.

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

문서 단계

1. `aws:createStack` - AWS CloudFormation 템플릿을 실행하여 Lambda 함수를 생성합니다.
2. `aws:invokeLambdaFunction` - Lambda를 실행하여 IAM 권한을 설정합니다.
3. `aws:deleteStack` - CloudFormation 템플릿을 삭제합니다.

출력

IAM.Payload 구성

AWSConfigRemediation-RemoveUserPolicies

설명

`AWSConfigRemediation-RemoveUserPolicies` 실행서는 AWS Identity and Access Management (IAM) 인라인 정책을 삭제하고 지정한 사용자에게 연결된 관리형 정책을 분리합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- IAMUserID

  유형: 문자열

  설명: (필수) 정책을 제거하려는 사용자의 ID입니다.
- PolicyType

  유형: 문자열

  유효한 값: All | Inline | Managed

  기본값: All

  설명: (필수) 사용자로부터 제거할 IAM 정책의 유형입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:DeleteUserPolicy`
- `iam:DetachUserPolicy`
- `iam:ListAttachedUserPolicies`

- `iam:ListUserPolicies`
- `iam:ListUsers`

문서 단계

- `aws:executeScript` - `IAMUserID` 파라미터에 지정한 사용자로부터 IAM 정책을 삭제하고 분리합니다.

AWSConfigRemediation-ReplaceIAMInlinePolicy

설명

`AWSConfigRemediation-ReplaceIAMInlinePolicy` 실행서는 인라인 AWS Identity and Access Management (IAM) 정책을 복제된 관리IAM형 정책으로 대체합니다. 사용자, 그룹 또는 역할에 연결된 인라인 정책의 경우 인라인 정책 권한이 관리형 IAM 정책으로 복제됩니다. 관리형 IAM 정책은 리소스에 추가되고 인라인 정책은 제거됩니다. 이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- InlinePolicyName

  유형: StringList

  설명: (필수) 교체하려는 인라인 IAM 정책입니다.
- ResourceId

  유형: 문자열

  설명: (필수) 인라인 정책을 대체하려는 IAM 사용자, 그룹 또는 역할의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeScript` - 인라인 IAM 정책을 지정한 리소스의 AWS 복제된 정책으로 바꿉니다.

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

설명

AWSConfigRemediation-RevokeUnusedIAMUserCredentials 런북은 사용되지 않은 AWS Identity and Access Management (IAM) 암호와 활성 액세스 키를 취소합니다. 또한 이 런북은 만료된 액세스 키를 비활성화하고 만료된 로그인 프로파일을 삭제합니다. 이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- IAMResourceId

  유형: 문자열

  설명: (필수) 미사용 보안 인증을 취소하려는 IAM 리소스의 ID입니다.
- MaxCredentialUsageAge

  유형: 문자열

  기본값: 90

  설명: (필수) 보안 인증을 사용했어야만 하는 기간 내의 일 수입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:ListDiscoveredResources`
- `iam:DeleteAccessKey`
- `iam:DeleteLoginProfile`
- `iam:GetAccessKeyLastUsed`
- `iam:GetLoginProfile`
- `iam:GetUser`
- `iam:ListAccessKeys`
- `iam:UpdateAccessKey`

문서 단계

- `aws:executeScript` - `IAMResourceId` 파라미터에 지정된 사용자의 IAM 자격 증명을 취소합니다. 만료된 액세스 키는 비활성화되고 만료된 로그인 프로파일은 삭제됩니다.

> **Note**
>
> 이 작업을 트리거하는 데 사용하는 AWS Config 규칙의 `MaxCredentialUsageAge`파라미터와 일치하도록 이 수정 작업의 `maxAccessKeyAge` 파라미터를 구성해야 합니다access-keys-rotated.

AWSConfigRemediation-SetIAMPasswordPolicy

설명

`AWSConfigRemediation-SetIAMPasswordPolicy` 실행서는 에 대한 AWS Identity and Access Management (IAM) 사용자 암호 정책을 설정합니다 AWS 계정.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- AllowUsersToChangePassword

  타입: 부울

  기본값: false

  설명: (선택 사항) `true` 로 설정하면 의 모든 IAM 사용자가 AWS Management Console 를 사용하여 암호를 변경할 AWS 계정 수 있습니다.
- HardExpiry

  타입: 부울

  기본값: false

  설명: (선택 사항) `true` 로 설정하면 암호가 만료된 후 IAM 사용자가 암호를 재설정할 수 없습니다.
- MaxPasswordAge

  유형: 정수

  기본값: 0

  설명: (선택 사항) IAM 사용자의 암호가 유효한 일수입니다.
- MinimumPasswordLength

유형: 정수

기본값: 6

설명: (선택 사항) IAM 사용자의 암호가 될 수 있는 최소 문자 수입니다.

- PasswordReusePrevention

  유형: 정수

  기본값: 0

  설명: (선택 사항) IAM 사용자가 재사용할 수 없는 이전 암호 수입니다.

- RequireLowercaseCharacters

  타입: 부울

  기본값: false

  설명: (선택 사항) `true` 로 설정하면 IAM 사용자의 암호에 ISO 기본 라틴 알파벳(a~z)의 소문자가 포함되어야 합니다.

- RequireNumbers

  타입: 부울

  기본값: false

  설명: (선택 사항) `true` 로 설정하면 IAM 사용자의 암호에 숫자(0~9)가 포함되어야 합니다.

- RequireSymbols

  타입: 부울

  기본값: false

  설명: (선택 사항) `true` 로 설정하면 IAM 사용자의 암호에 영숫자가 아닌 문자(! @ # $ % ^ * ( ) _ + - = [ ] { } | ')가 포함되어야 합니다.

- RequireUppercaseCharacters

  타입: 부울

  기본값: false

설명: (선택 사항) `true` 로 설정하면 IAM 사용자의 암호에 ISO 기본 라틴 알파벳(A~Z)의 대문자가 포함되어야 합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:GetAccountPasswordPolicy`
- `iam:UpdateAccountPasswordPolicy`

문서 단계

- `aws:executeScript` - 의 런북 파라미터에 대해 지정한 값을 기반으로 IAM 사용자 암호 정책을 설정합니다 AWS 계정.

Amazon Kinesis Data Streams

AWS Systems Manager 자동화는 Amazon Kinesis Data Streams에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-EnableKinesisStreamEncryption

`AWS-EnableKinesisStreamEncryption`

설명

`AWS-EnableKinesisStreamEncryption`런북은 아마존 키네시스 데이터 스트림 (Kinesis Data Streams) 에서 암호화를 지원합니다. 생산자 애플리케이션이 암호화된 스트림에 기록할 때 AWS Key Management Service ()AWS KMS키에 대한 액세스 권한이 없는 경우 오류가 발생합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- KinesisStreamName

  타입: 문자열

  설명: (필수) 암호화를 활성화하려는 스트림의 이름입니다.
- KeyId

  타입: 문자열

  기본값: 별칭/AWS/키네시스

  설명: (필수) 암호화에 사용하려는 고객 관리 키입니다 AWS KMS . 이 값은 앨리어스 또는 ARN 키에 대한 글로벌 고유 식별자 또는 접두사 “alias/”가 붙은 별칭 이름일 수 있습니다. 매개변수의 기본값을 사용하여 AWS 관리 키를 사용할 수도 있습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:GetAutomationExecution`

- `ssm:StartAutomationExecution`
- `kinesis:DescribeStream`
- `kinesis:StartStreamEncryption`
- `kms:DescribeKey`

문서 단계

- VerifyKinesisStreamStatus (`aws:waitforAwsResourceProperty`) - Kinesis 데이터 스트림의 상태를 확인합니다.
- EnableKinesisStreamEncryption (`aws:executeAwsApi`) - Kinesis Data Streams의 암호화를 활성화합니다.
- VerifyKinesisStreamUpdateComplete (`aws:waitForAwsResourceProperty`) - Kinesis Data Streams 상태가 로 돌아올 때까지 기다립니다. `ACTIVE`
- VerifyKinesisStreamEncryption (`aws:assertAwsResourceProperty`) - Kinesis Data Streams에 암호화가 활성화되어 있는지 확인합니다.

AWS KMS

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Key Management Service. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-CancelKeyDeletion
- AWSConfigRemediation-EnableKeyRotation

`AWSConfigRemediation-CancelKeyDeletion`

설명

`AWSConfigRemediation-CancelKeyDeletion` 실행서는 지정한 AWS Key Management Service (AWS KMS) 고객 관리형 키의 삭제를 취소합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- KeyId

  유형: 문자열

  설명: (필수) 삭제를 취소하려는 고객 관리형 키의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CancelKeyDeletion`
- `kms:DescribeKey`

문서 단계

- `aws:executeAwsApi` - `KeyId` 파라미터에서 지정하는 고객 관리형 키의 삭제를 취소합니다.
- `aws:assertAwsResourceProperty` - 고객 관리형 키에서 키 삭제가 비활성화되었는지 확인합니다.

AWSConfigRemediation-EnableKeyRotation

설명

`AWSConfigRemediation-EnableKeyRotation` 실행서는 대칭 AWS Key Management Service (AWS KMS) 고객 관리형 키의 자동 키 교체를 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- KeyId

  유형: 문자열

  설명: (필수) 자동 키 교체를 활성화하려는 고객 관리형 키의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `kms:EnableKeyRotation`
- `kms:GetKeyRotationStatus`

문서 단계

- `aws:executeAwsApi` - `KeyId` 파라미터에서 지정하는 고객 관리형 키에 대해 자동 키 교체를 활성화합니다.
- `aws:assertAwsResourceProperty` - 고객 관리형 키에서 자동 키 교체가 활성화되었는지 확인합니다.

Lambda

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Lambda. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing
- AWSConfigRemediation-DeleteLambdaFunction
- AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK
- AWSConfigRemediation-MoveLambdaToVPC
- AWSSupport-RemediateLambdaS3Event
- AWSSupport-TroubleshootLambdaInternetAccess
- AWSSupport-TroubleshootLambdaS3Event

AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing

설명

`AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing` 런북은 `FunctionName` 파라미터에 지정한 AWS Lambda 함수에서 AWS X-Ray 라이브 추적을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- FunctionName

  유형: 문자열

  설명: (필수) 추적을 활성화할 Lambda 함수ARN의 이름 또는 입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `lambda:UpdateFunctionConfiguration`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

문서 단계

- `aws:executeAwsApi` - `FunctionName` 파라미터에서 지정하는 Lambda 함수에서 X-Ray 추적을 활성화합니다.
- `aws:assertAwsResourceProperty` - Lambda 함수에서 X-Ray 추적이 활성화되었는지 확인합니다.

출력

UpdateLambdaConfig.UpdateFunctionConfigurationResponse - `UpdateFunctionConfiguration` API 호출의 응답입니다.

`AWSConfigRemediation-DeleteLambdaFunction`

설명

`AWSConfigRemediation-DeleteLambdaFunction` 실행서는 지정하는 AWS Lambda 함수를 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- LambdaFunctionName

  유형: 문자열

  설명: (필수) 삭제하려는 Lambda 함수의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`

- `ssm:GetAutomationExecution`
- `lambda:DeleteFunction`
- `lambda:GetFunction`

문서 단계

- `aws:executeAwsApi` - `LambdaFunctionName` 파라미터에 지정된 Lambda 함수를 삭제합니다.
- `aws:executeScript` - Lambda 함수가 삭제되었는지 확인합니다.

AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK

설명

`AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK` 실행서는 AWS Key Management Service () 고객 관리형 키를 사용하여 지정한 AWS Lambda (Lambda AWS KMS) 함수의 환경 변수를 저장 상태로 암호화합니다. 이 실행서는 Lambda 함수의 환경 변수가 최소 권장 보안 모범 사례에 따라 암호화되도록 하기 위한 기준으로만 사용해야 합니다. 다양한 고객 관리형 키를 사용하여 여러 함수를 암호화하는 것이 좋습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- FunctionName

  유형: 문자열

  설명: (필수) 환경 변수를 암호화하려는 Lambda 함수ARN의 이름 또는 입니다.

- KMSKeyArn

  유형: 문자열

  설명: (필수) Lambda 함수ARN의 환경 변수를 암호화하는 데 사용할 AWS KMS 고객 관리형 키의 입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

문서 단계

- `aws:waitForAwsResourceProperty` - `LastUpdateStatus` 속성이 `Successful`(으)로 지정될 때까지 기다립니다.
- `aws:executeAwsApi` - `FunctionName` 파라미터에 지정한 AWS KMS 고객 관리형 키를 사용하여 `KMSKeyArn` 파라미터에 지정한 Lambda 함수의 환경 변수를 암호화합니다.
- `aws:assertAwsResourceProperty` - Lambda 함수의 환경 변수에서 암호화가 활성화되었는지 확인합니다.

AWSConfigRemediation-MoveLambdaToVPC

설명

`AWSConfigRemediation-MoveLambdaToVPC` 실행서는 (Lambda) 함수를 AWS Lambda Amazon Virtual Private Cloud(Amazon)로 이동합니다VPC.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- FunctionName

  유형: 문자열

  설명: (필수) Amazon 로 이동할 Lambda 함수의 이름입니다VPC.
- SecurityGroupIds

  유형: 문자열

  설명: (필수) Lambda 함수와 연결된 탄력적 네트워크 인터페이스(ENIs)에 할당IDs하려는 보안 그룹입니다.
- SubnetIds

  유형: 문자열

  설명: (필수) Lambda 함수와 연결된 탄력적 네트워크 인터페이스(ENIs)를 생성IDs하려는 서브넷입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `lambda:GetFunction`
- `lambda:GetFunctionConfiguration`
- `lambda:UpdateFunctionConfiguration`

문서 단계

- `aws:executeAwsApi` - `FunctionName` 파라미터에서 지정한 Lambda 함수에 대한 Amazon VPC 구성을 업데이트합니다.
- `aws:waitForAwsResourceProperty` - Lambda 함수 `LastUpdateStatus`(이)가 `successful`(이)가 될 때까지 기다립니다.
- `aws:executeScript` - Lambda 함수 Amazon VPC 구성이 성공적으로 업데이트되었는지 확인합니다.

AWSSupport-RemediateLambdaS3Event

설명

이 `AWSSupport-TroubleshootLambdaS3Event` 실행서는 AWS 지식 센터 문서 내 Amazon S3 이벤트 알림이 Lambda 함수를 트리거하지 않는 이유는 무엇입니까? 및 Lambda 함수를 트리거하기 위해 Amazon S3 이벤트 알림을 생성할 때 '다음 대상 구성을 검증할 수 없음'이라는 오류가 발생하는 이유는 무엇입니까?에 설명된 절차에 대한 자동 솔루션을 제공합니다. 이 런북은 Amazon Simple Storage Service(Amazon S3) 이벤트 알림이 지정한 AWS Lambda 함수를 트리거하지 못한 이유를 식별하고 해결하는 데 도움이 됩니다. 실행서 출력에서 Lambda 함수 동시성의 유효성을 검사하고 구성하도록 제안하는 경우, 비동기 호출 및 AWS Lambda 함수 크기 조정을 참조하세요.

> **Note**
>
> “다음 대상 구성을 검증할 수 없음”은 잘못된 Amazon Simple Notification Service(Amazon SNS) 및 Amazon Simple Queue Service(Amazon SQS) Amazon S3 이벤트 구성으로 인해 오류가 발생할 수도 있습니다. 이 실행서는 Lambda 함수 구성만 검사합니다. 실행서를 사용한 후

에도 '다음 대상 구성을 검증할 수 없음' 오류가 계속 표시되는 경우 기존 Amazon SNS 및 SQS Amazon S3 이벤트 구성을 검토하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- LambdaFunctionArn

  유형: 문자열

  설명: (필수) Lambda 함수ARN의 입니다.
- S3BucketName

  유형: 문자열

  설명: (필수) 이벤트 알림이 Lambda 함수를 트리거하는 Amazon S3 버킷의 이름입니다.
- 작업

  유형: 문자열

유효한 값: 문제 해결 | 해결

설명: (필수) 실행서에서 수행하려는 작업입니다. `Troubleshoot` 옵션은 문제를 식별하는 데 도움이 되지만 문제 해결을 위한 변경 작업을 수행하지는 않습니다. `Remediate` 옵션은 문제를 식별하고 해결을 시도하는 데 도움이 됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetDocument`
- `ssm:ListDocuments`
- `ssm:DescribeAutomationExecutions`
- `ssm:DescribeAutomationStepExecutions`
- `ssm:GetAutomationExecution`
- `lambda:GetPolicy`
- `lambda:AddPermission`
- `s3:GetBucketNotification`

문서 단계

- `aws:branch` - `Action` 파라미터에 대해 지정된 입력을 기반으로 분기합니다.

  지정된 값이 `Troubleshoot`인 경우:

  - `aws:executeAutomation` - `AWSSupport-TroubleshootLambdaS3Event` 실행서를 실행합니다.
  - `aws:executeAwsApi` - 이전 단계에서 실행한 `AWSSupport-TroubleshootLambdaS3Event` 실행서의 출력을 확인합니다.

  지정된 값이 `Remediate`인 경우:

  - `aws:executeScript` - 스크립트를 실행하여 Amazon S3 이벤트 알림이 Lambda 함수를 트리거하지 않는 이유는 무엇입니까? 및 Lambda 함수를 트리거하는 Amazon S3 이벤트 알림을 생성할 때 “다음 대상 구성의 유효성을 검사할 수 없습니다”라는 오류가 발생하는 이유는 무엇입니까?에 설명된 문제를 해결합니다. 지식 센터 문서.

출력

checkoutput.Output

remediatelambdas3event.Output

AWSSupport-TroubleshootLambdaInternetAccess

설명

AWSSupport-TroubleshootLambdaInternetAccess 실행서는 Amazon Virtual Private Cloud(Amazon)에서 시작된 AWS Lambda 함수의 인터넷 액세스 문제를 해결하는 데 도움이 됩니다 VPC. 서브넷 경로, 보안 그룹 규칙 및 네트워크 액세스 제어 목록(ACL) 규칙과 같은 리소스를 검토하여 아웃바운드 인터넷 액세스가 허용되는지 확인합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- FunctionName

  유형: 문자열

설명: (필수) 인터넷 액세스 문제를 해결할 Lambda 함수의 이름입니다.

- destinationIp

  유형: 문자열

  설명: (필수) 아웃바운드 연결을 설정하려는 대상 IP 주소입니다.

- destinationPort

  유형: 문자열

  기본값: 443

  설명: (선택 사항) 아웃바운드 연결을 설정하려는 대상 포트입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `lambda:GetFunction`
- `ec2:DescribeRouteTables`
- `ec2:DescribeNatGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`

문서 단계

- `aws:executeScript` - Lambda 함수가 시작된 에서 다양한 리소스VPC의 구성을 확인합니다.
- `aws:branch` - 지정된 Lambda 함수가 에 있는지 여부에 따라 분기됩니다VPC.
- `aws:executeScript` - Lambda 함수가 시작된 서브넷의 라우팅 테이블 경로를 검토하고 네트워크 주소 변환(NAT) 게이트웨이 및 인터넷 게이트웨이로의 라우팅이 있는지 확인합니다. Lambda 함수가 퍼블릭 서브넷에 있지 않음을 확인합니다.
- `aws:executeScript` - `destinationIp` 및 `destinationPort` 파라미터에 대해 지정된 값을 기반으로 Lambda 함수와 연결된 보안 그룹이 아웃바운드 인터넷 액세스를 허용하는지 확인합니다.
- `aws:executeScript` - Lambda 함수의 서브넷과 연결된 ACL 규칙을 확인하고 NAT 게이트웨이는 `destinationIp` 및 `destinationPort` 파라미터에 지정된 값을 기반으로 아웃바운드 인터넷 액세스를 허용합니다.

출력

checkVpc.vpc - Lambda 함수VPC가 시작된 의 ID입니다.

checkVpc.subnet - Lambda 함수가 시작된 서브넷IDs의 입니다.

checkVpc.securityGroups - Lambda 함수와 연결된 보안 그룹입니다.

확인 NACL.NACL - 리소스 이름이 포함된 분석 메시지입니다. 는 Lambda 함수에 대한 탄력적 네트워크 인터페이스의 프라이빗 IP 주소를 `LambdaIp` 나타냅니다. `LambdaIpRules` 객체는 NAT 게이트웨이에 대한 경로가 있는 서브넷에 대해서만 생성됩니다. 다음 콘텐츠는 출력 예제입니다.

```
{
   "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 함수와 연결된 보안 그룹에 대한 분석입니다. 다음 콘텐츠는 출력 예제입니다.

```
{
```

```
   "sg-123456789":{
      "Status":"Allowed",
      "Analysis":"This security group has allowed destintion IP and port in its
 outbuond rule."
   }
}
```

checkSubnet.subnets - Lambda 함수와 VPC 연결된 의 서브넷에 대한 분석입니다. 다음 콘텐츠는 출력 예제입니다.

```
{
   "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

설명

이 AWSSupport-TroubleshootLambdaS3Event 실행서는 AWS 지식 센터 문서 내 Amazon S3 이벤트 알림으로 인해 Lambda 함수가 트리거되지 않는 이유는 무엇입니까? 그리고 Lambda 함수를 트리거하기 위해 Amazon S3 이벤트 알림을 생성할 때 '다음 대상 구성을 검증할 수 없음'이라는 오류가 발생하는 이유는 무엇입니까? 이 런북은 Amazon Simple Storage Service(Amazon S3) 이벤트 알림이 지정한 AWS Lambda 함수를 트리거하지 못한 이유를 식별하는 데 도움이 됩니다. 실행서 출력에서 Lambda 함수 동시성의 유효성을 검사하고 구성하도록 제안하는 경우, 비동기 호출 및 AWS Lambda 함수 크기 조정을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- LambdaFunctionArn

  유형: 문자열

  설명: (필수) Amazon S3 이벤트 알림이 트리거하는 ARN Lambda 함수의 입니다.
- S3BucketName

  유형: 문자열

  설명: (필수) 이벤트 알림이 Lambda 함수를 트리거하는 Amazon S3 버킷의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `lambda:GetPolicy`
- `s3:GetBucketNotification`

문서 단계

- `aws:executeScript` - 스크립트를 실행하여 Amazon S3 이벤트 알림의 구성 설정의 유효성을 검사합니다. Lambda 함수에 대한 리소스 기반 IAM 정책을 검증하고 정책에서 필요한 권한이 누락된

경우 필요한 권한을 추가하는 AWS Command Line Interface (AWS CLI) 명령을 생성합니다. 동일한 S3 버킷에 대한 이벤트 알림의 일부인 다른 Lambda 함수 리소스 정책을 검증하고 필요한 권한이 누락된 경우 AWS CLI 명령을 출력으로 생성합니다.

출력

lambdaS3Event.output

Amazon Managed Workflows for Apache Airflow

AWS Systems Manager 자동화는 Amazon Managed Workflows for Apache Airflow에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-TroubleshootMWAAEnvironmentCreation

`AWSSupport-TroubleshootMWAAEnvironmentCreation`

설명

이 `AWSSupport-TroubleshootMWAAEnvironmentCreation` 런북은 Apache Airflow용 Amazon Managed Workflow (MWAAAmazon) 환경 생성 문제를 디버깅하는 데 필요한 정보를 제공하고, 장애를 식별하는 데 도움이 되도록 최선의 노력을 다해 문서화된 이유와 함께 점검을 수행합니다.

어떻게 작동하나요?

런북은 다음 단계를 수행합니다.

- Amazon MWAA 환경의 세부 정보를 검색합니다.
- 실행 역할 권한을 확인합니다.
- 환경에 제공된 AWS KMS 키를 로깅에 사용할 권한이 있는지, 필수 CloudWatch 로그 그룹이 존재하는지 확인합니다.
- 제공된 로그 그룹의 로그를 분석하여 오류를 찾습니다.
- 네트워크 구성을 검사하여 Amazon MWAA 환경이 필수 엔드포인트에 액세스할 수 있는지 확인합니다.
- 조사 결과가 포함된 보고서를 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

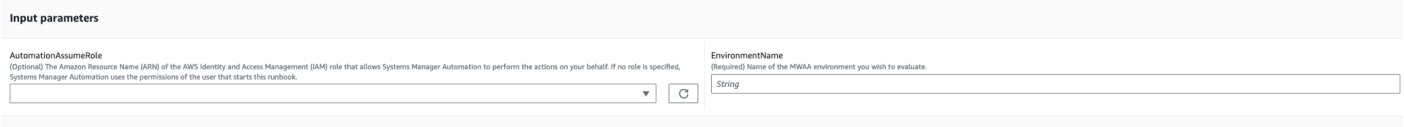
지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems `AWSSupport-TroubleshootMWAAEnvironmentCreation`Manager의 문서 아래로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - EnvironmentName (필수):

     평가하려는 Amazon MWAA 환경의 이름입니다.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - **`GetMWAAEnvironmentDetails:`**

     Amazon MWAA 환경의 세부 정보를 검색합니다. 이 단계가 실패하면 자동화 프로세스가 중단되고 다음과 같이 표시됩니다. `Failed`
   - **`CheckIAMPermissionsOnExecutionRole:`**

실행 역할에 Amazon, Amazon S3 MWAA CloudWatch, CloudWatch 로그 및 Amazon SQS 리소스에 필요한 권한이 있는지 확인합니다. 고객 관리 AWS Key Management Service (AWS KMS) 키가 감지되면 자동화가 키의 필수 권한을 검증합니다. 이 단계에서는 를 사용하여 자동화 실행 역할이 필요한 모든 권한을 충족하는지 확인합니다. `iam:SimulateCustomPolicy` API

- **`CheckKMSPolicyOnKMSKey:`**

  AWS KMS 키 정책이 Amazon MWAA 환경에서 CloudWatch 로그를 암호화하는 데 키를 사용할 수 있도록 허용하는지 확인합니다. AWS KMS 키가 AWS관리되는 경우 자동화에서는 이 검사를 건너뛰게 됩니다.

- **`CheckIfRequiredLogGroupsExists:`**

  Amazon MWAA 환경에 필요한 CloudWatch 로그 그룹이 있는지 확인합니다. 그렇지 않은 경우 자동화가 `CreateLogGroup` 및 `DeleteLogGroup` 이벤트를 확인합니다 CloudTrail . 이 단계에서는 `CreateLogGroup` 이벤트도 확인합니다.

- **`BranchOnLogGroupsFindings:`**

  Amazon MWAA 환경과 관련된 CloudWatch 로그 그룹의 존재 여부를 기반으로 하는 분기. 하나 이상의 로그 그룹이 존재하면 자동화가 해당 그룹을 파싱하여 오류를 찾습니다. 로그 그룹이 없는 경우 자동화는 다음 단계를 건너뛰습니다.

- **`CheckForErrorsInLogGroups:`**

  CloudWatch 로그 그룹을 분석하여 오류를 찾습니다.

- **`GetRequiredEndPointsDetails:`**

  Amazon 환경에서 사용하는 서비스 엔드포인트를 검색합니다. MWAA

- **`CheckNetworkConfiguration:`**

  Amazon MWAA 환경의 네트워크 구성이 보안 그룹, 네트워크ACLs, 서브넷 및 라우팅 테이블 구성에 대한 검사를 포함하여 요구 사항을 충족하는지 확인합니다.

- **`CheckEndpointsConnectivity:`**

  `AWSSupport-ConnectivityTroubleshooter`하위 자동화를 호출하여 필수 엔드포인트에 대한 MWAA Amazon의 연결을 검증합니다.

- **`CheckS3BlockPublicAccess:`**

  Amazon MWAA 환경의 Amazon S3 버킷이 `Block Public Access` 활성화되었는지 확인하고 계정의 전체 Amazon S3 퍼블릭 액세스 차단 설정도 검토합니다.

- **`GenerateReport:`**

  자동화에서 정보를 수집하고 각 단계의 결과 또는 출력을 인쇄합니다.

7. 완료 후 출력 섹션에서 실행의 세부 결과를 검토하십시오.

- Amazon MWAA 환경 실행 역할 권한 확인:

  실행 역할에 Amazon, Amazon S3 MWAA CloudWatch, CloudWatch 로그 및 Amazon SQS 리소스에 필요한 권한이 있는지 확인합니다. 고객 관리형 AWS KMS 키가 감지되면 자동화를 통해 키의 필수 권한을 검증합니다.

- Amazon MWAA 환경 AWS KMS 키 정책 확인:

  실행 역할에 Amazon, Amazon S3 MWAA CloudWatch, CloudWatch Logs 및 Amazon 리소스에 필요한 권한이 있는지 확인합니다. SQS 또한 고객 관리형 AWS KMS 키가 감지되면 자동화가 키의 필수 권한을 확인합니다.

- Amazon MWAA 환경 CloudWatch 로그 그룹 확인:

  Amazon MWAA 환경에 필요한 CloudWatch 로그 그룹이 존재하는지 확인합니다. 그렇지 않은 경우 자동화는 이벤트의 위치를 `CreateLogGroup` 확인하고 CloudTrail `DeleteLogGroup` 이벤트를 찾습니다.

- Amazon MWAA 환경 라우팅 테이블 확인:

  Amazon MWAA 환경의 Amazon VPC 라우팅 테이블이 제대로 구성되어 있는지 확인합니다.

- Amazon MWAA 환경 보안 그룹 확인:

  Amazon MWAA 환경 Amazon VPC 보안 그룹이 제대로 구성되어 있는지 확인합니다.

- Amazon MWAA 환경 네트워크 확인ACLs:

  Amazon MWAA 환경의 Amazon VPC 보안 그룹이 제대로 구성되어 있는지 확인합니다.

- Amazon MWAA 환경 서브넷 확인:

  Amazon MWAA 환경의 서브넷이 사설인지 여부를 확인합니다.

- Amazon MWAA 환경에 필요한 엔드포인트 연결 확인:

  Amazon MWAA 환경이 필요한 엔드포인트에 액세스할 수 있는지 확인합니다. 이를 위해 자동화는 자동화를 호출합니다. `AWSSupport-ConnectivityTroubleshooter`

- 아마존 MWAA 환경 아마존 S3 버킷 확인:

Amazon MWAA 환경의 Amazon S3 버킷이 `Block Public Access` 활성화되었는지 확인하고 계정의 Amazon S3 퍼블릭 액세스 차단 설정도 검토합니다.

- Amazon MWAA 환경 CloudWatch 로그 그룹 오류를 확인하는 중:

  Amazon MWAA 환경의 기존 CloudWatch 로그 그룹을 분석하여 오류를 찾습니다.

```
▾ Outputs

GenerateReport.AutomationReport
Troubleshooting report for MWAA environment

🔎 The automation found no issues with the MWAA environment configuration ✅

ℹ️ Checking the MWAA environment execution role permissions
All the required permissions for the MWAA environment execution role are in place ✅

ℹ️ Checking the MWAA environment KMS key policy
KMS key is an AWS managed key ✅

ℹ️ Checking the MWAA environment CloudWatch logs groups
The number of CloudWatch log groups found is 5 and the number of enabled log groups for the MWAA environment[redacted] is 5. This suggests that all log groups were created successfully ✅

ℹ️ Checking the MWAA environment Route Tables
NAT GW[redacted] has Internet route: subnet-[redacted] -> nat-[redacted] -> igw-[redacted] ✅
NAT GW[redacted] has Internet route: subnet-[redacted] -> nat-[redacted] -> igw-[redacted] ✅

ℹ️ Checking the MWAA environment Security Groups
Security group [redacted] has self-referencing rules for all traffic. ✅

ℹ️ Checking the MWAA environment Network ACLs
NACL: [redacted] allows port 5432 on egress ✅ and allows port 5432 on ingress ✅

ℹ️ Checking the MWAA environment Subnets
Subnet: subnet-[redacted] is private ✅
Subnet: subnet-[redacted] is private ✅

ℹ️ Checking the MWAA environment required endpoints connectivity

🧪 Testing connectivity with sqs.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and sqs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the sqs.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

🧪 Testing connectivity with api.ecr.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and api.ecr.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.ecr.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

🧪 Testing connectivity with monitoring.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and monitoring.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the monitoring.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

🧪 Testing connectivity with kms.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and kms.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the kms.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

🧪 Testing connectivity with s3.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and s3.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the s3.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

🧪 Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and env.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

🧪 Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and env.airflow.eu-west-1.amazonaws.com on port 5432 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

🧪 Testing connectivity with api.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and api.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.airflow.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

🧪 Testing connectivity with logs.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and logs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the logs.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

🧪 Testing connectivity with ops.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI [redacted] and ops.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the ops.airflow.eu-west-1.amazonaws.com service ✅
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution/[redacted]?region=eu-west-1

ℹ️ Checking the MWAA environment S3 bucket
Environment's S3 bucket and/or account block public access ✅

ℹ️ Checking the MWAA environment CloudWatch logs groups errors
Parsed log group [redacted] DAGProcessing - no errors found ✅
Parsed log group [redacted] Scheduler - no errors found ✅
Parsed log group [redacted] Task - no errors found ✅
Parsed log group [redacted] WebServer - no errors found ✅
Parsed log group [redacted] Worker - no errors found ✅
```

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행

- Automation 설정
- Support Automation Workflows 랜딩 페이지

Neptune

AWS Systems Manager 자동화는 Amazon Neptune 에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-EnableNeptuneDbAuditLogsToCloudWatch
- AWS-EnableNeptuneDbBackupRetentionPeriod
- AWS-EnableNeptuneClusterDeletionProtection

`AWS-EnableNeptuneDbAuditLogsToCloudWatch`

설명

`AWS-EnableNeptuneDbAuditLogsToCloudWatch`런북은 Amazon Neptune DB 클러스터에 대한 감사 로그를 Amazon Logs로 전송하는 데 도움이 됩니다. CloudWatch

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

타입: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- DbClusterResourceId

  타입: 문자열

  설명: (필수) 감사 로그를 활성화하려는 Neptune DB 클러스터의 리소스 ID입니다.

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

문서 단계

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Neptune DB 클러스터의 ID를 반환합니다.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Neptune DB 엔진 유형이 인지 확인합니다. `neptune`
- EnableNeptuneDbAuditLogs (`aws:executeAwsApi`) - Neptune DB 클러스터의 감사 로그를 로그로 전송할 수 있도록 합니다. CloudWatch
- VerifyNeptuneDbStatus (`aws:waitAwsResourceProperty`) - Neptune DB 클러스터 상태가 인지 확인합니다. `available`
- VerifyNeptuneDbAuditLogs (`aws:executeScript`) - 감사 로그가 Logs로 전송하도록 성공적으로 구성되었는지 확인합니다. CloudWatch

AWS-EnableNeptuneDbBackupRetentionPeriod

설명

`AWS-EnableNeptuneDbBackupRetentionPeriod`런북을 사용하면 Amazon Neptune DB 클러스터의 백업 보존 기간이 7일에서 35일 사이인 자동 백업을 활성화할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- DbClusterResourceId

  타입: 문자열

  설명: (필수) 백업을 활성화하려는 Neptune DB 클러스터의 리소스 ID입니다.
- BackupRetentionPeriod

  유형: 정수

  유효한 값: 7-35

  설명: (필수) 백업이 보존되는 일수입니다.

- PreferredBackupWindow

  타입: 문자열

  설명: (선택 사항) 매일 30분 이상 백업하는 기간입니다. 값은 협정 세계시 (UTC) 여야 하며 다음 `hh24:mm-hh24:mm` 형식을 사용해야 합니다. 백업 보존 기간은 기본 유지 관리 기간과 충돌할 수 없습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

문서 단계

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Neptune DB 클러스터의 ID를 반환합니다.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - Neptune DB 엔진 유형이 인지 확인합니다. `neptune`
- VerifyNeptuneDbStatus (`aws:waitAwsResourceProperty`) - Neptune DB 클러스터 상태가 인지 확인합니다. `available`
- ModifyNeptuneDbRetentionPeriod (`aws:executeAwsApi`) - Neptune DB 클러스터의 보존 기간을 설정합니다.
- VerifyNeptuneDbBackupsEnabled (`aws:executeScript`) - 보존 기간 및 백업 기간이 성공적으로 설정되었는지 확인합니다.

AWS-EnableNeptuneClusterDeletionProtection

설명

`AWS-EnableNeptuneClusterDeletionProtection`런북은 지정한 Amazon Neptune 클러스터에 대한 삭제 보호를 활성화합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- DbClusterResourceId

  타입: 문자열

  설명: (필수) 삭제 보호를 활성화하려는 Neptune 클러스터의 ID입니다.

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `neptune:DescribeDBCluster`
- `neptune:ModifyDBCluster`

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

문서 단계

- GetNeptuneDbClusterIdentifier (`aws:executeAwsApi`) - Neptune DB 클러스터의 ID를 반환합니다.
- VerifyNeptuneDbEngine (`aws:assertAwsResourceProperty`) - 지정된 DB 클러스터의 엔진 유형이 맞는지 확인합니다. `neptune`
- VerifyNeptuneStatus (`aws:waitForAwsResourceProperty`) - 클러스터의 상태가 인지 확인합니다. `available`
- EnableNeptuneDbDeletionProtection (`aws:executeAwsApi`) - Neptune DB 클러스터에서 삭제 보호를 활성화합니다.
- VerifyNeptuneDbDeletionProtection (`aws:assertAwsResourceProperty`) - DB 클러스터에서 삭제 방지가 활성화되어 있는지 확인합니다.

출력

- EnableNeptuneDbDeletionProtection. EnableNeptuneDbDeletionProtectionResponse - API 작업의 출력입니다.

Amazon RDS

AWS Systems Manager 자동화는 Amazon Relational Database Service 에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- 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

설명

`AWS-CreateEncryptedRdsSnapshot` 실행서는 암호화되지 않은 Amazon Relational Database Service(AmazonRDS) 인스턴스에서 암호화된 스냅샷을 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- DBInstanceIdentifier

  유형: 문자열

  설명: (필수) 스냅샷을 생성하려는 Amazon RDS 인스턴스의 ID입니다.

- DBSnapshotIdentifier

  유형: 문자열

  설명: (선택 사항) Amazon RDS 스냅샷의 이름 템플릿입니다. 기본 이름 템플릿은 입니다.*`DBInstanceIdentifier-yyyymmddhhmmss`*.

- E ncryptedDBSnapshot식별자

  유형: 문자열

  설명: (선택 사항) 암호화된 스냅샷의 이름입니다. 기본 이름은 에 추가된 `DBSnapshotIdentifier` 파라미터에 대해 지정한 값입니다`-encrypted`.

- InstanceTags

  유형: 문자열

설명: (선택 사항) DB 인스턴스에 추가할 태그입니다. (예: Key=tagKey1,Value=tagValue1,Key=tagKey2,Value=tagValue2)'

- KmsKeyId

  유형: 문자열

  기본값: `alias/aws/rds`

  설명: (선택 사항) 스냅샷을 암호화하는 데 사용할 고객 관리형 키의 , ARN키 ID 또는 키 별칭입니다.

- SnapshotTags

  유형: 문자열

  설명: (선택 사항) 스냅샷에 추가할 태그입니다. (예: Key=tagKey1,Value=tagValue1,Key=tagKey2,Value=tagValue2)'

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `rds:AddTagsToResource`
- `rds:CopyDBSnapshot`
- `rds:CreateDBSnapshot`
- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

문서 단계

- `aws:executeScript` - `DBInstanceIdentifier` 파라미터에서 지정한 DB 인스턴스의 스냅샷을 생성합니다.
- `aws:executeScript` - 이전 단계에서 생성된 스냅샷이 존재하고 인지 확인합니다`available`.
- `aws:executeScript` - 이전에 생성한 스냅샷을 암호화된 스냅샷에 복사합니다.
- `aws:executeScript` - 이전 단계에서 생성된 암호화된 스냅샷이 있는지 확인합니다.

출력

CopyRdsSnapshotToEncryptedRdsSnapshot.EncryptedSnapshotId - 암호화된 Amazon RDS 스냅샷의 ID입니다.

AWS-CreateRdsSnapshot

설명

Amazon 인스턴스에 대한 Amazon Relational Database Service(AmazonRDS) 스냅샷을 생성합니다. RDS

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- DBInstanceIdentifier

  유형: 문자열

  설명: (필수) 스냅샷을 생성할 RDS 인스턴스의 DBInstanceId ID입니다.

- DBSnapshotIdentifier

유형: 문자열

설명: (선택 사항) 생성할 RDS 스냅샷의 DBSnapshotIdentifier ID입니다.

- InstanceTags

  유형: 문자열

  설명: (선택 사항) 인스턴스에 대해 생성할 태그입니다.

- SnapshotTags

  유형: 문자열

  설명: (선택 사항) 스냅샷에 대해 생성할 태그입니다.

문서 단계

createRDSSnapshot - RDS 스냅샷을 생성하고 스냅샷 ID를 반환합니다.

verifyRDSSnapshot – 이전 단계에서 생성된 스냅샷이 존재하는지 확인합니다.

출력

createRDSSnapshot.SnapshotId – 생성된 스냅샷의 ID입니다.

AWSConfigRemediation-DeleteRDSCluster

설명

`AWSConfigRemediation-DeleteRDSCluster` 실행서는 지정한 Amazon Relational Database Service(Amazon RDS) 클러스터를 삭제합니다. 이 자동화를 AWS 리전 실행하는 에서 활성화해야 AWS Config 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DBClusterId

  유형: 문자열

  설명: (필수) 삭제 보호를 활성화하려는 DB 클러스터의 리소스 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DeleteDBCluster`
- `rds:DeleteDBInstance`
- `rds:DescribeDBClusters`

문서 단계

- `aws:executeScript` - `DBClusterId` 파라미터에서 지정하는 DB 클러스터를 삭제합니다.

AWSConfigRemediation-DeleteRDSClusterSnapshot

설명

`AWSConfigRemediation-DeleteRDSClusterSnapshot` 실행서는 지정된 Amazon Relational Database Service(AmazonRDS) 클러스터 스냅샷을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DBClusterSnapshotId

  유형: 문자열

  설명: (필수) 삭제할 Amazon RDS 클러스터 스냅샷 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBClusterSnapshot`
- `rds:DescribeDBClusterSnapshots`

문서 단계

- `aws:branch` - 클러스터 스냅샷이 `available` 상태에 있는지 확인합니다. 사용할 수 없는 경우, 흐름이 종료됩니다.
- `aws:executeAwsApi` - 데이터베이스(DB) RDS 클러스터 스냅샷 식별자를 사용하여 지정된 Amazon 클러스터 스냅샷을 삭제합니다.
- `aws:executeScript` - 지정된 Amazon RDS 클러스터 스냅샷이 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteRDSInstance

설명

`AWSConfigRemediation-DeleteRDSInstance` 실행서는 지정한 Amazon Relational Database Service(AmazonRDS) 인스턴스를 삭제합니다. 이때 데이터베이스(DB) 인스턴스를 삭제하면 해당 인스턴스의 자동 백업 파일도 모두 삭제되며 복구할 수 없습니다. 수동 DB는 삭제되지 않습니다. 삭제하려는 DB 인스턴스가 `failed`, `incompatible-network` 또는 `incompatible-restore` 상태인 경우, `SkipFinalSnapshot` 파라미터를 `true`(으)로 설정해야 합니다.

> **Note**
>
> 삭제하려는 DB 인스턴스가 Amazon Aurora DB 클러스터에 있는 경우, DB 인스턴스가 읽기 전용 복제본이고 DB 클러스터의 유일한 인스턴스라면, 실행서는 해당 DB 인스턴스를 삭제하지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- DbiResourceId

  유형: 문자열

  설명: (필수) 삭제하려는 DB 인스턴스의 리소스 식별자입니다.

- SkipFinalSnapshot

  타입: 부울

  기본값: false

  설명: (선택 사항) `true`로 설정하면, DB 인스턴스가 삭제되기 전에 최종 스냅샷이 생성되지 않습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DeleteDBInstance`
- `rds:DescribeDBInstances`

문서 단계

- `aws:executeAwsApi` - `DbiResourceId` 파라미터에서 지정하는 값에서 DB 인스턴스 이름을 수집합니다.
- `aws:branch` - `SkipFinalSnapshot` 파라미터에서 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - `DbiResourceId` 파라미터에서 지정하는 DB 인스턴스를 삭제합니다.
- `aws:executeAwsApi` - 최종 스냅샷이 생성된 후, `DbiResourceId` 파라미터에서 지정하는 DB 인스턴스를 삭제합니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스가 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteRDSInstanceSnapshot

설명

`AWSConfigRemediation-DeleteRDSInstanceSnapshot` 실행서는 지정한 Amazon Relational Database Service(AmazonRDS) 인스턴스 스냅샷을 삭제합니다. `available` 상태의 스냅샷만 삭제됩니다. 이 실행서는 Amazon Aurora 데이터베이스 인스턴스에서의 스냅샷 삭제를 지원하지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DbSnapshotId

  유형: 문자열

  설명: (필수) 삭제하려는 스냅샷의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `rds:DeleteDBSnapshot`
- `rds:DescribeDBSnapshots`

문서 단계

- `aws:executeAwsApi` - `DbSnapshotId` 파라미터에서 지정된 스냅샷의 상태를 수집합니다.
- `aws:assertAwsResourceProperty` - 스냅샷의 상태가 `available`인지 확인합니다.
- `aws:executeAwsApi` - `DbSnapshotId` 파라미터에서 지정된 스냅샷을 삭제합니다.
- `aws:executeScript` - 스냅샷이 삭제되었는지 확인합니다.

AWSConfigRemediation-DisablePublicAccessToRDSInstance

설명

`AWSConfigRemediation-DisablePublicAccessToRDSInstance` 런북은 지정한 Amazon Relational Database Service(AmazonRDS) 데이터베이스(DB) 인스턴스에 대한 퍼블릭 액세스를 비활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- DbiResourceId

  유형: 문자열

  설명: (필수) 퍼블릭 액세스를 비활성화하려는 DB 인스턴스의 리소스 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

문서 단계

- `aws:executeAwsApi` - DB 인스턴스 리소스 식별자에서 DB 인스턴스 식별자를 수집합니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스가 `AVAILABLE` 상태에 있는지 확인합니다.
- `aws:executeAwsApi` - DB 인스턴스의 퍼블릭 액세스를 비활성화합니다.
- `aws:waitForAwsResourceProperty` - DB 인스턴스가 `MODIFYING` 상태로 변경될 때까지 기다립니다.
- `aws:waitForAwsResourceProperty` - DB 인스턴스가 `AVAILABLE` 상태로 변경될 때까지 기다립니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스에서 퍼블릭 액세스가 비활성화되었는지 확인합니다.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster

설명

`AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster` 실행서는 지정한 Amazon Relational Database Service(AmazonRDS) 클러스터에서 `CopyTagsToSnapshot` 설정을 활성화합니다. 이 설정을 활성화하면 모든 태그를 DB 클러스터에서 DB 클러스터의 스냅샷으로 복사

합니다. 기본값은 복사하지 않는 것입니다. 이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- ApplyImmediately

  타입: 부울

  기본값: false

  설명: (선택 사항) 이 파라미터에 대해 `true`(을)를 지정하는 경우, DB 클러스터의 `PreferredMaintenanceWindow` 설정과 관계없이, 이 요청의 수정 사항과 보류 중인 모든 수정 사항을 비동기적으로 최대한 빨리 적용합니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- DbClusterResourceId

  유형: 문자열

  설명: (필수) `CopyTagsToSnapshot` 설정을 활성화하려는 DB 클러스터의 리소스 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

문서 단계

- `aws:executeAwsApi` - DB 클러스터 리소스 식별자에서 DB 클러스터 식별자를 수집합니다.
- `aws:assertAwsResourceProperty` - DB 클러스터가 `AVAILABLE` 상태인지 확인합니다.
- `aws:executeAwsApi` - DB 클러스터에서 `CopyTagsToSnapshot` 설정을 활성화합니다.
- `aws:assertAwsResourceProperty` - DB 클러스터에서 `CopyTagsToSnapshot` 설정이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance

설명

`AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance` 실행서는 지정한 Amazon Relational Database Service(AmazonRDS) 인스턴스에서 `CopyTagsToSnapshot` 설정을 활성화합니다. 이 설정을 활성화하면 모든 태그를 DB 인스턴스에서 DB 인스턴스의 스냅샷으로 복사합니다. 기본값은 복사하지 않는 것입니다. 이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- ApplyImmediately

  타입: 부울

  기본값: false

  설명: (선택 사항) 이 파라미터에 대해 `true`(을)를 지정하는 경우, DB 인스턴스의 `PreferredMaintenanceWindow` 설정과 관계없이, 이 요청의 수정 사항과 보류 중인 모든 수정 사항을 비동기적으로 최대한 빨리 적용합니다.
- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DbiResourceId

  유형: 문자열

  설명: (필수) 설정을 활성화하려는 DB 인스턴스의 리소스 식별자입니다.`CopyTagsToSnapshot`

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

문서 단계

- `aws:executeAwsApi` - DB 인스턴스 리소스 식별자에서 DB 인스턴스 식별자를 수집합니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스가 `AVAILABLE` 상태인지 확인합니다.
- `aws:executeAwsApi` - DB 인스턴스에서 `CopyTagsToSnapshot` 설정을 활성화합니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스에서 `CopyTagsToSnapshot` 설정이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance

설명

`AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance` 실행서는 지정한 Amazon RDS 데이터베이스 인스턴스에서 향상된 모니터링을 활성화합니다. 향상된 모니터링에 대한 자세한 내용은 Amazon RDS 사용 설명서의 향상된 모니터링을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- MonitoringInterval

유형: 정수

유효한 값: 1 | 5 | 10 | 15 | 30 | 60

설명: (필수) DB 인스턴스에서 확장 모니터링 지표가 수집되는 간격(초)입니다.

- MonitoringRoleArn

  유형: 문자열

  설명: (필수) Amazon이 향상된 모니터링 지표를 Amazon CloudWatch LogsRDS로 보낼 수 있도록 허용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다.

- ResourceId

  유형: 문자열

  설명: (필수) 확장 모니터링을 활성화하려는 DB 인스턴스의 리소스 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

문서 단계

- `aws:executeAwsApi` - DB 인스턴스 리소스 식별자에서 DB 인스턴스 식별자를 수집합니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스가 `AVAILABLE` 상태인지 확인합니다.
- `aws:executeAwsApi` - DB 인스턴스에서 확장 모니터링을 활성화합니다.
- `aws:executeScript` - DB 인스턴스에서 확장 모니터링이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS

설명

`AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS` 실행서는 지정한 Amazon RDS 데이터베이스 인스턴스에서 `AutoMinorVersionUpgrade` 설정을 활성화합니다. 이 설정을 활성화하는 것은 유지 관리 기간 동안 마이너 버전 업그레이드가 DB 인스턴스에 자동으로 적용됨을 나타냅니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- DbiResourceId

  유형: 문자열

  설명: (필수) `AutoMinorVersionUpgrade` 설정을 활성화하려는 DB 인스턴스의 리소스 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

문서 단계

- `aws:executeAwsApi` - DB 인스턴스 리소스 식별자에서 DB 인스턴스 식별자를 수집합니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스가 `AVAILABLE` 상태인지 확인합니다.
- `aws:executeAwsApi` - DB 인스턴스에서 `AutoMinorVersionUpgrade` 설정을 활성화합니다.
- `aws:executeScript` - DB 인스턴스에서 `AutoMinorVersionUpgrade` 설정이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableMultiAZOnRDSInstance

설명

`AWSConfigRemediation-EnableMultiAZOnRDSInstance` 실행서는 Amazon Relational Database Service(AmazonRDS) 데이터베이스(DB) 인스턴스를 다중 AZ 배포로 변경합니다. 이 설정을 변경해도 작동이 중단되지 않습니다. `ApplyImmediately` 파라미터를 `true`로 설정하지 않은 한, 변경 사항은 다음번 유지 관리 기간에 적용됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- ApplyImmediately

  타입: 부울

기본값: false

설명: (선택 사항) 이 파라미터에 대해 `true`(을)를 지정하는 경우, DB 인스턴스의 `PreferredMaintenanceWindow` 설정과 관계없이, 이 요청의 수정 사항과 보류 중인 모든 수정 사항을 비동기적으로 최대한 빨리 적용합니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- DbiResourceId

  유형: 문자열

  설명: (필수) `MultiAZ` 설정을 활성화하기 위한 DB 인스턴스의 AWS 리전고유하고 변경 불가능한 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

문서 단계

- `aws:executeAwsApi` - `DBInstanceId` 파라미터에서 제공된 값을 사용하여 DB 인스턴스 이름을 검색합니다.
- `aws:executeAwsApi` - `DBInstanceStatus`(이)가 `available`인지 확인합니다.
- `aws:branch` - `DbiResourceId` 파라미터에서 지정하는 DB 인스턴스에 `MultiAZ`(이)가 이미 `true`로 설정되어 있는지 확인합니다.
- `aws:executeAwsApi` - `DbiResourceId` 파라미터에서 지정하는 DB 인스턴스에서 `MultiAZ` 설정을 `true`로 변경합니다.

- `aws:assertAwsResourceProperty` - `DbiResourceId` 파라미터에서 지정하는 DB 인스턴스에 `MultiAZ`(이)가 `true`로 설정되어 있는지 확인합니다.

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

설명

`AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance` 실행서는 지정한 Amazon RDS DB 인스턴스에서 성능 개선 도우미를 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DbiResourceId

  유형: 문자열

  설명: (필수) Performance Insights를 활성화하려는 DB 인스턴스의 리소스 식별자입니다.
- PerformanceInsightsKMSKeyId

  유형: 문자열

기본값: `alias/aws/rds`

설명: (선택 사항) 잠재적으로 민감한 모든 데이터를 암호화하는 데 성능 개선 도우미가 사용할 (AWS KMS) 고객 관리형 키의 Amazon 리소스 이름 AWS Key Management Service (ARN), 키 ID 또는 키 별칭입니다. 이 파라미터의 키 별칭을 입력하는 경우 값에 **alias/** 접두사를 붙이십시오. 이 파라미터의 값을 지정하지 않으면 AWS 관리형 키 이 사용됩니다.

- PerformanceInsightsRetentionPeriod

  유형: 정수

  유효한 값: 7, 731

  기본값: 7

  설명: (선택 사항) Performance Insights 데이터를 유지하려는 일 수입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:CreateGrant`
- `kms:DescribeKey`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

문서 단계

- `aws:executeAwsApi` - DB 인스턴스 리소스 식별자에서 DB 인스턴스 식별자를 수집합니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스 상태가 `available`로 설정되어 있는지 확인합니다.
- `aws:executeAwsApi` - `PerformanceInsightsKMSKeyId` 파라미터에 지정된 AWS KMS 고객 관리형 키ARN의 를 수집합니다.
- `aws:branch` - DB 인스턴스의 `PerformanceInsightsKMSKeyId` 속성에 값이 이미 할당되었는지 확인합니다.

- `aws:executeAwsApi` - `DbiResourceId` 파라미터에서 지정하는 DB 인스턴스에서 Performance Insights를 활성화합니다.
- `aws:assertAwsResourceProperty` - `PerformanceInsightsKMSKeyId` 파라미터에 지정된 값이 DB 인스턴스의 Performance Insights 암호화를 활성화하는 데 사용되었는지 확인합니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스에서 Performance Insights가 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableRDSClusterDeletionProtection

설명

`AWSConfigRemediation-EnableRDSClusterDeletionProtection` 실행서는 지정한 Amazon Relational Database Service(Amazon RDS) 클러스터에서 삭제 방지를 활성화합니다. 이 자동화를 실행하는 AWS 리전 에서 를 활성화해야 AWS Config 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- ClusterId

  유형: 문자열

설명: (필수) 삭제 보호를 활성화하려는 DB 클러스터의 리소스 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `config:GetResourceConfigHistory`
- `rds:DescribeDBClusters`
- `rds:ModifyDBCluster`

문서 단계

- `aws:executeAwsApi` - DB 클러스터 리소스 식별자에서 DB 클러스터 이름을 수집합니다.
- `aws:assertAwsResourceProperty` - DB 클러스터 상태가 `available`인지 확인합니다.
- `aws:executeAwsApi` - `ClusterId` 파라미터에서 지정하는 DB 클러스터에서 삭제 보호를 활성화합니다.
- `aws:assertAwsResourceProperty` - DB 클러스터에서 삭제 보호가 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableRDSInstanceBackup

설명

`AWSConfigRemediation-EnableRDSInstanceBackup` 실행서는 지정한 Amazon Relational Database Service(AmazonRDS) 데이터베이스 인스턴스에 대한 백업을 활성화합니다. 이 실행서는 Amazon Aurora 데이터베이스 인스턴스에 대한 백업 활성화를 지원하지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- ApplyImmediately

  타입: 부울

  기본값: false

  설명: (선택 사항) 이 파라미터에 대해 `true`(을)를 지정하는 경우, DB 인스턴스의 `PreferredMaintenanceWindow` 설정과 관계없이, 이 요청의 수정 사항과 보류 중인 모든 수정 사항을 비동기적으로 최대한 빨리 적용합니다.
- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- BackupRetentionPeriod

  유형: 정수

  유효한 값: 1-35

  설명: (필수) 백업이 보관되는 일수입니다.
- DbiResourceId

  유형: 문자열

  설명: (필수) 백업을 활성화하려는 DB 인스턴스의 리소스 식별자입니다.
- PreferredBackupWindow

  유형: 문자열

  설명: (선택 사항) 백업이 생성되는 동안의 일일 시간 범위(에서UTC).

  제약 조건:

- `hh24:mi-hh24:mi` 형식이어야 합니다.
- 조정된 세계시(UTC)여야 합니다.
- 원하는 유지 관리 기간과 충돌하지 않아야 합니다.
- 30분 이상이어야 합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

문서 단계

- `aws:executeScript` - DB 인스턴스 리소스 식별자에서 DB 인스턴스 식별자를 수집합니다. DB 인스턴스의 백업을 활성화합니다. DB 인스턴스에서 백업이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableRDSInstanceDeletionProtection

설명

`AWSConfigRemediation-EnableRDSInstanceDeletionProtection` 실행서는 지정한 Amazon RDS 데이터베이스 인스턴스에서 삭제 방지를 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- ApplyImmediately

  타입: 부울

  기본값: false

  설명: (선택 사항) 이 파라미터에 대해 `true`(을)를 지정하는 경우, DB 인스턴스의 `PreferredMaintenanceWindow` 설정과 관계없이, 이 요청의 수정 사항과 보류 중인 모든 수정 사항을 비동기적으로 최대한 빨리 적용합니다.
- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DbInstanceResourceId

  유형: 문자열

  설명: (필수) 삭제 보호를 활성화하려는 DB 인스턴스의 리소스 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

문서 단계

- `aws:executeAwsApi` - DB 인스턴스 리소스 식별자에서 DB 인스턴스 식별자를 수집합니다.
- `aws:executeAwsApi` - DB 인스턴스에서 삭제 보호를 활성화합니다.

- `aws:assertAwsResourceProperty` - DB 인스턴스에서 삭제 보호가 활성화되었는지 확인합니다.

AWSConfigRemediation-ModifyRDSInstancePortNumber

설명

`AWSConfigRemediation-ModifyRDSInstancePortNumber` 실행서는 Amazon Relational Database Service(AmazonRDS) 인스턴스가 연결을 수락하는 포트 번호를 수정합니다. 이 자동화를 실행하면 데이터베이스가 다시 시작됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- PortNumber

  유형: 문자열

  설명: (선택 사항) DB 인스턴스가 연결을 허용할 포트 번호입니다.
- RDSDBInstanceResourceId

  유형: 문자열

설명: (필수) 인바운드 포트 번호를 수정하려는 DB 인스턴스의 리소스 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBInstances`
- `rds:ModifyDBInstance`

문서 단계

- `aws:executeAwsApi` - DB 인스턴스 리소스 식별자에서 DB 인스턴스 식별자를 수집합니다.
- `aws:assertAwsResourceProperty` - DB 인스턴스가 `AVAILABLE` 상태인지 확인합니다.
- `aws:executeAwsApi` - DB 인스턴스가 연결을 허용하는 인바운드 포트 번호를 수정합니다.
- `aws:waitForAwsResourceProperty` - DB 인스턴스가 `MODIFYING` 상태가 될 때까지 기다립니다.
- `aws:waitForAwsResourceProperty` - DB 인스턴스가 `AVAILABLE` 상태가 될 때까지 기다립니다.

AWSSupport-ModifyRDSSnapshotPermission

설명

`AWSSupport-ModifyRDSSnapshotPermission` 실행서는 여러 Amazon Relational Database Service(AmazonRDS) 스냅샷에 대한 권한을 수정하는 데 도움이 됩니다. 이 실행서를 사용하여 `Public` 또는 `Private` 스냅샷을 만들거나 다른 AWS 계정와 공유할 수 있습니다. 기본 KMS 키로 암호화된 스냅샷은 이 런북을 사용하여 다른 계정과 공유할 수 없습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- AccountIds

  유형: StringList

  기본값: 없음

  설명: (선택 사항) 스냅샷을 공유하려는 계정IDs의 입니다. `Private` 파라미터의 값에 대해 No(을)를 입력하는 경우 이 파라미터는 필수입니다.
- AccountPermissionOperation

  유형: 문자열

  유효한 값: add | remove

  기본값: 없음

  설명: (선택 사항) 수행할 작업의 유형입니다.
- 프라이빗

  유형: 문자열

  유효한 값: Yes | No

  설명: (필수) 스냅샷을 특정 계정과 공유하려는 경우 해당 값에 대해 No(을)를 입력합니다.

- SnapshotIdentifiers

  유형: StringList

  설명: (필수) 권한을 수정하려는 Amazon RDS 스냅샷의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `rds:DescribeDBSnapshots`
- `rds:ModifyDBSnapshotAttribute`

문서 단계

1. `aws:executeScript` - `SnapshotIdentifiers` 파라미터에 제공된 스냅샷IDs의 를 확인합니다. 를 확인한 후 스크립트IDs는 암호화된 스냅샷을 확인하고 검색된 경우 목록을 출력합니다.
2. `aws:branch` - `Private` 파라미터에 대해 입력하는 값을 기반으로 자동화를 분기합니다.
3. `aws:executeScript` - 지정된 스냅샷의 권한을 수정하여 지정된 계정과 해당 내용을 공유합니다.
4. `aws:executeScript` - 스냅샷의 권한을 수정하여 해당 내용을 `Public`에서 `Private`(으)로 변경합니다.

출력

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.결과

MakePrivate.결과

MakePrivate.명령

AWSPremiumSupport-PostgreSQLWorkloadReview

설명

`AWSPremiumSupport-PostgreSQLWorkloadReview` 실행서는 Amazon Relational Database Service(AmazonRDS) PostgreSQL 데이터베이스 사용 통계의 여러 스냅샷을 캡처합니다. 캡처된 통계는 AWS Support Proactive Services 전문가가 운영 검토를 수행하는 데 필요합니다. 통계는 사용자 지정 SQL 및 쉘 스크립트 세트를 사용하여 수집됩니다. 이러한 스크립트는 이 런북에서 생성된 의 임시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 다운로드 AWS 계정 됩니다. 실행서는 사용자 이름과 암호 키-값 쌍이 포함된 AWS Secrets Manager 보안 암호를 사용하여 보안 인증을 제공해야 합니다. 사용자 이름에는 표준 PostgreSQL 통계 보기 및 함수를 쿼리할 수 있는 권한이 있어야 합니다.

이 런북은 AWS CloudFormation 스택을 AWS 계정 사용하여 에 다음 AWS 리소스를 자동으로 생성합니다. AWS CloudFormation 콘솔을 사용하여 스택 생성을 모니터링할 수 있습니다.

- NAT 게이트웨이를 사용하여 인터넷에 VPC 선택적으로 연결하여 의 프라이빗 서브넷에서 시작된 가상 프라이빗 클라우드(VPC) 및 Amazon EC2 인스턴스입니다.
- Secrets Manager 보안 암호 값을 검색할 수 있는 권한이 있는 임시 Amazon EC2 인스턴스에 연결된 AWS Identity and Access Management (IAM) 역할입니다. 또한 역할은 선택한 Amazon Simple Storage Service(Amazon S3) 버킷에 파일을 업로드할 수 있는 권한을 제공하며, 선택적으로 AWS Support 사례에 업로드할 수 있는 권한을 제공합니다.
- DB 인스턴스와 임시 Amazon EC2 인스턴스 간의 연결을 허용하는 VPC 피어링 연결입니다.
- 임시 에 연결된 Systems Manager, Secrets Manager 및 Amazon S3 VPC 엔드포인트VPC.
- 임시 Amazon EC2 인스턴스를 주기적으로 시작 및 중지하고, 데이터 수집 스크립트를 실행하고, Amazon S3 버킷에 파일을 업로드하는 등록된 작업이 포함된 유지 관리 기간입니다. 등록된 작업을 수행할 수 있는 권한을 제공하는 유지 관리 기간에 대한 IAM 역할도 생성됩니다.

실행서가 완료되면 필요한 AWS 리소스를 생성하는 데 사용되는 AWS CloudFormation 스택이 삭제되고 보고서가 선택한 Amazon S3 버킷에 업로드되며, 선택적으로 AWS Support 케이스가 업로드됩니다.

> **Note**
>
> 기본적으로 임시 Amazon EC2 인스턴스의 루트 Amazon EBS 볼륨은 보존됩니다. `EbsVolumeDeleteOnTermination` 파라미터를 `true`로 설정해 이 옵션을 재정의할 수 있습니다.

사전 조건

- Enterprise Support 구독 이 실행서와 사전 대응 서비스 워크로드 진단 및 검토에는 Enterprise Support 구독이 필요합니다. 이 런북을 사용하기 전에 기술 계정 관리자(TAM) 또는 전문가 TAM(STAM)에게 지침을 문의하세요. 자세한 내용은 AWS Support 사전 대응 서비스를 참조하세요.
- 계정 및 AWS 리전 할당량 이 런북을 사용하는 계정 및 리전에서 생성할 수 VPCs 있는 Amazon EC2 인스턴스의 최대 수에 도달하지 않았는지 확인합니다. 제한 증가를 요청해야 하는 경우, 서비스 제한 증가 양식을 사용하십시오.
- 데이터베이스 구성
  1. `DatabaseName` 파라미터에서 지정하는 데이터베이스에는 `pg_stat_statements` 확장 프로그램이 구성되어 있어야 합니다. `shared_preload_libraries`에서 `pg_stat_statements`(을)를 구성하지 않은 경우, DB 파라미터 그룹에서 값을 편집하고 변경 내용을 적용해야 합니다. 파라미터 `shared_preload_libraries`(을)를 변경하려면 DB 인스턴스를 재부팅해야 합니다. 자세한 내용은 파라미터 그룹 작업을 참조하세요. `pg_stat_statements`(을)를 `shared_preload_libraries`에 추가하면 일부 성능 오버헤드가 추가됩니다. 하지만, 이는 개별 명령문의 성능을 추적하는 데 유용합니다. `pg_stat_statements` 확장에 대한 자세한 내용은 PostgreSQL 설명서 를 참조하세요. `pg_stat_statements` 확장을 구성하지 않거나 통계 수집에 사용되는 데이터베이스에 확장 프로그램이 없는 경우, 명령문 수준 분석은 운영 검토 시 제공되지 않습니다.
  2. `track_counts` 및 `track_activities` 파라미터가 꺼져 있지 않은지 확인하십시오. DB 파라미터 그룹에서 이러한 파라미터를 끄면 의미 있는 통계를 사용할 수 없습니다. 이러한 파라미터를 변경하려면 DB 인스턴스를 재부팅해야 합니다. 자세한 내용은 Amazon RDS for PostgreSQL DB 인스턴스의 파라미터 작업을 참조하세요.
  3. `track_io_timing` 파라미터를 끄면 I/O 수준 통계는 운영 검토에 포함되지 않습니다. `track_io_timing`(을)을 변경하면 DB 인스턴스를 재부팅해야 하며 DB 인스턴스 워크로드에 따라 추가 성능 오버헤드가 발생합니다. 중요한 워크로드의 성능 오버헤드에도 불구하고 이 파라미터는 쿼리당 I/O 시간과 연결된 유용한 정보를 제공합니다.

청구 및 요금 이 자동화가 실행되는 동안 전송된 임시 Amazon EC2 인스턴스, 연결된 Amazon EBS 볼륨, NAT 게이트웨이 및 데이터와 관련된 비용에 대해 요금이 AWS 계정 부과됩니다. 기본적으로, 이 실행서는 `t3.micro` Amazon Linux 2 인스턴스를 생성하여 통계를 수집합니다. 실행서는 단계 사이에 인스턴스를 시작 및 중지하여 비용을 절감합니다.

데이터 보안 및 거버넌스 이 실행서는 PostgreSQL 통계 보기 및 함수를 쿼리하여 통계를 수집합니다. `SecretId` 파라미터에 제공된 보안 인증이 통계 보기 및 함수에 대한 읽기 전용 권한만 허용하는지 확인하십시오. 자동화의 일환으로, 수집 스크립트는 Amazon S3 버킷에 업로드되며 `s3://`*`amzn-s3-demo-bucket`*`/`*`automation execution id`*`/queries/`에 위치할 수 있습니다.

이러한 스크립트는 AWS 전문가가 객체 수준에서 주요 성능 지표를 검토하는 데 사용하는 데이터를 수집합니다. 스크립트는 테이블 이름, 스키마 이름, 인덱스 이름과 같은 정보를 수집합니다. 이 정보에 수익 지표, 사용자 이름, 이메일 주소 또는 기타 개인 식별 정보와 같은 민감한 정보가 포함되어 있는 경우, 이 워크로드 검토를 중단하는 것이 좋습니다. 에 AWS TAM 문의하여 워크로드 검토를 위한 대체 접근 방식을 논의합니다.

이 자동화에서 수집한 통계 및 메타데이터를 와 공유하는 데 필요한 승인 및 권한이 있는지 확인합니다 AWS.

보안 고려 사항 `UpdateRdsSecurityGroup` 파라미터를 로 설정하면 `yes`실행서는 DB 인스턴스와 연결된 보안 그룹을 업데이트하여 임시 Amazon EC2 인스턴스의 프라이빗 IP 주소에서 들어오는 인바운드 트래픽을 허용합니다.

`UpdateRdsRouteTable` 파라미터를 로 설정하면 `yes`런북은 DB 인스턴스가 실행 중인 서브넷과 연결된 라우팅 테이블을 업데이트하여 VPC 피어링 연결을 통해 임시 Amazon EC2 인스턴스로의 트래픽을 허용합니다.

사용자 생성 컬렉션 스크립트를 Amazon RDS 데이터베이스에 연결하려면 통계 보기를 읽을 수 있는 권한이 있는 사용자를 설정해야 합니다. 그런 다음, 보안 인증 정보를 반드시 Secrets Manager에 저장해야 합니다. 이를 위한 새 전용 사용자를 생성하는 것이 좋습니다. 별도의 사용자를 생성하면 이 자동화로 수행된 활동을 감사하고 추적할 수 있습니다.

1. 새로운 사용자를 생성합니다.

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "CREATE USER <user_name> PASSWORD '<password>';"
   ```

2. 이 사용자가 읽기 전용 연결만 만들 수 있는지 확인합니다.

   ```
   psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
   -c "ALTER USER <user_name> SET default_transaction_read_only=true;"
   ```

3. 사용자 수준 제한을 설정합니다.

   ```
   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. 새 사용자에게 DB 통계에 액세스할 수 있도록 `pg_monitor` 권한을 부여합니다. (`pg_monitor` 역할은 `pg_read_all_settings`, `pg_read_all_stats` 및 `pg_stat_scan_table`의 구성원입니다.)

```
psql -h <database_connection_endpoint> -p <database_port> -U <admin_user>
-c "GRANT pg_monitor to <user_name>;"
```

이 Systems Manager Automation에 의해 임시 Amazon EC2 인스턴스 프로파일에 추가된 권한 다음 권한이 임시 Amazon EC2 인스턴스와 연결된 IAM 역할에 추가됩니다. 또한 `AmazonSSMManagedInstanceCore` 관리형 정책은 IAM 역할과 연결되어 Systems Manager에서 Amazon EC2 인스턴스를 관리할 수 있습니다.

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

이 Systems Manager Automation에 의해 임시 유지 관리 기간에 추가된 권한 다음 권한은 유지 관리 Windows 작업과 연결된 IAM 역할에 자동으로 추가됩니다. 유지 관리 Windows 작업은 시작, 중지 및 임시 Amazon EC2 인스턴스로 명령을 전송합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:ListCommands",
                "ssm:ListCommandInvocations",
                "ssm:GetCommandInvocation",
                "ssm:GetCalendarState",
                "ssm:CancelCommand",
                "ec2:DescribeInstanceStatus"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ssm:SendCommand",
                "ec2:StartInstances",
                "ec2:StopInstances",
```

```
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ec2:region:account id:instance/temporary instance id",
                "arn:aws:ssm:*:*:document/AWS-RunShellScript",
                "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:$DEFAULT",
                "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:$DEFAULT"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            },
            "Action": "iam:PassRole",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- DBInstanceIdentifier

  유형: 문자열

  설명: (필수) DB 인스턴스의 ID입니다.

- DatabaseName

  유형: 문자열

  설명: (필수) DB 인스턴스에서 호스팅되는 데이터베이스 이름입니다.

- SecretId

  유형: 문자열

  설명: (필수) 사용자 이름과 암호 키 값 페어가 포함된 ARN Secrets Manager 보안 암호의 입니다. AWS CloudFormation 스택은 이 에 대한 `GetSecretValue` 작업에 대한 권한이 있는 IAM 정책을 생성합니다ARN. 보안 인증은 임시 인스턴스가 데이터베이스 통계를 수집할 수 있도록 하는 데 사용됩니다. TAM 또는 STAM에 문의하여 최소 필수 권한에 대해 논의합니다.

- 확인

  유형: 문자열

  설명: (필수) 이 실행서가 계정에 임시 리소스를 생성하여 DB 인스턴스에서 통계를 수집한다는 사실을 확인하면 **`yes`**를 입력합니다. 이 자동화를 실행STAM하기 전에 TAM 또는 에 문의하는 것이 좋습니다.

- SupportCase

  유형: 문자열

  설명: (선택 사항) TAM 또는 에서 제공하는 AWS Support 사례 번호입니다STAM. 제공된 경우, 실행서는 케이스를 업데이트하고 수집된 데이터를 첨부합니다. 이 옵션을 사용하려면 엔드포인트에 액세스하려면 임시 Amazon EC2 인스턴스에 AWS Support API 인터넷 연결이 있어야 합니다. `AllowVpcInternetAccess` 파라미터를 `true`로 설정해야 합니다. 사례 제목에는 `AWSPremiumSupport-PostgreSQLWorkloadReview` 문구가 포함되어야 합니다.

- S3BucketName

  유형: 문자열

  설명: (필수) 자동화로 수집한 데이터를 업로드하려는 계정의 Amazon S3 버킷 이름입니다. 버킷 정책이 버킷 콘텐츠에 액세스할 필요가 없는 보안 주체에게 불필요한 읽기 또는 쓰기 권한을 부여하지 않는지 확인합니다. 이 자동화를 위해 임시 Amazon S3 버킷을 새로 생성하는 것이 좋습니다. 실행서는 임시 Amazon EC2 인스턴스에 연결된 IAM 역할에 `s3:PutObject` API 작업에 대한 권한을 제공합니다. 업로드된 파일은 `s3://`*`bucket name`*`/`*`automation execution id`*`/`에 있습니다.

- InstanceType

  유형: 문자열

  설명: (선택 사항) 사용자 지정 SQL 및 쉘 스크립트를 실행할 임시 Amazon EC2 인스턴스의 유형입니다.

  유효한 값: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.micro | t3.small | t3.medium | t3.large

  기본값: t3.micro

- VpcCidr

  유형: 문자열

  설명: (선택 사항) 새 에 대한 CIDR 표기법의 IP 주소 범위VPC입니다(예: `172.31.0.0/16`). DB 인스턴스에 대한 연결이 VPC 있는 기존 와 겹치거나 일치하지 CIDR 않는 를 선택해야 합니다. 생성할 VPC 수 있는 가장 작은 는 /28 서브넷 마스크를 사용하고, 가장 큰 는 /16 서브넷 마스크를 VPC 사용합니다.

  기본값: 172.31.0.0/16

- StackResourcesNamePrefix

  유형: 문자열

  설명: (선택 사항) AWS CloudFormation 스택 리소스 이름 접두사 및 태그입니다. 런북은 이 접두사를 사용하여 리소스에 적용된 이름 및 태그의 일부로 AWS CloudFormation 스택 리소스를 생성합니다. 태그 키-값 페어의 구조는 *`StackResourcesNamePrefix`*`:{{automation:EXECUTION_ID}}`입니다.

  기본값: AWSPostgreSQLWorkloadReview

- 일정

  유형: 문자열

  설명: (선택 사항) 유지 관리 기간 일정입니다. 유지 관리 기간에서 작업을 실행하는 빈도를 지정합니다. 기본값은 매 `1 hour`입니다.

  유효한 값: 15 minutes | 30 minutes | 1 hour | 2 hours | 4 hours | 6 hours | 12 hours | 1 day | 2 days | 4 days

  기본값: 1 hour
- 지속 시간

  유형: 정수

  설명: (선택 사항) 자동화 실행을 허용하려는 최대 기간(분)입니다. 지원되는 최대 기간은 8,640분(6일)입니다. 기본값은 4,320분(3일)입니다.

  유효한 값: 30-8640

  기본값: 4320
- UpdateRdsRouteTable

  유형: 문자열

  설명: (선택 사항) `true`로 설정하면 실행서가 DB 인스턴스가 실행되는 서브넷과 연결된 라우팅 테이블을 업데이트합니다. 새로 생성된 VPC 피어링 연결을 통해 트래픽을 임시 Amazon EC2 인스턴스 프라이빗 IPV4 주소로 라우팅하는 IPv4 경로가 추가됩니다.

  유효한 값: true | false

  기본값: false
- AllowVpcInternetAccess

  유형: 문자열

  설명: (선택 사항) 로 설정하면 `true`실행서는 엔드포인트와 통신하기 위해 임시 Amazon EC2 인스턴스에 인터넷 연결을 제공하는 NAT 게이트웨이를 AWS Support API 생성합니다. 실행서가 Amazon S3 버킷에 출력만 업로드하도록 하려는 경우처럼 이 파라미터를 `false`로 둘 수 있습니다.

  유효한 값: true | false

기본값: false

- UpdateRdsSecurityGroup

  유형: 문자열

  설명: (선택 사항) `true`로 설정하면 실행서가 DB 인스턴스와 연결된 보안 그룹을 업데이트하여 임시 인스턴스의 프라이빗 IP 주소에서 들어오는 트래픽을 허용합니다.

  유효한 값: false | true

  기본값: false

- EbsVolumeDeleteOnTermination

  유형: 문자열

  설명: (선택 사항) 로 설정하면 실행서`true`가 완료되고 AWS CloudFormation 스택이 삭제된 후 임시 Amazon EC2 인스턴스의 루트 볼륨이 삭제됩니다.

  유효한 값: false | true

  기본값: false

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

1. `aws:assertAwsResourceProperty` - DB 인스턴스가 `available` 상태에 있는지 확인합니다.
2. `aws:executeAwsApi` - DB 인스턴스에 대한 세부 정보를 수집합니다.
3. `aws:executeScript` - `S3BucketName`에 지정된 Amazon S3 버킷이 익명 또는 공개 읽기 또는 쓰기 액세스 권한을 허용하는지 확인합니다.
4. `aws:executeScript` - 에서 임시 AWS 리소스를 생성하는 데 사용되는 AWS CloudFormation 템플릿 콘텐츠를 자동화 실행서 첨부 파일에서 가져옵니다 AWS 계정.
5. `aws:createStack` - AWS CloudFormation 스택 리소스를 생성합니다.
6. `aws:waitForAwsResourceProperty` - AWS CloudFormation 템플릿에서 생성한 Amazon EC2 인스턴스가 실행될 때까지 기다립니다.
7. `aws:executeAwsApi` - 에서 생성한 임시 Amazon EC2 인스턴스 및 VPC 피어링 연결에 IDs 대한를 가져옵니다 AWS CloudFormation.
8. `aws:executeAwsApi` - 임시 Amazon EC2 인스턴스의 IP 주소를 가져와 DB 인스턴스와의 연결을 구성합니다.
9. `aws:executeAwsApi` - 임시 Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨에 태그를 지정합니다.
10. `aws:waitForAwsResourceProperty` - 임시 Amazon EC2 인스턴스가 상태 확인을 통과할 때까지 기다립니다.
11. `aws:waitForAwsResourceProperty` - Systems Manager에서 임시 Amazon EC2 인스턴스를 관리할 때까지 기다립니다. 이 단계가 제한 시간을 초과하거나 실패하면 실행서가 인스턴스를 재부팅합니다.
    a. `aws:executeAwsApi` - 이전 단계가 실패하거나 시간이 초과된 경우 임시 Amazon EC2 인스턴스를 재부팅합니다.

b. `aws:waitForAwsResourceProperty` - 재부팅 후 Systems Manager에서 임시 Amazon EC2 인스턴스를 관리할 때까지 기다립니다.

12. `aws:runCommand` - 임시 Amazon EC2 인스턴스에 메타데이터 수집기 애플리케이션 요구 사항을 설치합니다.

13. `aws:runCommand` - 임시 Amazon 인스턴스에 구성 파일을 생성하여 DB EC2 인스턴스에 대한 액세스를 구성합니다.

14. `aws:executeAwsApi` - Run Command를 사용하여 메타데이터 수집기 애플리케이션을 정기적으로 실행할 수 있는 유지 관리 기간을 생성합니다. 유지 관리 기간은 명령 간에 인스턴스를 시작하고 중지시킵니다.

15. `aws:waitForAwsResourceProperty` - AWS CloudFormation 템플릿에서 생성한 유지 관리 기간이 준비될 때까지 기다립니다.

16. `aws:executeAwsApi` - 에서 생성한 유지 관리 기간 및 변경 달력에 IDs 대한 를 가져옵니다 AWS CloudFormation.

17. `aws:sleep` - 유지 관리 기간의 종료 날짜가 될 때까지 기다립니다.

18. `aws:executeAwsApi` - 유지 관리 기간을 끕니다.

19. `aws:executeScript` - 유지 관리 기간 동안 실행된 작업의 결과를 가져옵니다.

20. `aws:waitForAwsResourceProperty` - 계속하기 전에 유지 관리 기간이 마지막 작업을 완료할 때까지 기다립니다.

21. `aws:branch` - `SupportCase` 파라미터 값을 제공했는지 여부를 기준으로 워크플로를 분기합니다.

    a. `aws:changeInstanceState` - 임시 Amazon EC2 인스턴스를 시작하고 보고서를 업로드하기 전에 상태 확인이 통과할 때까지 기다립니다.

    b. `aws:waitForAwsResourceProperty` - Systems Manager에서 임시 Amazon EC2 인스턴스를 관리할 때까지 기다립니다. 이 단계가 제한 시간을 초과하거나 실패할 경우 실행서가 인스턴스를 재부팅합니다.

       i. `aws:executeAwsApi` - 이전 단계가 실패하거나 시간이 초과된 경우 임시 Amazon EC2 인스턴스를 재부팅합니다.

       ii. `aws:waitForAwsResourceProperty` - 재부팅 후 Systems Manager에서 임시 Amazon EC2 인스턴스를 관리할 때까지 기다립니다.

    c. `aws:runCommand` - `SupportCase` 파라미터 값을 제공한 경우 메타데이터 보고서를 AWS Support 케이스에 첨부합니다. 스크립트는 보고서를 5MB 파일로 압축하고 분할합니다. 스크립트가 AWS Support 케이스에 첨부할 수 있는 최대 파일 수는 12개입니다.

22. `aws:changeInstanceState` - AWS CloudFormation 스택이 삭제되지 않는 경우 임시 Amazon EC2 인스턴스를 중지합니다.

23. `aws:executeAwsApi` - 실행서가 AWS CloudFormation 스택을 생성하거나 업데이트하지 못하는 경우 AWS CloudFormation 스택 이벤트를 설명합니다.
24. `aws:waitForAwsResourceProperty` - AWS CloudFormation 스택이 터미널 상태가 될 때까지 기다렸다가 삭제합니다.
25. `aws:executeAwsApi` - 유지 관리 기간을 제외한 AWS CloudFormation 스택을 삭제합니다. `EbsVolumeDeleteOnTermination` 파라미터 값이 로 설정된 경우 임시 Amazon EC2 인스턴스와 연결된 루트 Amazon EBS 볼륨이 보존됩니다`false`.

AWS-RebootRdsInstance

설명

`AWS-RebootRdsInstance` 런북이 아직 재부팅되지 않은 경우 Amazon Relational Database Service(AmazonRDS) DB 인스턴스를 재부팅합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

유형: 문자열

설명: (필수) 재부팅하려는 Amazon RDS DB 인스턴스의 ID입니다.

문서 단계

RebootInstance - DB 인스턴스가 아직 재부팅되지 않은 경우 재부팅합니다.

WaitForAvailableState - DB 인스턴스가 재부팅 프로세스를 완료할 때까지 기다립니다.

출력

이 자동화에는 출력이 없습니다.

AWSSupport-ShareRDSSnapshot

설명

`AWSSupport-ShareRDSSnapshot` 실행서는 Knowledge Center 문서에 설명된 암호화된 Amazon RDS DB 스냅샷을 다른 계정과 공유하려면 어떻게 해야 합니까? 절차에 대한 자동화된 솔루션을 제공합니다. Amazon 관계형 데이터베이스 서비스 (Amazon RDS) 스냅샷이 AWS 관리형 키기본값을 사용하여 암호화된 경우 스냅샷을 공유할 수 없습니다. 이 경우 고객 관리형 키를 사용하여 스냅샷을 복사한 다음 대상 계정과 스냅샷을 공유해야 합니다. 이 자동화는 `SnapshotName` 파라미터에서 지정하는 값 또는 선택한 Amazon RDS DB 인스턴스 또는 클러스터에서 찾은 최신 스냅샷을 사용하여 이러한 단계를 수행합니다.

> **Note**
>
> `KMSKey`파라미터 값을 지정하지 않으면 자동화가 스냅샷을 암호화하는 데 사용되는 새로운 AWS KMS 고객 관리 키를 계정에 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AccountIds

  다음을 입력합니다. StringList

  설명: (필수) 스냅샷을 공유할 계정 ID의 쉼표로 구분된 목록입니다.

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 데이터베이스

  타입: 문자열

  설명: (필수) 스냅샷을 공유하려는 Amazon RDS DB 인스턴스 또는 클러스터의 이름입니다. `SnapshotName` 파라미터의 값을 지정하는 경우, 이 파라미터는 선택 사항입니다.

- KMSKey

  타입: 문자열

  설명: (선택 사항) 스냅샷을 암호화하는 데 사용되는 AWS KMS 고객 관리형 키의 전체 Amazon 리소스 이름(ARN)입니다.

- SnapshotName

  타입: 문자열

  설명: (선택 사항) 사용하려는 DB 클러스터 또는 인스턴스 스냅샷의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:StartAutomationExecution
- rds:DescribeDBInstances
- rds:DescribeDBSnapshots
- rds:CopyDBSnapshot
- rds:ModifyDBSnapshotAttribute

DB 클러스터용 실행서를 성공적으로 시작하려면 AutomationAssumeRole에서 다음 작업이 필요합니다.

- ssm:StartAutomationExecution
- rds:DescribeDBClusters
- rds:DescribeDBClusterSnapshots
- rds:CopyDBClusterSnapshot
- rds:ModifyDBClusterSnapshotAttribute

ARNKmsKey 파라미터에서 지정된 KMS 키를 사용하려면 자동화를 실행하는 데 사용되는 IAM 역할을 키 사용자로 추가해야 합니다. KMS 키에 키 사용자를 추가하기에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 변경을 참조하세요.

KMSKey 파라미터 값을 지정하지 않은 경우 실행서를 성공적으로 시작하려면 AutomationAssumeRole에서 다음과 같은 추가 작업이 필요합니다.

- kms:CreateKey
- kms:ScheduleKeyDeletion
- kms:CreateGrant
- kms:DescribeKey

문서 단계

1. aws:executeScript- KMSKey 파라미터에 값이 제공되었는지 확인하고, 값이 없을 경우 AWS KMS 고객 관리 키를 생성합니다.
2. aws:branch - SnapshotName 파라미터에 값이 제공되었는지 확인하고, 그에 따라 분기합니다.

3. `aws:executeAwsApi` - 제공된 스냅샷이 DB 인스턴스의 내용인지 확인합니다.
4. `aws:executeScript` - 콜론을 하이픈으로 대체하여 `SnapshotName` 파라미터의 형식을 지정합니다.
5. `aws:executeAwsApi` - 지정된 `KMSKey`를 사용하여 스냅샷을 복사합니다.
6. `aws:waitForAwsResourceProperty` - 스냅샷 복사 작업이 완료될 때까지 기다립니다.
7. `aws:executeAwsApi` - 새 스냅샷을 지정된 `AccountIds`와 공유합니다.
8. `aws:executeAwsApi` - 제공된 스냅샷이 DB 클러스터의 내용인지 확인합니다.
9. `aws:executeScript` - 콜론을 하이픈으로 대체하여 `SnapshotName` 파라미터의 형식을 지정합니다.
10. `aws:executeAwsApi` - 지정된 `KMSKey`를 사용하여 스냅샷을 복사합니다.
11. `aws:waitForAwsResourceProperty` - 스냅샷 복사 작업이 완료될 때까지 기다립니다.
12. `aws:executeAwsApi` - 새 스냅샷을 지정된 `AccountIds`와 공유합니다.
13. `aws:executeAwsApi` - `Database` 파라미터에 제공된 값이 DB 인스턴스인지 확인합니다.
14. `aws:executeAwsApi` - `Database` 파라미터에 제공된 값이 DB 클러스터인지 확인합니다.
15. `aws:executeAwsApi` - 지정된 `Database`의 스냅샷 목록을 검색합니다.
16. `aws:executeScript` - 이전 단계에서 조합한 목록에서 사용 가능한 최신 스냅샷을 결정합니다.
17. `aws:executeAwsApi` - 지정된 `KMSKey`를 사용하여 DB 인스턴스 스냅샷을 복사합니다.
18. `aws:waitForAwsResourceProperty` - 스냅샷 복사 작업이 완료될 때까지 기다립니다.
19. `aws:executeAwsApi` - 새 스냅샷을 지정된 `AccountIds`와 공유합니다.
20. `aws:executeAwsApi` - 지정된 `Database`의 스냅샷 목록을 검색합니다.
21. `aws:executeScript` - 이전 단계에서 조합한 목록에서 사용 가능한 최신 스냅샷을 결정합니다.
22. `aws:executeAwsApi` - 지정된 `KMSKey`를 사용하여 DB 인스턴스 스냅샷을 복사합니다.
23. `aws:waitForAwsResourceProperty` - 스냅샷 복사 작업이 완료될 때까지 기다립니다.
24. `aws:executeAwsApi` - 새 스냅샷을 지정된 `AccountIds`와 공유합니다.
25. `aws:executeScript`- `KMSKey` 매개변수 값을 지정하지 않아 자동화가 실패하는 경우 자동화로 생성된 AWS KMS 고객 관리 키를 삭제합니다.

AWS-StartRdsInstance

설명

Amazon Relational Database Service(AmazonRDS) 인스턴스를 시작합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: 시작할 Amazon RDS 인스턴스의 (필수) ID입니다.

AWS-StartStopAuroraCluster

설명

이 런북은 Amazon Aurora 클러스터를 시작하거나 중지합니다.

> **Note**
>
> 클러스터를 시작하려면 클러스터가 `stopped` 상태여야 합니다. 클러스터를 중지하려면 클러스터가 `available` 상태여야 합니다. 이 런북은 Aurora Serverless 클러스터, Aurora 멀티 마

스터 클러스터, Aurora 글로벌 데이터베이스의 일부 또는 Aurora 병렬 쿼리를 사용하는 클러스터인 클러스터를 시작하거나 중지하는 데 사용할 수 없습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- ClusterName

  유형: 문자열

  설명: (필수) 중지하거나 시작하려는 Aurora 클러스터의 이름입니다.
- 작업

  유형: 문자열

  유효한 값: 시작 | 중지

  기본값: 시작

  설명: (필수) 중지하거나 시작하려는 Aurora 클러스터의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `rds:DescribeDBClusters`
- `rds:StartDBCluster`
- `rds:StopDBCluster`

문서 단계

- `aws:executeScript` - 에 대해 지정한 값을 기반으로 클러스터를 시작하거나 중지합니다.

출력

StartStopAuroraCluster.ClusterName - Aurora 클러스터의 이름

StartStopAuroraCluster.CurrentStatus - Aurora 클러스터의 현재 상태

StartStopAuroraCluster.Message - 자동화 세부 정보

AWS-StopRdsInstance

설명

Amazon Relational Database Service(AmazonRDS) 인스턴스를 중지합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: 중지할 Amazon RDS 인스턴스의 (필수) ID입니다.

`AWSSupport-TroubleshootConnectivityToRDS`

설명

`AWSSupport-TroubleshootConnectivityToRDS` 실행서는 EC2 인스턴스와 Amazon Relational Database Service 인스턴스 간의 연결 문제를 진단합니다. 자동화를 통해 DB 인스턴스를 사용할 수 있는지 확인한 다음 연결된 보안 그룹 규칙, 네트워크 액세스 제어 목록(네트워크 ACLs) 및 라우팅 테이블에 잠재적 연결 문제가 있는지 확인합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- DBInstanceIdentifier

  유형: 문자열

  설명: (필수) 연결을 테스트할 대상 DB 인스턴스 ID입니다.

- SourceInstance

  유형: 문자열

  허용 패턴: ^i-[a-z0-9]{8,17}$

  설명: (필수) 연결을 테스트할 EC2 인스턴스의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ec2:DescribeInstances`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`

문서 단계

- `aws:assertAwsResourceProperty` - DB 인스턴스 상태가 `available`로 설정되어 있는지 확인합니다.
- `aws:executeAwsApi` - DB 인스턴스에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - DB 인스턴스 네트워크 에 대한 정보를 가져옵니다ACLs.
- `aws:executeAwsApi` - DB 인스턴스 서브넷을 가져옵니다CIDR.
- `aws:executeAwsApi` - EC2 인스턴스에 대한 정보를 가져옵니다.

- `aws:executeAwsApi` - EC2 인스턴스 네트워크에 대한 정보를 가져옵니다ACLs.
- `aws:executeAwsApi` - EC2 인스턴스와 연결된 보안 그룹에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - DB 인스턴스와 연결된 보안 그룹에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - EC2 인스턴스와 연결된 라우팅 테이블에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - EC2 인스턴스의 Amazon과 연결된 기본 라우팅 테이블에 VPC 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - DB 인스턴스와 연결된 라우팅 테이블에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - DB 인스턴스의 Amazon과 연결된 기본 라우팅 테이블에 VPC 대한 정보를 가져옵니다.
- `aws:executeScript` - 보안 그룹 규칙을 평가합니다.
- `aws:executeScript` - 네트워크 를 평가합니다ACLs.
- `aws:executeScript` - 라우팅 테이블을 평가합니다.
- `aws:sleep` - 자동화를 종료합니다.

출력

getRDSInstance속성 DBInstanceIdentifier- 자동화에 사용되는 DB 인스턴스입니다.

getRDSInstance속성 DBInstanceStatus- 의 현재 상태입니다DBInstance.

evalSecurityGroupRules.SecurityGroupEvaluation - `SourceInstance` 보안 그룹 규칙을 DB 인스턴스 보안 그룹 규칙과 비교한 결과입니다.

evalNetworkAcl규칙 NetworkAclEvaluation - `SourceInstance` 네트워크를 DB 인스턴스 네트워크 ACLs 와 비교한 결과입니다ACLs.

evalRouteTableEntries.RouteTableEvaluation - `SourceInstance` 라우팅 테이블을 DB 인스턴스 라우팅과 비교한 결과입니다.

AWSSupport-TroubleshootRDSIAMAuthentication

설명

이는 Postgre용 Amazon, My용 Amazon, RDS RDS MariaDB용 SQL Amazon, Amazon RDS Aurora Postgre 및 SQL Amazon Aurora My 인스턴스에 대한 AWS Identity and Access Management (IAM) 인증 문제를 해결하는 `AWSSupport-TroubleshootRDSIAMAuthentication` 데 도움이 됩니다. SQL SQL 이 런북을 사용하여 Amazon RDS 인스턴스 또는 Aurora IAM 클러스터를 사용한 인증에 필

요한 구성을 확인할 수 있습니다. 또한 Amazon RDS 인스턴스 또는 Aurora 클러스터에 대한 연결 문제를 해결하는 단계를 제공합니다.

> **Important**
>
> 이 런북은 RDS 오라클용 아마존 또는 마이크로소프트 RDS SQL 서버용 아마존을 지원하지 않습니다.

> **Important**
>
> 소스 Amazon EC2 인스턴스가 제공되고 대상 데이터베이스가 RDS Amazon인 경우 연결 문제를 해결하기 TCP 위해 하위 자동화가 `AWSSupport-TroubleshootConnectivityToRDS` 호출됩니다. 또한 출력에는 IAM 인증을 사용하여 Amazon 인스턴스에 연결하기 위해 Amazon EC2 인스턴스 또는 소스 머신에서 실행할 수 있는 명령도 제공됩니다. RDS

어떻게 작동하나요?

이 런북은 6단계로 구성되어 있습니다.

- 1단계validateInputs: 자동화에 대한 입력을 검증합니다.
- 2단계 branchOnSourceEC2Provided: 입력 파라미터에 원본 Amazon EC2 인스턴스 ID가 제공되었는지 확인합니다.
- 3단계validateRDSConnectivity: 소스 Amazon EC2 인스턴스로부터 Amazon RDS 연결을 검증합니다 (제공된 경우).
- 4단계validateRDSIAMAuthentication: IAM 인증 기능이 활성화되었는지 확인합니다.
- 5단계validateIAMPolicies: 제공된 IAM 사용자/역할에 필요한 IAM 권한이 있는지 확인합니다.
- 6단계generateReport: 이전에 실행한 단계의 결과 보고서를 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- RDSType

  유형: 문자열

  설명: (필수): 연결 및 인증하려는 관계형 데이터베이스 유형을 선택합니다.

  허용된 값: 또는 `Amazon RDS` `Amazon Aurora Cluster.`

- DBInstanceIdentifier

  유형: 문자열

  설명: (필수) 대상 Amazon RDS 데이터베이스 인스턴스 또는 Aurora 데이터베이스 클러스터의 식별자입니다.

  허용된 패턴: `^[A-Za-z0-9]+(-[A-Za-z0-9]+)*$`

  최대 문자 수: 63자

- SourceEc2 InstanceIdentifier

  유형: `AWS::EC2::Instance::Id`

  설명: (선택 사항) 동일한 계정 및 지역에서 실행되는 Amazon EC2 인스턴스에서 Amazon RDS 데이터베이스 인스턴스에 연결하는 경우 Amazon EC2 인스턴스 ID입니다. 원본이 Amazon EC2 인스턴스가 아니거나 대상 Amazon RDS 유형이 Aurora 데이터베이스 클러스터인 경우에는 이 파라미터를 지정하지 마십시오.

  기본값: `""`

- DBIAMRoleName

  유형: 문자열

  설명: (선택 사항) IAM 기반 인증에 사용되는 IAM 역할 이름입니다. 매개 변수가 `DBIAMUserName` 제공되지 않은 경우에만 제공하고, 그렇지 않으면 비워 두십시오. `DBIAMRoleName`또는 를 `DBIAMUserName` 제공해야 합니다.

  허용된 패턴: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  최대 문자 수: 64자

  기본값: `""`

- DBIAMUserName

  유형: 문자열

  설명: (선택 사항) IAM 기반 인증에 사용되는 IAM 사용자 이름입니다. `DBIAMRoleName`매개 변수가 제공되지 않은 경우에만 제공하고, 그렇지 않으면 비워 두십시오. `DBIAMRoleName`또는 를 `DBIAMUserName` 제공해야 합니다.

  허용된 패턴: `^[a-zA-Z0-9+=,.@_-]{1,64}$|^$`

  최대 문자 수: 64자

  기본값: `""`

- DBUserName

  유형: 문자열

  설명: (선택 사항) 데이터베이스 내 IAM 기반 인증을 위해 IAM 역할/사용자에 매핑되는 데이터베이스 사용자 이름입니다. 기본 옵션은 데이터베이스의 모든 사용자에게 `rds-db:connect` 권한이 허용되는지 여부를 `*` 평가합니다.

  허용된 패턴: `^[a-zA-Z0-9+=,.@*_-]{1,64}$`

  최대 문자 수: 64자

  기본값: `*`

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

지침

1. roubleshootRDSIAMAuthentication AWS Systems Manager 콘솔에서 AWSSupport-T로 이동합니다.
2. 자동화 실행을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
   - AutomationAssumeRole(선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
   - RDSType(필수):

연결하고 RDS 인증하려는 Amazon 유형을 선택합니다. 허용되는 두 값 중에서 선택하십시오. `Amazon RDS` 또는 `Amazon Aurora Cluster.`

- DBInstanceIdentifier(필수):

  연결하려는 대상 Amazon RDS 데이터베이스 인스턴스 또는 Aurora 클러스터의 식별자를 입력하고 IAM 자격 증명을 인증에 사용합니다.

- SourceEc2 InstanceIdentifier (선택 사항):

  동일한 계정 및 지역에 있는 Amazon EC2 RDS 인스턴스에서 Amazon 데이터베이스 인스턴스에 연결하는 경우 Amazon EC2 인스턴스 ID를 제공하십시오. 소스가 Amazon이 EC2 아니거나 대상 Amazon RDS 유형이 Aurora 클러스터인 경우 공란으로 두십시오.

- DBIAMRoleName(선택 사항):

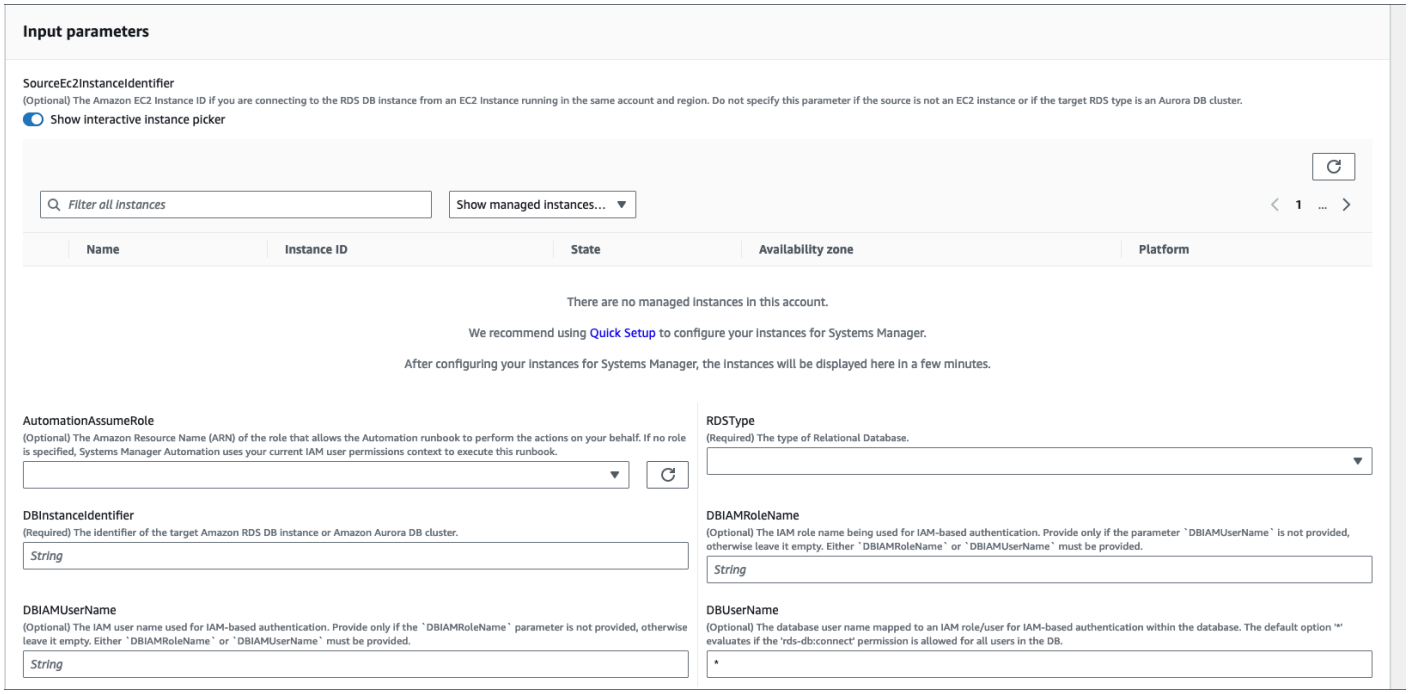
  IAM기반 인증에 사용되는 IAM 역할 이름을 입력합니다. 제공되지 않은 경우에만 `DBIAMUserName` 입력하고, 그렇지 않으면 비워 두십시오. `DBIAMRoleName`둘 중 하나를 `DBIAMUserName` 제공해야 합니다.

- DBIAMUserName(선택 사항):

  IAM기반 인증에 사용되는 IAM 사용자를 입력합니다. 제공되지 않은 경우에만 `DBIAMRoleName` 입력하고, 그렇지 않으면 비워 두십시오. 둘 중 하나를 `DBIAMRoleName` `DBIAMUserName` 입력하거나 입력해야 합니다.

- DBUserName(선택 사항):

  데이터베이스 내 IAM 기반 인증을 위해 IAM 역할/사용자에 매핑된 데이터베이스 사용자를 입력합니다. 평가에는 기본 옵션이 `*` 사용되며 이 필드에는 아무 것도 제공되지 않습니다.



4. 실행을 선택합니다.
5. 자동화가 시작되는 것을 알 수 있습니다.
6. 문서는 다음 단계를 수행합니다.
   - 1단계: validateInputs

     자동화에 대한 입력 `SourceEC2InstanceIdentifier` (선택 사항)`ClusterID`, `DBInstanceIdentifier` 또는 또는 또는 를 검증합니다`DBIAMRoleName`. `DBIAMUserName` 입력한 입력 매개변수가 계정 및 지역에 있는지 확인합니다. 또한 사용자가 IAM 매개변수 중 하나 (예: `DBIAMRoleName` 또는`DBIAMUserName`) 를 입력했는지도 확인합니다. 또한 언급된 데이터베이스가 Available 상태인지 여부와 같은 다른 확인도 수행합니다.
   - 2단계: branchOnSource EC2Provided

     입력 매개변수에 소스 EC2 Amazon이 제공되고 데이터베이스가 RDS Amazon인지 확인합니다. 그렇다면 3단계로 진행합니다. 그렇지 않은 경우 Amazon EC2 -Amazon RDS 연결 검증인 3단계를 건너뛰고 4단계로 진행합니다.
   - 3단계: validateRDSConnectivity

     입력 매개변수에 소스 EC2 Amazon이 제공되고 데이터베이스가 RDS Amazon인 경우 2단계에서 3단계가 시작됩니다. 이 단계에서는 하위 자동화를 `AWSSupport-TroubleshootConnectivityToRDS` 호출하여 소스 Amazon의 Amazon RDS 연결을 확인합니다. EC2 하위 자동화 런북은 Amazon 인스턴스에서 Amazon EC2 인스턴스로 연결할 수

있도록 필요한 네트워크 구성 (Amazon Virtual Private Cloud [Amazon VPCNACL], 보안 그룹, 네트워크 액세스 제어 목록 [], Amazon RDS 가용성) 이 제대로 되어 있는지 `AWSSupport-TroubleshootConnectivityToRDS` 확인합니다. RDS

- 4단계: validateRDSIAMAuthentication

  Amazon RDS 인스턴스 또는 Aurora 클러스터에서 IAM 인증 기능이 활성화되었는지 검증합니다.

- 5단계: validateIAMPolicies

  지정된 데이터베이스 사용자 (있는 경우) 의 Amazon RDS 인스턴스에 IAM 자격 증명을 인증할 수 있도록 전달된 IAM 사용자/역할에 필요한 IAM 권한이 있는지 확인합니다.

- 6단계: generateReport

  이전 단계에서 모든 정보를 가져와 각 단계의 결과 또는 출력을 인쇄합니다. 또한 IAM 자격 증명을 사용하여 Amazon RDS 인스턴스에 연결하기 위해 참조하고 수행할 단계를 나열합니다.

7. 자동화가 완료되면 출력 섹션에서 자세한 결과를 검토하십시오.

- 데이터베이스에 연결하기 위한 IAM 사용자/역할 권한 확인:

  지정된 데이터베이스 사용자 (있는 경우) 의 Amazon RDS 인스턴스에 IAM 자격 증명을 인증할 수 있도록 전달된 IAM 사용자/역할에 필요한 IAM 권한이 있는지 확인합니다.

- 데이터베이스의 검사 IAM 기반 인증 속성:

  지정된 Amazon RDS 데이터베이스/Aurora IAM 클러스터에 인증 기능이 활성화되어 있는지 확인합니다.

- Amazon 인스턴스에서 Amazon EC2 인스턴스로의 연결 확인: RDS

  Amazon 인스턴스에서 Amazon EC2 인스턴스로 연결할 수 있도록 필요한 네트워크 구성 (Amazon VPCNACL, 보안 그룹, Amazon RDS 가용성) 이 마련되어 있는지 확인합니다. RDS

- 다음 단계:

  IAM자격 증명을 사용하여 Amazon RDS 인스턴스에 연결하기 위해 참조하고 수행할 명령과 단계를 나열합니다.

Outputs

ScriptExecutionId

2e1d[redacted]a4

Output

```
[Troubleshooting Results]

1. Checking the IAM user/role permissions to connect to database:
 ✅ [PASSED]: Found permission 'rds-db:connect' for the resource 'a[redacted]-db1'.

2. Checking IAM-based authentication attribute for the database:
 ✅ [PASSED]: IAM-based authentication attribute is enabled for the database 'a[redacted]-db1'.

3. Checking connectivity from the EC2 instance to RDS instance:
 ❎ [SKIPPED]: No Source EC2 instance provided.
Run these commands to troubleshoot connectivity to your aurora-mysql DB instance:
    $ telnet a[redacted]-db1.cluster-[redacted].rds.amazonaws.com 3306
    $ nc -vz a[redacted]-db1.cluster-[redacted].rds.amazonaws.com 3306

[Next Steps]

1. Verify if the database user exists and have the required permissions to connect to the database using IAM authentication:
 - Connect to DB a[redacted]-db1 using admin/master db user.
 - Run the following query/command in your database:
    SELECT user, plugin, host from mysql.user WHERE user LIKE '%<name of the DB user>%';
 - From the output, verify if the user has the AWSAuthenticationPlugin.

2. Download the SSL bundle and connect to aurora-mysql database using IAM authentication by running the following commands:
    $ wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
    $ export DBPASS='$(aws rds generate-db-auth-token --hostname  a[redacted]-db1.cluster-[redacted].rds.amazonaws.com --port 3306 --region us-[redacted]2 --username <name of the DB user>)'
    mysql --host=a[redacted]-db1.cluster-[redacted].rds.amazonaws.com --port=3306 --ssl-ca=global-bundle.pem --enable-cleartext-plugin --user=<name of the DB user> --password=$DBPASS

Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html
```

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWSSupport-ValidateRdsNetworkConfiguration

설명

`AWSSupport-ValidateRdsNetworkConfiguration`자동화를 사용하면 작업을 수행하거나 운영하기 전에 기존 Amazon Relational Database Service (AmazonRDS)/Amazon Aurora/Amazon DocumentDB 인스턴스의 네트워크 비호환 상태를 방지할 수 있습니다. `ModifyDBInstance` `StartDBInstance` 인스턴스가 이미 네트워크 비호환 상태인 경우 런북에 그 이유가 나와 있습니다.

어떻게 작동하나요?

이 런북은 Amazon RDS 데이터베이스 인스턴스가 네트워크 비호환 상태로 전환되는지, 아니면 호환되지 않는 네트워크 상태가 되는 경우 호환되지 않는 네트워크 상태가 되는 이유를 확인합니다.

Runbook은 Amazon RDS 데이터베이스 인스턴스에 대해 다음 검사를 수행합니다.

- Amazon 엘라스틱 네트워크 인터페이스 (ENI) 지역별 할당량.
- 데이터베이스 서브넷 그룹의 모든 서브넷이 존재합니다.
- 서브넷에 사용할 수 있는 여유 IP 주소가 충분합니다.
- (공개적으로 액세스할 수 있는 Amazon RDS 인스턴스의 경우) VPC 속성 설정 (`enableDnsSupport`및`enableDnsHostnames`).

> **Important**
>
> Amazon Aurora/Amazon DocumentDB 클러스터에 대해 이 문서를 사용할 때는 반드시 대신 사용해야 합니다. `DBInstanceIdentifier` `ClusterIdentifier` 그렇지 않으면 문서가 첫 단계에서 실패합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `rds:DescribeDBInstances`
- `servicequotas:GetServiceQuota`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeSubnets`

샘플 정책:

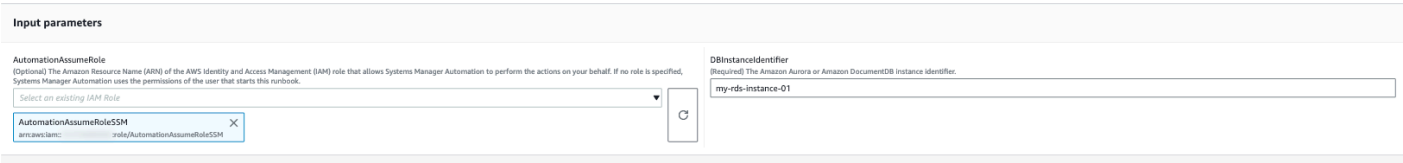
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ValidateRdsNetwork",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances",
                "servicequotas:GetServiceQuota",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "arn:aws:rds:{Region}:{Account}:db:{DbInstanceName}"
            ]
        }
    ]
}
```

지침

1. ValidateRdsNetworkConfiguration AWS Systems Manager 콘솔에서 AWSSupport-로 이동합니다.
2. 자동화 실행을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
   - AutomationAssumeRole(선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
   - DBInstanceIdentifier(필수):

     Amazon 관계형 데이터베이스 서비스 인스턴스 식별자를 입력합니다.



4. 실행을 선택합니다.

5. 자동화가 시작되는 것을 알 수 있습니다.
6. 문서는 다음 단계를 수행합니다.
   - 1단계: assertRdsState

     제공된 인스턴스 식별자가 존재하고 다음 상태 중 하나인지 확인합니다.`available`,`stopped`, 또는`incompatible-network`.
   - 2단계 gatherRdsInformation:

     나중에 자동화에서 사용할 Amazon RDS 인스턴스에 대한 필수 정보를 수집합니다.
   - 3단계: checkEniQuota

     해당 지역에서 현재 사용 가능한 Amazon ENI 할당량을 확인합니다.
   - 4단계 validateVpcAttributes:

     Amazon의 DNS 파라미터 (`enableDnsSupport`및`enableDnsHostnames`) 가 true로 설정되어 VPC 있는지 (또는 Amazon RDS 인스턴스가 true인 경우 아님`PubliclyAccessible`) 로 설정되어 있는지 확인합니다.
   - 5단계: validateSubnetAttributes

     에 서브넷이 있는지 확인하고 각 서브넷에서 IPs 사용할 수 있는지 확인합니다. `DBSubnetGroup`
   - 6단계: generateReport

     이전 단계에서 모든 정보를 가져와 각 단계의 결과 또는 출력을 인쇄합니다. 또한 IAM 자격 증명을 사용하여 Amazon RDS 인스턴스에 연결하기 위해 참조하고 수행할 단계를 나열합니다.
7. 자동화가 완료되면 Outputs 섹션에서 자세한 결과를 검토하십시오.

   네트워크 구성이 유효한 Amazon RDS 인스턴스:

▼ **Outputs**

generateReport.Report

```
# AWS RDS Network Configuration Checks: aws-rds-01rr (available)
## ✅ No Issue(s) Found

### [Troubleshooting Results]
1. Checking ENI Quota for region the RDS Instance is in:
 ✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4997) is sufficient at the moment.

2. Checking VPC Attribute (`enableDnsHostname` & `enableDnsSupport`) settings:
 ✅ [PASSED] : [PASSED] Value for both VPC attributes (`enableDnsHostnames` and `enableDnsSupport`) is set to `true`.

3. Checking if subnets required for RDS exists or not:
 ✅ [PASSED] : All subnets in `ap-south-1b` availability zone exists.

4. Checking if Available IPs are sufficient per subnets that are required:
 ✅ [PASSED] : There are sufficient available IPs in `ap-south-1b` availability zone.

5. Checking if other Availability zone satisfy Check No# 3 & 4:
  * Availability Zone: ap-south-1c
      i. Subnet Existance Check: ✅ [PASSED]
     ii. Available IP Check: ✅ [PASSED]
  * Availability Zone: ap-south-1a
      i. Subnet Existance Check: ✅ [PASSED]
     ii. Available IP Check: ✅ [PASSED]

### [Next Steps]

✅ All the checks has passed so the RDS Network configuration is correct.

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.
```

잘못된 네트워크 구성이 있는 Amazon RDS 인스턴스 (VPC속성이 enableDnsHostnames false로 설정됨):

▼ **Outputs**

generateReport.Report

```
# AWS RDS Network Configuration Checks: test-fail-sazrds-vpcattrs (stopped)
### ⛔ Issue(s) Found!!!

### [Troubleshooting Results]
1. Checking ENI Quota for region the RDS Instance is in:
 ✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4996) is sufficient at the moment.

2. Checking VPC Attribute (`enableDnsHostname` & `enableDnsSupport`) settings:
 ❌ [FAILED] : Value for `enableDnsHostnames` VPC Attribute is `false`.

3. Checking if subnets required for RDS exists or not:
 ✅ [PASSED] : All subnets in `ap-south-1b` availability zone exists.

4. Checking if Available IPs are sufficient per subnets that are required:
 ❗ [WARNING] : There are sufficient available IPs in `ap-south-1b` availability zone, but it is recommended to have more than 9 IPs.

5. Checking if other Availability zone satisfy Check No# 3 & 4:
  * Availability Zone: ap-south-1a
     i. Subnet Existance Check: ✅ [PASSED]
    ii. Available IP Check: ❗ [WARNING]

### [Next Steps]
o Please set the value of `enableDnsHostnames` VPC attribute to `true`.
   [+] View and update DNS attributes for your VPC: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-updating
o Please free up some IPs before performing Modify/Stop opeartion on the instance.
   [+] Learn why a subnet in your VPC has insufficient IP addresses : https://repost.aws/knowledge-center/subnet-insufficient-ips

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.
```

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 설명서

- 네트워크가 호환되지 않는 상태인 Amazon RDS 데이터베이스에서 문제를 해결하려면 어떻게 해야 합니까?
- 네트워크가 호환되지 않는 상태인 Amazon DocumentDB 인스턴스에서 발생하는 문제를 해결하려면 어떻게 해야 합니까?

Amazon Redshift

AWS Systems Manager 자동화는 Amazon Redshift에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-DeleteRedshiftCluster
- AWSConfigRemediation-DisablePublicAccessToRedshiftCluster
- AWSConfigRemediation-EnableRedshiftClusterAuditLogging
- AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot
- AWSConfigRemediation-EnableRedshiftClusterEncryption
- AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting
- AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster
- AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings
- AWSConfigRemediation-ModifyRedshiftClusterNodeType

`AWSConfigRemediation-DeleteRedshiftCluster`

설명

`AWSConfigRemediation-DeleteRedshiftCluster` 실행서는 지정하는 Amazon Redshift 클러스터를 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- ClusterIdentifier

  유형: 문자열

  설명: (필수) 삭제하려는 Amazon Redshift 클러스터의 ID입니다.
- SkipFinalClusterSnapshot

  타입: 부울

  기본값: false

  설명: (선택 사항) `false`로 설정하면 Amazon Redshift 클러스터를 삭제하기 전에 자동화가 스냅샷을 생성합니다. `true`로 설정하면 최종 클러스터 스냅샷이 생성되지 않습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DeleteCluster`
- `redshift:DescribeClusters`

문서 단계

- `aws:branch` - `SkipFinalClusterSnapshot` 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - `ClusterIdentifier` 파라미터에 지정된 Amazon Redshift 클러스터를 삭제합니다.

- `aws:assertAwsResourceProperty` - Amazon Redshift 클러스터가 삭제되었는지 확인합니다.

AWSConfigRemediation-DisablePublicAccessToRedshiftCluster

설명

`AWSConfigRemediation-DisablePublicAccessToRedshiftCluster` 실행서는 지정하는 Amazon Redshift 클러스터에 대한 퍼블릭 액세스를 비활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- ClusterIdentifier

  유형: 문자열

  설명: (필수) 퍼블릭 액세스를 비활성화하려는 클러스터의 고유 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

문서 단계

- `aws:executeAwsApi` - `ClusterIdentifier` 파라미터에 지정된 클러스터의 퍼블릭 액세스를 비활성화합니다.
- `aws:waitForAwsResourceProperty` - 클러스터 상태가 `available`로 변경될 때까지 기다립니다.
- `aws:assertAwsResourceProperty` - 클러스터에서 퍼블릭 액세스 설정이 비활성화되었는지 확인합니다.

AWSConfigRemediation-EnableRedshiftClusterAuditLogging

설명

`AWSConfigRemediation-EnableRedshiftClusterAuditLogging` 실행서는 지정하는 Amazon Redshift 클러스터에 대한 감사 로깅을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- BucketName

  유형: 문자열

  설명: (필수) 로그를 업로드하려는 Amazon Simple Storage Service(Amazon S3) 버킷의 이름입니다.

- ClusterIdentifier

  유형: 문자열

  설명: (필수) 감사 로깅을 활성화하려는 클러스터의 고유 식별자입니다.

- S3KeyPrefix

  유형: 문자열

  설명: (선택 사항) 로그를 업로드하려는 Amazon S3 키 접두사(하위 폴더)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeLoggingStatus`
- `redshift:EnableLogging`
- `s3:GetBucketAcl`
- `s3:PutObject`

문서 단계

- `aws:branch` - `S3KeyPrefix` 파라미터에 값이 지정되었는지 여부를 기반으로 분기합니다.
- `aws:executeAwsApi` - `ClusterIdentifier` 파라미터에 지정된 클러스터에서 감사 로깅을 활성화합니다.

- `aws:assertAwsResourceProperty` - 클러스터에서 감사 로깅이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot

설명

`AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot` 실행서는 지정하는 Amazon Redshift 클러스터에 대해 자동 스냅샷을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- AutomatedSnapshotRetentionPeriod

  유형: 정수

  유효한 값: 1-35

  설명: (필수) 자동 스냅샷이 보관되는 일 수입니다.
- ClusterIdentifier

유형: 문자열

설명: (필수) 자동 스냅샷을 활성화하려는 클러스터의 고유 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

문서 단계

- `aws:executeAwsApi` - `ClusterIdentifier` 파라미터에 지정된 클러스터에서 자동화 스냅샷을 활성화합니다.
- `aws:waitForAwsResourceProperty` - 클러스터 상태가 `available`로 변경될 때까지 기다립니다.
- `aws:executeScript` - 클러스터에서 자동 스냅샷이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableRedshiftClusterEncryption

설명

`AWSConfigRemediation-EnableRedshiftClusterEncryption` 실행서는 AWS Key Management Service (AWS KMS) 고객 관리형 키를 사용하여 지정한 Amazon Redshift 클러스터에서 암호화를 활성화합니다. 이 실행서는 Amazon Redshift 클러스터가 최소 권장 보안 모범 사례에 따라 암호화되도록 하기 위한 기준으로만 사용해야 합니다. 다양한 고객 관리형 키를 사용하여 여러 클러스터를 암호화하는 것이 좋습니다. 이 런북은 이미 암호화된 클러스터에 사용되는 AWS KMS 고객 관리형 키를 변경할 수 없습니다. 클러스터를 암호화하는 데 사용되는 AWS KMS 고객 관리형 키를 변경하려면 먼저 클러스터에서 암호화를 비활성화해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- ClusterIdentifier

  유형: 문자열

  설명: (필수) 암호화를 활성화하려는 클러스터의 고유 식별자입니다.
- KMSKeyARN

  유형: 문자열

  설명: (필수) 클러스터의 AWS KMS 데이터를 암호화하는 데 사용할 고객 관리형 키의 Amazon 리소스 이름(ARN)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

문서 단계

- `aws:executeAwsApi` - `ClusterIdentifier` 파라미터에 지정된 Amazon Redshift 클러스터에서 암호화를 활성화합니다.
- `aws:assertAwsResourceProperty` - 클러스터에서 암호화가 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting

설명

`AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting` 실행서는 지정한 Amazon Redshift 클러스터에 대해 향상된 가상 프라이빗 클라우드(VPC) 라우팅을 활성화합니다. 향상된 VPC 라우팅에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 Amazon Redshift 향상된 VPC 라우팅을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- ClusterIdentifier

  유형: 문자열

  설명: (필수) 향상된 VPC 라우팅을 활성화하려는 클러스터의 고유 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

문서 단계

- `aws:executeAwsApi` - `ClusterIdentifier` 파라미터에 지정된 클러스터에서 향상된 VPC 라우팅을 활성화합니다.
- `assertAwsResourceProperty` - 클러스터에서 향상된 VPC 라우팅이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster

설명

`AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster` 실행서는 지정한 Amazon Redshift 클러스터SSL에 사용할 수신 연결이 필요합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- ClusterIdentifier

  유형: 문자열

  설명: (필수) 향상된 VPC 라우팅을 활성화하려는 클러스터의 고유 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterParameters`
- `redshift:ModifyClusterParameterGroup`

문서 단계

- `aws:executeAwsApi` - `ClusterIdentifier` 파라미터에 지정된 클러스터에서 파라미터 세부 정보를 수집합니다.
- `aws:executeAwsApi` - `ClusterIdentifier` 파라미터에 지정된 클러스터의 `require_ssl` 설정을 활성화합니다.
- `aws:assertAwsResourceProperty` - 클러스터에서 `require_ssl` 설정이 활성화되었는지 확인합니다.
- `aws:executeScript` - 클러스터의 `require_ssl` 설정을 확인합니다.

AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings

설명

`AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings` 실행서는 지정하는 Amazon Redshift 클러스터의 유지 관리 설정을 수정합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AllowVersionUpgrade

  타입: 부울

  설명: (필수) `true`로 설정하면 유지 관리 기간 동안 메이저 버전 업그레이드가 클러스터에 자동으로 적용됩니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- AutomatedSnapshotRetentionPeriod

  유형: 정수

  유효한 값: 1-35

  설명: (필수) 자동 스냅샷이 보관되는 일수입니다.

- ClusterIdentifier

  유형: 문자열

설명: (필수) 향상된 VPC 라우팅을 활성화하려는 클러스터의 고유 식별자입니다.

- PreferredMaintenanceWindow

  유형: 문자열

  설명: (필수) 시스템 유지 관리가 발생할 수 있는 주간 시간 범위(에서UTC).

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ModifyCluster`

문서 단계

- `aws:executeAwsApi` - `ClusterIdentifier` 파라미터에 지정된 클러스터의 유지 관리 설정을 수정합니다.
- `aws:assertAwsResourceProperty` - 수정된 유지 관리 설정이 클러스터에 구성되었는지 확인합니다.

AWSConfigRemediation-ModifyRedshiftClusterNodeType

설명

`AWSConfigRemediation-ModifyRedshiftClusterNodeType` 실행서는 지정하는 Amazon Redshift 클러스터의 노드 유형과 노드 수를 수정합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- 클래식

  타입: 부울

  설명: (선택 사항) `true`로 설정하면 크기 조정 작업에 클래식 크기 조정 프로세스가 사용됩니다.
- ClusterIdentifier

  유형: 문자열

  설명: (필수) 노드 유형을 수정하려는 클러스터의 고유 식별자입니다.
- ClusterType

  유형: 문자열

  유효한 값: single-node | multi-node

  설명: (필수) 클러스터에 할당하려는 클러스터 유형입니다.
- NodeType

  유형: 문자열

  유효한 값: ds2.xlarge | ds2.8xlarge | dc1.large | dc1.8xlarge | dc2.large | dc2.8xlarge | ra3.4xlarge | ra3.16xlarge

  설명: (필수) 클러스터에 할당하려는 노드 유형입니다.
- NumberOfNodes

  유형: 정수

유효한 값: 2-100

설명: (선택 사항) 클러스터에 할당하려는 노드 수입니다. 클러스터가 `single-node` 유형인 경우 이 파라미터에 값을 지정하지 마십시오.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `redshift:DescribeClusters`
- `redshift:ResizeCluster`

문서 단계

- `aws:executeScript` - `ClusterIdentifier` 파라미터에 지정된 클러스터의 노드 유형과 노드 수를 수정합니다.

Amazon S3

AWS Systems Manager 자동화는 Amazon Simple Storage Service에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-ArchiveS3BucketToIntelligentTiering
- AWS-ConfigureS3BucketLogging
- AWS-ConfigureS3BucketVersioning
- AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock
- AWSConfigRemediation-ConfigureS3PublicAccessBlock
- AWS-CreateS3PolicyToExpireMultipartUploads
- AWS-DisableS3BucketPublicReadWrite
- AWS-EnableS3BucketEncryption

- AWS-EnableS3BucketKeys
- AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy
- AWSConfigRemediation-RestrictBucketSSLRequestsOnly
- AWSSupport-TroubleshootS3PublicRead

AWS-ArchiveS3BucketToIntelligentTiering

설명

`AWS-ArchiveS3BucketToIntelligentTiering` 런북은 지정한 Amazon Simple Storage Service(Amazon S3) 버킷에 대한 지능형 계층화 구성을 생성하거나 대체합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- BucketName

  유형: 문자열

  설명: (필수) 지능형 계층화 구성을 생성하려는 S3 버킷의 이름입니다.

- ConfigurationId

  유형: 문자열

  설명: (필수) 지능형 계층화 구성의 ID입니다. 이는 새 구성 ID 또는 기존 구성의 ID일 수 있습니다.
- NumberOfDaysToArchive

  유형: 문자열

  유효한 값: 90~730

  설명: (필수) 버킷의 객체가 아카이브 액세스 계층으로 전환될 수 있는 자격을 갖춘 후 연속 일수입니다.
- NumberOfDaysToDeepArchive

  유형: 문자열

  유효한 값: 180~730

  설명: (필수) 버킷의 객체가 Deep Archive Access 계층으로 전환될 수 있는 자격을 갖춘 후 연속 일수입니다.
- S3Prefix

  유형: 문자열

  설명: (선택 사항) 구성을 적용하려는 객체의 키 이름 접두사입니다.
- Tags

  유형: MapList

  설명: (선택 사항) 구성을 적용하려는 객체에 할당된 메타데이터입니다. 태그는 사용자 정의 키와 값으로 구성됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetIntelligentTieringConfiguration`

- `s3:PutIntelligentTieringConfiguration`

문서 단계

- PutsBucketIntelligentTieringConfiguration (aws:executeScript) - 지정된 버킷에 대한 Amazon S3 Intelligent-Tiering 구성을 생성하거나 업데이트합니다.
- VerifyBucketIntelligentTieringConfiguration (aws:assertAwsResourceProperty) - S3 버킷 Intelligent Configuration이 지정된 버킷에 적용되었는지 확인합니다.

AWS-ConfigureS3BucketLogging

설명

Amazon Simple Storage Service(Amazon S3) 버킷에 대한 로깅을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- BucketName

유형: 문자열

설명: (필수) 로깅을 구성하려는 Amazon S3 버킷의 이름입니다.

- GrantedPermission

  유형: 문자열

  유효한 값: FULL_CONTROL | READ | WRITE

  설명: (필수) 버킷의 피부여자에게 할당된 로깅 권한입니다.

- GranteeEmailAddress

  유형: 문자열

  (선택 사항) 피부여자의 이메일 주소입니다.

- GranteeId

  유형: 문자열

  설명: (선택 사항) 피부여자의 정식 사용자 ID입니다.

- GranteeType

  유형: 문자열

  유효한 값: CanonicalUser | AmazonCustomerByEmail | 그룹

  설명: (필수) 피부여자의 유형입니다.

- GranteeUri

  유형: 문자열

  설명: (선택 사항) 권한 부여자 그룹의 설명URI입니다.

- TargetBucket

  유형: 문자열

  설명: (필수) Amazon S3에서 서버 액세스 로그를 저장할 버킷을 지정합니다. 로그를 본인 소유의 버킷으로 전달되도록 할 수 있습니다. 또한 동일 대상 버킷으로 로그를 전달하도록 여러 버킷을 구성할 수도 있습니다. 이 경우 전달된 로그 파일을 키로 구분할 수 있도록 각 소스 버킷마다 다른 TargetPrefix 을 선택해야 합니다.

- TargetPrefix

  유형: 문자열

  기본값: /

  설명: (선택 사항) 로그 파일이 저장될 키의 접두사를 지정합니다.

AWS-ConfigureS3BucketVersioning

설명

Amazon Simple Storage Service(Amazon S3) 버킷에 대한 버전 관리를 구성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- BucketName

  유형: 문자열

설명: (필수) 버전 관리를 구성하려는 Amazon S3 버킷의 이름입니다.

- VersioningState

  유형: 문자열

  유효한 값: Enabled | Suspended

  기본값: Enabled

  설명: (선택 사항) VersioningConfiguration.Status에 적용됩니다. 'Enabled'로 설정된 경우 이 프로세스는 버킷의 객체에 대한 버전 관리를 활성화하며, 해당 버킷에 추가된 모든 객체마다 고유의 버전 ID를 받게 됩니다. `Suspended`로 설정된 경우 이 프로세스는 버킷의 객체에 대한 버전 관리를 비활성화합니다. 버킷에 추가된 모든 객체는 버전 ID `null`을 수신합니다.

`AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock`

설명

`AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock` 실행서는 사용자가 실행서 파라미터에서 지정하는 값을 기반으로 Amazon S3 버킷의 Amazon Simple Storage Service(Amazon S3) 퍼블릭 액세스 차단 설정을 구성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- BlockPublicAcls

  타입: 부울

  기본값: true

  설명: (선택 사항) `true` 로 설정하면 Amazon S3는 S3 버킷에 대한 퍼블릭 액세스 제어 목록(ACLs)과 `BucketName` 파라미터에서 지정한 S3 버킷에 저장된 객체를 차단합니다.

- BlockPublicPolicy

  타입: 부울

  기본값: true

  설명: (선택 사항) `true`로 설정하면 Amazon S3는 `BucketName` 파라미터에서 지정하는 S3 버킷에 대한 퍼블릭 버킷 정책을 차단합니다.

- BucketName

  유형: 문자열

  설명: (필수) 구성하려는 S3 버킷의 이름입니다.

- IgnorePublicAcls

  타입: 부울

  기본값: true

  설명: (선택 사항) `true` 로 설정하면 Amazon S3는 `BucketName` 파라미터에 지정한 S3 버킷ACLs의 모든 퍼블릭을 무시합니다.

- RestrictPublicBuckets

  타입: 부울

  기본값: true

  설명: (선택 사항) `true`로 설정하면 Amazon S3는 `BucketName` 파라미터에서 지정하는 S3 버킷에 대한 퍼블릭 버킷 정책을 제한합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`
- `s3:GetBucketPublicAccessBlock`
- `s3:PutBucketPublicAccessBlock`

문서 단계

- `aws:executeAwsApi` - `BucketName` 파라미터에 지정된 S3 버킷의 `PublicAccessBlock` 구성을 생성하거나 수정합니다.
- `aws:executeScript` - `BucketName` 파라미터에 지정된 S3 버킷에 대해 `PublicAccessBlock` 구성을 반환하고 실행서 파라미터에 지정된 값을 기반으로 변경이 성공적으로 수행되었는지 확인합니다.

AWSConfigRemediation-ConfigureS3PublicAccessBlock

설명

`AWSConfigRemediation-ConfigureS3PublicAccessBlock` 런북은 런북 파라미터에 지정한 값을 기반으로 AWS 계정의 Amazon Simple Storage Service(Amazon S3) 퍼블릭 액세스 블록 설정을 구성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AccountId

  유형: 문자열

  설명: (필수) 구성 중인 S3 버킷을 소유 AWS 계정 한 의 ID입니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- BlockPublicAcls

  타입: 부울

  기본값: true

  설명: (선택 사항) `true` 로 설정하면 Amazon S3는 `AccountId` 파라미터에서 AWS 계정 지정한 가 소유한 S3 버킷에 대한 퍼블릭 액세스 제어 목록(ACLs)을 차단합니다.

- BlockPublicPolicy

  타입: 부울

  기본값: true

  설명: (선택 사항) `true` 로 설정하면 Amazon S3는 `AccountId` 파라미터에 AWS 계정 지정한 가 소유한 S3 버킷에 대한 퍼블릭 버킷 정책을 차단합니다.

- IgnorePublicAcls

  타입: 부울

  기본값: true

  설명: (선택 사항) `true` 로 설정하면 Amazon S3는 `AccountId` 파라미터에서 AWS 계정 지정한 가 소유한 S3 버킷에 ACLs 대한 모든 퍼블릭을 무시합니다.

- RestrictPublicBuckets

타입: 부울

기본값: true

설명: (선택 사항) `true` 로 설정하면 Amazon S3는 `AccountId` 파라미터에 AWS 계정 지정한 가 소유한 S3 버킷에 대한 퍼블릭 버킷 정책을 제한합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetAccountPublicAccessBlock`
- `s3:PutAccountPublicAccessBlock`

문서 단계

- `aws:executeAwsApi` - `AccountId` 파라미터에 지정된 AWS 계정 에 대해 `PublicAccessBlock` 구성을 생성하거나 수정합니다.
- `aws:executeScript` - `AccountId` 파라미터에 AWS 계정 지정된 에 대한 `PublicAccessBlock` 구성을 반환하고 실행서 파라미터에 지정된 값을 기반으로 변경 사항이 성공적으로 이루어졌는지 확인합니다.

AWS-CreateS3PolicyToExpireMultipartUploads

설명

`AWS-CreateS3PolicyToExpireMultipartUploads` 런북은 정의된 일수 이후에 진행 중인 불완전한 다중 부분 업로드가 만료되는 지정된 버킷에 대한 수명 주기 정책을 생성합니다. 이 런북은 새 수명 주기 정책을 이미 존재하는 기존 수명 주기 버킷 정책과 병합합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- BucketName

  유형: 문자열

  설명: (필수) 구성하려는 S3 버킷의 이름입니다.

- DaysUntilExpire

  유형: 정수

  설명: (필수) Amazon S3가 업로드의 모든 부분을 영구적으로 제거하기 전에 대기하는 일수입니다.

- RuleId

  유형: 문자열

  설명: (필수) 수명 주기 버킷 규칙을 식별하는 데 사용되는 ID입니다. 고유한 값이어야 합니다.

- S3Prefix

  유형: 문자열

  설명: (선택 사항) 구성을 적용하려는 객체의 키 이름 접두사입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `s3:GetLifecycleConfiguration`
- `s3:PutLifecycleConfiguration`

문서 단계

- ConfigureExpireMultipartUploads (aws:executeScript) - 버킷의 수명 주기 정책을 구성합니다.
- VerifyExpireMultipartUploads (aws:executeScript) - 버킷에 대한 수명 주기 정책이 구성되었는지 확인합니다.

출력

- `VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse`
- `VerifyExpireMultipartUploads.LifecycleConfigurationRule`

AWS-DisableS3BucketPublicReadWrite

설명

Amazon Simple Storage Service(Amazon S3) `Block Public Access`를 사용하여 퍼블릭 S3 버킷에 대한 읽기 및 쓰기 액세스를 비활성화합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 퍼블릭 액세스 차단 사용을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- S3BucketName

  유형: 문자열

  설명: (필수) 액세스를 제한할 S3 버킷입니다.

AWS-EnableS3BucketEncryption

설명

Amazon Simple Storage Service(Amazon S3) 버킷에 대해 기본 암호화를 구성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- BucketName

  유형: 문자열

  설명: (필수) 내용을 암호화할 S3 버킷의 이름입니다.

- SSEAlgorithm

  유형: 문자열

  기본값: AES256

  설명: (선택 사항) 기본 암호화에 사용할 서버 측 암호화 알고리즘입니다.

`AWS-EnableS3BucketKeys`

설명

`AWS-EnableS3BucketKeys` 실행서는 지정한 Amazon Simple Storage Service(Amazon S3) 버킷에서 버킷 키를 활성화합니다. 이 버킷 수준 키는 수명 주기 동안 새 객체에 대한 데이터 키를 생성합니다. `KmsKeyId` 파라미터 값을 지정하지 않으면 Amazon S3 관리형 키(SSE-S3)를 사용한 서버 측 암호화가 기본 암호화 구성에 사용됩니다.

> **Note**
>
> Amazon S3 버킷 키는 AWS Key Management Service (AWS KMS) 키(-)를 사용한 이중 계층 서버 측 암호화에는 지원되지 않습니다DSSEKMS.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- BucketName

  유형: 문자열

  설명: (필수) 버킷 키를 활성화하려는 S3 버킷의 이름입니다.
- KMSKeyId

  유형: 문자열

  설명: (선택 사항) Amazon 리소스 이름(ARN), 키 ID 또는 서버 측 암호화에 사용할 AWS Key Management Service (AWS KMS) 고객 관리형 키의 키 별칭입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:GetEncryptionConfiguration`
- `s3:PutEncryptionConfiguration`

문서 단계

- ChooseEncryptionType (aws:branch) - `KmsKeyId` 파라미터에 제공된 값을 평가하여 SSE-S3(AES256) 또는 SSE-KMS 가 사용될지 결정합니다.
- PutBucketKeysKMS (aws:executeAwsApi) - 지정된 를 사용하여 지정된 S3 버킷`true`의 `BucketKeyEnabled` 속성을 로 설정합니다`KmsKeyId`.
- PutBucketKeysAES256 (aws:executeAwsApi) - AES256 암호화를 사용하여 지정된 S3 버킷에 `true` 대한 `BucketKeyEnabled` 속성을 로 설정합니다.
- VerifyS3BucketKeysEnabled (aws:assertAwsResourceProperty) - 대상 S3 버킷에서 버킷 키가 활성화되어 있는지 확인합니다.

AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy

설명

`AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy` 실행서는 Amazon Simple Storage Service(Amazon S3) 버킷 정책에서 `Allow` 작업에 대한 와일드카드(`Principal: *` 또는 `Principal: "AWS": *`)가 포함된 주요 정책 설명을 제거합니다. 조건이 포함된 정책 설명도 제거됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- BucketName

  유형: 문자열

  설명: (필수) 정책을 수정하려는 Amazon S3 버킷의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutBucketPolicy`

문서 단계

- `aws:executeScript` - 버킷 정책을 수정하고 와일드카드가 포함된 주요 정책 설명이 `BucketName` 파라미터에서 지정하는 Amazon S3 버킷에서 제거되었는지 확인합니다.

AWSConfigRemediation-RestrictBucketSSLRequestsOnly

설명

`AWSConfigRemediation-RestrictBucketSSLRequestsOnly` 실행서는 지정한 Amazon S3 버킷에 대한 요청을 명시적으로 거부하는 Amazon Simple Storage Service(SAmazon S3) 버킷 정책 문을 생성합니다. HTTP

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- BucketName

  유형: 문자열

  설명: (필수) HTTP 요청을 거부하려는 S3 버킷의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `s3:DeleteBucketPolicy`
- `s3:GetBucketPolicy`
- `s3:PutEncryptionConfiguration`
- `s3:PutBucketPolicy`

문서 단계

- `aws:executeScript` - 명시적으로 HTTP 요청을 거부하는 `BucketName` 파라미터에 지정된 S3 버킷에 대한 버킷 정책을 생성합니다.

AWSSupport-TroubleshootS3PublicRead

설명

`AWSSupport-TroubleshootS3PublicRead` 실행서는 `S3BucketName` 파라미터에서 지정하는 Amazon Simple Storage Service(Amazon S3) 버킷에서 객체를 읽는 데 발생하는 문제를 진단합니다. 또한 S3 버킷의 객체에 대한 설정 하위군도 분석됩니다.

이 자동화 실행(콘솔)

제한 사항

- 이 자동화는 객체에 대한 퍼블릭 액세스를 허용하는 액세스 포인트를 확인하지 않습니다.
- 이 자동화는 S3 버킷 정책의 조건 키를 평가하지 않습니다.
- 를 사용하는 경우 AWS Organizations이 자동화는 서비스 제어 정책을 평가하여 Amazon S3에 대한 액세스가 허용되는지 확인하지 않습니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- CloudWatchLogGroupName

  유형: 문자열

설명: (선택 사항) 자동화 출력을 보내려는 Amazon CloudWatch Logs 로그 그룹입니다. 지정하는 값과 일치하는 로그 그룹을 찾을 수 없는 경우, 자동화는 이 파라미터 값을 사용하여 로그 그룹을 생성합니다. 이 자동화로 생성된 로그 그룹의 보존 기간은 14일입니다.

- CloudWatchLogStreamName

  유형: 문자열

  설명: (선택 사항) 자동화 출력을 보내려는 로그 스트림 CloudWatch 입니다. 지정하는 값과 일치하는 로그 스트림을 찾을 수 없는 경우, 자동화는 이 파라미터 값을 사용하여 로그 스트림을 생성합니다. 이 파라미터의 값을 지정하지 않으면, 자동화에서는 로그 스트림 이름으로 `ExecutionId`(을)를 사용합니다.

- HttpGet

  타입: 부울

  유효한 값: true | false

  기본값: true

  설명: (선택 사항) 이 파라미터를 `true` 로 설정하면 자동화는 `S3BucketName` 지정한 의 객체에 부분 HTTP 요청을 합니다. 범위 HTTP 헤더를 사용하여 객체의 첫 번째 바이트만 반환됩니다.

- IgnoreBlockPublicAccess

  타입: 부울

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) 이 파라미터를 `true`로 설정하면, 자동화가 `S3BucketName` 파라미터에서 지정하는 S3 버킷의 퍼블릭 액세스 차단 설정을 무시합니다. 기본값의 이 파라미터를 변경하지 않는 것이 좋습니다.

- MaxObjects

  유형: 정수

  유효한 값: 1-25

  기본값: 5

설명: (선택 사항) `S3BucketName` 파라미터에서 지정하는 S3 버킷에서 분석할 객체 수입니다.

- S3BucketName

  유형: 문자열

  설명: (필수) 문제를 해결할 S3 버킷의 이름입니다.

- S3PrefixName

  유형: 문자열

  설명: (선택 사항) S3 버킷에서 분석하려는 객체의 키 이름 접두사입니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 객체 키를 참조하세요.

- StartAfter

  유형: 문자열

  설명: (선택 사항) 자동화를 통해 S3 버킷의 객체 분석을 시작하려는 객체 키 이름입니다.

- ResourcePartition

  유형: 문자열

  유효한 값: `aws` | `aws-us-gov` | `aws-cn`

  기본값: `aws`

  설명: (필수) S3 버킷이 위치한 파티션입니다.

- 상세 표시

  타입: 부울

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) 자동화 중에 더 자세한 정보를 반환하려면, 이 파라미터를 `true`로 설정합니다. 파라미터가 `false`로 설정된 경우 경고 및 오류 메시지만 반환됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

`logs:CreateLogGroup` , `logs:CreateLogStream` 및 `logs:PutLogEvents` 권한은 자동화가 로그 데이터를 CloudWatch 로그로 전송하도록 하려는 경우에만 필요합니다.

```
{
    "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"
        }
    ]
```

```
}
```

문서 단계

- `aws:assertAwsResourceProperty` - S3 버킷이 존재하고 액세스할 수 있는지 확인합니다.
- `aws:executeScript` - S3 버킷 위치와 표준 사용자 ID를 반환합니다.
- `aws:executeScript` - 계정 및 S3 버킷의 퍼블릭 액세스 차단 설정을 반환합니다.
- `aws:assertAwsResourceProperty` - S3 버킷 지급인이 `BucketOwner`(으)로 설정되었는지 확인합니다. S3 버킷에서 `Requester Pays`가 활성화된 경우 자동화가 종료됩니다.
- `aws:executeScript` - S3 버킷 정책 상태를 반환하고 퍼블릭으로 간주할지 여부를 결정합니다. 퍼블릭 S3 버킷에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 "퍼블릭"의 의미를 참조하세요.
- `aws:executeAwsApi` - S3 버킷 정책을 반환합니다.
- `aws:executeAwsApi` - S3 버킷 정책에 있는 모든 컨텍스트 키를 반환합니다.
- `aws:assertAwsResourceProperty` - `GetObject` API 작업에 대한 S3 버킷 정책에 명시적 거부가 있는지 확인합니다.
- `aws:executeAwsApi` - S3 버킷에 대한 액세스 제어 목록(ACL)을 반환합니다.
- `aws:executeScript` - `CloudWatchLogGroupName` 파라미터 값을 지정하는 경우 CloudWatch 로그 로그 그룹 및 로그 스트림을 생성합니다.
- `aws:executeScript` - 실행서 입력 파라미터에서 지정하는 값을 기반으로 자동화 중에 수집된 S3 버킷 설정이 퍼블릭의 객체 액세스를 방해하는지 여부를 평가합니다. 이 스크립트는 다음 기능을 수행합니다.
  - 퍼블릭 액세스 차단 설정을 평가합니다.
  - `MaxObjects`, `S3PrefixName`, `StartAfter` 파라미터에서 지정하는 값을 기반으로 S3 버킷에서 객체를 반환합니다.
  - S3 버킷 정책을 반환하여 S3 버킷에서 반환된 객체에 대한 사용자 지정 IAM 정책을 시뮬레이션합니다.
  - `HttpGet` 파라미터가 `true` 로 설정된 경우 반환HTTP된 객체에 대한 부분 요청을 수행합니다. 범위 HTTP 헤더를 사용하여 객체의 첫 번째 바이트만 반환됩니다.
  - 반환된 객체의 키 이름을 검사하여 마침표가 한 개 또는 두 개로 끝나는지 확인합니다. 기간으로 끝나는 객체 키 이름은 Amazon S3 콘솔에서 다운로드할 수 없습니다.
  - 반환된 객체의 소유자가 S3 버킷의 소유자와 일치하는지 확인합니다.
  - 객체가 익명 사용자에게 권한 `READ` 또는 `FULL_CONTROL` 권한을 ACL 부여하는지 확인합니다.

- 객체와 연결된 태그를 반환합니다.
- 시뮬레이션된 IAM 정책을 사용하여 `GetObject` API 작업에 대한 S3 버킷 정책에서 이 객체에 대한 명시적 거부가 있는지 확인합니다.
- 객체의 메타데이터를 반환하여 스토리지 클래스가 지원되는지 확인합니다.
- 객체의 서버 측 암호화 설정을 확인하여 AWS Key Management Service (AWS KMS) 고객 관리형 키를 사용하여 객체가 암호화되었는지 확인합니다.

출력

AnalyzeObjects.bucket

AnalyzeObjects.object

Amazon SES

AWS Systems Manager 자동화는 Amazon Simple Email Service에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSSupport-AnalyzeSESMessageSendingStatus

`AWSSupport-AnalyzeSESMessageSendingStatus`

설명

`AWSSupport-AnalyzeSESMessageSendingStatus` 자동화 실행서는 전송되지 않은 이메일 메시지의 이메일 전송 상태를 요약하고 전송되지 않은 이유를 해결할 수 있는 조언을 제공합니다. 실행서는 Amazon 에서 게시한 Amazon CloudWatch Logs 그룹에 저장된 Amazon Simple Email Service(Amazon SES) 이메일 전송 이벤트를 검색합니다SES. Amazon SES 이벤트 게시 세부 정보는 Amazon Simple Email Service 이벤트 게시를 사용한 모니터링을 참조하세요. 또한 실행서는 이메일 전송의 요약 및 타임라인과 전송되지 않은 이메일 메시지에 잠재적으로 영향을 미칠 수 있는 권장 사항을 제공합니다. 각 실행의 출력 섹션에서 이러한 메시지를 찾을 수 있습니다. 이 런북은 이벤트 스토어 배포 후에만 이벤트 문제를 해결할 수 있습니다.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- 동일한 CloudWatch 로그 그룹에 대한 동시 자동화 실행을 확인합니다.
- 자동화 파라미터에서 IDs 제공한 메시지에 해당하는 Amazon SES 이벤트를 분석합니다.
- 자동화 실행의 출력 섹션에 대한 출력 전송 요약입니다.

> **Important**
>
> - 이 런북을 실행하기 전에 게시된 Amazon SES 이벤트를 자동화 파라미터에 지정된 CloudWatch Logs 로그 그룹에 저장해야 합니다. 이 실행서는 로그 그룹에 저장된 Amazon SES 이벤트만 분석합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `logs:StartQuery`
- `logs:GetQueryResults`
- `ses:GetIdentityMailFromDomainAttributes`

- `ses:GetSendQuota`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager`AWSSupport-AnalyzeSESMessageSendingStatus`의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
   - AutomationAssumeRole (선택 사항):

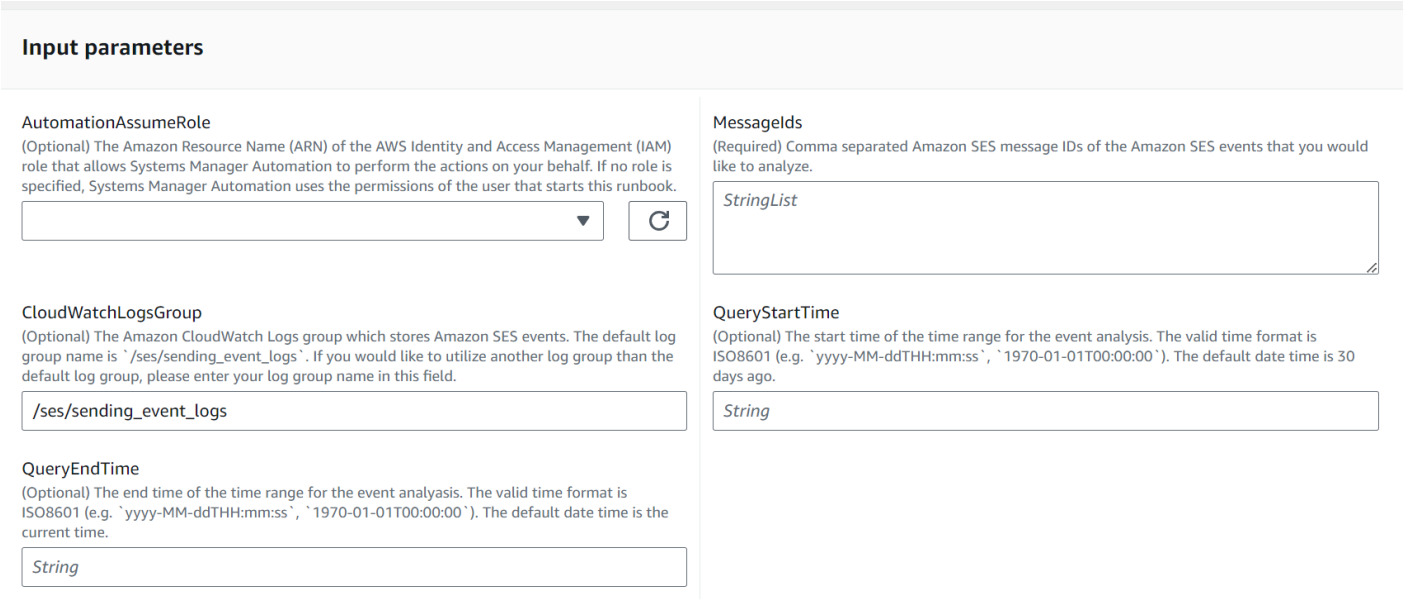
     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (IAM)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - MessageIds (필수)

     Comma는 분석하려는 Amazon Simple Email Service 이벤트IDs의 Amazon Simple Email Service 메시지를 구분했습니다.
   - CloudWatchLogsGroup (선택 사항)

     Amazon Simple Email Service 이벤트를 저장하는 Amazon CloudWatch Logs 그룹입니다. 기본 로그 그룹 이름은 `/ses/sending_event_logs`입니다. 기본 로그 그룹 이외의 다른 로그 그룹을 사용하려면 이 필드에 로그 그룹 이름을 입력하세요.”,
   - QueryStartTime (선택 사항)

     이벤트 분석을 위한 시간 범위의 시작 시간입니다. 유효한 시간 형식은 ISO8601(예: `yyyy-MM-dd THH:mm:ss`, `1970-01-01T00:00:00`)입니다. 기본 날짜 시간은 30일 전입니다.
   - QueryEndTime (선택 사항)

     이벤트 분석의 시간 범위의 종료 시간입니다. 유효한 시간 형식은 ISO8601(예: `yyyy-MM-dd THH:mm:ss`, `1970-01-01T00:00:00`)입니다. 기본 날짜 시간은 현재 시간입니다.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - **`CheckConcurrency`:**

     Amazon CloudWatch Logs 그룹을 대상으로 하는 이 실행서의 실행이 하나뿐인지 확인합니다. 실행서가 동일한 로그 그룹을 대상으로 하는 다른 실행을 찾으면 오류가 반환되고 종료됩니다.
   - **`AnalyzeSesEvents`:**

     자동화 파라미터에 의해 지정된 Amazon CloudWatch Logs 그룹에 저장된 Amazon Simple Email Service 이벤트를 분석합니다.
   - **`OutputFailureReason`:**

     단계가 실패할 때 출력 실행 `AnalyzeSESMessageSendingStatus` 단계 실패 메시지입니다.
7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.
   - 반송으로 인해 전송되지 않은 이메일 메시지에 대한 분석 출력

     반송으로 인해 대상 사서함에 도달하지 못한 이메일 메시지에 대한 자동화 실행의 출력입니다.

참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

SageMaker

AWS Systems Manager 자동화는 Amazon 에 사전 정의된 실행서를 제공합니다 SageMaker. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-DisableSageMakerNotebookRootAccess

AWS-DisableSageMakerNotebookRootAccess

설명

`AWS-DisableSageMakerNotebookRootAccess` 실행서는 Amazon SageMaker 노트북 인스턴스의 루트 액세스를 비활성화합니다. 자동화 중에는 필요한 변경을 위해 노트북 인스턴스가 중지됩니다. SageMaker Studio 노트북 인스턴스는 지원되지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- NotebookInstanceName

  유형: 문자열

  설명: (필수) 루트 액세스를 비활성화할 SageMaker 노트북 인스턴스의 이름입니다.

- StartInstanceAfterUpdate

  타입: 부울

  기본값: true

  설명: (선택 사항) 루트 액세스를 비활성화한 후 노트북 인스턴스를 시작할지 여부를 결정합니다. 이 파라미터의 기본 설정은 입니다`true`. 로 설정하면 루트 액세스가 비활성화`true`된 후 인스턴스가

시작됩니다. 로 설정하면 루트 액세스가 비활성화`false`된 후 인스턴스가 `stopped` 상태로 유지됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sagemaker:DescribeNotebookInstance`
- `sagemaker:StartNotebookInstance`
- `sagemaker:StopNotebookInstance`
- `sagemaker:UpdateNotebookInstance`

문서 단계

- CheckNotebookInstanceStatus (aws:executeAwsApi): 노트북 인스턴스의 현재 상태를 확인합니다.
- StopOrUpdateNotebookInstance (aws:branch): 노트북 인스턴스의 상태를 기반으로 분기합니다.
- StopNotebookInstance (aws:executeAwsApi): 상태가 인 경우 인스턴스를 시작합니다`stopped`.
- WaitForInstanceToStop (aws:waitForAwsResourceProperty): 인스턴스가 인지 확인합니다`stopped`.
- UpdateNotebookInstance (aws:executeAwsApi): 노트북 인스턴스의 루트 액세스를 비활성화합니다.
- WaitForNotebookUpdate (aws:waitForAwsResourceProperty): 루트 액세스가 비활성화되었고 인스턴스 `stopped` 상태가 있는지 확인합니다.
- ChooseInstanceStart (aws:branch): 인스턴스를 시작해야 하는지 여부에 따라 분기합니다.
- StartNotebookInstance (aws:executeAwsApi): 노트북 인스턴스를 시작합니다.
- VerifyNotebookInstanceStatus (aws:waitForAwsResourceProperty): 루트 액세스를 비활성화`available`하기 전에 인스턴스가 있는지 확인합니다.
- VerifyNotebookInstanceRootAccess (aws:assertAwsResourceProperty): 노트북 인스턴스 루트 액세스 설정이 성공적으로 비활성화되었는지 확인합니다.

Secrets Manager

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Secrets Manager. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-DeleteSecret
- AWSConfigRemediation-RotateSecret

AWSConfigRemediation-DeleteSecret

설명

`AWSConfigRemediation-DeleteSecret` 실행서는 보안 암호와 에 저장된 모든 버전을 삭제합니다 AWS Secrets Manager. 보안 암호를 복원할 수 있는 복구 기간을 선택적으로 지정할 수 있습니다. `RecoveryWindowInDays` 파라미터에 대한 값을 지정하지 않으면 작업의 기본값은 30일입니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- RecoveryWindowInDays

  유형: 정수

  유효한 값: 7-30

  기본값: 30

  설명: (선택 사항) 보안 암호를 복원할 수 있는 일 수입니다.
- SecretId

  유형: 문자열

  설명: (필수) 삭제하려는 보안 암호의 Amazon 리소스 이름(ARN)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `secretsmanager:DeleteSecret`
- `secretsmanager:DescribeSecret`

문서 단계

- `aws:executeAwsApi` - `SecretId` 파라미터에서 지정하는 보안 암호를 삭제합니다.
- `aws:executeScript` - 보안 암호가 삭제되도록 예약되었는지 확인합니다.

AWSConfigRemediation-RotateSecret

설명

`AWSConfigRemediation-RotateSecret` 런북은 에 저장된 보안 암호를 교대로 사용합니다 AWS Secrets Manager.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- RotationInterval

  유형: 간격

  유효한 값: 1-365

  설명: (필수) 보안 암호의 교체 사이의 일수입니다.
- RotationLambdaArn

  유형: 문자열

  설명: (필수) 암호를 교체할 수 있는 함수의 AWS Lambda Amazon 리소스 이름(ARN)입니다.
- SecretId

  유형: 문자열

  설명: (필수) 교체하려는 보안 암호의 Amazon 리소스 이름(ARN)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `lambda:InvokeFunction`
- `secretsmanager:DescribeSecret`
- `secretsmanager:RotateSecret`

문서 단계

- `aws:executeAwsApi` - `SecretId` 파라미터에서 지정하는 보안 암호를 교체합니다.
- `aws:executeScript` - 보안 암호에서 교체가 활성화되었는지 확인합니다.

Security Hub

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Security Hub. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-EnableSecurityHub

`AWSConfigRemediation-EnableSecurityHub`

설명

`AWSConfigRemediation-EnableSecurityHub` 실행서는 자동화를 실행하는 AWS 계정 및 AWS 리전 위치에 대해 (Security Hub)를 활성화합니다 AWS Security Hub . Security Hub에 대한 자세한 내용은 AWS Security Hub 사용 설명서AWS Security Hub의 ?란 무엇입니까?를 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- EnableDefaultStandards

  타입: 부울

  기본값: true

  설명: (필수) `true`로 설정하면 Security Hub에서 지정한 기본 보안 표준이 활성화됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `securityhub:DescribeHub`
- `securityhub:EnableSecurityHub`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

문서 단계

- `aws:executeAwsApi` - 현재 계정 및 리전에서 Security Hub를 활성화합니다.
- `aws:executeAwsApi` - Security Hub가 활성화되었는지 확인합니다.

AWS Shield

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS Shield. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSPremiumSupport-DDoSResiliencyAssessment

AWSPremiumSupport-DDoSResiliencyAssessment

설명

AWS Systems Manager 자동화 런북을 사용하면 AWS Shield Advanced 보호 수준에 따라 DDoS 취약성과 리소스 구성을 확인할 수 있습니다. `AWSPremiumSupport-DDoSResiliencyAssessment` AWS 계정분산 서비스 거부 () DDoS 공격에 취약한 리소스에 대한 구성 설정 보고서를 제공합니다. 이는 보호 권장 모범 사례에 따라 Amazon Route 53, Amazon 로드 밸런서, Amazon CloudFront 배포판, AWS Elastic AWS Global Accelerator IPs 등의 리소스를 수집, 분석 및 평가하는 데 사용됩니다. AWS Shield Advanced 최종 구성 보고서는 선택한 Amazon S3 버킷에서 HTML 파일로 제공됩니다.

어떻게 작동하나요?

이 런북에는 퍼블릭 액세스가 가능한 다양한 유형의 리소스와 AWS DDoS모범 사례 백서의 권장 사항에 따라 구성된 보호 기능이 있는지 여부에 대한 일련의 검사가 포함되어 있습니다. 실행서는 다음을 수행합니다.

- 구독이 활성화되었는지 확인합니다. AWS Shield Advanced
- 활성화되어 있다면, Shield Advanced로 보호되는 리소스가 있는지 확인합니다.
- AWS 계정 에서 모든 글로벌 및 지역 리소스를 찾아 Shield로 보호되는지 확인합니다.
- 평가를 위한 리소스 유형 파라미터, Amazon S3 버킷 이름, Amazon S3 버킷 AWS 계정 ID (S3BucketOwner) 가 필요합니다.
- 제공된 Amazon S3 버킷에 저장된 HTML 보고서로 결과를 반환합니다.

입력 파라미터 `AssessmentType`은 모든 리소스에 대한 검사를 수행할지 여부를 결정합니다. 기본적으로, 실행서는 모든 유형의 리소스를 검사합니다. `GlobalResources` 또는 `RegionalResources` 파라미터만 선택한 경우, 실행서는 선택한 리소스 유형에 대한 검사만 수행합니다.

> **Important**
>
> - `AWSPremiumSupport-*` 실행서에 액세스하려면 Enterprise 또는 Business Support 구독이 필요합니다. 자세한 내용은 AWS Support 플랜 비교를 참조하세요.
> - 이 실행서에는 `ACTIVE` AWS Shield Advanced 구독이 필요합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- AssessmentType

  유형: 문자열

  설명: (선택 사항) DDoS 복원력 평가를 위해 평가할 리소스 유형을 결정합니다. 기본적으로, 실행서는 글로벌 및 지역 리소스를 모두 평가합니다. 지역 리소스의 경우 런북에는 /region의 모든 Auto Scaling 그룹뿐만 아니라 모든 Application (ALBNLB) 및 Network () 로드 밸런서가 설명되어 있습니다. AWS 계정

  유효값: `['Global Resources', 'Regional Resources', 'Global and Regional Resources']`

  기본값: Global and Regional Resources

- S3 BucketName

  유형: `AWS::S3::Bucket::Name`

  설명: (필수) 보고서가 업로드될 Amazon S3 버킷 이름입니다.

  허용된 패턴: `^[0-9a-z][a-z0-9\-\.]{3,63}$`

- S3 BucketOwnerAccount

유형: 문자열

설명: (선택 사항) Amazon S3 버킷을 AWS 계정 소유한 사람입니다. Amazon S3 버킷이 다른 AWS 계정버킷에 속하는 경우 이 파라미터를 지정하십시오. 그렇지 않으면 이 파라미터를 비워 둘 수 있습니다.

허용된 패턴: `^$|^[0-9]{12,13}$`

- S3 BucketOwnerRoleArn

  유형: `AWS::IAM::Role::Arn`

  설명: (선택 사항) Amazon S3 버킷을 설명하고 퍼블릭 액세스를 AWS 계정 차단할 수 있는 권한을 가진 IAM 역할 (버킷이 다른 위치에 있는 경우) AWS 계정. ARN 이 파라미터가 지정되지 않은 경우, 런북은 이 런북을 시작하는 IAM 사용자 `AutomationAssumeRole` 또는 사용자 (지정되지 않은 경우`AutomationAssumeRole`) 를 사용합니다. 실행서 설명의 필수 권한 섹션을 참조하세요.

  허용된 패턴: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12,13}:role/.*$`

- S3 BucketPrefix

  유형: 문자열

  설명: (선택 사항) 결과를 저장하기 위한 Amazon S3 내 경로의 접두사입니다.

  허용된 패턴: `^[a-zA-Z0-9][-./a-zA-Z0-9]{0,255}$|^$`

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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

자동화 역할 수임 IAM 정책에 대한 예제

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

지침

1. DDoSResiliencyAssessment AWS Systems Manager 콘솔에서 AWSPremiumSupport-로 이동합니다.
2. 자동화 실행을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
   - AutomationAssumeRole(선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
   - AssessmentType(선택 사항):

     DDoS복원력 평가를 위해 평가할 리소스 유형을 결정합니다. 기본적으로, 실행서는 글로벌 및 지역 리소스를 모두 평가합니다.
   - S3 BucketName (필수):

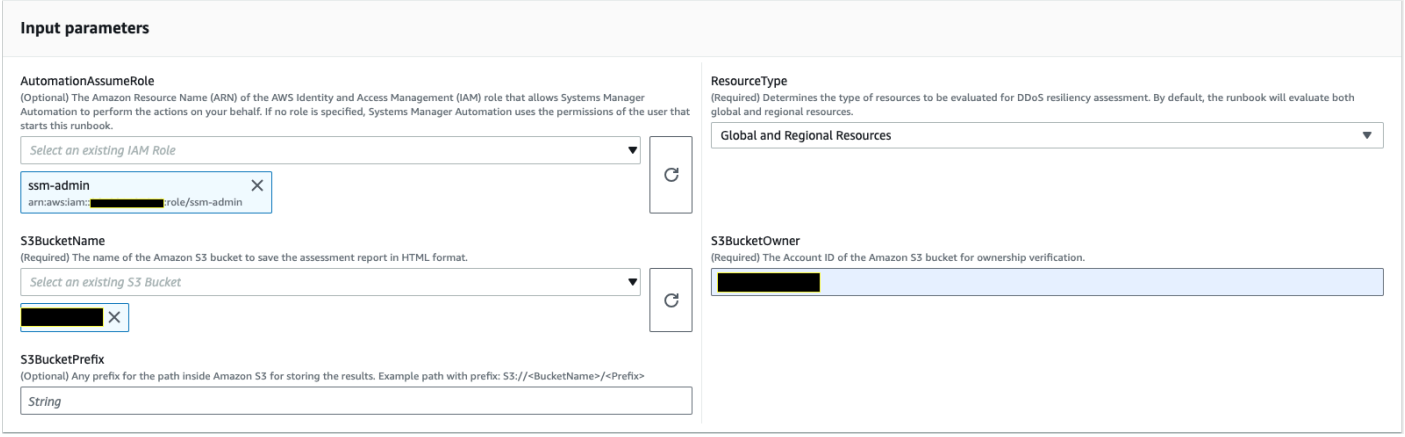
     평가 보고서를 HTML 형식으로 저장하기 위한 Amazon S3 버킷의 이름.

- S3 BucketOwner (선택 사항):

  소유권 확인을 위한 Amazon S3 버킷의 AWS 계정 ID입니다. 보고서를 교차 계정 Amazon S3 버킷에 게시해야 하는 경우 AWS 계정 ID가 필요하고, Amazon S3 버킷이 자동화 시작과 AWS 계정 동일한 위치에 있는 경우에는 선택 사항입니다.

- S3 BucketPrefix (선택 사항):

  결과를 저장하기 위한 Amazon S3 내 경로의 모든 접두사입니다.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - CheckShieldAdvancedState:

     “BucketNameS3"에 지정된 Amazon S3 버킷이 익명 또는 공개 읽기 또는 쓰기 액세스 권한을 허용하는지, 버킷에 저장된 암호화가 활성화되어 있는지, “BucketOwnerS3"에 제공된 AWS 계정 ID가 Amazon S3 버킷의 소유자인지 확인합니다.

   - S3BucketSecurityChecks:

     “BucketNameS3"에 지정된 Amazon S3 버킷이 익명 또는 공개 읽기 또는 쓰기 액세스 권한을 허용하는지, 버킷에 저장된 암호화가 활성화되어 있는지, “BucketOwnerS3"에 제공된 AWS 계정 ID가 Amazon S3 버킷의 소유자인지 확인합니다.

   - BranchOnShieldAdvancedStatus:

     AWS Shield Advanced 구독 상태 및/또는 Amazon S3 버킷 소유권 상태를 기반으로 문서 단계를 분기합니다.

   - ShieldAdvancedConfigurationReview:

Shield Advanced 구성을 검토하여 필요한 최소한의 세부 정보가 있는지 확인합니다. 예: AWS Shield 대응팀 (SRT) 팀에 대한 IAM 액세스, 연락처 목록 세부 정보, SRT 사전 참여 상태.

- ListShieldAdvancedProtections:

  Shield Protected 리소스를 나열하고, 각 서비스에 대한 보호 리소스 그룹을 생성합니다.

- BranchOnResourceTypeAndCount:

  리소스 유형 파라미터의 값과 Shield로 보호되는 글로벌 리소스 수를 기준으로 문서 단계를 분기합니다.

- ReviewGlobalResources:

  Route 53 호스팅 영역, CloudFront 배포 및 글로벌 액셀러레이터와 같은 Shield Advanced로 보호되는 글로벌 리소스를 검토합니다.

- BranchOnResourceType:

  리소스 유형 선택(글로벌, 지역 또는 둘 다)을 기반으로 문서 단계를 분기합니다.

- ReviewRegionalResources:

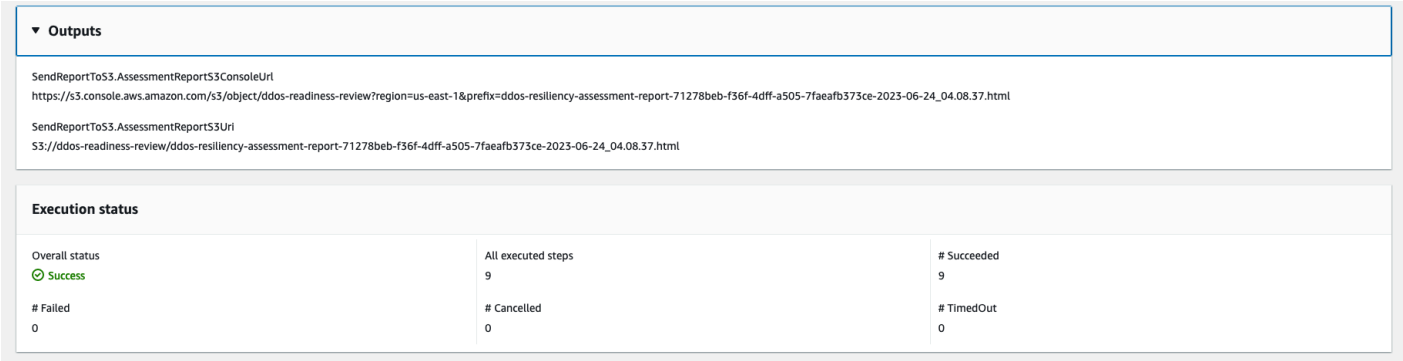
  애플리케이션 로드 밸런서, 네트워크 로드 밸런서, 클래식 로드 밸런서, Amazon Elastic Compute Cloud (AmazonEC2) 인스턴스 (Elastic) 와 같은 Shield Advanced의 보호 대상 지역 리소스를 검토합니다. IPs

- SendReportToS3:

  DDoS평가 보고서 세부 정보를 Amazon S3 버킷에 업로드합니다.

7. 완료되면 Amazon S3 URI 버킷에 평가 보고서 HTML 파일이 제공됩니다.

런북의 성공적인 실행에 대한 보고서를 URI 위한 S3 콘솔 링크 및 Amazon S3



참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 설명서

- AWS Shield Advanced

Amazon SNS

AWS Systems Manager 자동화는 Amazon Simple Notification Service에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-EnableSNSTopicDeliveryStatusLogging
- AWSConfigRemediation-EncryptSNSTopic
- AWS-PublishSNSNotification

`AWS-EnableSNSTopicDeliveryStatusLogging`

설명

`AWS-EnableSNSTopicDeliveryStatusLogging` 실행서는 `HTTP`, Amazon Data Firehose, Lambda, `Platform application`또는 Amazon Simple Queue Service(AmazonSQS) 엔드포인트에 대한 전송 상태 로깅을 구성합니다. 이를 통해 AmazonSNS은 실패한 알림과 성공한 알림의 샘플 비율을 Amazon 에 로깅할 수 있습니다 CloudWatch. 주제에 대한 전송 상태 로깅이 이미 구성된 경우 실행서는 기존 구성을 입력 파라미터에 지정한 새 값으로 바꿉니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- EndpointType

  유형: 문자열

  유효 값:
  - HTTP
  - Firehose
  - Lambda
  - 애플리케이션
  - SQS

  설명: (필수) 전송 상태 알림 메시지를 로깅하려는 Amazon SNS 주제 엔드포인트의 유형입니다.
- TopicArn

  유형: 문자열

  설명: (필수) 전송 상태 로깅을 구성하려는 Amazon SNS 주제ARN의 입니다.
- SuccessFeedbackRoleArn

  유형: 문자열

설명: (필수) Amazon이 성공적인 알림 메시지에 대한 로그를 로 전송하는 데 SNS 사용하는 IAM 역할ARN의 입니다 CloudWatch.

- SuccessFeedbackSampleRate

  유형: 문자열

  유효한 값: 0~100

  설명: (필수) 지정된 Amazon SNS 주제에 대해 샘플링할 성공 메시지의 백분율입니다.

- FailureFeedbackRoleArn

  유형: 문자열

  설명: (필수) Amazon이 실패 알림 메시지에 대한 로그를 로 보내는 데 SNS 사용하는 IAM 역할ARN의 입니다 CloudWatch.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:PassRole`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

문서 단계

- `aws:executeAwsApi` - Amazon SNS 주제에 `SuccessFeedbackRoleArn` 파라미터 값을 적용합니다.
- `aws:executeAwsApi` - Amazon SNS 주제에 `SuccessFeedbackSampleRate` 파라미터 값을 적용합니다.
- `aws:executeAwsApi` - Amazon SNS 주제에 `FailureFeedbackRoleArn` 파라미터 값을 적용합니다.
- `aws:executeScript` - Amazon SNS 주제에서 전송 상태 로깅이 활성화되었는지 확인합니다.

출력

VerifyDeliveryStatusLoggingEnabled.GetTopicAttributesResponse - `GetTopicAttributes` API 작업의 응답입니다.

VerifyDeliveryStatusLoggingEnabled.VerifyDeliveryStatusLoggingEnabled - 전송 상태 로깅을 성공적으로 확인했음을 나타내는 메시지입니다.

AWSConfigRemediation-EncryptSNSTopic

설명

`AWSConfigRemediation-EncryptSNSTopic` 실행서는 AWS Key Management Service (SNS) 고객 관리형 키를 사용하여 지정한 Amazon Simple Notification Service(Amazon AWS KMS) 주제에 대한 암호화를 활성화합니다. 이 런북은 Amazon SNS 주제가 최소 권장 보안 모범 사례에 따라 암호화되도록 하기 위한 기준으로만 사용해야 합니다. 다양한 고객 관리형 키를 사용하여 여러 주제를 암호화하는 것이 좋습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- KmsKeyArn

유형: 문자열

설명: (필수) Amazon SNS 주제를 암호화하는 데 사용할 고객 관리형 키의 AWS KMS Amazon 리소스 이름(ARN)입니다.

- TopicArn

  유형: 문자열

  설명: (필수) 암호화하려는 Amazon SNS 주제ARN의 입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `sns:GetTopicAttributes`
- `sns:SetTopicAttributes`

문서 단계

- `aws:executeAwsApi` - `TopicArn` 파라미터에 지정한 Amazon SNS 주제를 암호화합니다.
- `aws:assertAwsResourceProperty` - Amazon SNS 주제에 암호화가 활성화되어 있는지 확인합니다.

AWS-PublishSNSNotification

설명

Amazon 에 알림을 게시합니다SNS.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 메시지

  유형: 문자열

  설명: (필수) SNS 알림에 포함할 메시지입니다.
- TopicArn

  유형: 문자열

  설명: (필수) 알림을 게시할 SNS 주제ARN의 입니다.

Amazon SQS

AWS Systems Manager 자동화는 Amazon Simple Queue Service(Amazon)에 사전 정의된 실행서를 제공합니다SQS. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-EnableSQSEncryption

AWS-EnableSQSEncryption

설명

`AWS-EnableSQSEncryption`Runbook은 Amazon 심플 큐 서비스 (AmazonSQS) 대기열의 저장 중 암호화를 지원합니다. Amazon SQS 대기열은 Amazon SQS 관리 키 (SSE-SQS) 또는 () 관리 키 AWS Key Management Service (SSE-AWS KMS KMS) 를 사용하여 암호화할 수 있습니다. 대기열에 할당하는 키에는 대기열을 사용할 권한이 있는 모든 보안 주체에 대한 권한이 포함된 키 정책이 있어야 합니다. 암호화가 활성화되면 익명 `SendMessage` 및 암호화된 대기열에 대한 `ReceiveMessage` 요청이 거부됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- QueueUrl

  타입: 문자열

  설명: (필수) 암호화를 활성화하려는 Amazon SQS 대기열입니다. URL

- KmsKeyId

  타입: 문자열

설명: (선택 사항) 암호화에 사용할 AWS KMS 키입니다. 이 값은 별칭이나 ARN 키에 대한 글로벌 고유 식별자 또는 접두사 “alias/”가 붙은 별칭 이름일 수 있습니다. 별칭 aws/sqs를 지정하여 AWS 관리 키를 사용할 수도 있습니다.

- KmsDataKeyReusePeriodSeconds

  타입: 문자열

  유효한 값: 60-86400

  기본값: 300

  설명: (선택 사항) Amazon SQS 대기열이 데이터 키를 재사용하여 메시지를 암호화하거나 해독한 후 다시 호출할 수 있는 시간 (초) 입니다. AWS KMS

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `sqs:GetQueueAttributes`
- `sqs:SetQueueAttributes`

문서 단계

- SelectKeyType (`aws:branch`): 지정된 키를 기반으로 분기합니다.
- PutAttributeSseKms (`aws:executeAwsApi`) - 암호화에 지정된 AWS KMS 키를 사용하도록 Amazon SQS 대기열을 업데이트합니다.
- PutAttributeSseSqs (`aws:executeAwsApi`) - 암호화에 기본 키를 사용하도록 Amazon SQS 대기열을 업데이트합니다.
- VerifySqsEncryptionKms (`aws:assertAwsResourceProperty`) - Amazon SQS 대기열에 암호화가 활성화되어 있는지 확인합니다.
- VerifySqsEncryptionDefault (`aws:assertAwsResourceProperty`) - Amazon SQS 대기열에 암호화가 활성화되어 있는지 확인합니다.

Step Functions

AWS Systems Manager 자동화는 AWS Step Functions (단계 함수)에 대한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-EnableStepFunctionsStateMachineLogging

AWS-EnableStepFunctionsStateMachineLogging

설명

`AWS-EnableStepFunctionsStateMachineLogging`런북은 지정한 AWS Step Functions 상태 머신의 로깅을 활성화하거나 업데이트합니다. 최소 로깅 수준은 `ALLERROR`, 또는 `FATAL` 로 설정해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 수준

  유형: 문자열

  유효한 값: 모두 | 오류 | 치명적

  설명: (필수) 암호화를 활성화하려는 Amazon SQS 대기열의 URL입니다.
- LogGroupArn

  유형: 문자열

  설명: (필수) 상태 머신 CloudWatch 로그를 전송하려는 Amazon Logs 로그 그룹의 ARN입니다.
- StateMachineArn

  유형: 문자열

  설명: (필수) 로그온을 활성화하려는 상태 머신의 ARN입니다.
- IncludeExecutionData

  유형: 부울

  기본값: False

  설명: (선택 사항) 실행 데이터를 로그에 포함할지 여부를 결정합니다.
- TracingConfiguration

  유형: 부울

  기본값: False

  설명: (선택 사항) AWS X-Ray 추적 활성화 여부를 결정합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `states:DescribeStateMachine`
- `states:UpdateStateMachine`

문서 단계

- `EnableStepFunctionsStateMachineLogging (aws:executeAwsApi)`- 지정된 상태 머신을 지정된 로깅 구성으로 업데이트합니다.
- `VerifyStepFunctionsStateMachineLoggingEnabled (aws:assertAwsResourceProperty)`- 지정된 상태 머신에 대해 로깅이 활성화되었는지 확인합니다.

출력

- EnableStepFunctionsStateMachineLogging.Response - UpdateStateMachine API 호출의 응답입니다.

Systems Manager

AWS Systems Manager Automation은 Systems Manager에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- 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

설명

AWS-BulkDeleteAssociation 실행서는 한 번에 최대 50개의 Systems Manager State Manager 연결을 삭제하는데 도움이 됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- AssociationIds

  유형: StringList

  설명: (필수) 삭제하려는 IDs 연결의 쉼표로 구분된 목록입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:DeleteAssociation`

문서 단계

- `aws:executeScript` - `AssociationIds` 파라미터에서 지정하는 연결을 삭제합니다.

AWS-BulkEditOpsItems

설명

`AWS-BulkEditOpsItems` 실행서는 의 상태, 심각도, 범주 또는 우선 순위를 편집하는 데 도움이 됩니다 AWS Systems Manager OpsItems. 이 자동화는 한 번에 최대 50개까지 편집할 수 OpsItems 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 범주

  유형: 문자열

  유효한 값:

  - 가용성
  - 비용
  - No change
  - 성능
  - 복구
  - 보안

  기본값: 변경 없음

  설명: (선택 사항) 편집된 에 지정하려는 새 범주입니다 OpsItems.

- OpsItemIds

  유형: StringList

  설명: (필수) 편집하려는 의 OpsItems IDs 쉼표로 구분된 목록(예: oi-,XXXXXXXXXXXXoi-XXXXXXXXXXXX).

- 우선 순위

  유형: 문자열

  유효한 값:

  - No change
  - 1
  - 2
  - 3
  - 4
  - 5

  기본값: 변경 없음

  설명: (선택 사항) 시스템의 다른 와 OpsItems 관련하여 편집된 의 중요성 OpsItems 입니다.

- 심각도

유형: 문자열

유효한 값:

- No change
- 1
- 2
- 3
- 4

기본값: 변경 없음

설명: (선택 사항) 편집된 의 심각도입니다 OpsItems.

- WaitTimeBetweenEditsInSecs

  유형: 문자열

  유효한 값: 0.0-2.0

  기본값: 0.8

  설명: (선택 사항) `UpdateOpsItems` 작업 호출 사이에 자동화가 대기하는 시간입니다.

- 상태 표시기

  유형: 문자열

  유효한 값:

  - InProgress
  - No change
  - Open
  - Resolved

  기본값: 변경 없음

  설명: (선택 사항) 편집된 의 새 상태입니다 OpsItems.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- `aws:executeScript` - , `Priority` , `Severity` 및 `OpsItemIds` 파라미터에 OpsItems 대해 지정한 값을 기반으로 `Status` 파라미터에 지정한 `Category` 를 편집합니다.

AWS-BulkResolveOpsItems

설명

`AWS-BulkResolveOpsItems` 런북은 지정한 필터 AWS Systems Manager OpsItems 와 일치하는 문제를 해결합니다. `OpsInsightsId` 파라미터를 OpsItems 사용하여 확인된 에 OpsItemId 추가할 를 지정할 수도 있습니다. `S3BucketName` 파라미터 값을 지정하는 경우, 결과 요약이 Amazon Simple Storage Service(Amazon S3) 버킷으로 전송됩니다. 결과 요약이 Amazon S3 버킷으로 전송된 후 알림을 받으려면, `SnsTopicArn` 파라미터 값을 지정합니다. 이 자동화는 한 번에 최대 1,000개의 문제를 해결 OpsItems 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 필터

  유형: 문자열

  설명: (필수) 확인 OpsItems 하려는 를 반환하는 필터의 키-값 페어입니다. 예: `[{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]`. OpsItems 응답을 필터링하는 데 사용할 수 있는 옵션에 대한 자세한 내용은 AWS Systems Manager API 참조OpsItemFilters의 섹션을 참조하세요.

- OpsInsightId

  유형: 문자열

  설명: (선택 사항) 해결된 에 추가하려는 관련 리소스 식별자입니다 OpsItems.

- S3BucketName

  유형: 문자열

  설명: (선택 사항) 결과 요약을 보내려는 Amazon S3 버킷의 이름입니다.

- SnsMessage

  유형: 문자열

  설명: (선택 사항) 자동화가 완료될 때 Amazon Simple Notification Service(Amazon SNS)에서 보낼 알림입니다.

- SnsTopicArn

  유형: 문자열

  설명: (선택 사항) 결과 요약이 Amazon S3로 전송되었을 때 알리려는 Amazon SNS 주제ARN의 입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `s3:GetBucketAcl`
- `s3:PutObject`
- `sns:Publish`
- `ssm:DescribeOpsItems`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:UpdateOpsItem`

문서 단계

- `aws:executeScript` - 지정한 필터를 OpsItems 기반으로 를 수집하고 해결합니다. `OpsInsightId` 파라미터 값을 지정한 경우, 해당 값이 관련 리소스로 추가됩니다.
- `aws:executeScript` - `S3BucketName` 파라미터 값을 지정한 경우, 결과 요약이 Amazon S3 버킷으로 전송됩니다.
- `aws:executeScript` - `SnsTopicArn` 파라미터 값을 지정한 경우 지정된 파라미터 값을 포함하여 결과 요약이 Amazon S3로 전송된 후 Amazon SNS 주제로 알림이 전송됩니다`SnsMessage`.

AWS-ConfigureMaintenanceWindows

설명

`AWS-ConfigureMaintenanceWindows` 실행서는 여러 Systems Manager 유지 관리 기간을 활성화하거나 비활성화하는 데 도움이 됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- MaintenanceWindows

  유형: StringList

  설명: (필수) 활성화 또는 비활성화하려는 유지 관리 기간의 에 IDs 대한 쉼표로 구분된 목록입니다.
- MaintenanceWindowsStatus

  유형: 문자열

  유효한 값: "True" | "False"

  기본값: "False"

  설명: (필수) 유지 관리 기간을 활성화할지 비활성화할지 결정합니다. 유지 관리 기간을 활성화하려면 “True”를 지정하고 유지 관리 기간을 비활성화하려면 “False”를 지정합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:GetMaintenanceWindow`
- `ssm:UpdateMaintenanceWindow`

문서 단계

- `aws:executeScript` - `MaintenanceWindows` 파라미터에서 지정하는 유지 관리 기간의 상태를 수집하고 유지 관리 기간을 활성화하거나 비활성화합니다.

AWS-CreateManagedLinuxInstance

설명

Systems Manager에 대해 구성된 Linux EC2 인스턴스를 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

Parameters

- AmiId

  유형: 문자열

  설명: (필수) AMI 인스턴스를 시작하는 데 사용할 ID입니다.
- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- GroupName

  유형: 문자열

  기본값: SSMSecurityGroupForLinuxInstances

  설명: (필수) 생성할 보안 그룹 이름입니다.
- HttpTokens

  유형: 문자열

  유효한 값: optional | required

기본값: optional

설명: (선택 사항)은 토큰 지원 세션을 IMDSv2 사용합니다. HTTP 토큰 사용을 `optional` 또는 로 설정`required`하여 IMDSv2 가 선택 사항인지 필수 사항인지 여부를 결정합니다.

- InstanceType

  유형: 문자열

  기본값: t2.medium

  설명: (필수) 시작할 인스턴스 유형을 선택합니다. 기본값은 t2.medium입니다.

- KeyPairName

  유형: 문자열

  설명: (필수) 인스턴스를 생성할 때 사용할 키 페어입니다.

- RemoteAccessCidr

  유형: 문자열

  기본값: 0.0.0.0/0

  설명: (필수) 포트가 로 IPs 지정된 SSH(포트 범위 22)에 대한 포트가 열려 있는 보안 그룹을 생성합니다CIDR(기본값은 0.0.0.0/0). 보안 그룹이 이미 존재하는 경우, 해당 보안 그룹이 수정되지 않으며 규칙이 변경되지 않습니다.

- RoleName

  유형: 문자열

  기본값: SSMManagedInstanceProfileRole

  설명: (필수) 생성할 역할 이름입니다.

- StackName

  유형: 문자열

  기본값: CreateManagedInstanceStack{{automation:EXECUTION_ID}}

  설명: (선택 사항) 이 실행서에 사용되는 스택 이름을 지정합니다.

- SubnetId

유형: 문자열

기본값: Default

설명: (필수) 새 인스턴스가 이 서브넷이나 기본 서브넷(지정하지 않은 경우)에 배포됩니다.

- VpcId

  유형: 문자열

  기본값: Default

  설명: (필수) 새 인스턴스는 이 Amazon Virtual Private Cloud(AmazonVPC)에 배포되거나 지정되지 않은 VPC 경우 기본 Amazon에 배포됩니다.

AWS-CreateManagedWindowsInstance

설명

에 대한 EC2 인스턴스 생성 Windows Server Systems Manager에 대해 구성된 .

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

Parameters

Parameters

- AmiId

  유형: 문자열

기본값: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

설명: (필수) AMI 인스턴스를 시작하는 데 사용할 ID입니다.

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- GroupName

  유형: 문자열

  기본값: SSMSecurityGroupForLinuxInstances

  설명: (필수) 생성할 보안 그룹 이름입니다.

- HttpTokens

  유형: 문자열

  유효한 값: optional | required

  기본값: optional

  설명: (선택 사항)은 토큰 지원 세션을 IMDSv2 사용합니다. HTTP 토큰 사용을 `optional` 또는 로 설정`required`하여 IMDSv2 가 선택 사항인지 필수 사항인지 여부를 결정합니다.

- InstanceType

  유형: 문자열

  기본값: t2.medium

  설명: (필수) 시작할 인스턴스 유형을 선택합니다. 기본값은 t2.medium입니다.

- KeyPairName

  유형: 문자열

설명: (필수) 인스턴스를 생성할 때 사용할 키 페어입니다.

- RemoteAccessCidr

  유형: 문자열

  기본값: 0.0.0.0/0

  설명: (필수) 포트RDP가 (포트 범위 3389)에 대해 로 IPs 지정된 에 대해 열린 보안 그룹을 생성합니다CIDR(기본값은 0.0.0.0/0). 보안 그룹이 이미 존재하는 경우, 해당 보안 그룹이 수정되지 않으며 규칙이 변경되지 않습니다.

- RoleName

  유형: 문자열

  기본값: SSMManagedInstanceProfileRole

  설명: (필수) 생성할 역할 이름입니다.

- StackName

  유형: 문자열

  기본값: CreateManagedInstanceStack{{automation:EXECUTION_ID}}

  설명: (선택 사항) 이 실행서에 사용되는 스택 이름을 지정합니다.

- SubnetId

  유형: 문자열

  기본값: Default

  설명: (필수) 새 인스턴스가 이 서브넷이나 기본 서브넷(지정하지 않은 경우)에 배포됩니다.

- VpcId

  유형: 문자열

  기본값: Default

  설명: (필수) 새 인스턴스는 이 Amazon Virtual Private Cloud(AmazonVPC)에 배포되거나 지정되지 않은 VPC 경우 기본 Amazon에 배포됩니다.

AWSConfigRemediation-EnableCWLoggingForSessionManager

설명

`AWSConfigRemediation-EnableCWLoggingForSessionManager` 런북을 사용하면 AWS Systems Manager Session Manager(Session Manager) 세션이 출력 로그를 Amazon CloudWatch(CloudWatch) 로그 그룹에 저장할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DestinationLogGroup

  유형: 문자열

  설명: (필수) CloudWatch 로그 그룹의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `ssm:GetDocument`
- `ssm:UpdateDocument`
- `ssm:CreateDocument`
- `ssm:UpdateDefaultDocumentVersion`
- `ssm:DescribeDocument`

문서 단계

- `aws:executeScript` - CloudWatch 로그 그룹을 수락하여 Session Manager 세션 출력 로그 기본 설정을 저장하는 문서를 업데이트하거나 없는 경우 생성합니다.

AWS-ExportOpsDataToS3

설명

이 런북은 AWS Systems Manager Explorer에서 OpsData 요약 목록을 검색하여 지정된 Amazon Simple Storage Service(Amazon S3) 버킷의 객체로 내보냅니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- columnFields

  유형: StringList

  설명: (필수 사항) 출력 파일에 쓸 열 필드입니다.
- 필터

  유형: 문자열

  설명: (선택 사항) getOpsSummary 요청에 대한 필터입니다.
- resultAttribute

  유형: 문자열

  설명: (선택 사항) 요청에 대한 getOpsSummary 결과 속성입니다.
- s3BucketName

  유형: 문자열

  설명: (필수) 출력 파일을 다운로드할 S3 버킷입니다.
- snsSuccessMessage

  유형: 문자열

  설명: (선택 사항) 실행서가 완료될 때 보낼 메시지입니다.
- snsTopicArn

  유형: 문자열

  설명: (필수) 다운로드가 완료되면 알려주ARN는 Amazon Simple Notification Service(Amazon SNS) 주제입니다.
- syncName

  유형: 문자열

  설명: (선택 사항) 리소스 데이터 동기화의 이름입니다.

문서 단계

getOpsSummary단계 - 최대 5,000개의 ops 요약을 검색하여 지금 CSV 파일로 내보냅니다.

출력

OpsData 객체 - 실행서가 성공적으로 실행되면 대상 S3 버킷에서 내보낸 OpsData 객체를 찾을 수 있습니다.

AWS-ExportPatchReportToS3

설명

이 실행서는 AWS Systems Manager 패치 관리자에서 패치 요약 데이터 및 패치 세부 정보 목록을 검색하고 지정된 Amazon Simple Storage Service(Amazon S3) 버킷의 .csv 파일로 내보냅니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- assumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우 Systems Manager Automation에서는 이 문서를 실행하는 사용자의 권한을 사용합니다.
- s3BucketName

  유형: 문자열

  설명: (필수) 출력 파일을 다운로드할 S3 버킷입니다.
- snsTopicArn

유형: 문자열

설명: (선택 사항) 다운로드가 완료될 때 알릴 Amazon Simple Notification Service(Amazon SNS) 주제 Amazon 리소스 이름(ARN)입니다.

- snsSuccessMessage

  유형: 문자열

  설명: (선택 사항) 실행서가 완료될 때 전송할 메시지의 텍스트입니다.

- targets

  유형: 문자열

  설명: (필수) 특정 인스턴스에 대한 패치 데이터를 보고할지 아니면 모든 인스턴스에 대한 패치 데이터를 보고할지 여부를 나타내는 인스턴스 ID 또는 와일드카드 문자(*)입니다.

문서 단계

ExportReportStep – 이 단계의 작업은 `targets` 파라미터 값에 따라 달라집니다. `targets`가 `instanceids=*` 형식인 경우, 단계는 계정의 인스턴스에 대해 최대 10,000개의 패치 요약을 검색하고 데이터를 .csv 파일로 내보냅니다.

`targets`가 `instanceids=<instance-id>` 형식인 경우, 단계는 계정의 지정된 인스턴스에 대한 패치 요약과 모든 패치를 모두 검색하여 .csv 파일로 내보냅니다.

출력

PatchSummary/패치 객체 - 실행서가 성공적으로 실행되면 내보낸 패치 보고서 객체가 대상 S3 버킷에 다운로드됩니다.

AWS-SetupInventory

설명

한 개 이상의 관리형 인스턴스에 대해 Systems Manager Inventory 연결을 생성합니다. 시스템에서 연결의 일정에 따라 인스턴스에서 메타데이터를 수집합니다. 자세한 내용은 AWS Systems Manager 인벤토리를 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- 애플리케이션

  유형: 문자열

  기본값: Enabled

  설명: (선택 사항) 설치한 애플리케이션에 대한 메타데이터를 수집합니다.
- AssociatedDocName

  유형: 문자열

  기본값: `AWS-GatherSoftwareInventory`

  설명: (선택 사항) 관리형 인스턴스에서 인벤토리를 수집하는 데 사용되는 실행서의 이름입니다.
- AssociationName

  유형: 문자열

  설명: (선택 사항) 인스턴스에 할당할 인벤토리 연결 이름입니다.
- AssocWaitTime

  유형: 문자열

  기본값: PT5M

  설명: (선택 사항) 인벤토리 연결 시작 시간에 도달했을 때 인벤토리 수집을 일시 중지해야 하는 시간 길이입니다. 시간은 ISO 8601 형식을 사용합니다.
- AutomationAssumeRole

유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- `AwsComponents`

  유형: 문자열

  기본값: Enabled

  설명: (선택 사항) 와 같은 AWS 구성 요소에 대한 메타데이터를 수집합니다 amazon-ssm-agent.

- CustomInventory

  유형: 문자열

  기본값: Enabled

  설명: (선택 사항) 사용자 지정 인벤토리 메타데이터를 수집합니다.

- 파일

  유형: 문자열

  설명: (선택 사항) 인스턴스의 파일에 대한 메타데이터를 수집합니다. 이러한 유형의 인벤토리 데이터를 수집하는 방법에 대한 자세한 내용은 파일 및 Windows 레지스트리 인벤토리 작업을 참조하세요. SSMAgent 버전 2.2.64.0 이상이 필요합니다. Linux 예: `[{"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

  유형: 문자열

  기본값: Enabled

  설명: (선택 사항) CPU 모델, 속도 및 코어 수를 포함하여 인스턴스에 대한 추가 정보를 수집하여 몇 가지 예를 들어 보겠습니다.

- InstanceIds

  유형: 문자열

  기본값: *

  설명: 인벤토리를 만들려는 (필수) EC2 인스턴스입니다.

- LambdaAssumeRole

  유형: 문자열

  설명: (선택 사항) AutomationARN에서 생성한 Lambda가 사용자를 대신하여 작업을 수행하도록 허용하는 역할의 입니다. 지정하지 않을 경우 Lambda 함수를 실행할 임시 역할이 생성됩니다.

- NetworkConfig

  유형: 문자열

  기본값: Enabled

  설명: (선택 사항) 네트워크 구성에 대한 메타데이터를 수집합니다.

- OutputS3BucketName

  유형: 문자열

  설명: (선택 사항) 인벤토리 로그 데이터를 기록할 Amazon S3 버킷의 이름입니다.

- OutputS3KeyPrefix

  유형: 문자열

  설명: (선택 사항) 인벤토리 로그 데이터를 기록할 Amazon S3 키 접두사(하위 폴더)입니다.

- OutputS3Region

  유형: 문자열

  설명: (선택 사항) Amazon S3 AWS 리전 가 있는 의 이름입니다.

- 일정

  유형: 문자열

  기본값: cron(0 */30 * * * ? *)

설명: (선택 사항) 인벤토리 연결 일정의 Cron 표현식입니다. 기본값은 30분입니다.

- 서비스

  유형: 문자열

  기본값: Enabled

  설명: (선택 사항, Windows OS만 해당, SSMAgent 버전 2.2.64.0 이상 필요) 서비스 구성을 위한 데이터를 수집합니다.

- WindowsRegistry

  유형: 문자열

  설명: (선택 사항) Microsoft Windows 레지스트리 키에 대한 메타데이터를 수집합니다. 이러한 유형의 인벤토리 데이터를 수집하는 방법에 대한 자세한 내용은 파일 및 Windows 레지스트리 인벤토리 작업을 참조하세요. SSM 에이전트 버전 2.2.64.0 이상이 필요합니다. 예: [{'Path':'HKEY_CURRENT_CONFIG\System', 'Recursive':true}, {'Path':'HKEY_LOCAL_MACHINESOFTWARE\Amazon\MachineImage', 'ValueNames': ['AMIName']}]

- WindowsRoles

  유형: 문자열

  기본값: Enabled

  설명: (선택 사항) 인스턴스의 Windows 역할에 대한 정보를 수집합니다. Windows 운영 체제에만 적용합니다. SSMAgent 버전 2.2.64.0 이상이 필요합니다.

- WindowsUpdates

  유형: 문자열

  기본값: Enabled

  설명: (선택 사항) 인스턴스의 모든 Windows 업데이트에 대한 데이터를 수집합니다.

AWS-SetupManagedInstance

설명

Systems Manager 액세스에 대한 AWS Identity and Access Management (IAM) 역할이 있는 인스턴스를 구성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: 구성할 EC2 인스턴스의 (필수) ID
- LambdaAssumeRole

  유형: 문자열

  설명: (선택 사항) AutomationARN에서 생성한 Lambda가 사용자를 대신하여 작업을 수행하도록 허용하는 역할의 입니다. 지정하지 않을 경우 Lambda 함수를 실행할 임시 역할이 생성됩니다.
- RoleName

  유형: 문자열

기본값: SSMRoleForManagedInstance

설명: (선택 사항) EC2 인스턴스의 IAM 역할 이름입니다. 이 역할이 없는 경우에는 생성됩니다. 이 값을 지정할 때 역할에 mazonSSMManagedInstanceCore 관리형 정책이 포함되어 있는지 확인합니다.

AWS-SetupManagedRoleOnEC2Instance

설명

Systems Manager 액세스에 대한 SSMRoleForManagedInstance 관리형 IAM 역할로 인스턴스를 구성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  유형: 문자열

설명: 구성할 EC2 인스턴스의 (필수) ID

- LambdaAssumeRole

  유형: 문자열

  설명: (선택 사항) AutomationARN에서 생성한 Lambda가 사용자를 대신하여 작업을 수행하도록 허용하는 역할의 입니다. 지정하지 않을 경우 Lambda 함수를 실행할 임시 역할이 생성됩니다.

- RoleName

  유형: 문자열

  기본값: SSMRoleForManagedInstance

  설명: (선택 사항) EC2 인스턴스의 IAM 역할 이름입니다. 이 역할이 없는 경우에는 생성됩니다. 이 값을 지정할 때 역할에 mazonSSMManagedInstanceCore 관리형 정책이 포함되어 있는지 확인합니다.

AWSSupport-TroubleshootManagedInstance

설명

`AWSSupport-TroubleshootManagedInstance` 실행서를 통해 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 AWS Systems Manager에 의해 관리됨으로 보고되지 않는 이유를 파악할 수 있습니다. 이 실행서는 보안 그룹 규칙, VPC 엔드포인트, 네트워크 액세스 제어 목록(ACL) 규칙, 라우팅 테이블을 비롯한 인스턴스의 VPC 구성을 검토합니다. 또한 필수 권한이 포함된 AWS Identity and Access Management(IAM) 인스턴스 프로파일이 인스턴스에 연결되어 있는지 확인합니다.

> **Important**
>
> 이 자동화 런북은 IPv6 규칙을 평가하지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId

  유형: 문자열

  설명: (필수) Systems Manager에서 관리하는 것으로 보고되지 않는 Amazon EC2 인스턴스의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeScript` - 인스턴스의 `PingStatus`를 수집합니다.
- `aws:branch` - 인스턴스가 이미 Systems Manager에서 관리하는 것으로 보고되고 있는지 여부를 기반으로 분기합니다.
- `aws:executeAwsApi` - VPC 구성을 포함하여 인스턴스에 대한 세부 정보를 수집합니다.
- `aws:executeScript` - 해당하는 경우, Systems Manager와 함께 사용하도록 배포된 VPC 엔드포인트와 관련된 추가 세부 정보를 수집하고, VPC 엔드포인트에 연결된 보안 그룹이 인스턴스의 TCP 포트 443을 통한 인바운드 트래픽을 허용하는지 확인합니다.
- `aws:executeScript` - 라우팅 테이블이 VPC 엔드포인트 또는 퍼블릭 Systems Manager 엔드포인트에 대한 트래픽을 허용하는지 확인합니다.
- `aws:executeScript` - 네트워크 ACL 규칙이 VPC 엔드포인트 또는 퍼블릭 Systems Manager 엔드포인트에 대한 트래픽을 허용하는지 확인합니다.
- `aws:executeScript` - VPC 엔드포인트 또는 퍼블릭 Systems Manager 엔드포인트로 향하는 아웃바운드 트래픽이 인스턴스와 연결된 보안 그룹에서 허용되는지 확인합니다.
- `aws:executeScript` - 인스턴스에 연결된 인스턴스 프로파일에 필요한 권한을 제공하는 관리형 정책이 포함되어 있는지 확인합니다.
- `aws:branch` - 인스턴스의 운영 체제를 기반으로 분기합니다.
- `aws:executeScript` - `ssmagent-toolkit-linux` 쉘 스크립트에 대한 참조를 제공합니다.
- `aws:executeScript`- 스크립트에 대한 참조를 제공합니다. `ssmagent-toolkit-windows` PowerShell

- `aws:executeScript` - 자동화를 위한 최종 출력을 생성합니다.
- `aws:executeScript` - 인스턴스의 `PingStatus`가 `Online`인 경우 Systems Manager에서 인스턴스를 이미 관리하고 있다는 사실을 반환합니다.

AWSSupport-TroubleshootPatchManagerLinux

설명

`AWSSupport-TroubleshootPatchManagerLinux`런북은 “Patch Manager” AWS Systems Manager 기능을 사용하여 Linux 기반 관리 노드에서 패치 실패를 일으킬 수 있는 일반적인 문제를 해결합니다. 이 런북의 주요 목표는 패치 명령 오류의 근본 원인을 식별하고 수정 계획을 제안하는 것입니다.

어떻게 작동하나요?

`AWSSupport-TroubleshootPatchManagerLinux`런북은 문제 해결을 위해 사용자가 제공한 두 개의 인스턴스 ID/명령 ID를 고려합니다. 명령 ID가 제공되지 않은 경우 제공된 인스턴스에서 지난 30일 이내에 실패한 최신 패치 명령을 선택합니다. 명령 상태, 사전 요구 사항 이행 및 OS 배포를 확인한 후 Runbook은 로그 분석기 패키지를 다운로드하고 실행합니다. 출력에는 문제의 근본 원인과 문제 해결에 필요한 조치가 포함됩니다.

문서 유형

자동화

소유자

Amazon

플랫폼

- 아마존 리눅스 2와 AL2 023
- 레드햇 엔터프라이즈 리눅스 8.X 및 9.X
- 센토스 8.X 및 9.X
- SUSE15.X

Parameters

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:SendCommand`
- `ssm:DescribeDocument`
- `ssm:GetCommandInvocation`
- `ssm:ListCommands`
- `ssm:DescribeInstanceInformation`
- `ssm:ListCommandInvocations`
- `ssm:GetDocument`
- `ssm:DescribeAutomationExecutions`
- `ssm:GetAutomationExecution`

지침

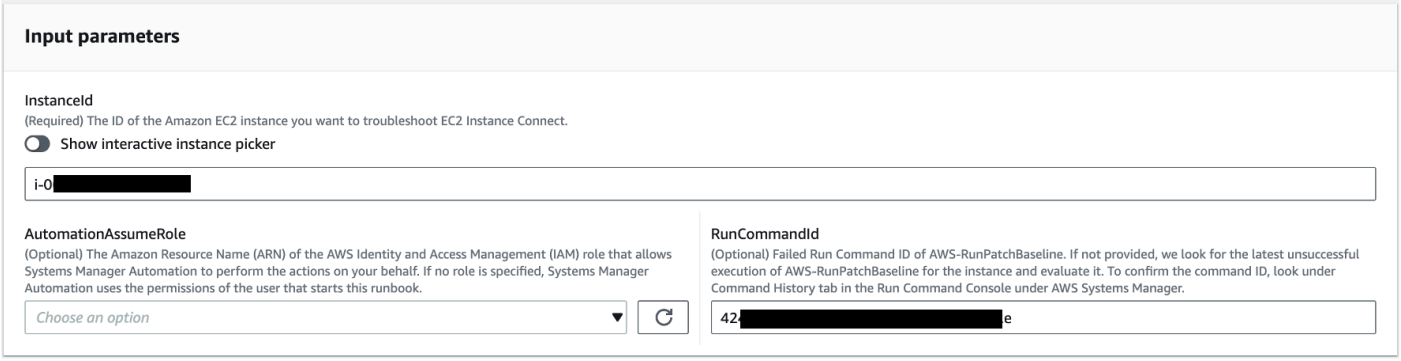
다음 단계에 따라 자동화를 구성합니다.

1. `AWSSupport-TroubleshootPatchManagerLinux` AWS Systems Manager 콘솔에서 로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 매개변수에 다음을 입력합니다.
   - InstanceId (필수):

     대화형 인스턴스 선택기를 사용하여 패치 명령이 실패한 Linux 기반 SSM 관리형 노드 (Amazon Elastic Compute Cloud (AmazonEC2) 또는 하이브리드 활성화 서버) 의 ID를 선택하거나 SSM 관리형 인스턴스의 ID를 수동으로 입력합니다.
   - AutomationAssumeRole (선택 사항):

     자동화가 사용자 대신 작업을 수행하도록 허용하는 IAM 역할을 입력합니다. ARN 역할이 지정되지 않은 경우 자동화는 이 런북을 시작하는 사용자의 권한을 사용합니다.
   - RunCommandId (선택 사항):

     `AWS-RunPatchBaseline`문서의 실행 실패 명령 ID를 입력합니다. 명령 ID를 제공하지 않으면 Runbook은 선택한 인스턴스에서 최근 30일 이내에 실패한 최신 패치 명령을 찾습니다.



4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
   - CheckConcurrency:

     동일한 인스턴스를 대상으로 하는 이 런북이 한 번만 실행되도록 합니다. 런북에서 동일한 인스턴스를 대상으로 진행 중인 다른 실행을 발견하면 오류가 반환되고 종료됩니다.
   - ValidateCommandID:

     입력 매개변수로 제공된 명령 ID가 `AWS-RunPatchBaseline` SSM 문서에 대해 실행되었는지 확인합니다. 명령 ID가 제공되지 않은 경우 Runbook은 선택한 인스턴스에서 최근 30일 `AWS-RunPatchBaseline` 이내에 실행이 실패한 것으로 간주합니다.
   - BranchOnCommandStatus:

     제공된 명령의 상태가 실패했음을 확인합니다. 그렇지 않으면 런북은 실행을 종료하고 제공된 명령이 성공적으로 실행되었음을 알리는 보고서를 생성합니다.
   - VerifyPrerequistes:

     위에서 언급한 사전 요구 사항이 충족되었는지 확인합니다.
   - GetPlatformDetails:

     운영 체제 (OS) 배포판 및 버전을 검색합니다.
   - GetDownloadURL:

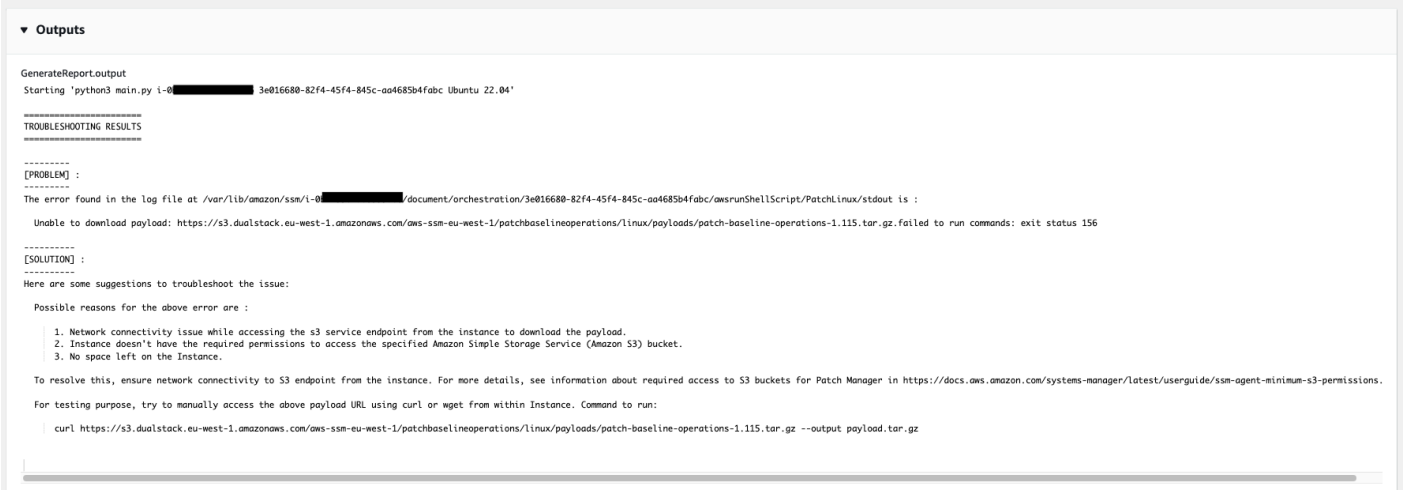
     PatchManager 로그 분석기 패키지의 다운로드를 URL 검색합니다.
   - EvaluatePatchManagerLogs:

     인스턴스에서 PatchManager Log Analyzer python 패키지를 다운로드하고 실행하여 로그 파일을 평가합니다.

- GenerateReport:

  식별된 문제와 제안된 해결 방법을 포함하는 런북 실행의 최종 보고서를 생성합니다.

7. 완료 후 출력 섹션에서 실행의 세부 결과를 검토하십시오.



참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWSSupport-TroubleshootSessionManager

설명

`AWSSupport-TroubleshootSessionManager` 실행서는 Session Manager를 사용하여 관리형 Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스에 연결할 수 없는 일반적인 문제를 해결하는 데 도움이 됩니다. Session Manager는 의 기능입니다 AWS Systems Manager. 이 실행서는 다음 내용을 확인합니다.

- 인스턴스가 실행되고 있고 Systems Manager에서 관리하는 것으로 보고되고 있는지 확인합니다.
- 인스턴스가 Systems Manager에서 관리하는 것으로 보고되고 있지 않은 경우 `AWSSupport-TroubleshootManagedInstance` 실행서를 실행합니다.

- 인스턴스에 설치된 SSM 에이전트의 버전을 확인합니다.
- Session Manager에 권장되는 (IAM) 정책이 AWS Identity and Access Management 포함된 인스턴스 프로파일이 Amazon EC2 인스턴스에 연결되어 있는지 확인합니다.
- 인스턴스에서 SSM 에이전트 로그를 수집합니다.
- Session Manager 기본 설정을 분석합니다.
- `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 실행서를 실행하여 Session Manager, AWS Key Management Service (AWS KMS), Amazon Simple Storage Service(Amazon S3) 및 Amazon CloudWatch Logs(CloudWatch Logs)의 엔드포인트에 대한 인스턴스의 연결을 분석합니다.

고려 사항

- 하이브리드 관리형 노드는 지원되지 않습니다.
- 이 런북은 권장 관리형 IAM 정책이 인스턴스 프로파일에 연결되어 있는지 여부만 확인합니다. 인스턴스 프로파일에 포함된 IAM 또는 AWS KMS 권한은 분석하지 않습니다.

> **Important**
>
> `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 실행서는 VPC Reachability Analyzer를 사용하여 소스와 서비스 엔드포인트 간의 네트워크 연결을 분석합니다. 소스와 대상 간의 분석 실행당 요금이 부과됩니다. 자세한 내용은 Amazon VPC 요금 섹션을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- InstanceId

  유형: 문자열

  설명: (필수) Session Manager를 사용하여 연결할 수 없는 Amazon EC2 인스턴스의 ID입니다.
- SessionPreferenceDocument

  유형: 문자열

  기본값: SSM-SessionManagerRunShell

  설명: (선택 사항) 세션 기본 설정 문서의 이름입니다. 세션을 시작할 때 사용자 지정 세션 기본 설정 문서를 지정하지 않으면 기본값을 사용합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

1. `aws:waitForAwsResourceProperty`: 대상 인스턴스가 상태 검사를 통과할 때까지 최대 6분 동안 기다립니다.
2. `aws:executeScript`: 세션 기본 설정 문서를 구문 분석합니다.
3. `aws:executeAwsApi`: 인스턴스에 연결된 인스턴스 프로파일ARN의 를 가져옵니다.
4. `aws:executeAwsApi`: 인스턴스가 Systems Manager에서 관리하는 것으로 보고되고 있는지 확인합니다.

5. `aws:branch`: 인스턴스가 Systems Manager에서 관리하는 것으로 보고되고 있는지 여부를 기반으로 분기합니다.
6. `aws:executeScript`: 인스턴스에 설치된 SSM 에이전트가 Session Manager를 지원하는지 확인합니다.
7. `aws:branch`: 인스턴스의 플랫폼을 기반으로 분기하여 `ssm-cli` 로그를 수집합니다.
8. `aws:runCommand`: `ssm-cli`에서 로그 출력을 수집합니다.Linux 또는 macOS 인스턴스.
9. `aws:runCommand`: `ssm-cli`에서 로그 출력을 수집합니다.Windows 인스턴스.
10. `aws:executeScript`: `ssm-cli` 로그를 구문 분석합니다.
11. `aws:executeScript`: 권장 IAM 정책이 인스턴스 프로파일에 연결되어 있는지 확인합니다.
12. `aws:branch`: `ssm-cli` 로그를 기반으로 `ssmmessages` 엔드포인트 연결을 평가할지 여부를 결정합니다.
13. `aws:executeAutomation`: 인스턴스를 `ssmmessages` 엔드포인트에 연결할 수 있는지 여부를 평가합니다.
14. `aws:branch`: `ssm-cli` 로그와 세션 기본 설정을 기반으로 Amazon S3 엔드포인트 연결을 평가할지 여부를 결정합니다.
15. `aws:executeAutomation`: 인스턴스를 Amazon S3 엔드포인트에 연결할 수 있는지 여부를 평가합니다.
16. `aws:branch`: `ssm-cli` 로그 및 세션 기본 설정을 기반으로 AWS KMS 엔드포인트 연결을 평가할지 여부를 결정합니다.
17. `aws:executeAutomation`: 인스턴스가 AWS KMS 엔드포인트에 연결할 수 있는지 여부를 평가합니다.
18. `aws:branch`: CloudWatch 로그 및 세션 기본 설정을 기반으로 `ssm-cli` 로그 엔드포인트 연결을 평가할지 여부를 결정합니다.
19. `aws:executeAutomation`: 인스턴스가 CloudWatch Logs 엔드포인트에 연결할 수 있는지 여부를 평가합니다.
20. `aws:executeAutomation`: `AWSSupport-TroubleshootManagedInstance` 실행서를 실행합니다.
21. `aws:executeScript`: 이전 단계의 출력을 컴파일하고 보고서를 출력합니다.

출력

- `generateReport.EvalReport` - 실행서에서 수행한 검사 결과를 일반 텍스트로 표시합니다.

타사

AWS Systems Manager Automation은 타사 제품 및 서비스에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-CreateJiraIssue
- AWS-CreateServiceNowIncident
- AWS-RunPacker

AWS-CreateJiraIssue

설명

Jira에서 문제를 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AssigneeName

  유형: 문자열

  설명: (선택 사항) 문제가 할당되어야 할 사람의 사용자 이름입니다.
- DueDate

  유형: 문자열

설명: (선택 사항) 형식의 문제에 대한 기한입니다 yyyy-mm-dd.

- IssueDescription

  유형: 문자열

  설명: (필수) 문제에 대한 자세한 설명입니다.

- IssueSummary

  유형: 문자열

  설명: (필수) 문제에 대한 간략한 설명입니다.

- IssueTypeName

  유형: 문자열

  설명: (필수) 생성하려는 문제의 유형 이름입니다(예: 작업, 하위 작업, 버그 등).

- JiraURL

  유형: 문자열

  설명: (필수) Jira 인스턴스의 URL입니다.

- JiraUsername

  유형: 문자열

  설명: (필수) 문제를 생성할 사용자의 이름입니다.

- PriorityName

  유형: 문자열

  설명: (선택 사항) 문제의 우선 순위 이름입니다.

- ProjectKey

  유형: 문자열

  설명: (필수) 문제가 생성되어야 하는 프로젝트의 키입니다.

- SSMParameterName

  유형: 문자열

설명: (필수) Jira 사용자의 API 키 또는 암호를 포함하는 암호화된 SSM 파라미터의 이름입니다.

문서 단계

`aws:createStack` - CloudFormation 스택을 생성하여 Lambda IAM 역할 및 함수를 생성합니다.

`aws:invokeLambdaFunction` - Lambda 함수를 호출하여 Jira 문제를 생성합니다.

`aws:deleteStack` - 생성된 CloudFormation 스택을 삭제합니다.

출력

IssueId: 새로 생성된 Jira 문제의 ID

AWS-CreateServiceNowIncident

설명

인시던트 테이블에 ServiceNow 인시던트를 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 범주

  유형: 문자열

  설명: (선택 사항) 인시던트의 범주입니다.

  유효한 값: None | Inquiry/Help | Software | Hardware | Network | Database

  기본값: None
- 설명

  유형: 문자열

  설명: (필수) 인시던트에 대한 자세한 설명입니다.
- 영향

  유형: 문자열

  설명: (선택 사항) 인시던트가 비즈니스에 미치는 영향입니다.

  유효한 값: High | Medium | Low

  기본값: Low
- ServiceNowInstanceUsername

  유형: 문자열

  설명: (필수) 인시던트가 생성되는 사용자의 이름입니다.
- ServiceNowInstancePassword

  유형: 문자열

  설명: (필수) ServiceNow 사용자의 암호가 포함된 암호화된 SSM 파라미터의 이름입니다.
- ServiceNowInstanceURL

  유형: 문자열

  설명: (필수) ServiceNow 인스턴스URL의
- ShortDescription

  유형: 문자열

설명: (필수) 인시턴트에 대한 간략한 설명입니다.

- Subcategory

  유형: 문자열

  설명: (선택 사항) 인시던트의 하위 범주입니다.

  유효한 값: 없음 | 바이러스 백신 | 이메일 | 내부 애플리케이션 | 운영 체제 | CPU 디스크 | 키보드 | 하드웨어 | 메모리 | 모니터 | 마우스 | DHCP DNS | IP 주소 VPN | 무선 | DB2 | MS SQL 서버 | Oracle

  기본값: None

문서 단계

Push_incident – 인시던트 정보를 에 푸시합니다 ServiceNow.

출력

Push_incident.incidentID - 생성된 인시던트 ID.

AWS-RunPacker

설명

이 런북은 HashiCorp Packer 도구를 사용하여 기계 이미지를 생성하는 데 사용되는 Packer 템플릿을 검증, 수정 또는 빌드합니다. 이 실행서는 Packer v1.7.2를 사용합니다.

> **Note**
>
> `vpc_id` 값을 지정하는 경우 퍼블릭 서브넷의 `subnet_id` 값도 지정해야 합니다. 서브넷의 IPv4 퍼블릭 주소 지정 속성을 수정하지 않는 한 true`associate_public_ip_address`로도 설정해야 합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- Force

  타입: 부울

  설명: 이전 빌드의 아티팩트가 빌드 실행을 금지할 때 빌더가 강제로 실행되도록 하는 Packer 옵션입니다.

- Mode

  유형: 문자열

  설명: 템플릿에 대해 유효성을 검사할 때 Packer를 사용하는 모드 또는 명령입니다. 옵션에는 `Build`, `Validate` 및 `Fix`이 포함됩니다.

- TemplateFileName

  유형: 문자열

  설명: S3 버킷에 있는 템플릿 파일의 이름 또는 키입니다.

- TemplateS3BucketName

  유형: 문자열

  설명: Packer 템플릿이 포함된 S3 버킷의 이름입니다.

문서 단계

RunPackerProcessTemplate - Packer 도구를 사용하여 템플릿에 대해 선택한 모드를 실행합니다.

출력

RunPackerProcessTemplate.output – Packer 도구의 stdout입니다.

RunPackerProcessTemplate.fixed_template_key - S3 버킷에 저장된 템플릿의 이름으로, 'Fix' 모드에서 실행할 때만 사용합니다.

RunPackerProcessTemplate.s3_bucket - “Fix” 모드에서 실행할 때만 사용할 고정 템플릿이 포함된 S3 버킷의 이름입니다.

Amazon VPC

AWS Systems Manager 자동화는 Amazon Virtual Private Cloud 에 사전 정의된 런북을 제공합니다. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- 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

설명

이 실행서는 지정한 보안 그룹에서 모든 수신 및 송신 규칙을 제거합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역

할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- SecurityGroupId

  유형: 문자열

  설명: (필수) 종료하려는 보안 그룹의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

문서 단계

- `aws:executeScript` - `SecurityGroupId` 파라미터에 지정한 보안 그룹에서 모든 수신 및 송신 규칙을 제거합니다.

AWSSupport-ConfigureDNSQueryLogging

설명

`AWSSupport-ConfigureDNSQueryLogging` 실행서는 가상 프라이빗 클라우드(VPC)에서 시작된 DNS 쿼리 또는 Amazon Route 53 호스팅 영역에 대한 로깅을 구성합니다. Amazon CloudWatch Logs, Amazon Simple Storage Service(Amazon S3) 또는 Amazon Data Firehose에 쿼리 로그를 게시하도록 선택할 수 있습니다. 쿼리 로깅 및 해석기 쿼리 로그에 대한 자세한 내용은 퍼블릭 DNS 쿼리 로깅 및 해석기 쿼리 로깅을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- LogDestinationArn

  유형: 문자열

  설명: (선택 사항) 쿼리 CloudWatch 로그를 보내려는 로그 그룹, Amazon S3 버킷 또는 Firehose 스트림ARN의 입니다. Route 53 퍼블릭 DNS 쿼리 로깅은 CloudWatch 로그 그룹만 지원합니다. 이 파라미터의 값을 지정하지 않으면 자동화는 형식 `AWSSupport-ConfigureDNSQueryLogging-{automation: EXECUTION_ID }` 이 인 CloudWatch 로그 그룹과 쿼리 로그를 게시하는 IAM 리소스 정책을 생성합니다. 자동화에서 생성한 CloudWatch 로그 그룹의 보존 기간은 14일입니다.

- QueryLogType

  유형: 문자열

  설명: (선택 사항) 기록하려는 쿼리 유형입니다.

  유효한 값: Public | Resolver/Private

  기본값: Public

- ResourceId

  유형: 문자열

  설명: (필수) 쿼리를 기록하려는 리소스의 ID입니다. `QueryLogType` 파라미터에 대해 `Public`을 지정하는 경우 리소스는 Route 53 프라이빗 호스팅 영역의 ID여야 합니다. `QueryLogType` 파라미터에 `Resolver/Private` 를 지정하는 경우 리소스는 의 ID여야 합니다VPC.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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`

문서 단계

- `aws:executeScript` - `ResourceId` 파라미터에 대해 지정하는 리소스가 존재하는지 확인하고, 리소스 유형이 필수 `QueryLogType` 옵션과 일치하는지 확인합니다.
- `aws:executeScript` - `LogDestinationArn` 파라미터에 대해 지정하는 값이 필수 `QueryLogType` 값과 일치하는지 확인합니다.
- `aws:executeScript` - Route 53이 로그 로그 로그 그룹에 CloudWatch 로그를 게시하는 데 필요한 권한을 확인하고, 로그가 없는 경우 필요한 IAM 리소스 정책을 생성합니다.
- `aws:executeScript` - 선택한 대상에 대한 DNS 쿼리 로깅을 활성화합니다.

AWSSupport-ConfigureTrafficMirroring

설명

`AWSSupport-ConfigureTrafficMirroring` 실행서는 로드 밸런서와 Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스 간의 연결 문제를 해결하는 데 도움이 되도록 트래픽 미러링을 구성합니다. 트래픽 미러링은 인스턴스에 연결된 네트워크 인터페이스의 인바운드 및 아웃바운드 트래픽을 복사합니다. 트래픽 미러링을 구성할 수 있도록 이 실행서는 필수 대상, 필터 및 세션을 생성합니다. 기본적으로 실행서는 Amazon 를 제외한 모든 프로토콜의 모든 인바운드 및 아웃바운드 트래픽에 대해 미러링을 구성합니다DNS. 특정 소스 및 대상의 트래픽을 미러링하려는 경우 자동화가 완료된 후 인바운드 및 아웃바운드 규칙을 수정할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- 소스ENI

  유형: 문자열

  설명: (필수) 트래픽 미러링을 구성하려는 탄력적 네트워크 인터페이스입니다.
- 대상

  유형: 문자열

  설명: (필수) 미러링된 트래픽의 대상입니다. 네트워크 인터페이스, Network Load Balancer 또는 Gateway Load Balancer 엔드포인트의 ID를 지정해야 합니다. Network Load Balancer 를 지정하는 경우 포트 4789에 UDP리스너가 있어야 합니다.
- SessionNumber

  유형: 문자열

  유효한 값: 1-32766

  설명: (필수) 사용하려는 미러 세션 수입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ec2:CreateTrafficMirrorTarget`

- `ec2:CreateTrafficMirrorFilter`
- `ec2:CreateTrafficMirrorFilterRule`
- `ec2:CreateTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorFilter`
- `ec2:DeleteTrafficMirrorSession`
- `ec2:DeleteTrafficMirrorFilterRule`
- `iam:ListRoles`
- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`

문서 단계

- `aws:executeScript` - 스크립트를 실행하여 대상을 생성합니다.
- `aws:executeAwsApi` - 필터 규칙을 생성합니다.
- `aws:executeAwsApi` - 모든 인바운드 트래픽에 대한 미러 필터 규칙을 생성합니다.
- `aws:executeAwsApi` - 모든 아웃바운드 트래픽에 대한 미러 필터 규칙을 생성합니다.
- `aws:executeAwsApi` - 트래픽 미러 세션을 생성합니다.
- `aws:executeAwsApi` - 필터 또는 세션 생성에 실패할 경우 필터를 삭제합니다.
- `aws:executeAwsApi` - 필터 또는 세션 생성에 실패할 경우 대상을 삭제합니다.

출력

CreateFilter.FilterId

CreateSession.SessionId

CreateTarget.TargetIDOutput

AWSSupport-ConnectivityTroubleshooter

설명

`AWSSupport-ConnectivityTroubleshooter` 실행서는 다음 항목 간의 연결 문제를 진단합니다.

- AWS Amazon Virtual Private Cloud 내의 리소스(AmazonVPC)

- AWS VPC 피어링을 사용하여 AWS 리전 연결된 동일한 VPCs 내 다른 Amazon의 리소스
- AWS Amazon의 리소스 VPC 및 인터넷 게이트웨이를 사용하는 인터넷 리소스
- AWS 네트워크 주소 변환(NAT) 게이트웨이를 사용하는 Amazon VPC 및 인터넷 리소스의 리소스

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- DestinationIP

  유형: 문자열

  설명: (필수) 연결하려는 리소스의 IPv4 주소입니다.
- DestinationPort

  유형: 문자열

  기본값: true

  설명: (필수) 대상 리소스에서 연결하려는 포트 번호입니다.
- DestinationVpc

유형: 문자열

기본값: All

설명: (선택 사항) 연결을 테스트VPC하려는 Amazon의 ID입니다.

- SourceIP

  유형: 문자열

  설명: (필수) 연결을 테스트VPC하려는 Amazon AWS 리소스의 프라이빗 IPv4 주소입니다.

- SourcePortRange

  유형: 문자열

  설명: (선택 사항) 연결을 테스트VPC하려는 Amazon의 AWS 리소스에서 사용하는 포트 범위입니다.

- SourceVpc

  유형: 문자열

  기본값: All

  설명: (선택 사항) 연결을 테스트VPC하려는 Amazon의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcPeeringConnections`

문서 단계

- `aws:executeScript` - `SourceIP` 파라미터에서 지정한 AWS 리소스에 대한 세부 정보를 수집합니다.

- `aws:executeScript` - 이전 단계에서 수집한 경로를 사용하여 AWS 리소스에서 네트워크 트래픽의 대상을 결정합니다.
- `aws:branch` - 네트워크 트래픽의 대상을 기반으로 분기합니다.
- `aws:executeAwsApi` - 대상 리소스에 대한 세부 정보를 수집합니다.
- `aws:executeScript` - Amazon이 대상에 대해 반환한 ID가 `DestinationVpc` 파라미터에 지정된 값과 VPC 일치하는지 확인합니다.
- `aws:executeAwsApi` - 소스 및 대상 리소스에 대한 보안 그룹 규칙을 수집합니다.
- `aws:executeScript` - 보안 그룹 규칙이 소스 및 대상 리소스 간에 필요한 트래픽을 허용하는지 확인합니다.
- `aws:executeAwsApi` - 소스 및 대상 리소스의 서브넷과 연결된 네트워크 액세스 제어 목록 (NACLs)을 수집합니다.
- `aws:executeScript` - 가 소스 리소스와 대상 리소스 간에 필요한 트래픽을 NACLs 허용하는지 확인합니다.
- `aws:executeScript` - 라우팅 대상이 인터넷 게이트웨이인 경우 소스에 리소스와 연결된 퍼블릭 IP 주소가 있는지 확인합니다.
- `aws:executeAwsApi` - 소스 리소스의 보안 그룹 규칙을 수집합니다.
- `aws:executeScript` - 보안 그룹 규칙이 소스에서 대상 리소스로 필요한 트래픽을 허용하는지 확인합니다.
- `aws:executeAwsApi` - 소스 리소스의 서브넷과 NACLs 연결된 를 수집합니다.
- `aws:executeScript` - 가 소스 리소스에서 필요한 트래픽을 NACLs 허용하는지 확인합니다.
- `aws:executeAwsApi` - NAT 게이트웨이에 대한 세부 정보를 수집합니다.
- `aws:executeAwsApi` - NAT 게이트웨이의 서브넷과 NACLs 연결된 를 수집합니다.
- `aws:executeScript` - 가 NAT 게이트웨이의 서브넷에서 필요한 트래픽을 NACLs 허용하는지 확인합니다.
- `aws:executeScript` - NAT 게이트웨이의 서브넷과 연결된 경로를 수집합니다.
- `aws:executeScript` - NAT 게이트웨이에 인터넷 게이트웨이에 대한 경로가 있는지 확인합니다.
- `aws:executeAwsApi` - VPC 피어링 연결에 대한 세부 정보를 수집합니다.
- `aws:executeScript` - 둘 다 동일한 리전에 있고 대상에 대해 반환된 IDVPCs가 `DestinationVpc` 파라미터에 지정된 값과 VPC 일치하는지 확인합니다.
- `aws:executeAwsApi` - 대상 리소스의 서브넷을 반환합니다.
- `aws:executeScript` - 피어링된 의 서브넷과 연결된 경로를 수집합니다VPC.
- `aws:executeScript` - 피어링된 에 피어링 연결에 대한 경로VPC가 있는지 확인합니다.

- `aws:executeScript` - 자동화가 대상을 지원하지 않는 경우 소스 리소스로부터 트래픽이 허용되는지 확인합니다.

AWSSupport-TroubleshootVPN

설명

`AWSSupport-TroubleshootVPN`런북은 AWS Site-to-Site VPN 연결의 오류를 추적하고 해결하는 데 도움이 됩니다. 자동화에는 AWS Site-to-Site VPN 연결 터널과 관련된 `IKEv2` 오류를 `IKEv1` 추적하거나 오류를 추적하도록 설계된 여러 가지 자동 검사가 포함됩니다. 자동화는 특정 오류를 일치시키려고 시도하고 해당 해결 방법은 일반적인 문제 목록을 형성합니다.

참고: 이 자동화는 오류를 수정하지 않습니다. 언급된 시간 범위 동안 실행되며 로그 그룹에서 로그 그룹의 오류를 VPN CloudWatch 스캔합니다.

어떻게 작동하나요?

Runbook은 파라미터 검증을 실행하여 입력 파라미터에 포함된 Amazon CloudWatch 로그 그룹이 있는지, 로그 그룹에 VPN 터널 로깅에 해당하는 로그 스트림이 있는지, VPN 연결 ID가 존재하는지, 터널 IP 주소가 존재하는지 확인합니다. VPN로깅을 위해 구성된 CloudWatch 로그 그룹에서 Logs Insights API 호출을 수행합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정

하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- LogGroupName

  유형: 문자열

  설명: (필수) AWS Site-to-Site VPN 연결 로깅을 위해 구성된 Amazon CloudWatch 로그 그룹 이름

  허용된 패턴: `^[\.\-_/#A-Za-z0-9]{1,512}`

- VpnConnectionId

  유형: 문자열

  설명: (필수) 문제를 해결할 AWS Site-to-Site VPN 연결 ID입니다.

  허용된 패턴: `^vpn-[0-9a-f]{8,17}$`

- T unnelAIPAddress

  유형: 문자열

  설명: (필수) 귀하와 관련된 터널 번호 1 IPv4 주소 AWS Site-to-Site VPN.

  허용된 패턴: `^((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}$`

- T unnelBIPAddress

  유형: 문자열

  설명: (선택 사항) 귀하와 관련된 터널 번호 2 IPv4 주소 AWS Site-to-Site VPN.

  허용된 패턴: `^((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

  유형: 문자열

  설명: (필수) 사용 중인 IKE 버전을 선택합니다. 허용된 값:IKEv1, IKEv2

  유효값: `['IKEv1', 'IKEv2']`

- StartTimeinEpoch

유형: 문자열

설명: (선택 사항) 로그 분석 시작 시간입니다. 로그 분석에는 StartTimeinEpoch/EndTimeinEpoch 또는 LookBackPeriod 를 사용할 수 있습니다.

허용된 패턴: `^\d{10}|^$`

- EndTimeinEpoch

  유형: 문자열

  설명: (선택 사항) 로그 분석 종료 시간입니다. StartTimeinEpoch/EndTimeinEpoch 또는 로그 LookBackPeriod 분석에 사용할 수 있습니다. StartTimeinEpochEndTimeinEpoch /를 둘 다 지정하면 LookBackPeriod 이후가 LookBackPeriod 우선합니다.

  허용된 패턴: `^\d{10}|^$`

- LookBackPeriod

  유형: 문자열

  설명: (선택 사항) 로그 분석을 위해 되돌아보는 두 자리 시간(시간)입니다. 유효 범위: 01~99. 다음과 같이 입력하면 이 값이 우선합니다. StartTimeinEpoch EndTime

  허용된 패턴: `^(\d?[1-9]|[1-9]0)|^$`

필수 권한 IAM

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `logs:DescribeLogGroups`
- `logs:GetQueryResults`
- `logs:DescribeLogStreams`
- `logs:StartQuery`
- `ec2:DescribeVpnConnections`

지침

참고: 이 자동화는 로깅 출력 형식이 다음과 같은 경우 VPN 터널 로깅용으로 구성된 CloudWatch 로그 그룹에서 작동합니다JSON.

다음 단계에 따라 자동화를 구성합니다.

1. VPN콘솔에서 AWSSupport-Troubleout으로 이동합니다. AWS Systems Manager
2. 입력 파라미터의 경우, 다음 내용을 입력합니다.
   - AutomationAssumeRole (선택 사항):

     Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있게 해주는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름 (). ARN 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
   - LogGroupName (필수):

     검증할 Amazon CloudWatch 로그 그룹 이름. 로그를 VPN 전송하도록 구성된 CloudWatch 로그 그룹이어야 합니다.
   - VpnConnectionId (필수):

     로그 그룹에 VPN 오류가 있는지 추적되는 AWS Site-to-Site VPN 연결 ID.
   - T unnelAIPAddress (필수):

     AWS Site-to-Site VPN 연결과 관련된 터널 A IP 주소.
   - T unnelBIPAddress (선택 사항):

     AWS Site-to-Site VPN 연결과 관련된 터널 B IP 주소.
   - IKEVersion(필수):

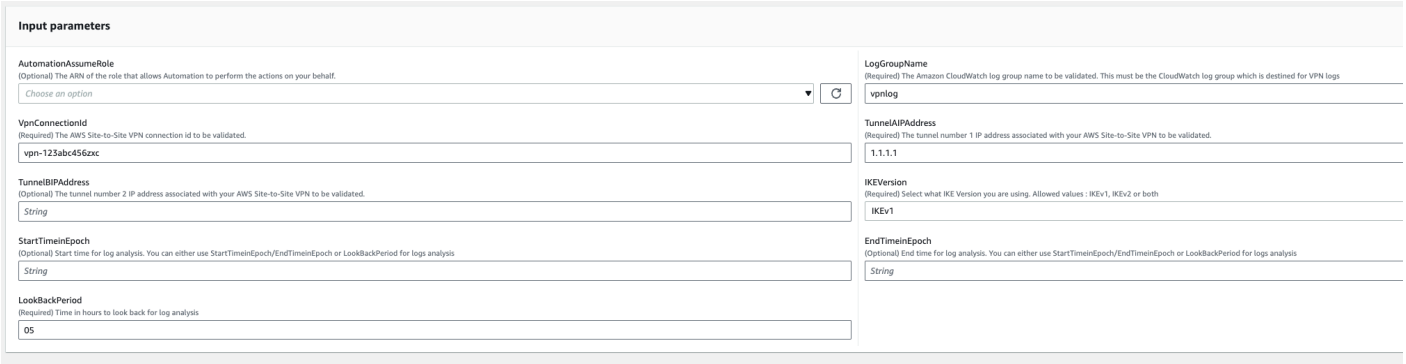
     사용 중인 IKEversion 항목을 선택합니다. 허용된 값:IKEv1,IKEv2.
   - StartTimeinEpoch (선택 사항):

     오류를 쿼리할 시간 범위의 시작입니다. 범위가 포함되므로, 지정된 시작 시간이 쿼리에 포함됩니다. 에포크 타임으로 지정되며, 1970년 1월 1일 00:00:00 이후 경과된 초 수입니다. UTC
   - EndTimeinEpoch (선택 사항):

     오류를 쿼리할 시간 범위의 끝입니다. 범위가 포함되므로, 지정된 종료 시간이 쿼리에 포함됩니다. 에포크 타임으로 지정되며, 1970년 1월 1일 00:00:00 이후 경과된 초 수입니다. UTC
   - LookBackPeriod (필수):

     오류에 대한 쿼리를 다시 검토하는 데 걸리는 시간(시간)입니다.

참고: 로그 분석을 위한 시간 범위를 LookBackPeriod 수정하려면 a StartTimeinEpoch EndTimeinEpoch, or를 구성하십시오. 두 자리 숫자를 시간 단위로 부여하여 자동화 시작 시간부터 과거에 오류가 발생했는지 확인하세요. 또는 특정 시간 범위 내에서 오류가 과거에 발생한 EndTimeinEpoch 경우 대신 StartTimeinEpoch 및 를 LookBackPeriod 포함하십시오.



3. 실행을 선택합니다.
4. 자동화가 시작됩니다.
5. 자동화 실행서는 다음 단계를 수행합니다.
   - parameterValidation:

     자동화에 포함된 입력 파라미터에 대해 일련의 검증을 실행합니다.
   - branchOnValidationOfLogGroup:

     파라미터에 언급된 로그 그룹이 유효한지 확인합니다. 유효하지 않은 경우, 자동화 단계의 추가 시작을 중단합니다.
   - branchOnValidationOfLogStream:

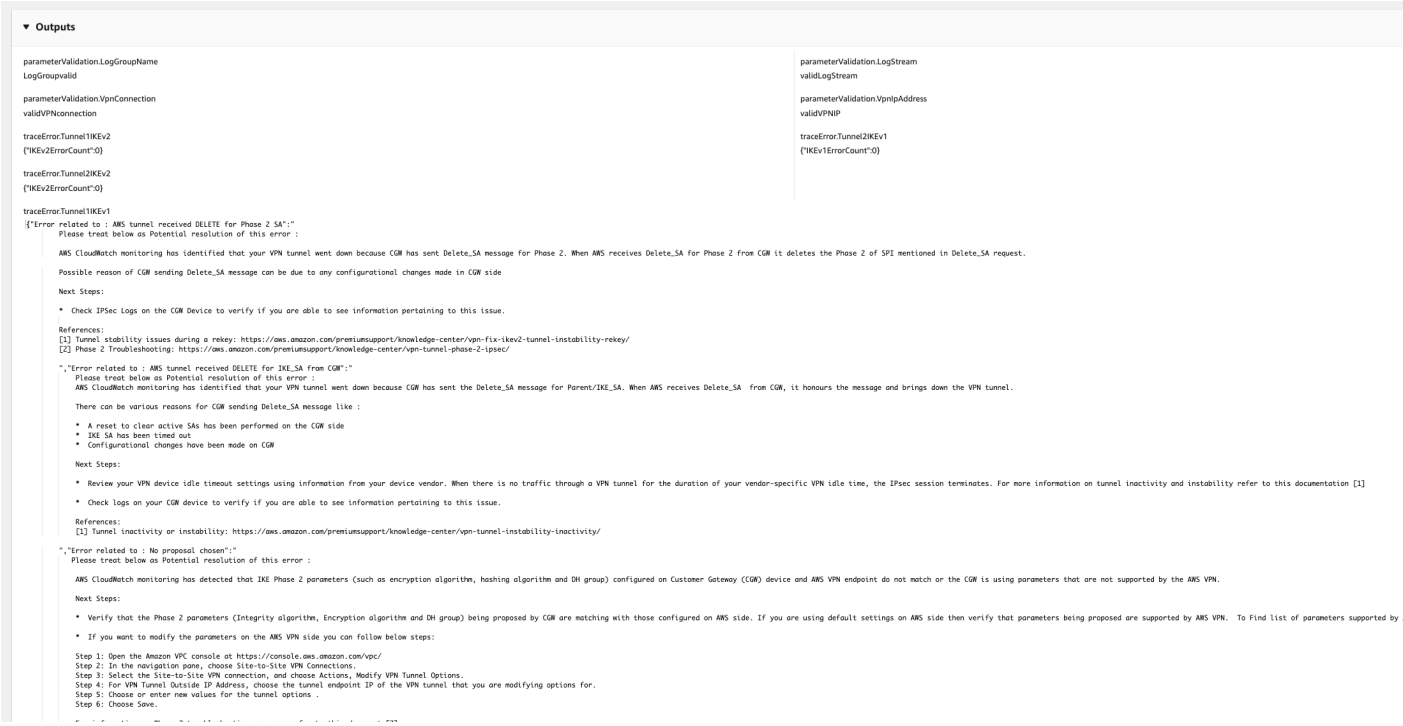
     포함된 로그 그룹에 CloudWatch 로그 스트림이 있는지 확인합니다. 유효하지 않은 경우, 자동화 단계의 추가 시작을 중단합니다.
   - branchOnValidationOfVpnConnectionId:

     매개변수에 포함된 VPN 연결 ID가 유효한지 확인합니다. 유효하지 않은 경우, 자동화 단계의 추가 시작을 중단합니다.
   - branchOnValidationOfVpnIp:

     파라미터에 언급된 터널 IP 주소가 유효한지 확인합니다. 유효하지 않은 경우, 자동화 단계의 추가 실행을 중단합니다.
   - traceError:

포함된 로그 그룹에서 CloudWatch 로그 인사이트 API 호출을 수행하고 관련 제안 해결 방법과 IKEv2 함께 IKEv1 /와 관련된 오류를 검색합니다.

6. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.



참조

Systems Manager Automation

- 이 자동화 실행(콘솔)
- 자동화 실행
- Automation 설정
- Support Automation Workflows 랜딩 페이지

AWS 서비스 설명서

- 사이트 간 로그의 VPN 내용

AWSConfigRemediation-DeleteEgressOnlyInternetGateway

설명

`AWSConfigRemediation-DeleteEgressOnlyInternetGateway` 실행서는 지정하는 송신 전용 인터넷 게이트웨이를 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- EgressOnlyInternetGatewayId

  유형: 문자열

  설명: (필수) 삭제하려는 송신 전용 인터넷 게이트웨이의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteEgressOnlyInternetGateway`
- `ec2:DescribeEgressOnlyInternetGateways`

문서 단계

- `aws:executeScript` - `EgressOnlyInternetGatewayId` 파라미터에서 지정된 송신 전용 인터넷 게이트웨이를 삭제합니다.
- `aws:executeScript` - 송신 전용 인터넷 게이트웨이가 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteUnusedENI

설명

`AWSConfigRemediation-DeleteUnusedENI` 실행서는 연결 상태가 `detached` 인 탄력적 네트워크 인터페이스(ENI)를 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- NetworkInterfaceId

  유형: 문자열

  설명: (필수) 삭제하려는 의 IDENI입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`

문서 단계

- `aws:executeAwsApi` - `NetworkInterfaceId` 파라미터에서 ENI 지정한 를 삭제합니다.
- `aws:executeScript` - 이 삭제ENI되었는지 확인합니다.

AWSConfigRemediation-DeleteUnusedSecurityGroup

설명

`AWSConfigRemediation-DeleteUnusedSecurityGroup` 실행서는 `GroupId` 파라미터에서 지정하는 보안 그룹을 삭제합니다. Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스와 연결되어 있거나 다른 보안 그룹에서 참조하는 보안 그룹을 삭제하려고 하면 자동화가 실패합니다. 이 자동화는 기본 보안 그룹을 삭제하지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- GroupId

  유형: 문자열

  설명: (필수) 삭제하려는 보안 그룹의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:DeleteSecurityGroup`

문서 단계

- `aws:executeAwsApi` - `GroupId` 파라미터에 제공하는 값을 사용하여 보안 그룹 이름을 반환합니다.
- `aws:branch` - 그룹 이름이 “기본”이 아님을 확인합니다.
- `aws:executeAwsApi` - `GroupId` 파라미터에서 지정된 보안 그룹을 삭제합니다.
- `aws:executeScript` - 보안 그룹이 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteUnusedVPCNetworkACL

설명

`AWSConfigRemediation-DeleteUnusedVPCNetworkACL` 실행서는 서브넷과 연결되지 않은 네트워크 액세스 제어 목록(ACL)을 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- NetworkAclId

  유형: 문자열

  설명: (필수) 삭제하려는 네트워크의 IDACL입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAcl`
- `ec2:DescribeNetworkAcls`

문서 단계

- `aws:executeAwsApi` - `NetworkAclId` 파라미터에 ACL 지정된 네트워크를 삭제합니다.
- `aws:executeScript` - `NetworkAclId` 파라미터에 ACL 지정된 네트워크가 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteVPCFlowLog

설명

`AWSConfigRemediation-DeleteVPCFlowLog` 실행서는 지정한 가상 프라이빗 클라우드(VPC) 흐름 로그를 삭제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- FlowLogId

  유형: 문자열

  설명: (필수) 삭제하려는 흐름 로그의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

문서 단계

- `aws:executeAwsApi` - `FlowLogId` 파라미터에서 지정하는 흐름 로그를 삭제합니다.
- `aws:executeScript` - 흐름 로그가 삭제되었는지 확인합니다.

AWSConfigRemediation-DetachAndDeleteInternetGateway

설명

`AWSConfigRemediation-DetachAndDeleteInternetGateway` 실행서는 지정하는 인터넷 게이트웨이를 분리하고 삭제합니다. 가상 프라이빗 클라우드(VPC)의 Amazon EC2 인스턴스에 탄력적 IP 주소 또는 퍼블릭 IPv4 주소가 연결된 경우 실행서는 실패합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- InternetGatewayId

  유형: 문자열

  설명: (필수) 삭제하려는 인터넷 게이트웨이의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

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

- `ec2:DeleteInternetGateway`
- `ec2:DescribeInternetGateways`
- `ec2:DetachInternetGateway`

문서 단계

- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 수락하고 가상 프라이빗 게이트웨이의 상태 속성이 `available`로 변경되거나 제한 시간이 초과될 때까지 기다립니다.
- `aws:executeAwsApi` - 지정된 가상 프라이빗 게이트웨이 구성을 검색합니다.
- `aws:branch` - VpcAttachments.state 파라미터 값을 기반으로 분기합니다.

- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 수락하고 가상 프라이빗 게이트웨이의 VpcAttachments.state 속성이 `attached` 또는 시간 초과로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - 가상 프라이빗 게이트웨이의 ID와 Amazon의 ID를 입력VPC으로 수락하고 가상 프라이빗 게이트웨이를 Amazon 에서 분리합니다VPC.
- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 수락하고 가상 프라이빗 게이트웨이의 VpcAttachments.state 속성이 `detached` 또는 시간 초과로 변경될 때까지 기다립니다.

- `aws:executeAwsApi` - 가상 프라이빗 게이트웨이의 ID를 입력으로 수락하고 해당 내용을 삭제합니다.

- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 입력으로 수락하고 해당 삭제 내용을 확인합니다.

  `aws:executeAwsApi` - 인터넷 게이트웨이 VPC ID에서 ID를 수집합니다.
- `aws:executeAwsApi` - 에서 인터넷 게이트웨이 ID를 분리합니다VPC.
- `aws:executeAwsApi` - 인터넷 게이트웨이를 삭제합니다.

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

설명

`AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway` 실행서는 Amazon Virtual Private Cloud(Amazon)로 생성된 가상 프라이빗 클라우드(EC2)에 연결된 지정된 Amazon Elastic Compute Cloud(AmazonVPC) 가상 프라이빗 게이트웨이를 분리하고 삭제합니다VPC. Amazon Virtual Private Cloud

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- VpnGatewayId

  유형: 문자열

  설명: (필수) 삭제할 가상 프라이빗 게이트웨이의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteVpnGateway`
- `ec2:DetachVpnGateway`

- `ec2:DescribeVpnGateways`

문서 단계

- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 수락하고 가상 프라이빗 게이트웨이의 상태 속성이 `available`로 변경되거나 제한 시간이 초과될 때까지 기다립니다.
- `aws:executeAwsApi` - 지정된 가상 프라이빗 게이트웨이 구성을 검색합니다.
- `aws:branch` - VpcAttachments.state 파라미터 값을 기반으로 분기합니다.

- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 수락하고 가상 프라이빗 게이트웨이의 VpcAttachments.state 속성이 `attached` 또는 시간 초과로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - 가상 프라이빗 게이트웨이의 ID와 Amazon의 ID를 입력VPC으로 수락하고 가상 프라이빗 게이트웨이를 Amazon 에서 분리합니다VPC.
- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 수락하고 가상 프라이빗 게이트웨이의 VpcAttachments.state 속성이 `detached` 또는 시간 초과로 변경될 때까지 기다립니다.

- `aws:executeAwsApi` - 가상 프라이빗 게이트웨이의 ID를 입력으로 수락하고 해당 내용을 삭제합니다.

- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 입력으로 수락하고 해당 삭제 내용을 확인합니다.

AWS-DisableIncomingSSHOnPort22

설명

`AWS-DisableIncomingSSHOnPort22` 실행서는 보안 그룹에 대해 TCP 포트 22에서 무제한 수신 SSH 트래픽을 허용하는 규칙을 제거합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- SecurityGroupIds

  유형: 문자열

  설명: (필수) SSH 트래픽을 제한하려는 보안 그룹의 쉼표로 구분IDs된 목록입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

문서 단계

- `aws:executeAwsApi` - `SecurityGroupIds` 파라미터에 지정한 보안 그룹에서 TCP 포트 22의 수신 SSH 트래픽을 허용하는 모든 규칙을 제거합니다.

출력

DisableIncomingSSHTemplate.RestrictedSecurityGroupIds - 인바운드 SSH 규칙IDs이 제거된 보안 그룹의 목록입니다.

AWS-DisablePublicAccessForSecurityGroup

설명

이 런북은 모든 IP 주소에 열려 있는 기본 포트SSH와 RDP포트를 비활성화합니다.

> **Important**
>
> 이 런북은 다음 기준을 모두 충족하는 보안 그룹에 대해 “InvalidPermission.NotFound” 오류와 함께 실패합니다. 1) 보안 그룹이 기본값이 아닌 에 있고VPC, 2) 보안 그룹의 인바운드 규칙은 다음 네 가지 패턴을 모두 사용하여 열린 포트를 지정하지 않습니다.
>
> - `0.0.0.0/0`
> - `::/0`
> - `SSH or RDP port + 0.0.0.0/0`
> - `SSH or RDP port + ::/0`

> **Note**
>
> 이 런북은 중국 내에 AWS 리전 있는 에서는 사용할 수 없습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

유형: 문자열

설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- GroupId

  유형: 문자열

  설명: (필수) 비활성화되어야 하는 포트의 보안 그룹 ID입니다.

- IpAddressToBlock

  유형: 문자열

  설명: (선택 사항) 형식의 액세스를 차단해야 하는 추가 IPv4 주소입니다`1.2.3.4/32`.

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

설명

`AWSConfigRemediation-DisableSubnetAutoAssignPublicIP` 런북은 지정한 서브넷의 IPv4 퍼블릭 주소 지정 속성을 비활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- SubnetId

  유형: 문자열

  설명: (필수) 퍼블릭 IPv4 주소 속성 자동 할당을 비활성화하려는 서브넷의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSubnets`
- `ec2:ModifySubnetAttribute`

문서 단계

- `aws:executeAwsApi` - `SubnetId` 파라미터에 지정한 서브넷에 대한 퍼블릭 IPv4 주소 속성 자동 할당을 비활성화합니다.
- `aws:assertAwsResourceProperty` - 속성이 비활성화되었는지 확인합니다.

AWSSupport-EnableVPCFlowLogs

설명

`AWSSupport-EnableVPCFlowLogs` 실행서는 사용자의 AWS 계정에서 서브넷, 네트워크 인터페이스 및 VPC에 대한 Amazon Virtual Private Cloud(VPC) 흐름 로그를 생성합니다. 서브넷이나 VPC에 대한 흐름 로그를 생성할 경우, 서브넷 또는 Amazon VPC의 각각의 탄력적 네트워크 인터페이스가 모니터링됩니다. 흐름 로그 데이터는 지정한 Amazon CloudWatch Logs 로그 그룹 또는 Amazon Simple Storage Service (Amazon S3) 버킷에 게시됩니다. 흐름 로그에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC 흐름 로그를 참조하세요.

> **Important**
>
> 벤디드 로그의 데이터 수집 및 보관 요금은 흐름 로그를 Logs 또는 Amazon S3에 게시할 CloudWatch 때 적용됩니다. 자세한 내용은 흐름 로그 요금을 참조하세요.

이 자동화 실행(콘솔)

> **Note**
>
> 로그 s3 대상으로 선택할 때는 버킷 정책이 로그 전송 서비스가 버킷에 액세스할 수 있도록 허용하는지 확인하십시오. 자세한 내용은 흐름 로그에 대한 Amazon S3 버킷 권한을 참조하십시오.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

Parameters

- AutomationAssumeRole

  타입: 문자열

  설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- DeliverLogsPermissionArn

  타입: 문자열

설명: (선택 사항) Amazon Elastic Compute Cloud (Amazon EC2) 가 사용자 계정의 로그 로그 그룹에 흐름 로그를 게시할 수 있도록 허용하는 IAM 역할용 ARN입니다. CloudWatch `LogDestinationType` 파라미터에 대해 `s3`을 지정하는 경우, 이 파라미터의 값을 제공하지 마십시오. 자세한 내용은 Amazon VPC 사용 설명서의 CloudWatch 로그에 흐름 로그 게시를 참조하십시오.

- LogDestinationARN

  타입: 문자열

  설명: (선택 사항) 흐름 로그 데이터가 게시되는 리소스의 ARN입니다. `LogDestinationType`매개 변수에 `cloud-watch-logs` 가 지정된 경우 흐름 로그 데이터를 게시하려는 CloudWatch 로그 로그 그룹의 ARN을 제공하십시오. 또는 `LogGroupName`을 대신 사용합니다. `s3`이 `LogDestinationType` 파라미터에 대해 지정되는 경우, 이 파라미터에 대해 흐름 로그 데이터를 게시하려는 Amazon S3 버킷의 ARN을 지정해야 합니다. 버킷에 폴더를 지정할 수도 있습니다.

  > **Important**
  >
  > `LogDestinationType`를 선택할 `s3` 때는 선택한 버킷이 Amazon S3 버킷 보안 모범 사례를 따르고 조직 및 지역의 데이터 개인 정보 보호법을 준수하는지 확인해야 합니다.

- LogDestinationType

  타입: 문자열

  유효한 값: | s3 cloud-watch-logs

  설명: (필수) 흐름 로그 데이터가 게시되는 위치를 결정합니다. `LogDestinationType`을 `s3`로 지정한 경우 `DeliverLogsPermissionArn` 또는 `LogGroupName`을 지정하지 마십시오.

- LogFormat

  타입: 문자열

  설명: (선택 사항) 흐름 로그 레코드에 포함할 필드 및 레코드에 표시되는 순서입니다. 사용 가능한 필드 목록은 Amazon VPC 사용 설명서의 흐름 로그 레코드를 참조하세요. 이 파라미터에 대해 값을 제공하지 않으면 기본 형식을 사용하여 흐름 로그가 생성됩니다. 이 파라미터를 지정하는 경우 하나 이상의 필드를 지정해야 합니다.

- LogGroupName

타입: 문자열

설명: (선택 사항) 흐름 CloudWatch 로그 데이터가 게시되는 로그 로그 그룹의 이름입니다. `LogDestinationType` 파라미터에 대해 `s3`을 지정하는 경우, 이 파라미터의 값을 제공하지 마십시오.

- ResourceIds

  유형: StringList

  설명: (필수) 흐름 로그를 생성하려는 서브넷, 탄력적 네트워크 인터페이스 또는 VPC의 ID를 쉼표로 구분한 목록입니다.

- TrafficType

  타입: 문자열

  유효한 값: ACCEPT | REJECT | ALL

  설명: (필수) 로그할 트래픽의 유형입니다. 리소스가 수락하거나 거부하는 트래픽 또는 모든 트래픽을 로깅할 수 있습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `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

샘플 정책

```
{
    "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}/*"
                    ]
                }
            ]
        }
```

문서 단계

- `aws:branch` - `LogDestinationType` 파라미터에 대해 지정된 값을 기반으로 분기합니다.
- `aws:executeScript`- 대상 Amazon Simple Storage 서비스 (Amazon S3) 가 잠재적으로 해당 객체에 대한 읽기 또는 `public` 쓰기 액세스 권한을 부여하는지 확인합니다.
- `aws:executeScript` - `LogDestinationARN` 파라미터에 값이 지정되지 않고 `LogDestinationType` 파라미터에 대해 `cloud-watch-logs` 값이 지정된 경우 로그 그룹을 생성합니다.
- `aws:executeScript` - 실행서 파라미터에서 지정된 값을 기반으로 흐름 로그를 생성합니다.

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch

설명

AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch 실행서는 흐름 VPC 로그 데이터를 Amazon Simple Storage Service(Amazon S3)에 게시하는 기존 Amazon 흐름 로그를 사용자가 지정한 Amazon CloudWatch Logs(CloudWatch Logs) 로그 그룹에 흐름 로그 데이터를 게시하는 흐름 로그로 대체합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DestinationLogGroup

  유형: 문자열

  설명: (필수) 흐름 로그 데이터를 게시하려는 로그 로그 그룹의 이름 CloudWatch 입니다.
- DeliverLogsPermissionArn

  유형: 문자열

  설명: (필수) Amazon Elastic Compute Cloud(Amazon IAM)에 흐름 로그 데이터를 CloudWatch Logs에 게시하는 데 필요한 권한을 제공하는 사용하려는 AWS Identity and Access Management (EC2) 역할ARN의 입니다.

- FlowLogId

  유형: 문자열

  설명: (필수) 교체하려는 Amazon S3에 게시하는 흐름 로그의 ID입니다.
- MaxAggregationInterval

  유형: 정수

  유효한 값: 60 | 600

  설명: (선택 사항) 패킷 흐름을 캡처하고 흐름 로그 레코드로 집계하는 최대 시간 간격(초)입니다.
- TrafficType

  유형: 문자열

  유효한 값: ACCEPT | REJECT | ALL

  설명: (필수) 기록하고 게시하려는 흐름 로그 데이터의 유형입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

문서 단계

- `aws:executeAwsApi` - `FlowLogId` 파라미터에 지정한 값VPC에서 에 대한 세부 정보를 수집합니다.
- `aws:executeAwsApi` - 실행서 파라미터에 대해 지정하는 값을 기반으로 흐름 로그를 생성합니다.
- `aws:assertAwsResourceProperty` - 새로 생성된 흐름 로그가 CloudWatch 로그에 게시되는지 확인합니다.
- `aws:executeAwsApi` - Amazon S3에 게시하는 흐름 로그를 삭제합니다.

- `aws:executeScript` - Amazon S3에 게시된 흐름 로그가 삭제되었는지 확인합니다.

AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket

설명

`AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket` 실행서는 Amazon Logs(CloudWatch Logs)에 VPC 흐름 로그 데이터를 게시하는 기존 Amazon CloudWatch 흐름 로그를 지정한 Amazon Simple Storage Service(Amazon S3) 버킷에 흐름 로그 데이터를 게시하는 흐름 로그로 대체합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DestinationS3BucketArn

  유형: 문자열

  설명: (필수) 흐름 로그 데이터를 게시하려는 Amazon S3 버킷ARN의 입니다.
- FlowLogId

  유형: 문자열

설명: (필수) 교체하려는 로그에 게시하는 흐름 CloudWatch 로그의 ID입니다.

- MaxAggregationInterval

  유형: 정수

  유효한 값: 60 | 600

  설명: (선택 사항) 패킷 흐름을 캡처하고 흐름 로그 레코드로 집계하는 최대 시간 간격(초)입니다.

- TrafficType

  유형: 문자열

  유효한 값: ACCEPT | REJECT | ALL

  설명: (필수) 기록하고 게시하려는 흐름 로그 데이터의 유형입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:CreateFlowLogs`
- `ec2:DeleteFlowLogs`
- `ec2:DescribeFlowLogs`

문서 단계

- `aws:executeAwsApi` - `FlowLogId` 파라미터에 지정한 값VPC에서 에 대한 세부 정보를 수집합니다.
- `aws:executeAwsApi` - 실행서 파라미터에 대해 지정하는 값을 기반으로 흐름 로그를 생성합니다.
- `aws:assertAwsResourceProperty` - 새로 생성된 흐름 로그가 Amazon S3에 게시되는지 확인합니다.
- `aws:executeAwsApi` - 로그에 게시하는 흐름 CloudWatch 로그를 삭제합니다.
- `aws:executeScript` - Logs에 게시된 흐름 CloudWatch 로그가 삭제되었는지 확인합니다.

AWS-ReleaseElasticIP

설명

할당 ID를 사용하여 지정된 탄력적 IP 주소의 사용을 해제합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- AllocationId

  유형: 문자열

  설명: (필수) 탄력적 IP 주소의 할당 ID입니다.

AWS-RemoveNetworkACLUnrestrictedSSHRDP

설명

`AWS-RemoveNetworkACLUnrestrictedSSHRDP` 실행서는 모든 소스 주소에서 기본 SSH 및 RDP 포트로 트래픽을 수신할 수 ACL 있도록 지정된 네트워크에서 모든 네트워크 액세스 제어 목록(ACL)

규칙을 제거합니다. 기본 SSH 및 포트와 겹치는 RDP 포트 범위를 포함하는 규칙은 제거되지 않습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- NetworkAclId

  유형: 문자열

  설명: (필수) 모든 소스 주소에서 기본 SSH 및 RDP 포트로의 트래픽 수신을 허용하는 무제한 규칙을 제거ACL하려는 네트워크의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DeleteNetworkAclEntry`

- `ec2:DescribeNetworkAcls`

문서 단계

- `aws:executeScript` - `SecurityGroupId` 파라미터에서 사용자가 지정한 보안 그룹에서 모든 소스 주소의 트래픽을 허용하는 모든 수신 규칙을 제거합니다.

출력

RemoveNaclEntriesAndVerify.VerificationMessage - 성공적으로 삭제된 네트워크 ACL 규칙의 확인 메시지입니다.

RemoveNaclEntriesAndVerify.RulesDeletedAndApiResponses - 삭제된 네트워크 ACL 규칙과 `DeleteNetworkAclEntry` API 작업 응답입니다.

AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules

설명

`AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules` 실행서는 모든 소스 주소의 트래픽을 허용하는 지정하는 보안 그룹에서 모든 수신 규칙을 제거합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- SecurityGroupId

  유형: 문자열

  설명: (필수) 모든 소스 주소의 트래픽을 허용하는 수신 규칙을 제거하려는 보안 그룹의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupIngress`

문서 단계

- `aws:executeScript` - `SecurityGroupId` 파라미터에서 사용자가 지정한 보안 그룹에서 모든 소스 주소의 트래픽을 허용하는 모든 수신 규칙을 제거합니다.

AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules

설명

`AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules` 실행서는 지정한 가상 프라이빗 클라우드(VPC)의 기본 보안 그룹에서 모든 규칙을 제거합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- GroupId

  유형: 문자열

  설명: (필수) 모든 규칙을 제거하려는 보안 그룹의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `ec2:DescribeSecurityGroups`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`

문서 단계

- `aws:assertAwsResourceProperty` - `GroupId` 파라미터에 지정한 보안 그룹의 이름이 default 인지 확인합니다.
- `aws:executeScript` - `GroupId` 파라미터에서 지정된 보안 그룹에서 모든 규칙을 제거합니다.

AWSSupport-SetupIPMonitoringFromVPC

설명

`AWSSupport-SetupIPMonitoringFromVPC` 는 지정된 서브넷에 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 생성하고 ping, MTR, traceroute 및 tracetcp 테스트를 지속적으로 실행하여 선택한 대상IPs(IPv4 또는 IPv6)을 모니터링합니다. 결과는 Amazon CloudWatch Logs 로그에 저장되고 지표 필터가 적용되어 CloudWatch 대시보드에서 지연 시간 및 패킷 손실 통계를 빠르게 시각화합니다.

추가 정보

CloudWatch 로그 데이터는 네트워크 문제 해결 및 패턴/트렌드 분석에 사용할 수 있습니다. 또한 패킷 손실 및/또는 지연 시간이 임계값에 도달하면 Amazon SNS 알림을 사용하여 CloudWatch 경보를 구성할 수 있습니다. 또한 로 사례를 열 때 데이터를 사용하여 문제를 신속하게 AWS Support격리하고 네트워크 문제를 조사할 때 해결 시간을 줄일 수 있습니다.

> **Note**
>
> `AWSSupport-SetupIPMonitoringFromVPC`에서 생성한 리소스를 정리하려면 `AWSSupport-TerminateIPMonitoringFromVPC` 실행서를 사용하면 됩니다. 자세한 정보는 `AWSSupport-TerminateIPMonitoringFromVPC`을 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역

할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- CloudWatchLogGroupNamePrefix

  유형: 문자열

  기본값: / `AWSSupport-SetupIPMonitoringFromVPC`

  설명: (선택 사항) 테스트 결과에 대해 생성된 각 CloudWatch 로그 그룹에 사용되는 접두사입니다.

- CloudWatchLogGroupRetentionInDays

  유형: 문자열

  유효한 값: 1 | 3 | 5 | 7 | 14 | 30 | 60 | 90 | 120 | 150 | 180 | 365 | 400 | 545 | 731 | 1827 | 3653

  기본값: 7

  설명: (선택 사항) 네트워크 모니터링 결과를 유지하려는 일수입니다.

- InstanceType

  유형: 문자열

  유효한 값: t2.micro | t2.small | t2.medium | t2.large | t3.micro | t3.small | t3.medium | t3.large | t3.large | t4g.micro | t4g.small | t4g.medium | t4g.large

  기본값: t2.micro

  설명: (선택 사항) EC2 인스턴스의 EC2Rescue 인스턴스 유형입니다. 권장 크기: t2.micro.

- SubnetId

  유형: 문자열

  설명: (필수) 모니터 인스턴스의 서브넷 ID입니다. 프라이빗 서브넷을 지정하는 경우 모니터 인스턴스가 테스트를 설정하도록 허용하는 인터넷 액세스가 있어야 합니다(즉, CloudWatch Logs 에이전트 설치, Systems Manager 및 와 상호 작용 CloudWatch).

- TargetIPs

  유형: 문자열

설명: (필수) IPv6s 모니터링할 IPv4s 및/또는 의 쉼표로 구분된 목록입니다. 공백은 사용할 수 없습니다. 최대 크기는 255자입니다. 잘못된 IP를 지정하는 경우 자동화가 작동하지 않으며, 테스트 설정이 롤백됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

자동화를 실행하는 사용자는 mazonSSMAutomation역할 IAM 관리형 정책을 연결하는 것이 좋습니다. 또한, 사용자의 사용자 계정, 그룹 또는 역할에 다음 정책이 연결되어 있어야 합니다.

```
            {
"Version": "2012-10-17",
"Statement": [
    {
        "Action": [
            "iam:CreateRole",
            "iam:CreateInstanceProfile",
            "iam:GetRole",
            "iam:GetInstanceProfile",
            "iam:DetachRolePolicy",
            "iam:AttachRolePolicy",
            "iam:PassRole",
            "iam:AddRoleToInstanceProfile",
            "iam:RemoveRoleFromInstanceProfile",
            "iam:DeleteRole",
            "iam:DeleteInstanceProfile",
            "iam:PutRolePolicy",
            "iam:DeleteRolePolicy"
        ],
        "Resource": [
            "arn:aws:iam::
            AWS_account_ID
            :role/AWSSupport/SetupIPMonitoringFromVPC_*",
            "arn:aws:iam::
            AWS_account_ID
            :instance-profile/AWSSupport/SetupIPMonitoringFromVPC_*"
        ],
        "Effect": "Allow"
    },
    {
```

```
            "Action": [
                "iam:DetachRolePolicy",
                "iam:AttachRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudwatch:DeleteDashboards"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeInstanceTypes",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceStatus"
                "ec2:CreateTags",
                "ec2:AssignIpv6Addresses",
                "ec2:DescribeTags",
                "ec2:DescribeInstances",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ssm:GetParameter",
                "ssm:SendCommand",
                "ssm:ListCommands",
```

```
                "ssm:ListCommandInvocations",
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

문서 단계

1. **aws:executeAwsApi** - 제공된 서브넷을 설명합니다.
2. **aws:branch** - T argetIPs 입력을 평가합니다.

   (IPv6) T에 가 argetIPs 포함된 경우IPv6:

   aws:assertAwsResourceProperty - 제공된 서브넷에 연결된 IPv6 풀이 있는지 확인합니다.
3. **aws:executeScript** - 최신 Amazon Linux 2에 대한 인스턴스 유형 및 퍼블릭 파라미터 경로의 아키텍처 가져오기 AMI.
4. **aws:executeAwsApi** - 최신 Amazon Linux 2 가져오기 AMI Parameter Store에서.
5. **aws:executeAwsApi** - 서브넷의 에서 테스트에 대한 보안 그룹을 생성합니다VPC.

   (정리) 보안 그룹 생성에 실패하는 경우:

   aws:executeAwsApi - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).
6. **aws:executeAwsApi** - 테스트 보안 그룹에서 모든 아웃바운드 트래픽을 허용합니다.

   (정리) 보안 그룹 송신 규칙 생성에 실패하는 경우:

   aws:executeAwsApi - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).
7. **aws:executeAwsApi** - 테스트 EC2 인스턴스에 대한 IAM 역할 생성

   (정리) 역할 생성에 실패하는 경우:

   a. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할이 있는 경우 삭제합니다.

   b. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).
8. **aws:executeAwsApi** - mazonSSMManagedInstanceCore 관리형 정책 연결

(정리) 정책 연결에 실패하는 경우:

a. **aws:executeAwsApi** - 연결된 경우 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

b. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

c. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

9. **aws:executeAwsApi** - CloudWatch 로그 그룹 보존 설정 및 CloudWatch 대시보드 생성을 허용하는 인라인 정책 연결

(정리) 인라인 정책 연결에 실패하는 경우:

a. **aws:executeAwsApi** - 생성된 경우 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

b. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

d. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

10. **aws:executeAwsApi** - IAM 인스턴스 프로파일을 생성합니다.

(정리) 인스턴스 프로파일 생성에 실패하는 경우:

a. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일이 있는 경우 삭제합니다.

b. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

e. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

11. **aws:executeAwsApi** - IAM 인스턴스 프로파일을 IAM 역할에 연결합니다.

(정리) 인스턴스 프로파일 및 역할 연결에 실패하는 경우:

a. **aws:executeAwsApi** - 연결된 경우 역할에서 IAM 인스턴스 프로파일을 제거합니다.

b. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

e. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

f. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

12 **aws:sleep** - 인스턴스 프로파일을 사용할 수 있을 때까지 기다립니다.

13 **aws:runInstances** - 이전에 생성 및 연결된 인스턴스 프로파일을 사용하여 지정된 서브넷에서 테스트 인스턴스를 생성합니다.

(정리) 단계가 실패하는 경우:

a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.

b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

14 **aws:branch** - T argetIPs 입력을 평가합니다.

(IPv6) T에 가 argetIPs 포함된 경우IPv6:

aws:executeAwsApi - 테스트 인스턴스에 IPv6를 할당합니다.

15 **aws:waitForAwsResourceProperty** - 테스트 인스턴스가 관리형 인스턴스가 될 때까지 기다립니다.

(정리) 단계가 실패하는 경우:

a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.

b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

16 **aws:runCommand** - 테스트 사전 요구 사항을 설치합니다:

(정리) 단계가 실패하는 경우:

a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.

b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

17 **aws:runCommand** - 제공된 IPs 가 구문적으로 올바르IPv4고/바르거나 IPv6 주소가 맞는지 확인합니다.

(정리) 단계가 실패하는 경우:

a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.

b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

18 **aws:runCommand** - 제공된 각 에 대한 MTR 테스트를 정의합니다IPs.

(정리) 단계가 실패하는 경우:

a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.

b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

19 **aws:runCommand** - 제공된 각 에 대한 첫 번째 ping 테스트를 정의합니다IPs.

(정리) 단계가 실패하는 경우:

a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.

b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

20. **aws:runCommand** - 제공된 각 에 대한 두 번째 ping 테스트를 정의합니다IPs.

(정리) 단계가 실패하는 경우:

a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.

b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

21. **aws:runCommand** - 제공된 각 에 대한 tracepath 테스트를 정의합니다IPs.

(정리) 단계가 실패하는 경우:

a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.

b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.

g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

22. **`aws:runCommand`** - 제공된 각 에 대한 traceroute 테스트를 정의합니다IPs.

    (정리) 단계가 실패하는 경우:

    a. **`aws:changeInstanceState`** - 테스트 인스턴스를 종료합니다.

    b. **`aws:executeAwsApi`** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

    c. **`aws:executeAwsApi`** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

    d. **`aws:executeAwsApi`** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

    e. **`aws:executeAwsApi`** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

    f. **`aws:executeAwsApi`** - 자동화에서 생성한 IAM 역할을 삭제합니다.

    g. **`aws:executeAwsApi`** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

23. **`aws:runCommand`** - CloudWatch 로그를 구성합니다.

    (정리) 단계가 실패하는 경우:

    a. **`aws:changeInstanceState`** - 테스트 인스턴스를 종료합니다.

    b. **`aws:executeAwsApi`** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

    c. **`aws:executeAwsApi`** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

    d. **`aws:executeAwsApi`** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

    e. **`aws:executeAwsApi`** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

    f. **`aws:executeAwsApi`** - 자동화에서 생성한 IAM 역할을 삭제합니다.

    g. **`aws:executeAwsApi`** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

24. **`aws:runCommand`** - 1분마다 각 테스트를 실행하도록 cronjob을 예약합니다.

    (정리) 단계가 실패하는 경우:

    a. **`aws:changeInstanceState`** - 테스트 인스턴스를 종료합니다.

    b. **`aws:executeAwsApi`** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.

    c. **`aws:executeAwsApi`** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.

    d. **`aws:executeAwsApi`** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.

    e. **`aws:executeAwsApi`** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

    f. **`aws:executeAwsApi`** - 자동화에서 생성한 IAM 역할을 삭제합니다.

    g. **`aws:executeAwsApi`** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

25. **aws:sleep** - 테스트가 특정 데이터를 생성할 때까지 기다립니다.
26. **aws:runCommand** - 원하는 CloudWatch 로그 그룹 보존을 설정합니다.

    (정리) 단계가 실패하는 경우:

    a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.
    b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.
    c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.
    d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.
    e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.
    f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.
    g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).
27. **aws:runCommand** - CloudWatch 로그 그룹 지표 필터를 설정합니다.

    (정리) 단계가 실패하는 경우:

    a. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.
    b. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.
    c. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.
    d. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.
    e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.
    f. **aws:executeAwsApi** - 자동화에서 생성한 IAM 역할을 삭제합니다.
    g. **aws:executeAwsApi** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).
28. **aws:runCommand** - CloudWatch 대시보드를 생성합니다.

    (정리) 단계가 실패하는 경우:

    a. **aws:executeAwsApi** - CloudWatch 대시보드가 있는 경우 삭제합니다.
    b. **aws:changeInstanceState** - 테스트 인스턴스를 종료합니다.
    c. **aws:executeAwsApi** - 역할에서 IAM 인스턴스 프로파일을 제거합니다.
    d. **aws:executeAwsApi** - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.
    e. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.
    f. **aws:executeAwsApi** - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.

g. **`aws:executeAwsApi`** - 자동화에서 생성한 IAM 역할을 삭제합니다.

h. **`aws:executeAwsApi`** - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

출력

createCloudWatchDashboards.Output - CloudWatch 대시보드URL의 입니다.

createManagedInstance.InstanceIds - 테스트 인스턴스 ID입니다.

AWSSupport-TerminateIPMonitoringFromVPC

설명

`AWSSupport-TerminateIPMonitoringFromVPC`AWSSupport-`SetupIPMonitoringFromVPC`에서 이전에 시작한 IP 모니터링 테스트를 종료합니다. 지정된 테스트 ID와 관련된 데이터가 삭제됩니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- AutomationExecutionId

유형: 문자열

설명: (필수) 이전에 `AWSSupport-SetupIPMonitoringFromVPC` 실행서를 실행했을 때의 자동화 실행 ID입니다. 이 실행 ID와 연결된 모든 리소스가 삭제됩니다.

- InstanceId

  유형: 문자열

  설명: (필수) 모니터 인스턴스의 인스턴스 ID입니다.

- SubnetId

  유형: 문자열

  설명: (필수) 모니터 인스턴스의 서브넷 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

자동화를 실행하는 사용자는 mazonSSMAutomation역할 IAM 관리형 정책을 연결하는 것이 좋습니다. 또한, 사용자, 그룹 또는 역할에 다음 정책이 연결되어 있어야 합니다.

```
{
"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"
    ]
}
```

문서 단계

1. `aws:assertAwsResourceProperty` - AutomationExecutionId 및 InstanceId 가 동일한 테스트와 관련이 있는지 확인합니다.
2. `aws:assertAwsResourceProperty` - SubnetId 및 InstanceId 가 동일한 테스트와 관련이 있는지 확인합니다.
3. `aws:executeAwsApi` - 테스트 보안 그룹을 검색합니다.
4. `aws:executeAwsApi` - CloudWatch 대시보드를 삭제합니다.

5. `aws:changeInstanceState` - 테스트 인스턴스를 종료합니다.
6. `aws:executeAwsApi` - 역할에서 IAM 인스턴스 프로파일을 제거합니다.
7. `aws:executeAwsApi` - 자동화에서 생성한 IAM 인스턴스 프로파일을 삭제합니다.
8. `aws:executeAwsApi` - 자동화에서 생성한 역할에서 CloudWatch 인라인 정책을 삭제합니다.
9. `aws:executeAwsApi` - 자동화에서 생성한 역할에서 mazonSSMManagedInstanceCore 관리형 정책을 분리합니다.
10. `aws:executeAwsApi` - 자동화에서 생성한 IAM 역할을 삭제합니다.
11. `aws:executeAwsApi` - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

출력

None

AWS WAF

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS WAF. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-AddWAFRegionalRuleToRuleGroup
- AWS-AddWAFRegionalRuleToWebAcl
- AWSConfigRemediation-EnableWAFClassicLogging
- AWSConfigRemediation-EnableWAFClassicRegionalLogging
- AWSConfigRemediation-EnableWAFV2Logging

AWS-AddWAFRegionalRuleToRuleGroup

설명

`AWS-AddWAFRegionalRuleToRuleGroup` 실행서는 기존 AWS WAF 리전 규칙을 AWS WAF 리전 규칙 그룹에 추가합니다. AWS WAF 클래식 리전 규칙 그룹만 지원됩니다. AWS WAF 클래식 리전 규칙 그룹에는 최대 10개의 규칙이 있을 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- RuleGroupId

  유형: 문자열

  설명: (필수) 업데이트하려는 규칙 그룹의 ID입니다.

- RulePriority

  유형: 정수

  설명: (필수) 새 규칙의 우선 순위입니다. 규칙 우선 순위는 리전 그룹의 규칙이 평가되는 순서를 결정합니다. 값이 낮은 규칙은 값이 높은 규칙보다 우선 순위가 높습니다. 이 값은 고유한 정수여야 합니다. 리전 규칙 그룹에 여러 규칙을 추가하는 경우 값이 연속적일 필요는 없습니다.

- RuleId

  유형: 문자열

  설명: (필수) 리전 규칙 그룹에 추가할 규칙의 ID입니다.

- RuleAction

  유형: 문자열

  설명: (필수) 웹 요청이 규칙 조건과 일치할 때 AWS WAF 수행하는 작업을 지정합니다.

  유효한 값: ALLOW | BLOCK | COUNT

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetChangeTokenStatus`
- `waf-regional:ListActivatedRulesInRuleGroup`
- `waf-regional:UpdateRuleGroup`

문서 단계

- G etWAFChange토큰(aws:executeAwsApi) - AWS WAF 변경 토큰을 검색하여 실행서가 서비스에 충돌하는 요청을 제출하지 않도록 합니다.
- ddWAFRuleToWAFRegionalRuleGroup (aws:executeScript) - 지정된 규칙을 AWS WAF 리전 규칙 그룹에 추가합니다.
- VerifyChangeTokenPropagating (aws:waitForAwsResourceProperty) - 변경 토큰의 상태가 `PENDING` 또는 인지 확인합니다`INSYNC`.
- VerifyRuleAddedToRuleGroup (aws:executeScript) - 지정된 AWS WAF 규칙이 대상 리전 규칙 그룹에 추가되었는지 확인합니다.

출력

- VerifyRuleAddedToRuleGroup.VerifyRuleAddedToRuleGroupResponse - 새 규칙이 리전 규칙 그룹에 어디딩되었는지 확인하는 단계의 출력입니다.
- VerifyRuleAddedToRuleGroup.ListActivatedRulesInRuleGroupResponse - `ListActivatedRulesInRuleGroup` API 작업의 출력입니다.

AWS-AddWAFRegionalRuleToWebAcl

설명

`AWS-AddWAFRegionalRuleToWebAcl` 실행서는 기존 AWS WAF 리전 규칙, 규칙 그룹 또는 속도 기반 규칙을 AWS WAF Classic 리전 웹 액세스 제어 목록()에 추가합니다ACL. 이 런북ACL은 에서 관리하는 기존 AWS WAF Classic 리전 웹을 업데이트하지 않습니다 AWS Firewall Manager.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- WebACLId

  유형: 문자열

  설명: (필수) 업데이트하려는 웹의 IDACL입니다.

- ActivatedRulePriority

  유형: 정수

설명: (필수) 새 규칙의 우선 순위입니다. 규칙 우선 순위는 웹에서 규칙을 ACL 평가하는 순서를 결정합니다. 값이 낮은 규칙은 값이 높은 규칙보다 우선 순위가 높습니다. 이 값은 고유한 정수여야 합니다. 리전 웹 에 여러 규칙을 추가하는 경우 ACL값이 연속적일 필요는 없습니다.

- ActivatedRuleRuleId

  유형: 문자열

  설명: (필수) 웹에 추가할 일반 규칙, 속도 기반 규칙 또는 그룹의 ID입니다ACL.

- ActivatedRuleAction

  유형: 문자열

  유효한 값: ALLOW | BLOCK | COUNT

  설명: (선택 사항) 웹 요청이 규칙의 조건과 일치할 때 AWS WAF 수행하는 작업을 지정합니다.

- ActivatedRuleType

  유형: 문자열

  유효한 값: REGULAR | RATE_BASED | GROUP

  기본값: REGULAR

  설명: (선택 사항) 웹 에 추가할 규칙 유형입니다ACL. 이 필드는 선택 사항이지만 유형을 설정ACL하지 않고 웹에 `RATE_BASED` 규칙을 추가하려고 하면 요청의 기본값이 `REGULAR` 규칙이므로 요청이 실패합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `waf-regional:GetChangeToken`
- `waf-regional:GetWebACL`
- `waf-regional:UpdateWebACL`

문서 단계

- DetermineWebACLNotInFMSAndRulePriority (aws:executeScript) - AWS WAF 웹ACL이 Firewall Manager 보안 정책에 있는지 확인하고 우선 순위 ID가 기존 와 충돌하지 않는지 확인합니다ACL.
- AddRuleOrRuleGroupToWebACL (aws:executeScript) - 지정된 규칙을 AWS WAF 웹 에 추가합니다ACL.
- VerifyRuleOrRuleGroupAddedToWebAcl (aws:executeScript) - 지정된 AWS WAF 규칙이 대상 웹 에 추가되었는지 확인합니다ACL.

출력

- DetermineWebACLNotInFMSAndRulePriority.PrereqResponse: `DetermineWebACLNotInFMSAndRulePriority` 단계에서 출력합니다.
- VerifyRuleOrRuleGroupAddedToWebAcl.VerifyRuleOrRuleGroupAddedToWebACLResponse: `AddRuleOrRuleGroupToWebACL` 단계의 출력입니다.
- VerifyRuleOrRuleGroupAddedToWebAcl.ListActivatedRulesOrRuleGroupsInWebACLResponse: `VerifyRuleOrRuleGroupAddedToWebAcl` 단계의 출력입니다.

AWSConfigRemediation-EnableWAFClassicLogging

설명

`AWSConfigRemediation-EnableWAFClassicLogging` 런북을 사용하면 지정한 AWS WAF 웹 액세스 제어 목록(웹)에 대해 Amazon Data Firehose(FirehoseACL)에 로깅할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- DeliveryStreamName

  유형: 문자열

  설명: (필수) 로그를 보내려는 Firehose 전송 스트림의 이름입니다.
- WebACLId

  유형: 문자열

  설명: (필수) 로그온ACL을 활성화하려는 AWS WAF 웹의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf:GetLoggingConfiguration`
- `waf:GetWebAcl`
- `waf:PutLoggingConfiguration`

문서 단계

- `aws:executeAwsApi` - `DeliveryStreamName`에서 지정하는 전송 스트림이 존재하는지 확인합니다.
- `aws:executeAwsApi` - `WebACLId` 파라미터에 ACL 지정된 AWS WAF 웹ARN의 를 수집합니다.
- `aws:executeAwsApi` - 웹 에 대한 로깅을 활성화합니다ACL.
- `aws:assertAwsResourceProperty` - AWS WAF 웹 에서 로깅이 활성화되었는지 확인합니다 ACL.

AWSConfigRemediation-EnableWAFClassicRegionalLogging

설명

`AWSConfigRemediation-EnableWAFClassicRegionalLogging` 런북을 사용하면 지정한 AWS WAF 웹 액세스 제어 목록()에 대해 Amazon Data Firehose(FirehoseACL)에 로깅할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- LogDestinationConfigs

  유형: 문자열

  설명: (필수) 로그를 보내려는 Firehose 전송 스트림의 Amazon 리소스 이름(ARN)입니다.
- WebACLId

  유형: 문자열

  설명: (필수) 로그온ACL을 활성화하려는 AWS WAF 웹의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `iam:CreateServiceLinkedRole`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:GetWebAcl`
- `waf-regional:PutLoggingConfiguration`

문서 단계

- `aws:executeAwsApi` - `WebACLId` 파라미터에 ACL 지정된 AWS WAF 웹ARN의 를 수집합니다.
- `aws:executeAwsApi` - 웹 에 대한 로깅을 활성화합니다ACL.
- `aws:assertAwsResourceProperty` - AWS WAF 웹 에서 로깅이 활성화되었는지 확인합니다 ACL.

AWSConfigRemediation-EnableWAFV2Logging

설명

`AWSConfigRemediation-EnableWAFV2Logging` 실행서는 지정된 Amazon Data Firehose(Firehose) 전송 스트림을 사용하여 AWS WAF (AWS WAF V2ACL) 웹 액세스 제어 목록(웹) 에 대한 로깅을 활성화합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

유형: 문자열

설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.

- LogDestinationConfigs

  유형: 문자열

  설명: (필수) 웹 에 연결ARN하려는 Firehose 전송 스트림입니다ACL.

> **Note**
>
> Firehose 전송 스트림은 접두사 `aws-waf-logs-` 로 시작해야 ARN 합니다. 예: `aws-waf-logs-us-east-2-analytics`. 자세한 내용은 Amazon Data Firehose를 참조하세요.

- WebAclArn

  유형: 문자열

  설명: 로깅이 활성화ACL될 웹ARN의 (필수)입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `firehose:DescribeDeliveryStream`
- `wafv2:PutLoggingConfiguration`
- `wafv2:GetLoggingConfiguration`

문서 단계

- `aws:executeScript` - AWS WAF V2 웹에 대한 로깅을 활성화ACL하고 로깅에 지정된 구성이 있는지 확인합니다.

Amazon WorkSpaces

AWS Systems Manager 자동화는 Amazon 에 사전 정의된 실행서를 제공합니다 WorkSpaces. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWS-CreateWorkSpace
- AWSSupport-RecoverWorkSpace

AWS-CreateWorkSpace

설명

`AWS-CreateWorkSpace` 런북은 입력 파라미터에 지정한 값을 WorkSpace기반으로 로 알려진 새 Amazon WorkSpaces 가상 데스크톱을 생성합니다. 에 대한 자세한 내용은 Amazon 관리 안내서의 Amazon WorkSpaces?란 무엇입니까?를 WorkSpaces참조하세요. WorkSpaces

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역

할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- BundleId

  유형: 문자열

  설명: (필수) 에 사용할 번들의 ID입니다 WorkSpace.

- ComputeTypeName

  유형: 문자열

  유효한 값: VALUE | STANDARD | PERFORMANCE | | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

  설명: (선택 사항) 의 컴퓨팅 유형입니다 WorkSpace.

- DirectoryId

  유형: 문자열

  설명: (필수) 를 추가할 디렉터리의 ID입니다 WorkSpace.

- RootVolumeEncryptionEnabled

  타입: 부울

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) 의 루트 볼륨 WorkSpace 이 암호화되는지 여부를 결정합니다.

- RootVolumeSizeGib

  유형: 정수

  설명: (필수) 의 루트 볼륨 크기입니다 WorkSpace.

- RunningMode

  유형: 문자열

  유효한 값: ALWAYS_ON | AUTO_STOP

  설명: (필수) 의 실행 모드입니다 WorkSpace.

- RunningModeAutoStopTimeoutInMinutes

  유형: 정수

  설명: (선택 사항) 가 중지될 때 사용자가 로그오프한 시간입니다 WorkSpaces. 60분 간격으로 값을 지정합니다.

- Tags

  유형: 문자열

  설명: (선택 사항) 에 적용할 태그입니다 WorkSpace.

- UserName

  유형: 문자열

  설명: (필수) 에 연결할 사용자 이름입니다 WorkSpace.

- UserVolumeEncryptionEnabled

  타입: 부울

  유효한 값: true | false

  기본값: false

  설명: (선택 사항) 의 사용자 볼륨 WorkSpace 이 암호화되는지 여부를 결정합니다.

- UserVolumeSizeGib

  유형: 정수

  설명: (필수) 의 사용자 볼륨 크기입니다 WorkSpace.

- VolumeEncryptionKey

  유형: 문자열

  설명: (선택 사항) 에 저장된 데이터를 암호화하는 데 사용할 대칭 AWS Key Management Service 키입니다 WorkSpace.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `workspaces:CreateWorkspaces`
- `workspaces:DescribeWorkspaces`

문서 단계

- `aws:executeScript` - 입력 파라미터에 대해 지정한 값을 WorkSpace 기반으로 를 생성합니다.
- `aws:waitForAwsResourceProperty` - 의 상태가 WorkSpace 인지 확인합니다`AVAILABLE`.

출력

`CreateWorkspace.WorkspaceId`

AWSSupport-RecoverWorkSpace

설명

`AWSSupport-RecoverWorkSpace` 런북은 WorkSpace지정한 로 알려진 Amazon WorkSpaces 가상 데스크톱에서 복구 단계를 수행합니다. 실행서는 를 재부팅하고 WorkSpace, 상태가 여전히 `UNHEALTHY` 인 경우 는 입력 파라미터에 대해 지정한 값을 WorkSpace 기반으로 를 복원하거나 재구축합니다. 이 런북을 사용하기 전에 Amazon WorkSpaces 관리 안내서의 WorkSpaces 문제 해결을 검토하는 것이 좋습니다.

> **Important**
>
> 를 복원하거나 재구축하는 WorkSpace 것은 데이터 손실을 초래할 수 있는 잠재적으로 파괴적인 작업입니다. 이는 WorkSpace 가 마지막으로 사용 가능한 스냅샷에서 복원되고 스냅샷에서 복구된 데이터가 12시간만큼 오래되었을 수 있기 때문입니다.
> 복원 옵션은 최신 스냅샷을 기반으로 루트 볼륨과 사용자 볼륨을 모두 재생성합니다. 재구축 옵션은 최신 스냅샷에서 사용자 볼륨을 다시 생성하고 WorkSpace 에서 생성된 번들과 연결된 이미지 WorkSpace 에서 를 다시 생성합니다. 설치된 애플리케이션 또는 이 WorkSpace 생성된 후 변경된 시스템 설정이 손실됩니다. 복원 및 재구축에 대한 자세한 내용은 Amazon WorkSpaces 관리 안내서의 복원 WorkSpace 및 재구축 WorkSpace을 WorkSpaces참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
- 확인

  유형: 문자열

  유효한 값: Yes

  설명: (필수) 예를 입력하면 복원 및 재구축 작업이 가장 최근 스냅샷 WorkSpace 에서 를 복구하려고 시도하고 이러한 스냅샷에서 복원된 데이터는 12시간만큼 오래될 수 있음을 이해하게 됩니다.
- 재부팅

  유형: 문자열

  유효한 값: Yes | No

  기본값: Yes

  설명: (필수) WorkSpace 이 재부팅되는지 여부를 결정합니다.
- 재빌드

  유형: 문자열

  유효한 값: Yes | No

기본값: 아니요

설명: (필수) WorkSpace 이 재구축되었는지 여부를 결정합니다.

- 복원

  유형: 문자열

  유효한 값: Yes | No

  기본값: 아니요

  설명: (필수) WorkSpace 이 복원되는지 여부를 결정합니다.

- WorkspaceId

  유형: 문자열

  설명: (필수) 복구 WorkSpace 하려는 의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `workspaces:DescribeWorkspaces`
- `workspaces:DescribeWorkspaceSnapshots`
- `workspaces:RebootWorkspaces`
- `workspaces:RebuildWorkspaces`
- `workspaces:RestoreWorkspace`
- `workspaces:StartWorkspaces`

문서 단계

- `aws:executeAwsApi` - `WorkspaceId` 파라미터에서 WorkSpace 지정한 의 상태를 수집합니다.
- `aws:assertAwsResourceProperty` - 의 상태가 `AVAILABLE` , `ERROR` , `IMPAIRED` , `STOPPED` 또는 `UNHEALTHY` WorkSpace 인지 확인합니다.

- `aws:branch` - 의 상태를 기반으로 분기합니다 WorkSpace.
- `aws:executeAwsApi` - 를 시작합니다 WorkSpace.
- `aws:branch` - `Action` 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- `aws:waitForAwsResourceProperty` - 시작 후 WorkSpace 상태를 기다립니다.
- `aws:waitForAwsResourceProperty` - WorkSpace 상태가 시작 `UNHEALTHY` 후 `AVAILABLE` , `ERROR` , 또는 `IMPAIRED` 로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - 시작된 WorkSpace 후 의 상태를 수집합니다.
- `aws:branch` - 시작된 WorkSpace 후 의 상태를 기반으로 분기합니다.
- `aws:executeAwsApi` - 를 복원하거나 재구축하기 위해 사용 가능한 스냅샷을 수집합니다 WorkSpace.
- `aws:branch` - `Reboot` 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - 를 재부팅합니다 WorkSpace.
- `aws:executeAwsApi` - 시작된 WorkSpace 후 의 상태를 수집합니다.
- `aws:waitForAwsResourceProperty` - 상태가 `REBOOTING` 로 WorkSpace 변경될 때까지 기다립니다.
- `aws:waitForAwsResourceProperty` - 재부팅된 `UNHEALTHY` 후 WorkSpace 상태가 `AVAILABLE` , 또는 `ERROR` 로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - 재부팅된 WorkSpace 후 의 상태를 수집합니다.
- `aws:branch` - 재부팅 WorkSpace 후 의 상태를 기반으로 분기합니다.
- `aws:branch` - `Restore` 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - 를 복원합니다 WorkSpace. 복원에 실패하면 실행서는 를 다시 빌드하려고 시도합니다 WorkSpace.
- `aws:waitForAwsResourceProperty` - 상태가 `RESTORING` 로 WorkSpace 변경될 때까지 기다립니다.
- `aws:waitForAwsResourceProperty` - WorkSpace 상태가 복원된 `UNHEALTHY` 후 `AVAILABLE` , 또는 `ERROR` 로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - 복원된 WorkSpace 후 의 상태를 수집합니다.
- `aws:branch` - 복원 WorkSpace 후 의 상태를 기반으로 분기합니다.
- `aws:branch` - `Rebuild` 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - 를 재구축합니다 WorkSpace.
- `aws:waitForAwsResourceProperty` - 상태가 `REBUILDING` 로 WorkSpace 변경될 때까지 기다립니다.

- `aws:waitForAwsResourceProperty` - WorkSpace 상태가 다시 빌드된 `UNHEALTHY` 후 `AVAILABLE` , 또는 `ERROR` 로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - 다시 빌드된 WorkSpace 후 의 상태를 수집합니다.
- `aws:assertAwsResourceProperty` - 의 상태가 `AVAILABLE` WorkSpace 인지 확인합니다.

X-Ray

AWS Systems Manager 자동화는 에 사전 정의된 실행서를 제공합니다 AWS X-Ray. 실행서에 대한 자세한 내용은 실행서 작업을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 실행서 콘텐츠 보기(을)를 참조하세요.

주제

- AWSConfigRemediation-UpdateXRayKMSKey

AWSConfigRemediation-UpdateXRayKMSKey

설명

`AWSConfigRemediation-UpdateXRayKMSKey` 실행서는 AWS Key Management Service (AWS KMS) 키를 사용하여 AWS X-Ray 데이터에 대한 암호화를 활성화합니다. 이 런북은 최소 권장 보안 모범 사례에 따라 AWS X-Ray 데이터를 암호화하기 위한 기준으로만 사용해야 합니다. 다양한 KMS 키로 여러 데이터 세트를 암호화하는 것이 좋습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux,macOS, Windows

Parameters

- AutomationAssumeRole

  유형: 문자열

  설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 (ARN) 역할의 AWS Identity and Access Management Amazon 리소스 이름(IAM)입니다.
- KeyId

  유형: 문자열

  설명: (필수) Amazon 리소스 이름(ARN), 키 ID 또는 데이터를 암호화하는 데 AWS X-Ray 사용할 키의 KMS 키 별칭입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`
- `kms:DescribeKey`
- `xray:GetEncryptionConfig`
- `xray:PutEncryptionConfig`

문서 단계

- `aws:executeAwsApi` - `KeyId` 파라미터에 지정한 KMS 키를 사용하여 X-Ray 데이터에 대한 암호화를 활성화합니다.
- `aws:waitForAwsResourceProperty` - X-Ray의 암호화 구성 상태가 `ACTIVE`가 될 때까지 기다립니다.
- `aws:executeAwsApi` - `KeyId` 파라미터에 지정한 키ARN의 를 수집합니다.
- `aws:assertAwsResourceProperty` - X-Ray에서 암호화가 활성화되었는지 확인합니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.